CAPÍTULO 18

O quinto domínio como palco da rivalidade entre China e EUA no século XXI

Mario Augusto dos Santos

Resumo

O presente artigo parte do pressuposto que no atual século, com o recrudescimento dos imperativos tecnológicos por parte dos Estados no sistema internacional, que vislumbram o desenvolvimento de redes de dados de última geração, bem como da Inteligência Artificial (IA), de tecnologias quantum e de armas cibernéticas como forma de aumentar seus respectivos poderes e/ou se proteger de prováveis ameaças cibernéticas, o denominado Quinto Domínio (o ciberespaço) vem se tornando cada vez mais palco de conflitos entre os Estados, observando-se, inclusive, uma crescente militarização neste domínio. Tendo em vista essa dinâmica vigente no atual século, sobretudo a partir da década de 2010 e que perpassa os governos Obama e se intensifica no governo Trump, pretende-se analisar as rivalidades entre China e EUA no quinto domínio, atentando-se para seus respectivos condicionantes e implicações, tanto para ambos os países quanto para o resto do mundo.

Palavras-chave: quinto domínio; rivalidades China-EUA; governos Obama e Trump; governo Xi Jinping.

1. Introdução

Não estamos assim tão distantes da época em que os prováveis domínios de conflito existentes compreendiam o mar, a terra, o espaço e o ar, todos estes domínios naturais, ou seja, independem da criação e vontade humana. Contudo, no presente século, como fruto inequívoco da tecnologia e da criação humana, aos quatro domínios iniciais é acrescentado um outro, o ciberespaço, também denominado de quinto domínio. Impulsionado pela revolução tecnológica que traz em seu bojo a internet, a economia digital, a alta velocidade de comunicação dentre outros inúmeros benefícios associados à revolu-

ção digital, o ciberespaço também é visto como um constante alvo de novas e difusas ameaças, que podem ser direcionadas tanto a bancos ou demais componentes do setor econômico e financeiro, quanto a instalações militares de países, de ambas as formas ocasionando sérios impactos de ordem global.

No que tange aos imperativos de segurança cada vez mais presentes em um cenário mundial multipolar e de baixa previsibilidade, observa-se que a segurança cibernética vem galgando importância crescente na política externa de vários Estados, demandando ações muitas vezes orquestradas em conjunto por um grupo de atores estatais, em parceria com o setor privado. Em adição, por serem ameaças difusas, executadas tanto por atores estatais como por não-estatais, ataques cibernéticos causam bastante instabilidade política e demandam respostas urgentes. Não obstante, a interconectividade em nível global se, por um lado, tem gerado benefícios significativos para Estados e para a economia como um todo, por outro acentua exponencialmente os riscos de ameaças cibernéticas.

Tendo como foco central de análise China e EUA, é possível vislumbrar, no que tange ao ciberespaço, preocupações recorrentes com iniciativas que contemplem o desenvolvimento de potencialidades nesta área, tanto visando à defesa quanto à ofensiva cibernética. Por vezes os discursos de ambos se mostram conflitantes e impregnados de acusações mútuas envolvendo ataques cibernéticos, espionagem cibernética e políticas ostensivas. Por outro lado, é possível, também, visualizar arranjos de segurança cooperativa em assuntos cibernéticos entre China e EUA. Dado o atual contexto mundial, no qual China e EUA se mostram os mais poderosos e influentes Estados nos mais variados aspectos, as relações entre estes têm acentuado peso nos rumos do cenário político mundial. Ambos desenvolvem ações importantes no ciberespaço, duelam pelo liderança mundial

no uso de IA, assim como defendem posições contrárias na adoção do padrão de redes de internet de quinta geração (5G).

De acordo com Lieberthal e Singer:

The spillover effect of cybersecurity on the broader U.S.-China relationship is also perhaps more critical than for any other bilateral relationship. This is both because of the enormous importance of U.S.-China relations in the emerging world order and, in turn, the growing role of cyber issues in eroding strategic trust and poisoning public and elite attitudes. If this trend can be reversed through improved engagement by the U.S. and China on cybersecurity, the outcome would be a triple win. It would bolster U.S.-China bilateral relations, serve as a crucial building block for multilateral efforts in the cyber arena, and also aid in broader US-Chinese engagement on other Cybersecurity and U.S.-China Relations v issues of importance, like global finance and the environment, where the two nations must learn to work better together (2012, p. 4/5).

