

TRIPOLARIDADE CIBERNÉTICA: A EVOLUÇÃO DO CIBERPODER DE EUA, CHINA E RÚSSIA

Giovanna Castro Gonçalves¹

RESUMO:

O presente artigo analisa o uso estratégico do ciberespaço por Estados como instrumento de poder no cenário internacional, destacando a crescente importância das tecnologias digitais na política global. A pesquisa parte da distinção conceitual entre ciberespaço e internet, refletindo sobre a influência das transformações tecnológicas na reorganização do poder. A partir de uma abordagem qualitativa, descritiva, exploratória e bibliográfica, são analisadas fontes primárias e secundárias, com destaque para o índice de ciberpoder do Belfer Center (Harvard). A análise considera o impacto do hard power, soft power e smart power, conceitos formulados por Joseph Nye, no contexto cibernético. Observa-se que o ciberespaço possui características singulares, como acessibilidade, baixo custo de entrada e multiplicidade de atores, o que o torna um ambiente propício à disputa por influência. Os dados demonstram que, apesar da multipolaridade do cenário digital, Estados Unidos, China e Rússia se destacam como as três principais potências cibernéticas, sugerindo uma possível reconfiguração tripolar do Sistema Internacional. Conclui-se que o ciberpoder é um fator determinante na atual dinâmica geopolítica, refletindo a centralidade das tecnologias digitais nas relações de poder entre os Estados.

Palavras-chave: Ciberespaço; Internet; Ciberpoder; Tripolaridade; Estados Unidos; China; Rússia.

ABSTRACT:

This article analyzes the strategic use of cyberspace by states as an instrument of power in the international arena, highlighting the growing importance of digital technologies in global politics. The research begins with a conceptual distinction between cyberspace and the internet, reflecting on the influence of technological transformations on the reorganization of power. Using a qualitative, descriptive, exploratory, and bibliographic approach, the study analyzes primary and secondary sources, with emphasis on the Cyber Power Index developed by the Belfer Center (Harvard). The analysis considers the impact of hard power, soft power, and smart power—concepts developed by Joseph Nye—within the cyber context. It is observed that cyberspace has unique characteristics, such as accessibility, low entry costs, and a multiplicity of actors, making it a favorable environment for influence disputes. Data show that despite the multipolar nature of the digital landscape, the United States, China, and Russia stand out as the three main cyber powers, suggesting a possible tripolar reconfiguration of the international system. It is concluded that cyber power is a determining factor in the current geopolitical dynamics, reflecting the centrality of digital technologies in the power relations among states.

Keywords: Cyberspace; Internet; Cyberpower; Tripolarity; United States; China; Russia.

INTRODUÇÃO

O presente artigo, desenvolvido originalmente como uma monografia², busca demonstrar que o ciberespaço, compreendendo a internet e os diversos equipamentos interconectados de comunicação eletrônica digital, a nível global têm sido utilizado por alguns países como forma de expandir sua influência. Os Estados têm utilizado o poder cibernético como uma ferramenta política para obtenção e exercício de poder no cenário internacional.

A abordagem inicia-se com a explanação e conceituação entre ciberespaço e internet, trazendo elucidações de como se deu o estabelecimento destas duas realidades tão vitais para os dias atuais.

Considerando que a tecnologia é fator preponderante de poder para alguns indivíduos, grupos ou nações, se faz importante reconhecer a falta de neutralidade desta para debater sobre as desigualdades e os desafios que surgem com a sua evolução. Visto que este trabalho aborda temas mais atuais do que nunca — como a ciberpolítica e o ciberpoder —, torna-se evidente que não é possível concluir que haja uma preponderância no surgimento do poder ou da política. Isso destaca que o ciberespaço é apenas mais um meio no qual essas realidades se manifestam. A pesquisa é descritiva e exploratória, fundamentada na análise de dados já existentes obtidos através de fontes primárias e secundárias, como, a título de exemplo, estudos realizados por pesquisadores da área e o índice de ciberpoder promovido por Belfer Center for Science and International Affairs de Harvard foram analisados a coleta de dados e tratamento das informações acerca das capacidades de exercer o ciberpoder das diversas potências analisadas, com ênfase às seguintes nações: os Estados Unidos, a China e a Rússia.

A abordagem utilizada é qualitativa, pois buscou-se compreender a complexidade do caso a partir de conhecimentos já construídos e da análise de indicadores relativos à temática. Além disso, a pesquisa é bibliográfica e documental, sendo utilizados relatórios, livros, documentos, assim como, investigações acadêmicas que ajudaram no desenvolvimento do trabalho.

Essa pesquisa parte de uma contextualização histórica e conceitual do ciberespaço e da internet, distinguindo-os e refletindo sobre os desafios trazidos pela era digital, como a exclusão digital em um mundo cada vez mais globalizado e conectado. Em seguida, são discutidos os conceitos de ciberpolítica e poder no ciberespaço, conectando essas ideias aos conceitos de poder propostos por Joseph S. Nye Jr., como *hard*, *soft* e *smart power*.

Por fim, a análise se volta à configuração do poder cibernético em nível global, considerando a possibilidade de uma estrutura tripolar dominada por Estados Unidos, China e Rússia, com base em indicadores que apontam como essas potências se destacam no cenário global.

A NOVA ERA DA INFORMAÇÃO E SEUS DESAFIOS

O ciberespaço tornou-se um recurso indispensável para o funcionamento do mundo atual, seja pela adoção da cibercultura e pela facilidade de interação e troca de informações, seja pela crescente presença de aparelhos eletrônicos que se tornaram essenciais em todas as esferas da sociedade. Esse período histórico, conhecido como 'Era da Informação', é marcado por avanços significativos na adoção de tecnologias e por seu impacto profundo na sociedade, especialmente pela modernização dos meios de comunicação e pelas transformações sociais decorrentes desse processo.

A rapidez com que os sistemas eletrônicos possibilitam a troca e o processamento de informações, levando em conta ainda a facilidade de interações entre usuários em qualquer lugar do planeta promoveu grandes transformações para a sociedade no século XXI (Dos Santos Júnior, 2016). Com essa nova realidade o comportamento humano tem sofrido mudanças nas relações interpessoais e sociais afetando a forma de interagir e se relacionar com os outros, assim como o surgimento de novas visões de mundo. Como posto por Hilbert (2016, p. 12):

Este novo paradigma de organização social foi chamado de "Era da Informação" e se caracteriza pela transformação do modo de vida baseado em tecnologias mecânicas oriundas da revolução industrial para o uso intenso da informação eletrônica e computadorizada.