Isto posto, faz-se mister buscar um entendimento acerca do estado da relação entre China e EUA no que tange ao ciberespaço, priorizando o desenvolvimento do campo em ambos os países e as implicações desta para o resto do mundo. Assim, no intuito de se desenvolver o presente artigo utilizou-se predominantemente consulta a bibliografias selecionadas e, também, a alguns documentos oficiais elaborados pelos governos de China e de EUA, os quais são de assumida importância na medida em que se pode constatar nestes a presença de visões conflitantes entre ambos os países, o que denota indícios da construção de uma retórica de rivalidade entre estes. Neste sentido, a análise dos comportamentos dos governos Obama e Trump, por parte dos EUA, e do governo Xi Jinping, por parte da China, no que tange a matérias relacionadas ao ciberespaço (espionagem cibernética, estratégia militar no ciberespaço, segurança cibernética, desenvolvimento de armas quantum, acusações mútuas, tentativas de construção de consensos e etc.) propicia a elaboração de hipótese acerca de uma escalada conflituosa entre China e EUA no quinto domínio, sobretudo com a militarização do ciberespaço.

Interessante aspecto é o de identificar, com base na bibliografia utilizada, que o discurso mais belicista do governo Trump não encontra eco no governo chinês. Dada a natureza da pesquisa, que se estrutura com base em uma metodologia qualitativa, visando desenvolver um estudo exploratório gerador de hipóteses, não se verifica aqui o recurso a softwares de tratamento de dados estatísticos.

Não obstante, a análise procura identificar a construção das estratégias de China e EUA no quinto domínio e como esta tende a gerar rivalidades entre ambos em diversos aspectos, sobretudo no que tange a espionagem cibernética, tecnologias quantum, adoção do padrão de redes de internet de quinta geração e escalada armamentista. Cumpre ressaltar que, ao se analisar as relações entre China e EUA no quinto domínio durante os governos Trump e Xi Jinping, pode-se constatar que o tom mais belicoso do governo Trump e suas respectivas estratégias de atuação neste domínio tendem a impulsionar as rivalidades entre ambos. Desta forma, no intuito de se desenvolver o presente artigo, optou-se, em um primeiro momento, pelo trato do tema ciberespaço nos governos Obama e Trump. Em seguida buscou-se contemplar o cenário chinês sob a mesma ótica. Em um terceiro momento, tendo estabelecido como China e EUA atuam no quinto domínio, cabe analisar a relação entre os dois neste âmbito. Por fim, cabem algumas considerações sobre o atual estado da relação e sobre as implicações no cenário mundial.

2. A questão cibernética na agenda norte-americana

Mesmo sem ser preciso recorrer a análises comparativas bastante detalhadas, pode-se verificar a existência de uma significativa diferença de postura e concepção no trato de importantes pautas militares, políticas, econômicas e comerciais norteamericanas por parte dos ex-presidentes Barack Obama (20/01/2009 a 20/01/2017)

e Donald Trump (20/01/2017 a 20/01/2021). Características pessoais, concepções políticas e condições estruturais vigentes ajudam a diferenciar ambas as administrações. No que tange aos propósitos deste trabalho, importa abordar o trato de questões cibernéticas importantes em ambos os governos.

Obama identificou a segurança cibernética como um dos mais sérios desafios econômicos e de segurança nacional com os que os EUA teriam de se deparar, assumindo que o país não estava adequadamente preparado para tanto. Assim, tão logo assumiu a presidência empreendeu esforços visando uma completa revisão nos esforços federais para defender a infraestrutura de informação e comunicação norte-americana e desenvolver uma abordagem abrangente no intuito de salvaguardar a infraestrutura digital dos EUA, daí resultando, em maio de 2009, a *Cyberspace Policy Review* do governo Obama, a qual indicou importantes recomendações de forma a dar um mais adequado tratamento às questões cibernéticas pelo governo, destacando-se a seleção de um *Executive Branch Cybersecurity Coordinator*. Este deveria ter acesso fácil e regular ao Presidente, bem como trabalhar próximo aos atores chave do campo da segurança cibernética norte-americana, a fim de promover uma organizada e unificada resposta a futuros acidentes cibernéticos (CNCI, 2009).

Cumpre registrar que a *Comprehensive National Cybersecurity Initiative* (CNCI) – lançada pelo ex-presidente George W. Bush na *National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23)*, de janeiro de 2008 – e suas atividades associadas deveriam, segundo determinações do governo Obama, evoluir de forma a se tornarem elementos chave de uma mais abrangente e atualizada estratégia nacional de segurança cibernética norte-americana. Neste sentido, visando dar mais segurança aos EUA no ciberespaço, seus maiores objetivos concentravam-se em: a) estabelecer uma linha frontal de defesa contra

ameaças imediatas; b) defender o país contra o total espectro de ameaças via desenvolvimento das capacidades de contrainteligência norte-americanas e aumento da segurança da cadeia de suprimentos para informações tecnológicas essenciais; e c) fortalecer o futuro ambiente de segurança cibernética via expansão da educação cibernética, coordenação de pesquisas e desenvolvimento de esforços com o governo o governo federal, e trabalho visando definir e desenvolver estratégias para deter atividades hostis ou maliciosas no ciberespaço (CNCI, 2009).