Consideramos o fim do século XX e o começo do século XXI o início da 'Era da Informação'. Este marco representou a profunda mudança da sociedade com a "grande proliferação de tecnologias e capacidades emergentes de informação e comunicação que possibilitarão à

humanidade superar as barreiras de interação impostas pelo tempo, distância e localização, além de ampliar a capacidade de processar informações e tomar decisões" (Alberts; Papp, 1997, p 13).

A criação da internet se realizou devido a um estudo feito por Joseph Carl Robnett Licklider e Weldon E. Clark em 1962 onde os autores apontaram a possibilidade do emprego dos computadores na sociedade no âmbito civil e militar, além da criação do que chamaram "rede galáctica" que possibilitaria o acesso à informação. Esse trabalho levou Licklider a assumir a chefia do primeiro programa de pesquisa computacional da Agência de Pesquisa e Projetos Avançados do Departamento de Defesa (DoD, na sigla em inglês) dos Estados Unidos, que em 1969 desenvolveu a primeira rede eletrônica interconectada nomeada de Rede da Agência de Pesquisas em Projetos Avançados (ARPANET, do inglês Advanced Research Projects Agency Network)

A ARPANET foi criada para garantir a troca segura de informações entre bases militares e institutos de pesquisa universitários nos EUA, utilizando pacotes de dados (Honório, 2016). Desde o início, sua arquitetura era descentralizada, visando conectividade e resiliência. Com a revolução científico-tecnológica da década de 1970, as redes passaram a se apoiar nas Tecnologias da Informação e Comunicação (TIC), favorecendo sua expansão.

O crescimento da internet coincidiu com o fim da Guerra Fria. Nesse contexto, os Estados Unidos passaram a explorar a ARPANET de forma mais eficiente e comercial. A criação dos protocolos *Transmission Control Protocol/Internet Protocol* (TCP/IP) e dos domínios permitiu a comunicação entre computadores. Em 1995, o lançamento do navegador Netscape marcou a popularização da rede.

A Revolução da Informação foi favorecida pela ampla disseminação de computadores pessoais e pela oferta de cursos superiores em ciência da computação nos países desenvolvidos (Honório, 2016). Empresas como *International Business Machines* (IBM), Microsoft, Apple e Netscape tornaram a tecnologia mais acessível ao público, adaptando-a ao uso doméstico e profissional.

Esse cenário permitiu a consolidação de protocolos especializados como o SMTP (e-mails), FTP (arquivos) e HTTP (acesso à web), fundamentais para a criação da *World Wide Web* (www) (Cepik; Canabarro; Borne, 2014). A web, por sua interface gráfica, facilitou o acesso de usuários leigos, ampliando ainda mais o alcance global da internet.

Mesmo com o rápido desenvolvimento do ciberespaço e o surgimento da internet nos anos 1990, ainda não havia uma definição clara para esses termos, nem haviam sido implementadas políticas públicas para lidar com os novos desafios de segurança. Havia, portanto, a necessidade de definir os conceitos e implementar medidas simultaneamente. Kramer (2009) esclarece que no começo do século XXI o Departamento de Defesa norte-americano elaborou diversos documentos que contêm elaboradas definições do que seria o ciberespaço, mas sem sucesso em trazer uma definição precisa e abrangente o suficiente. Kuehl (2009, p. 29) traz uma definição amplamente aceita no meio acadêmico em que conceitua o ciberespaço como:

Um domínio global dentro do ambiente de troca de informações cuja característica única e distintiva é utilizar-se da eletrônica e do espectro eletromagnético para criar, armazenar, modificar, trocar e processar informações via redes interconectadas e interdependentes usando tecnologias de informação e comunicação.

Percebe-se então que o ciberespaço abrange todos os tipos de equipamentos eletrônicos que podem comunicar-se entre si e trocar informações, como o rádio, sistema telefonia móvel/fixa, televisão entre outros. Essa definição é tão abrangente devido a tendência da conectividade entre os meios de comunicação eletrônica que impulsionam o crescimento dessa rede computadorizada cada vez maior, acarretando em um sistema dinâmico e diverso que é o ciberespaço. Ele é formado por inúmeras redes interconectadas, sendo a maior delas a internet, responsável por conectar todas as redes menores (Singer; Friedman, 2014).

Já internet faz a transmissão dos dados existentes e exerce o papel de intermediador da comunicação entre as redes agindo como centralizador, facilitador e disseminador da cultu-

ra digital. Logo, “A internet não é uma rede única mas sim um meio de conexão entre diferentes redes espalhadas pelo mundo” (Ceruzzi, 2023, p. 295) entre seus atributos o que mais chama atenção é a aceitação da internet por diferentes países e centros de pesquisa por causa de suas características específicas, como o uso de padrões abertos, uma governança técnica participativa e a neutralidade no tratamento do conteúdo, o que favoreceu seu crescimento entre iniciativas públicas e privadas e consolidou seu status como a “rede das redes” (Kurbalija; Gelbstein, 2005).

À medida que a internet ganha um status quase onipresente em grande parte do mundo, a governança da internet se tornou um tema de estudo importante. Essa governança afeta diversas questões fundamentais como o acesso aberto, a liberdade de expressão, inovações e suas aplicações, como o comércio e a segurança. Grande parte das discussões em volta da governança da internet são pautadas por questões geopolíticas e “têm ocorrido entre políticos, analistas políticos, bem como pesquisadores de Escolas de Informação e Comunicação” (Subramanian, 2013, p.1).

CIBERPOLÍTICA

Para compreendermos a ciberpolítica e o poder cibernético é necessário reconhecer que ambos surgem em virtude do fenômeno político e se influenciam mutuamente. Não há precedentes ontológicos estabelecidos entre poder e política dado que o poder se manifesta no âmbito da política ao mesmo tempo que a política surge das dinâmicas de poder (Honório, 2016) e o ciberespaço é apenas um dos meios pelos quais essas relações são exercidas.

Nazli Choucri (2012, p. 4) descreve a ciberpolítica como “a junção das interações humanas (políticas) que envolvem a decisão de quem obtém o quê, quando e como e as ações habilitadas pelo uso de espaços virtuais (ciber) como um novo cenário de disputas com suas próprias realidades”. As relações internacionais envolvem política de uma forma ou outra, e mesmo que haja diferentes perspectivas sobre o termo existe uma compreensão geral do significado de ‘política’, o que gera complexidade

o prefixo ‘ciber’ que se difere nesse novo termo criado.

Ao combinarmos a definição de política de Bobbio (1883, p. 1185) de “atos como o ordenar ou proibir alguma coisa com efeitos vinculadores para todos os membros de um determinado grupo social, o exercício de um domínio exclusivo sobre um determinado território” com a visão de Lasswell (1950) de definir o termo como “quem obtém o quê, quando e como” podemos concluir que a política é relevante para todos em diversos contextos e lugares, sendo assim atemporal.