Em adição, ressaltava o governo Obama:

In building the plans for the CNCI, it was quickly realized that these goals could not be achieved without also strengthening certain key strategic foundational capabilities within the Government. Therefore, the CNCI includes funding within the federal law enforcement, intelligence, and defense communities to enhance such key functions as criminal investigation; intelligence collection, processing, and analysis; and information assurance critical to enabling national cybersecurty efforts (CNCI, 2009, p. 2).

Pela observância às medidas implementadas pelo governo Obama não se percebe um caráter militar acentuado nem um discurso explícito de confrontação no que tange ao ciberespaço, ainda que fortalecer as defesas cibernéticas norte-americanas seja um objetivo bastante presente. A se ressaltar que pela *Presidential Policy Directive 20 (PPD 20)*¹, implementada em outubro de 2012, qualquer significativa ação ciberofensiva que viesse a ser tomada deveria contar com a prévia aprovação do Presidente Obama (Clarke e Knake, 2019).

Ao se observar o tratamento do tema segurança cibernética pelo governo Trump pode-se notar um tom mais assertivo e um caráter mais militarizado, o que talvez seja devido ao aumento das amea-

¹ Esta garante a implementação de um arcabouço específico para segurança cibernética norte-americana via estabelecimento de princípios e processos para a área.

ças cibernéticas no período e às novas estratégias de política externa adotadas pelo governo. Neste aspecto, pelo *National Security Presidential Memorandum (NSPM) 13* o processo decisório quanto a operações cibernéticas passou a ser da alçada exclusiva do Pentágono, derrubando o PPD 20. Assim, atuando em conjunto, o NSPM 13 e a *White House's National Cyber Strategy* formaram a base de atuação do Pentágono face ao ciberespaço, tornando claras as intenções do governo Trump, expressas na visão de que o dominar o ciberespaço era o buscado, ou seja, o Departamento de Defesa deveria garantir que as forças militares norteamericanas estivessem prontas para lutar e vencer qualquer adversário, dominando, assim, o ciberespaço (Clarke e Knake, 2019).

De acordo com o expresso na *2018 Department of Defense Cyber Strategy*:

The Department must take action in cyberspace during day-to-day competition to preserve U.S. military advantages and to defend U.S. interests. Our focus will be on the States that can pose strategic threats to U.S. prosperity and security, particularly China and Russia (...) We will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict (Clarke e Knake, 2019, p. 172/173).

Presente nesta concepção estava o pensamento de que, mesmo na ausência de uma guerra declarada, já estava em curso uma constante competição no ciberespaço com outros Estados (China e Rússia, dentre outros) e, desta forma, a lógica de atuação adotada pelo Pentágono possibilitaria a criação de estabilidade no ciberespaço. Por outro lado, não parece crível que uma lógica de competição, aumentando a possibilidade de conflitos, possa vir a gerar estabilidade no ciberespaço (Clarke e Knake, 2019). O que de fato se observou no governo Trump foi o aumento da instabilidade no ciberespaço e a tese de se eleger um inimigo comum de forma a justificar a lógica

de confrontação adotada no ciberespaço. E, na grande maioria das vezes, esse inimigo escolhido pelo governo Trump foi a China.

3. A questão cibernética na agenda chinesa

Segundo com estimativas do Statista, o número de usuários de internet na China no final de 2020 era de cerca de 989 milhões de pessoas, o que faz com que o país não somente busque adotar medidas visando se proteger de ameaças cibernéticas, como também engendre esforços no sentido de aproveitar oportunidades que a exploração e o controle do ciberespaço possam vir a gerar. Destaca-se, em adição, a constante formação de pessoal especializado no campo do ciberespaço pelo governo chinês, como forma de potencializar o domínio do país neste campo, o que acaba gerando crescentes antagonismos com relação a outros países, sobretudo no que tange a matérias relacionadas à proteção de dados, vigilância e espionagem cibernética. Neste sentido, aponta Raud que:

As with most states, China is heavily dependent on technology, making the government highly concerned about developments regarding the internet and the information flow that it generates. The Chinese see uncontrolled information as a threat to the regime, paying great efforts to obtain the economic gains that the internet provides, but simultaneously maintain political control. It is believed that, for the Chinese, the whole concept of the internet is built around controlling information through real-time censorship, constituting a completely different view from that in the West. Indeed, ever since the internet became a publicly available communication platform in China, the question was not whether to control it, but rather how to control it. The most explicit example of such regulatory measures is of course the Great Firewall of China, which by monitoring all traffic in Chinese cyberspace enables the authorities to deny access to a variety of selected websites and disconnect all Chinese networks from the global internet network (2016, p. 6).

Importantes especificidades marcam a pauta cibernética na China, a começar pela diferenciação de conceitos comparativamente

te aos demais países ocidentais. Em primeiro lugar, tudo relacionado a desenvolvimentos cibernéticos é percebido como um ampla transformação de uma sociedade industrial para uma sociedade informacional, referindo-se a esse processo como um processo de informatização. Em segundo lugar, para os chineses o ciberespaço é apenas parte de um espaço informacional, o qual inclui o processamento humano de informação e o espaço cognitivo. Tais especificações implicam em uma abordagem diferenciada do ciberespaço pelo país, a qual se baseia em dois pontos cruciais: o uso do ciberespaço dentro do espaço territorial deve ser controlado pelo Estado, tendo em vista que na cultura política chinesa a manutenção da ordem social é inquestionavelmente mais importante do que a privacidade individual; o direito de soberania no ciberespaço é essencial, não se admitindo quaisquer interferências externas, seja de outros Estados ou de organizações internacionais, descartando, assim, a validade do Direito Internacional no ciberespaço² (Raud, 2016).

Em adição, vale a pena ressaltar que

It is also important to distinguish between cyber security and information security. The West, including the NATO allies, sees cyber security as the security of computer and information systems as physical and logical entities, and information assurance or information security as referring to security of the content. The Chinese, however, view both the information systems and the content of information as integral and connected parts of information security. This holistic understanding thus extends the use of the term from purely ICT-related issues to mental aspects and explains why the Chinese government's approach to information security has been control-seeking and restrictive (Raud, 2016, p. 10).

2 No Encontro Nacional de Segurança Cibernética e Tecnologia da Informação, ocorrido em abril de 2016, Xi Jinping reafirmou a importância da soberania chinesa no ciberespaço, implicando na rejeição da aplicabilidade do Direito Internacional e de leis preexistentes no ciberespaço.

A concepção chinesa de que o ciberespaço vem se transformando em um novo e essencial domínio de conflitos militares no mundo é recente, datando de 2013, ano em que a Academia de Ciências Militares chinesa desenvolve uma nova versão do estudo A Ciência da Estratégia Militar. Esta nova concepção acerca do ciberespaço está diretamente relacionada à chegada ao poder de Xi Jinping, escolhido no XVIII Congresso do Partido Comunista Chinês, realizado em 8 de novembro de 2012, para ser o novo presidente chinês, cargo que assume em 14 de março de 2013. A partir de então, o ciberespaço passa ser definido como o novo pilar do desenvolvimento econômico e social, bem como um novo domínio de segurança nacional chinesa (Jinghua and Levite, 2019).

Igualmente, cresce a percepção chinesa acerca do surgimento de sérias ameaças à infraestrutura cibernética do país e da existência de uma competição internacional estratégica no ciberespaço, em um cenário no qual outros países vêm buscando desenvolver suas respectivas forças militares cibernéticas. Desta forma, observa-se que a China vem desenvolvendo suas capacidades cibernéticas em resposta às crescentes ameaças de outros países (Jinghua and Levite, 2019).

Isto posto, cumpre registrar que com a criação da *Central Cyberspace Affairs Commission* (anteriormente *Central Internet Security and Information Leading Group*), em 2014, sob a liderança e responsabilidade de Xi Jinping, começou a ser definida a estratégia cibernética chinesa, fato este que demonstram que a China entende as questões cibernéticas como fortemente integradas à sociedade. Destaca-se também a existência de objetivos econômicos e políticos presentes na estratégia cibernética chinesa relacionados ao uso da espionagem em outros países e/ou empresas, bem como no que tange à vigilância feita a cidadãos chineses suspeitos de atentar contra a estabilidade política do sistema comunista, sem contar o fato de que a busca por superioridade no ciberespaço reside na crença de que de-

sabilitar o mais importante sistema operacional do inimigo nas fases iniciais de um conflito resultaria em uma rápida vitória (Raud, 2016).