Toda política, seja no ciberespaço ou no mundo físico, envolve conflito, negociação e acordos para determinar os meios, institucionais ou não, de resolver de maneira autoritária as disputas sobre o que seria os valores fundamentais ou o que é considerado o certo. Como destacado por Lasswell (1950), o estudo da política é o estudo da influência e dos influentes.

PODER

Poder é um tema central para as Relações Internacionais, pois contribui para compreender como os países interagem entre si e como funciona o Sistema Internacional. Existem diversas formas de entender essa dinâmica, a depender da abordagem adotada por cada teórico. Diversos elementos influenciam esse cenário, variando desde a capacidade militar e econômica de um Estado até sua influência política e cultural.

Os estudos sobre o conceito de poder são diversos, e cada autor apresenta uma perspectiva distinta e válida sobre como o poder é concebido, exercido e contestado no cenário global. Trata-se de um tema amplamente explorado na produção acadêmica. Nesta pesquisa, contudo, a análise será orientada pelos trabalhos de Joseph Nye, um dos autores mais reconhecidos no campo dos estudos sobre poder, especialmente por suas contribuições relacionadas às noções de poder no mundo contemporâneo.

DEFINIÇÕES DE NYE: HARD POWER, SOFT POWER E SMART POWER

Nye (2014) questiona a falta de consenso sobre a

definição de poder no mundo moderno. Sob o pretexto de que as atuais teorias de Relações Internacionais não são capazes de compreender toda a complexidade do Sistema Internacional, ele argumenta que o conceito tem que levar em consideração suas duas faces: *behavioral power*, ou poder comportamental, que é definido como resultados comportamentais; e *resource power*, ou fonte de poder, definido como os recursos.

O poder comportamental divide-se em: poder de comando (*command power*) e poder cooptivo (*co-optive power*). O poder de comando é definido por Nye como a “habilidade de mudar o que os outros fazem” (Nye, 1990, p. 267, tradução própria) e se manifesta por meio da coerção. Já o poder cooptivo, refere-se à capacidade de mudar as preferências dos outros atores, ou seja, moldar o pensamento dos outros para que ajam de uma determinada maneira, como se fosse um ator invisível.

De acordo com essa conceituação, cada forma de poder comportamental se baseia em uma fonte de poder. Logo, o poder de comando — por ser uma ação de coerção — está associado às fontes de *hard power*, enquanto o poder cooptivo — ligado à persuasão — está associado às fontes de *soft power*. Nye faz uma ressalva sobre a precisão dessa relação, destacando que em alguns casos o poder de comando pode estar relacionado às fontes de *soft power*, assim como o poder cooptivo pode estar ligado às fontes de *hard power*.

Analisando a conceituação do autor, entende-se por *hard power* a conceituação tradicional de poder para os realistas, que além da força militar e abrange também inclui a imposição de sanções econômicas, restrições comerciais, e a diplomacia coercitiva como meio de influenciar a conduta de outros Estados. Por outro lado, o *soft power* é o poder que um país possui de influenciar de forma indireta o comportamento de outro país, através de recursos culturais, ideias e valores políticos. Nye defende a necessidade de um maior equilíbrio entre o *soft* e o *hard power* e isso seria possível através do *smart power* — ou poder inteligente —, que segundo ele seria a capacidade de combinar os recursos de poder de forma estratégica e efetiva. Como afirma o autor:

O poder inteligente vai ao cerne do problema da conversão do poder. Como vimos anteriormente

alguns países e atores podem possuir mais recursos de poder do que outros, mas não serem muito eficazes em converter toda a gama de seus recursos de poder em estratégias que produzam os resultados desejados (Nye, 2011, p. 38).

Em resumo, constatamos que não basta possuir recursos de poder — é fundamental saber utilizá-los estrategicamente. A combinação de diferentes tipos de poder aumenta as chances de se alcançar os resultados desejados.

CIBERPODER

As mudanças tecnológicas e o surgimento do ciberespaço aumentaram a complexidade do conceito de poder. Nye (2012) faz uma dupla conceituação: comportamental e de domínio. No primeiro, ciberpoder pode ser definido com o conjunto de recursos relacionados a capacidade de atuação no ciberespaço, segundo o autor:

O poder cibernético pode ser definido como um conjunto de recursos que relacionam-se à criação, ao controle e à comunicação de informações eletrônicas e baseadas em computador – infraestrutura, redes, softwares e habilidades humanas. Isso inclui não somente a Internet dos computadores ligados à rede, mas também intranets, tecnologias de celulares e comunicações via satélite (Nye, 2012, p. 127, tradução própria).

Em termos comportamentais, ele também caracteriza o ciberpoder como a capacidade de alcançar os resultados desejados utilizando como recurso as informações eletronicamente interconectadas que o ciberespaço oferece. Esse poder pode ser usado para alcançar resultados dentro do ciberespaço ou essas tecnologias também podem ser usadas para produzir resultados em outros domínios que não sejam virtuais.

No segundo, ciberpoder é como um poder de domínio englobando os recursos e a capacidade de geração de *soft* e *hard power* dentro de um determinado âmbito. Sendo assim, o poder cibernético pode ser comparado por analogia, com “poder naval”, “poder aéreo” e “poder terrestre”. No entanto, há uma característica distinta entre o poder cibernético e os outros conceitos, “tal diferença reside na amplitude do domínio cibernético, a dependência de muitas es-

truturas das sociedades modernas em sistemas interconectados em rede” (Maier, 2015, p. 11).

O ciberespaço, por ser uma criação humana, é um domínio estratégico singular, sujeito a rápidas transformações tecnológicas que o tornam mais dinâmico do que os domínios tradicionais como o terrestre, marítimo ou aéreo. Sua acessibilidade e as baixas barreiras de entrada facilitam a difusão de poder, permitindo que não apenas grandes potências, mas também atores não estatais e Estados com menos recursos exerçam influência significativa. Diferentemente de domínios que exigem pesadas infraestruturas físicas e investimentos robustos, o ciberespaço permite a movimentação de informação com velocidade incomparável, como destaca Nye (2011), “é muito mais rápido mover elétrons pelo globo do que grandes navios pelo mar”. Essas características desafiam as hierarquias tradicionais de poder, tornando o ciberespaço um campo estratégico fluido e em constante disputa.