Fato importante a ser destacado diz respeito à ênfase na natureza defensiva do conflito adotada pela China, sobretudo no que tange ao ciberespaço, o que se encontra explicitado no Livro Branco de Defesa Chinês de 2013 (*The 2013 Defence White Paper*) que proclama o direito da China de proteger seus interesses pertinentes à segurança nacional e ratifica a estratégia chinesa de não engendrar ataques a menos que seja atacada primeiro. As implicações desta estratégia no que tange à relação com os EUA será descrita mais adiante.

Pode-se constatar que apesar de alguns esforços chineses no sentido de se construir uma agenda de cooperação internacional no que tange ao ciberespaço, uma das características bastante presentes no pensamento chinês com relação à governança no setor é a declarada antipatia com relação aos EUA. De acordo com Raud:

China is concerned about the US using its status and influence as the world's leading technology power to establish international rules and norms favourable to the US. Thus, China often justifies its actions in cyberspace as a response to hostile developments by the US military (2019, p. 7).

Sem embargo, a complexidade presente nas relações entre China e EUA engendra inúmeras preocupações no cenário internacional, gerando sérias implicações para o sistema internacional, sobretudo na medida em que estas podem vir a ser motivadoras de potenciais conflitos Quinto Domínio. Sendo assim, faz-se essencial termos considerações sobre tais relações neste âmbito.

4. As relações China – EUA no quinto domínio

Um panorama inicial de como se apresentam as relações entre China e EUA no âmbito do ciberespaço é ilustrado por Levite et al (2021). Desta forma, segundo os autores:

The two countries have wrangled over a number of cyber and cyber-related issues, including internet governance, freedom of speech, online theft of commercial secrets, massive cyber surveillance, and cyber-attacks. The stability of their cyber relations has been further disrupted by mutual accusations, such as Washington's blaming of China for cyber espionage for commercial purposes and national security objectives, and Beijing rebuking U.S. cyber operations against China and Chinese companies, as revealed by Edward Snowden. These have poisoned the two countries' attitudes toward each other in the security and commercial realms, leading to diplomatic, political, and economic confrontations and conflicts. These tensions have been further inflamed by widespread suspicions and allegations that both countries have manipulated supply chains or cryptographic equipment to introduce back doors into products and services (Levite et al., 2021, p. 14).

Dotadas de grande complexidade e permeadas por narrativas tendenciosas de ambos os lados, as relações China-EUA no que diz respeito à questão cibernética ora apresentam momentos de calma e acordância, ora momentos de exacerbação de discursos e de potenciais conflitos, dado que China e EUA por vezes demonstram visões bastante discordantes no ciberespaço, as quais engendram posicionamentos por vezes antagônicos.

Se, por um lado, afirma-se que a liderança norteamericana é necessária para que se garanta o futuro da liberdade de pensamento e individualidade no ciberespaço e que a China representa a maior ameaça cibernética do planeta, devido a uma primazia em espionagem cibernética e ao desenvolvimento contínuo de mecanismos de ataque no ciberespaço contra os quais os EUA não possuem defesa (Duke, 2020), por outro, alega-se que a China apenas apresenta um

comportamento reativo face ao recrudescimento das ameaças norte-americanas no ciberespaço. Segundo Duke:

The United States government did not prioritize cyber advancements until faced with the threat of other states, China, in particular, developing attack mechanisms in cyberspace that the United States had no defense against. This has set the U.S. behind in the cyber arms race, allowing the PRC to take the lead in cyber developments, perpetually. Unless the U.S. catches up with the PRC's cyber developments and surpasses them, Americans and American organizations will continue to be targeted, manipulated, and exploited by PRC cyber espionage efforts, unable to defend themselves, unable to distinguish between what is real or fake online, and unable to establish effective cybersecurity (2020, p. 3).

Narrativas que caracterizam um ator como a personificação do mal e o outro como a do bem, decerto se mostram eivadas de preconceitos e camuflam a verdadeira realidade dos fatos. Assim, não se deve assumir que as relações China – EUA no ciberespaço são pautadas pela luta do bem contra o mal. Isso levaria a um total empobrecimento da análise. Tampouco se pode pensar que o conflito irá sempre imperar, sem que haja concertação em certos aspectos, ainda que ambos os países possuam visões por vezes conflitantes. Na verdade, visando manter-se a estabilidade global a tendência é de que ambos os países busquem o diálogo em suas relações pois possuem pleno conhecimento dos riscos que um conflito entre estes atinja o mundo como um todo. Ademais, tendo em vista a atipicidade da área cibernética, na qual é bastante difícil de se detectar as intenções de um invasor nas redes estratégicas de computadores de um determinado país – as quais podem ser defensivas, procurando se prevenir antecipadamente de um futuro ataque rival, ou ofensivas, por meio de ataques iniciais disruptivos ou visando destruir os sistemas preventivos do rival – os riscos da explosão de um conflito por conta de um mero incidente de menores proporções é elevado, sobretudo nas relações entre China e EUA.