Nye (2011) também observa que o ciberespaço compartilha com a guerra terrestre três características marcantes: o grande número de participantes, a facilidade de entrada e a possibilidade de ocultação. Na terra a dominância não é um critério facilmente alcançável. Embora alguns países, como os Estados Unidos, Rússia, Grã-Bretanha, França e China, sejam considerados mais capacitados que outros - segundo o *National Cyber Power Index* -, não faz sentido falar de dominância no ciberespaço da mesma forma que se fala no poder naval ou aéreo. Na realidade, a dependência dos sistemas cibernéticos complexos para apoiar atividades militares e econômicas cria novas vulnerabilidades nos grandes Estados, as quais podem ser exploradas por atores não estatais e por outros países também (Nye, 2011).

Isso leva a uma modificação crucial quando pensamos sobre o papel do Estado em controlar e manejar o poder advindo da informação. O Estado-nação não possui mais o monopólio de controle sobre a informação e, além disso, lança-se num ambiente onde deve se relacionar com outros atores que competirão com ele em uma série de temáticas e, inclusive, pelo próprio poder de regulação do ambiente cibernético (Maier, 2015, p. 12).

No entanto, isso não significa, para Nye, que estamos caminhando para o fim do Estado — muito pelo contrário. Para o autor, o Estado continua sendo um ator central, embora cada vez mais vulnerável diante dos desafios transnacionais, os quais já não consegue enfrentar de forma totalmente autônoma.

CIBERPODERE A TRIPOLARIDADE

Em *The Tragedy of Great Power Politics* (2001), John Mearsheimer desenvolve a teoria do realismo ofensivo, em oposição às visões de Kenneth Waltz e à abordagem clássica de Hans J. Morgenthau. A partir dessa perspectiva, o autor considera que o Sistema Internacional, por ser anárquico, necessita de uma autoridade superior capaz de subjugar a irracionalidade dos Estados que estão em constante busca pela expansão para garantir sua sobrevivência e seus recursos essenciais. Nessa visão, os Estados não contam com verdadeiros amigos no cenário internacional. Na melhor das hipóteses, têm rivais, nos quais não é prudente depositar confiança.

O autor também discorre sobre o equilíbrio e a divisão de poder no Sistema Internacional. O poder, segundo ele, pode ser distribuído entre as grandes potências de três maneiras: sistemas bipolares são dominados por duas grandes potências de forças militares aproximadamente iguais; sistemas multipolares desequilibrados contêm três ou mais grandes potências, onde uma delas é um potencial hegemônico; e sistemas multipolares equilibrados não têm um aspirante a hegemônico, em vez disso, o poder é distribuído de maneira bastante uniforme entre as grandes potências, ou pelo menos entre os dois Estados mais poderosos no sistema (Mearsheimer, J., 2001).

A bipolaridade é a configuração de poder que gera relativamente menos medo entre grandes potências, pois tende a haver um equilíbrio entre os dois Estados centrais (Mearsheimer, 2001). O conceito se tornou explícito durante a Guerra Fria, quando restaram apenas duas superpotências – EUA e URSS – com amplo domínio político, econômico e nuclear (Williams; McDonald, 2018). Essa estrutura refletia uma divisão ideológica global entre capitalismo e comunismo. A rivali-

dade era intencionalmente alimentada por essas potências e os demais países se posicionavam em função dessa disputa. O fim da Guerra Fria encerrou tanto a estrutura bipolar quanto o embate ideológico que a sustentava.

A teoria de polaridade se baseava na ideia de uma única distinção entre grandes potências e outros Estados, com o fim da Guerra Fria havia apenas três possibilidades. O sistema poderia ser 1) unipola, caso em que os EUA eram o único candidato a superpotência; 2) multipolar, caso em que Rússia, China, Japão e a União Europeia precisavam ser elevados a paridade com os EUA como grandes potências; ou 3) a polaridade de alguma forma se tornaria obsoleta.

Atualmente, a estrutura multipolar mais aceita entre os realistas possui uma divisão $2 + 5^3$, sendo: Estados Unidos, China, a União Europeia, Reino Unido, Rússia, Japão e a Índia. Embora a multipolaridade seja, em geral, mais propensa a guerras do que a bipolaridade, algumas configurações de poder multipolares são mais perigosas do que outras. As guerras entre grandes potências são mais prováveis quando os sistemas multipolares são desequilibrados, ou seja, quando há uma diferença marcante nas capacidades entre o primeiro e o segundo estado no sistema, de modo que o mais poderoso possui os meios para buscar a hegemonia (Nye, 2014)

Mearsheimer (2014) propõe que as três possíveis arquiteturas do Sistema Internacional variam quanto à sua propensão à guerra: da instabilidade característica da multipolaridade desequilibrada à relativa estabilidade da bipolaridade, situando a multipolaridade equilibrada em uma posição intermediária entre esses dois extremos. Além disso, para o autor, a guerra tende a ser mais provável em sistemas multipolares, pois esses apresentam maior número de conflitos potenciais e maior propensão ao desequilíbrio de poder. Nesse contexto, as grandes potências têm mais chances de possuir capacidade para vencer uma guerra, o que dificulta a dissuasão e torna os confrontos mais prováveis. Ademais, o potencial para erros de cálculo é maior: os Estados podem superestimar sua força e acreditar que são capazes de coagir ou conquistar outros, quando, na realidade, não são.

MUNDO MULTIPOLAR NO CIBERESPAÇO

Na última década, os incidentes cibernéticos tornaram-se mais caros, mais disruptivos e, em muitos casos, mais políticos, com uma nova esfera para competição entre as grandes potências mundiais e com isso podemos perceber a expansão das capacidades de projeção e a minimização das suas vantagens no contexto do ciberespaço. Sendo assim, o gap de ciberpoder entre os EUA, China e Rússia é significativamente menor quando comparado ao que se observa nas esferas econômica e militar..

Mais do que nunca os Estados passaram a encarar o poder cibernético como uma ferramenta central de política abrangente, ao mesmo tempo em que tratam a segurança cibernética como um desafio fundamental. Paralelamente, com o avanço da digitalização de diversos aspectos da economia e da sociedade, as preocupações com a segurança no ciberespaço têm se expandido também para o domínio político.

O Belfer Center for Science and International Affairs, desenvolveu o National Cyber Power Index (NCPI) que explora em que medida certos Estados buscam alcançar determinados objetivos estratégicos através de meios cibernéticos, além de fornecer uma avaliação mais completa do poder cibernético. O estudo mede as estratégias governamentais, capacidades para operações defensivas e destrutivas, alocação de recursos, capacidades do setor privado dentro de um país, como empresas de tecnologia, força de trabalho e inovação, visando apresentar a capacidade e o potencial das nações analisadas por meio de oito objetivos nacionais, usando 29 indicadores de capacidade, com dados coletados em informações públicas. O índice apresenta um ranking com os 10 países com o mais alto nível de intenção e capacidades nas oito metas.

As ciberpotências são aquelas mais bem posicionadas no ranking, demonstrando elevada intenção e capacidade de alcançar a maioria de seus objetivos por meio de recursos cibernéticos, enquanto os Estados com pontuações mais baixas tendem a buscar apenas objetivos mínimos, usando tais meios com níveis reduzidos

de intenção e capacidade. Os dois primeiros colocados, Estados Unidos e China, respectivamente, mantêm suas posições desde a última análise feita em 2020.

Analisando os dados do *ranking* notamos que a Rússia passou do 4º para o 3º lugar e o Reino Unido caiu uma posição ficando em 5º lugar. Em dois objetivos, ganho comercial e capacidade destrutiva, o poder cibernético russo aumentou em relação ao do Reino Unido, principalmente devido à realização de mais operações cibernéticas que foram publicamente relatadas.

Fazendo um comparativo entre o *Overall Ranking of Cyber Powers* e o *Military Expenditure* percebemos uma diminuição drástica da vantagem entre os principais países. Enquanto os gastos militares têm uma diferença de trilhões de dólares do primeiro colocado em relação ao segundo, essa relação continua nos demais países da lista. Em contraponto, no *ranking* de ciberpotências existe uma diferença mínima comparada.

Como posto por Nye (2011) o que é distintivo sobre o poder no domínio cibernético não é que os governos estão fora de cena, como previam os primeiros libertários cibernéticos, mas sim os diferentes recursos de poder que diferentes atores possuem e a redução da lacuna entre atores estatais e não estatais em muitos casos. No entanto, a redução relativa das diferenças de poder não é o mesmo que igualação. Grandes governos ainda têm mais recursos.

CYBER POWER INDEX E AS TRÊS PRINCIPAIS POTÊNCIAS

Embora os Estados tenham desenvolvido políticas abrangentes para o uso do poder cibernético nos últimos anos, podemos observar uma série de ciberataques significativos ocorrendo. Nesse período, não apenas os ataques de *ransomware*⁴ em grande escala aumentaram, mas também houve um crescimento no uso de cadeias de suprimento digitais como vetor para ciberataques (Voo; Hemani; Cassidy; 2022, p. 12).

À medida que nos tornamos mais conectados e integrados, os ciberataques se

tornam mais atraentes para criminosos e Estados. Isso faz com que os Estados precisem fortalecer o seu poder no ciberespaço para que possam proteger os seus interesses. Nesse cenário, o ciberespaço se torna mais uma face que gera disputas, conforme os Estados buscam superar-se uns aos outros através de meios cibernéticos e ampliar seu poder cibernético. Como posto pelo NCPI:

Os Estados buscam não apenas destruir e desativar a infraestrutura e as capacidades de um adversário (a percepção tradicional, mas estreita e enganosa do poder cibernético), mas também fortalecer e aprimorar as defesas cibernéticas nacionais, coletar inteligência em outros países, aumentar a competência nacional em tecnologia cibernética e comercial, controlar e manipular o ambiente informacional e estender sua influência definindo normas cibernéticas e padrões técnicos internacionais (NCPI, 2022, p. 12).

Nesta seção iremos analisar os dados do NCPI publicado em 2022 pelo Belfer Center for Science and International Affairs de Harvard. Um dos índices mais atuais, e que realiza uma análise abrangente e precisa para medir o poder cibernético. Ele mede estratégias governamentais, capacidades para operações defensivas e destrutivas, alocação de recursos, capacidades do setor privado dentro de um país, como empresas de tecnologia, força de trabalho e inovação.

O Índice fornece avaliação do poder cibernético de 30 Estados — tendo sido escolhidos apenas os países que possuem banco de dados publicamente disponíveis — levando em consideração os indicadores que contribuem tanto para a intenção quanto para as capacidades. Foram utilizados 29 indicadores de capacidade em 8 objetivos para medir a capacidade e avaliar as estratégias nacionais de todos os estados participantes.

A partir da análise desses objetivos, identificados como: Capacidade Financeira; Vigilância e Monitoramento; Coleta de Inteligência; Cibertecnologia e Tecnologia Comercial; Defesa; Controle e Manipulação de Informação; Capacidade Destrutiva; e Normas, é possível comparar os Estados Unidos, China e Rússia, nações que compõem o top 3 do *ranking* e o suposto sistema tripolar.

A Capacidade Financeira corresponde às operações cibernéticas realizadas por Estados com o objetivo de acumular recursos financeiros.

Tais ações envolvem ataques de ransomware, invasões a infraestruturas digitais de instituições financeiras, extração de dados sensíveis e extorsão baseada em informações obtidas ilegalmente. No ranking analisado, destacam-se Coreia do Norte, China, Vietnã e Irã, respectivamente. Essas atividades geram instabilidade no Sistema Internacional, prejudicando a credibilidade dos Estados que as admitem. A ausência da Federação Russa nesse indicador se justifica pela ausência de declarações oficiais que reconheçam a intenção governamental de empregar ataques cibernéticos com fins financeiros, apesar da atuação de grupos independentes em seu território.

A Vigilância e o Monitoramento referem-se à concessão de permissões legais e capacidades técnicas para vigilância digital dentro das fronteiras nacionais. Essas ações incluem a vigilância de indivíduos, interceptação de comunicações e bloqueio de serviços estrangeiros considerados ameaçadores. A República Popular da China ocupa a primeira posição nesse critério, sendo amplamente conhecida pelo monitoramento contínuo de seus cidadãos. Os Estados Unidos figuram na quarta posição e a Rússia na sétima.

A Coleta de Inteligência Estrangeira contempla esforços estatais para adquirir informações sensíveis de outros países por meio do ciberespaço, envolvendo dados diplomáticos, militares e estratégicos. Os Estados Unidos lideram nesse quesito, com uma infraestrutura robusta composta por agências como a Agência de Segurança Nacional (NSA) e o Comando Cibernético dos Estados Unidos (USCYBERCOM). O caso Edward Snowden, em 2013, revelou a dimensão dessas práticas, incluindo a interceptação de comunicações de chefes de Estado, como a ex-presidente Dilma Rousseff. China e Rússia completam os três primeiros colocados.

O Desenvolvimento Nacional em Cibertecnologia e Tecnologia Comercial refere-se ao fortalecimento da base tecnológica nacional, seja por meio de investimentos diretos em pesquisa e desenvolvimento, seja pelo uso do espaço cibernético para impulsionar setores industriais. A China ocupa a liderança, seguida por Estados Unidos e Rússia, refletindo a crescente

centralidade da tecnologia no poder nacional.