Excetuando-se fatos pontuais, as relações China-EUA vinham sendo pautadas, até pouco tempo, pelo diálogo e pela cooperação, haja vista que em 2013, por ocasião do encontro presidencial entre Obama e Xi Jinping, ocorrido em Sunnylands (CA), ambos acordaram colaborar em questões cibernéticas por meio de um grupo de trabalho bilateral. Outro encontro entre ambos, ocorrido em 2015, em Washington, teve como resultado o compromisso mútuo de não se conduzir ou apoiar roubos cibernéticos de propriedade intelectual, bem como o estabelecimento de uma diálogo de alto nível no combate de crimes cibernéticos. Já em 2017, China e EUA desenvolveram um mecanismo de aplicação de leis e instituíram diálogo em segurança cibernética (Levite et al, 2021).

Contudo, identifica-se que nos últimos anos o quinto domínio vem se tornando cada vez mais um espaço crítico no cenário das relações internacionais devido ao fato de ser global, não facilmente delimitado no âmbito doméstico e/ou internacional e permear praticamente todas as atividades humanas, que vem tornando de forma exponencialmente mais dependentes deste domínio. Dentro desta perspectiva, o quinto domínio vem se tornando um crescente fator de estabilidade ou de desordem no cenário internacional, elevando-se, assim, a existência de tensões neste campo (Jinghua and Levite, 2019).

Neste sentido, a conjuntura que emerge a partir do governo Trump vem se caracterizando, segundo Levite et al, pelo fato de que:

Each side's growing cyber capabilities now assume special importance in its overall homeland security, intelligence, and military posture. The capabilities are symbols of state power and have practical operational significance. Cyberspace is now a leading domain for intelligence collection, covert operations, military encounters, and even outright warfare. Cyber operations are central not only in a conflict but also during the buildup to conflict and in peacetime. Cyberspace is increasingly a medium for influencing cognition and behavior as well as affecting physical capabilities (...) The lure of cyberspace

seems almost irresistible. Cyber tools are less expensive to acquire and operate than conventional weapons. They offer huge potential geographic coverage, economies of scale, and force-projection capabilities. They are also largely of a dual-use nature, emerging naturally from commercial applications at little or no additional cost. Cyber operations are typically highly secretive. This avoids the scrutiny associated with other types of operations and presents options for plausible deniability. Cyber operations are subject to fewer formal legal constraints and moral inhibitions. Despite the risks of spurring escalation in other domains, cyber operations are still appealing because they are often opaque and do not necessarily cause obvious physical damage. These features could mitigate fears that adversaries will respond by escalating across domains (Levite et al. 2021, p. 27).

Durante o governo Trump, os EUA procuraram evidenciar suas capacidades cibernéticas, explicando seus propósitos e publicamente discutindo algumas de suas doutrinas de emprego, por acreditarem que inúmeros outros países que estavam desenvolvendo capacidades cibernéticas militares ofensivas, sobretudo a China, deveria conhecer e, sobretudo, temer o poderio cibernético norteamericano. Por outro lado, a China vem publicamente defendendo o uso pacífico do ciberespaço e se recusa de maneira firme a discutir capacidades cibernéticas ofensivas e doutrinas que perpassem tais concepções, defendendo que a chave para estabilidade no ciberespaço reside na renúncia do uso de ferramentas cibernéticas para cometer agressões e interferir nos assuntos internos de outros países (Levite et al, 2021).

O discurso mais agressivo explicitado pelo governo Trump no que tange à apropriação do ciberespaço³ reforça a percepção

3 A estratégia cibernética do Departamento de Defesa dos EUA enfatiza a defesa prévia (*defending forward*) para quebrar ou cessar atividades cibernéticas maliciosas em suas próprias fontes. Além dessas mudanças doutrinárias, a diretiva presidencial de 2018 facilitou a aprovação de operações cibernéticas ofensivas que tragam em seu bojo o uso moderado de força, sendo as operações cibernéticas empreendidas os sistema de mísseis da Coreia do Norte um exemplo pertinente das diretrizes da estratégia cibernética norteamericana, que refletem a atração pela prevenção/preempção no ciberespaço.