A Defesa Cibernética engloba as medidas adotadas pelos Estados para proteger ativos estratégicos e promover uma cultura de cibersegurança entre instituições e cidadãos. A Austrália lidera esse aspecto, com políticas públicas voltadas à construção de uma postura cibernética resiliente. Os Estados Unidos ocupam a terceira posição, enquanto Rússia e China aparecem mais distantes no ranking.

O Controle e a Manipulação da Informação dizem respeito ao uso de capacidades cibernéticas para censurar, redirecionar ou moldar narrativas tanto internamente quanto no exterior. Os Estados Unidos ocupam a primeira colocação, destacando-se pelo uso seletivo e muitas vezes invisível de filtragens informacionais. A Rússia, em segundo lugar, adota um arcabouço legal e tecnológico para restringir o acesso à internet. A China, em terceiro, aplica um modelo altamente restritivo, conhecido por sua robusta arquitetura de censura digital.

A Capacidade Destrutiva refere-se à habilidade de um Estado em executar ataques cibernéticos com efeitos disruptivos ou destrutivos, visando minar a capacidade de ação de adversários. Os Estados Unidos mantêm a liderança neste domínio, com uma estrutura estratégica voltada tanto para a defesa quanto para a ofensiva cibernética. A Rússia, impulsionada pela guerra na Ucrânia e pela atuação coordenada de suas agências e grupos afiliados, ocupa a segunda posição. A China aparece em terceiro lugar.

Por fim, a dimensão “Normas” avalia a atuação dos Estados na formulação de regras internacionais sobre o uso do ciberespaço. Os Estados Unidos se destacam por sua participação ativa e histórica na construção da governança da internet, por meio de instituições como a Corporação da Internet para Atribuição de Nomes e Números (ICANN) e a Força Tarefa de Engenharia de Internet (IETF). A China figura na quarta posição, com ênfase em uma abordagem baseada na soberania estatal e no controle sobre a rede. Já a Rússia ocupa uma posição inferior, em parte devido à sua postura agressiva no ambiente cibernético e à promulgação de legislações como a “Lei de Soberania da Internet”, que visa ao isolamento da internet russa em caso de ameaças externas.

ESTADOS UNIDOS

A dominação no ciberespaço tem sido um objetivo estratégico dos Estados Unidos desde meados da década de 1990. É o único país com uma presença global significativa tanto em usos civis quanto militares do ciberespaço, embora agora se perceba seriamente ameaçado pela China e Rússia nesse domínio (IISS, 2021, p. 15). Para o país, o espaço cibernético é trabalhado no âmbito da Estratégia Nacional de Defesa e é considerado como um domínio prioritário, tanto para a segurança de sistemas internos quanto para suas ambições no exterior nos âmbitos diplomático, político, econômico e militar.

Os EUA avançaram de maneira mais eficiente que qualquer outro país na defesa da infraestrutura crítica nacional no ciberespaço, mas reconhecem que é uma tarefa complexa e que grandes vulnerabilidades ainda existem. Tendo isso em vista, eles têm assumido, por mais de duas décadas, um papel de liderança em mobilizar a comunidade global para desenvolver princípios comuns de cibersegurança.

Além disso, o país mantém uma clara vantagem no âmbito do TIC, mas isso não confere uma posição de monopólio. Pelo menos seis países europeus ou asiáticos ocupam posições de liderança em certos aspectos do setor de TIC, embora todos, exceto um (China), sejam aliados próximos ou parceiros estratégicos dos EUA. “Sua capacidade provavelmente é a mais desenvolvida em relação aos outros países, embora o seu pleno potencial permaneça em grande parte não demonstrado” (IISS, 2021, p. 22).

CHINA

Os líderes chineses agiram de maneira decisiva para adotar a revolução da informação. Na década de 1990 eles se encontravam em posição de relativo atraso no desenvolvimento eletrônico, porém com a vantagem de uma economia em rápido crescimento e projeção internacional de suas tecnologias. “Desde então o país estabeleceu o sistema de vigilância e censura doméstica no ciberespaço, um dos mais extensos do mundo controlado pelo governo” (IISS, 2021,

p. 90).

Desde dos anos 2000 a China realiza operações cibernéticas larga escala no exterior com o objetivo de adquirir propriedade intelectual, influência política, além de realizar espionagem e posicionar suas capacidades com o intuito de causar disruptividade em caso de futuros conflitos. Essa postura gerou grandes disputas com os EUA— e seus aliados—, travando uma batalha sobre a governança cibernética global que se agravou com a decisão americana no ano de 2017 em sancionar as empresas de tecnologia chinesas por causa das atividades maliciosas que o país tem executado.

É possível constatar sua intenção em se tornar uma potência cibernética através da sua estratégia militar, divulgada em 2015, e de sua estratégia formal em cibersegurança, tornada pública no ano seguinte. Seu objetivo é se tornar o líder mundial na produção de tecnologias fundamentais que a internet é dependente. Atualmente, ocupa o segundo lugar no ranking, mas devido a sua crescente base industrial em tecnologia digital é o país mais bem posicionado para se juntar aos EUA no primeiro nível.

RÚSSIA

A governança cibernética é centralizada e hierárquica, comandada pessoalmente pelo presidente russo. É um país altamente dependente de corporações estrangeiras de tecnologia da informação e comunicação e sua economia digital deixa a desejar, estando atrás de países como o Reino Unido e a França. A Rússia tem buscado corrigir grandes vulnerabilidades na área de segurança cibernética e tem feito isso através da regulamentação governamental e a criação de uma internet soberana, além de incentivar o desenvolvimento de uma indústria digital nacional. Porém considerando suas condições econômicas essas ambições podem ser irrealistas.

Durante as duas últimas décadas, tem liderado esforços diplomáticos para conter o que percebe como a predominância ocidental no ciberespaço, particularmente pelos Estados Unidos. E, utiliza das suas capacidades ofensivas como uma es-

estratégia para desestabilizar politicamente outros países, principalmente os EUA. Além de realizar diversas operações de ciberinteligência que revelam níveis crescentes de sofisticações técnicas. No entanto, a Rússia parece não ter dado prioridade ao desenvolvimento da capacidade cibernética necessárias para uma guerra de alta intensidade (IISS, 2021).

A estratégia cibernética da Rússia é ditada pelo seu confronto com Ocidente e as operações no ciberespaço são um elemento essencial na guerra de informações, pois a torna ainda mais ampla. Em resumo, a Rússia é uma potência cibernética de segundo escalão e para alcançar os EUA é necessário fazer mudanças na sua segurança cibernética, aumentar sua participação no mercado digital e avançar no desenvolvimento de ferramentas cibernéticas ofensivas mais sofisticadas.

TRIPOLARIDADE CIBERNÉTICA

Combinando as pontuações de intenção e capacidade em todos os oito objetivos, é possível refletir um Ranking de Poder Cibernético Abrangente, onde a potência cibernética mais abrangente é aquela que tem a intenção de perseguir múltiplos objetivos usando o ciberespaço e possui a capacidade para perseguir e alcançar esses objetivos. Podemos constatar, então, que os Estados no topo do *ranking* são os mais eficazes em usar os meios cibernéticos para alcançar objetivos em várias áreas.

Dada sua estrutura interna e as diferentes tecnologias utilizadas para facilitar o anonimato, o ciberespaço configura um domínio de inerente incerteza; e a forma como diferentes atores exploram essa característica, corresponde à uma dinâmica de poder diferente dos demais domínios. Logo, as decisões tomadas pelos envolvidos possuem alto valor estratégico — sendo, portanto — classificadas de forma que é improvável determinar quais ações foram tomadas primeiro.

Isto é, assim como o posicionamento norte americano mais ofensivo contra a Rússia pode ser interpretada como um reflexo do acordo estratégico com a China; a aproximação entre

China e Rússia pode ter sido ocasionada justamente pela postura mais agressiva pelos Estados Unidos da América.

Concluimos então que essas três potências se destacam por sua influência e ciberpoder em relação às outras nações, formando assim um sistema tripolar. A diferença de capacidades no âmbito do ciberespaço entre os Estados Unidos, China e Rússia pode ser considerada mínima comparada ao poder material tradicional, portanto nos vemos diante de uma nova reorganização do Sistema Internacional.

CONSIDERAÇÕES FINAIS

Toda a política envolve conflitos, negociações e acordos, assim os Estados buscam constantemente, no ciberespaço, formas de estenderem sua influência, domínio e poderio, seja pelas suas capacidades ou pela disposição de usá-las como forma de resolver disputas, manter o controle ou influência sobre outros Estados.

A crescente presença de aparelhos eletrônicos conectados, cada dia mais necessária para a vida cotidiana em aplicações comuns, aliada à internet e as facilidades de conectividade, tornou possível a criação do ciberespaço e conseqüentemente do exercício do ciberpoder. O indivíduo, mesmo que não tenha uma posição de poder, pode manifestar a sua opinião e dar voz a ela através da internet, mesmo com todos os esforços governamentais para controlar o ciberespaço.

Com base na análise dos dados coletados, sobretudo no índice de ciberpoder desenvolvido por Harvard, verifica-se que alguns países, mesmo não sendo potências mundiais se destacaram em alguns indicadores, como por exemplo o indicador de Capacidade Financeira que diz respeito às operações cibernéticas que um Estado conduz para acumular riqueza, ocasião em que apenas a República Popular Democrática da Coreia, a China, o Vietnã e o Irã, pontuaram.

A configuração atual do ciberpoder é multipolar, com destaque para três grandes potências: Estados Unidos, China e Rússia, nessa ordem. Os Estados Unidos continuam sendo a

principal potência, embora já não estejam em uma posição totalmente confortável. A China ainda mantém sua colocação em segundo lugar, enquanto a Rússia ultrapassou o Reino Unido nos rankings mais recentes. Conclui-se, assim, que essas três nações se sobressaem em termos de influência e ciberpoder, estabelecendo um sistema tripolar e contribuindo para uma nova reorganização do Sistema Internacional.

NOTAS

¹Bacharel em Relações Internacionais pela Universidade Católica de Brasília, giovannacastrogoncalves@gmail.com

²O texto integral pode ser acessado no Repositório Institucional da Universidade Católica de Brasília, disponível em: <https://repositorio.ucb.br:9443/jspui/handle/123456789/14421>.

³O conceito “2+5” em um mundo multipolar refere-se a uma configuração geopolítica emergente em que sete países concentram as maiores influências globais — sendo dois deles considerados superpotências predominantes, enquanto os outros cinco exercem poder relevante, mas em menor escala. Essa fórmula destaca a diferença de peso entre os dois polos principais e os demais atores influentes na ordem internacional contemporânea.

⁴É um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (ransom) para restabelecer o acesso ao usuário. Ver mais em: <https://cartilha.cert.br/ransomware/>.

REFERÊNCIAS

A new global ranking of cyber-power throws up some surprises. **The Economist**, 19 set. 2020. Disponível em: <https://www.economist.com/science-and-technology/2020/09/17/a-new-global-ranking-of-cyber-power-throws-up-some-surprises>. Acesso em: 27 abr. 2024.

BARNETT, M; DURVALL, R. Power in International Politics. **International Organization**, v. 59, n. 1, p.39–75. 2005. Disponível em: <https://www.cambridge.org/core/journals/international-organization/article/power-in-international-politics/F5F3C74D30A12A5C4CC9B4EFEA152967>. Acesso em: 15 maio 2024.

BRANFORD, B. Wikeleaks volta aos holofotes com apoio a Snowden. **BBC News**, Brasil, 27 jun. 2013. Disponível em: https://www.bbc.com/portuguese/noticias/2013/06/130627_snowden_wikileaks_gm. Acesso em: 05 jun. 2024.

BRITES, R. C. A construção do ciberespaço e seu impacto nas Relações Internacionais: a inserção brasileira no debate de Governança da Internet. **Comitê Gestor da Internet no Brasil**, ago. 2017. Disponível em: https://www.academia.edu/35394199/A_constru%C3%A7%C3%A3o_do_ciberespa%C3%A7o_e_seu_impacto_nas_Rela%C3%A7%C3%B5es_Internacionais_a_inser%C3%A7%C3%A3o_brasileira_no_debate_de_Governan%C3%A7a_da_Internet. Acesso em: 10 nov. 2023.

BLUMENTHAL, M. S. CLARK, D. D. Rethinking the Design of the Internet: The End-to-End Arguments vs. the Brave New World. **ACM Transactions on Internet Technology (TOIT)**, v. 1, n. 1, p. 70-109, 2001. Disponível em: <https://dl.acm.org/doi/abs/10.1145/383034.383037>. Acesso em: 08 nov. 2023.

CASTELLS, M. **The Network Society From Knowledge to Policy**. In: CASTELLS, M; CARDOSO, G. (org.). *The Network Society From Knowledge to Policy*. Washington DC: Center for Transatlantic Relations, 2005. cap. , p. 23-76.

CÁRCERES, A. 'Periféricos' atualiza a visão de futuro de William Gibson, o mestre do cyberpunk. **Estadão**, São Paulo, 08 mar. 2021. Disponível em: <https://www.estadao.com.br/cultura/perifericos-atualiza-a-visao-de-futuro-de-william-gibson-o-mestre-do-cyberpunk/>. Acesso em: 21. out. 2023.