chinesa quanto a uma maior agressividade por parte dos EUA no ciberespaço, a qual pode vir a aumentar a probabilidade de ocorrência de crises cibernéticas, forçando ambos os países a se prepararem para o pior cenário, ou seja, fazendo com que ambos os países venham a expandir, intensificar e acelerar operações cibernéticas assertivas visando garantir uma maior sensação de segurança no ciberespaço. Neste sentido, o Livro Branco de Defesa Chinês assevera que as forças armadas chinesas devem acelerar a construção de suas capacidades cibernéticas, desenvolvendo meios de defesa e segurança cibernética e construindo capacidades cibernéticas de defesa, as quais, juntamente com as unidades cibernéticas militares, são defensivas por natureza e destinadas somente a defender e reagir como suporte estratégico, evitando-se a corrida de armas no ciberespaço e a consequentemente militarização e confrontação no quinto domínio do poder (Levite et al, 2021).

Por outro lado, a indicação de uma capacidade cibernética defensiva por natureza de parte da China gera uma interpretação diversa e pode vir a ser um indicativo de uma ameaça no ciberespaço, como nos mostra Raud (2016). Segundo Raud:

Whereas several Western countries have communicated a similar position, the Chinese attitude relies on Mao Zedong's 'active defense' as already emphasized in Document 27 in 2003, assuming to attack only after being attacked. Yet, Mao's 'active defense' can also be interpreted as the alternative use of defensive and offensive. This, together with different strategic cultures, creates a situation where an act considered defensive by the Chinese might seem offensive to the West. As an interesting parallel, 'active cyber defense' is widely discussed in the West, referring to the ability to detect and mitigate key threats before suffering from any damage, including the capacity to launch aggressive and offensive countermeasures. Thus, Western actions taken under the concept of 'active cyber defense' might similarly seem offensive to the Chinese. (By) connecting the Chinese and the Western understandings of active defense, it seems that each has understood that in cyberspace, mere defensive capabilities are not enough to deter adversaries from attacking one's networks. As the Chinese have recently admitted the existence of purely offensive

cyber units in the PLA, it is increasingly clear that conflict in cyberspace has achieved fundamental importance in the Chinese understandings of policy making, both in peacetime, and in any future war (2016, p. 20).

O pensamento predominante no governo Trump era o de que inúmeros outros países já possuíam ou estavam envidando esforços visando desenvolver capacidades militares cibernéticas ofensivas, sendo a China líder deste grupo. Por outro lado, o governo Xi Jinping se mostra comprometido com o uso pacífico do ciberespaço e se nega a discutir questões pertinentes à adoção de capacidades cibernéticas ofensivas, advogando que a chave para estabilidade no quinto domínio reside na renúncia por parte dos países do uso ferramentas cibernéticas para cometer agressões e interferir nos assuntos internos de outros países (Levite et al, 2021).

A propaganda chinesa embasada na concepção de que o desenvolvimento da segurança cibernética e da informatização irão contribuir decisivamente para uma guinada chinesa rumo ao desenvolvimento de uma economia modernizada e que possa atingir um alto grau de qualidade, gerando um novo modelo de industrialização, urbanização e modernização agrícola vem sendo exaustivamente difundida, e se encontra embasada na visão de ciberespaço do governo chinês, que toma como prioritário promover o desenvolvimento da economia digital e de uma profunda integração entre internet, big data, inteligência artificial e economia real, bem como tornando a manufatura, a agricultura e o setor de serviços mais digitalizado e inteligente (Jinghua and Levite, 2019).

Até que ponto esta propaganda chinesa se faz verídica apenas estudos mais aprofundados e que fogem do escopo deste artigo podem investigar. O que se faz presente no momento, de forma bastante recente, é mais uma acusação por parte do Departamento de Estado dos EUA de que a China vem adotando um comportamento irrespon-

sável e desestabilizador no quinto domínio. De acordo com Antony J. Blinken, Secretário de Estado do Governo Joe Biden:

The United States and countries around the world are holding the People’s Republic of China (PRC) accountable for its pattern of irresponsible, disruptive, and destabilizing behavior in cyberspace, which poses a major threat to our economic and national security. The PRC’s Ministry of State Security (MSS) has fostered an ecosystem of criminal contract hackers who carry out both state-sponsored activities and cybercrime for their own financial gain. In addition, the United States government, alongside our allies and partners, has formally confirmed that cyber actors affiliated with the MSS exploited vulnerabilities in Microsoft Exchange Server in a massive cyber espionage operation that indiscriminately compromised thousands of computers and networks, mostly belonging to private sector victims. As evidenced by the indictment of three MSS officers and one of their contract hackers unsealed by the Department of Justice today, the United States will impose consequences on PRC malicious cyber actors for their irresponsible behavior in cyberspace (...) Responsible states do not indiscriminately compromise global network security nor knowingly harbor cyber criminals – let alone sponsor or collaborate with them. These contract hackers cost governments and businesses billions of dollars in stolen intellectual property, ransom payments, and cybersecurity mitigation efforts, all while the MSS had them on its payroll (US Department of State, 2021).