CEPIK, M. CANABARRO, D. R. BORNE, T. A Securitização do Ciberespaço e o Terrorismo: Uma Abordagem Crítica. In: SOUZA, A. M. NASSER, R. M. MORAES, R. F. **Do 11 de setembro de 2001 à guerra ao terror: reflexões sobre o terrorismo no século XXI**. Brasília, Ipea, 2014.

CORREIA, C. O Poder em Relações Internacionais: o núcleo realista e o calcanhar de Aquiles liberal. **Orbis**. 2021. Disponível em: <https://orbisirsa.pt/o-poder-em-relacoes-internacionais-o-nucleo-realista-e-o-calcanhar-de-aquiles-liberal/>. Acesso em: 27 abr. 2024.

CHOUCRI, N. **Cyberpolitics in international relations**. MIT press, 2012.

CLARK, D. D. **Characterizing cyberspace: past, present and future**. MIT, Massachusetts. 2010. ECIR Working Paper No. 2010-3. Disponível em: <https://dspace.mit.edu/handle/1721.1/141692>. Acesso em: 10 out. 2023.

DOS SANTOS JR, P. C. G. **O Uso do Ciberespaço para a Obtenção de Poder no Cenário Internacional durante o Início do Século XXI**. 2016. Dissertação (Graduação em Relações Internacionais) - Instituto Universitário de Pesquisas do Rio de Janeiro, Rio de Janeiro, 2016.

HONÓRIO, T. J. **Segurança na era da informação: reflexões teóricas sobre a ciber política internacional**. 2016. Dissertação (Mestrado em Estudos Estratégicos) - Universidade Federal Fluminense, Rio de Janeiro, 2016.

IISS. **Cyber Capabilities and National Power: A Net Assessment**. 2021 Disponível em: <https://www.iiss.org/research-paper/2021/06/cyber-capabilities-national-power/>. Acesso em: 10 set. 2024.

ISSHIKI, J. N. MIYAZAKI, S. Y. M.. Soft Power como estratégia de Marketing: a manifestação da cultura pop japonesa no Brasil. **Estudos Japoneses**, n. 36, p. 59-70, 2016. Disponível em: <https://www.revistas.usp.br/ej/article/view/127690>. Acesso em: 07 mar. 2024.

KAUPPI, M. V. VIOTTI, P. R. **International relations theory**. 2. ed. Longman, 2012.

KELLO, L. Cyber disorders: Rivalry & Conflict in a Global Information Age. **International Security Program**, Minerva Project (Harvard-MIT), Belfer Center, Harvard Kennedy School, v. 3, 2012.

KEOHANE, R. O. NYE JR, J. S. **Power and interdependence**. 4. ed. Longman, 2012

KUEHL, D. T. From Cyberspace to Cyberpower: Defining the Problem. In: KRAMER, F. D. STARR, S. H. WENTZ, L. K. (Ed.). **Cyberpower and national security**. Potomac Books, Inc., 2009. cap. 2, p. 24-42.

KURBALIJA, J. **An introduction to internet governance**. Diplo Foundation, 2016.

KURBALIJA, J. GELBSTEIN, E. **Governança da Internet**. Tradução: Renato Aguiar. 1. ed. 2005.

LASSWELL, H. D. **Who Gets What, When, How**. New York: P. Smith, 1950.

MAIER, F. A Revolução da Informação e o Poder Cibernético: Um mapeamento conceitual na obra de Joseph S. Nye. Jr. **Revista de Iniciação Científica da FFC (Cessada)**, v. 14, n. 1. Disponível em: <https://revistas.marilia.unesp.br/index.php/ric/article/view/6345>. Acesso em: 17 abr. 2024.

MARIANO, M. P. PIGATTO, J. T. ALMEIDA, R. A. R. Atores Internacionais e Poder Cibernético: O papel das transnacionais de tecnologia na era digital. **Monções**, Dourados, v. 7. n.13, p. 199-229. 2018. Disponível em: <https://ojs.ufgd.edu.br/index.php/moncoes>. Acesso em: 02 dez. 2023.

MEARSHEIMER, J. J. **The Tragedy of Great Power Politics**. WW Norton & Company, 2001.

MEARSHEIMER, J. J. **Structural realism**. International relations theories: Discipline and diversity, v. 3, p. 77-93, 2013. Disponível em: https://www.comackschools.org/Downloads/8_mearsheimer-_structural_realism.pdf. Acesso em: 15 abr. 2024.

MONTEIRO, S.D. O Ciberespaço: o termo, a definição e o conceito. **DataGramaZero**, v.8 n.3 Jun, 2007. Disponível em: <https://cip.brapci.inf.br/autoridade/v/6089>.

MORGENTHAU, H. J. **Politics Among Nations**. 4. ed. New York: Knopf, 1966.

NYE JR, J. S. **Power in the global information age: From realism to globalization**. Routledge, 2004.

NYE JR, J. S. **The future of power**. PublicAffairs, 2011.

RANA, W. Theory of Complex Interdependence: A Comparative Analysis of Realist and Neoliberal Thoughts. **International journal of business and social science**, v. 6, n. 2, 2015. Disponível em: https://www.ijbssnet.com/journals/Vol_6_No_2_February_2015/33.pdf. Acesso em: 20 abr. 2024.

SANTANA, B. O Que é o Protocolo TCP/IP e Como Ele Funciona? **Hostinger**. 07 maio 2022. Disponível em: <https://www.hostinger.com.br/tutoriais/tcp-ip>. Acesso em: 02 out. 2023.

SUBRAMANIAN, R. **Internet Governance: A Developing Country Perspective**. Communications of the IIMA, vol. 13, n. 1. 2013. Disponível em: https://scholarworks.lib.csusb.edu/ciima/vol13/iss4/1/?utm_source=scholarworks.lib.csusb.edu%2Fciima%2Fvol13%2Fiss4%2F1&utm_medium=PDF&utm_campaign=PDFCoverPages. Acesso em: 12 de out. 2023.

VOO, J. HEMANI, I. CASSIDY, D. National Cyber Power Index 2022. Belfer Center for Science and International Affairs. **Harvard Kennedy School**, 2022. Disponível em: <https://www.belfercenter.org/publication/national-cyber-power-index-2022>. Acesso em: 10 set. 2023.

WALTZ, K. N. **Man, the state, and war: A theoretical analysis**. Columbia University Press, 2018.

WALTZ, K. N. **Theory of International Politics**. Waveland Press, 2010.

WORLD INTERNET USERS AND POPULATIONS. **Internet usage statistics: the Internet big picture**. 2012. Disponível em: <http://goo.gl/L8hG>.