Em suma, o quinto domínio apresenta inúmeros desafios distintos para as relações China-EUA, os quais derivam das diferenças de perspectiva entre China e EUA, haja vista que enquanto a China se mostra preocupada com o aumento da agressividade norte-americana na política e doutrina cibernética, os EUA enfatizam a presença de inúmeras discordâncias sobre o ciberespaço, dentre estas como se aplicar leis internacionais no ambiente e o que constitui um ataque armado no quinto domínio. Em adição, pairam sobre os EUA a desconfiança quanto à sinceridade das intenções chinesas dado que a China formalmente se aliou à Rússia no terreno da diplomacia cibernética, e esta última se caracteriza por uma duplicidade de atuação no ciberespaço, haja vista que defende o banimento do conflito armado no ciberespaço ao mesmo tempo em que apresenta conduta

agressiva no que tange a atividades cibernéticas, tais como espionagem, operações de informação contra vários estados (Levite et al, 2021).

5. Considerações finais

Pode-se inferir que está em curso o recrudescimento das rivalidades entre China e EUA no quinto domínio, o que pode ser observado mediante a análise das estratégias adotadas sobretudo pelo governo do ex-presidente Donald Trump com relação à atuação norteamericana no ciberespaço e inclusive com o tom que o atual governo Biden parece dar ao tema. O crescimento dessas rivalidades inclusive motivou a cunhagem do termo *China-US Tech War*, que se aplica às rivalidades entre ambos os países no quinto domínio e compreende os mais diversos aspectos, não somente de cunho militar e estatal, mas também no âmbito privado e econômico, no qual os imbrólios envolvendo a empresa chinesa Huawei, bem como as descobertas vazadas por Edward Snowden sobre casos de espionagem cibernéticas feitas levadas a cabo pelo governo dos EUA em empresas chinesas são exemplos concretos.

Não obstante, observa-se, durante o governo de Donald Trump, a adoção de uma estratégia cibernética que se utiliza, em determinadas situações, de ataques cibernéticos disruptivos e pre-emptivos, que são cancelados pelo *National Security Presidential Memorandum (NSPM) 13* – que transfere para a alçada exclusiva do Pentágono o processo decisório quanto a operações cibernéticas – e pela *White House's National Cyber Strategy*, formando, ambas, a base de atuação do Pentágono face ao quinto domínio. Entretanto, inexistente até o momento um confronto aberto e declarado entre ambos os países, ainda que visões e concepções divergentes se façam bastante presentes no que tange ao quinto domínio, que não apenas se

restringe a China e EUA, mas também abarca os demais países do mundo.

Ataques militares cibernéticos disruptivos vêm sendo usados por vários países, mesmo em um contexto de aparente paz mundial, o que aumenta a ocorrência de crises internacionais. Vislumbra-se uma corrida em curso por visando aumentar capacidades cibernéticas militares, as quais, juntamente com a atuação constante de atores não-estatais contribuem para o aumento da insegurança. Em analogia ao período da Guerra Fria há uma escalada pelo poder como instrumento de paz. Entretanto, considero que a melhor política seja, nesse caso, o desenvolvimento de uma resiliência cibernética, conceito que pode muito bem ser aplicado no trato das ameaças cibernéticas.

Faz-se mister desacelerar a escalada de tensões no ciberespaço, do contrário o risco de conflitos eminentes tende a crescer de forma exponencial. Caso China e EUA não empreendam, de forma conjunta, passos no sentido de reduzir os riscos de uma guerra cibernética, não se engajem em um programa multidimensional visando o desenvolvimento de um processo de paz cibernética, o risco de ataques cibernéticos cada vez mais destrutivos pode levar a sociedade ao caos. Cabe, assim, advogar em prol de uma resiliência cibernética como forma de conter o avanço dos conflitos no ciberespaço e de se conjugar esforços para se aumentar a segurança no ciberespaço sem que se seja mediante uma corrida cibernética armamentista.

Neste sentido, por entender que ameaças cibernéticas são de natureza *cross-border*, a União Europeia (EU), por intermédio da *European Union Agency for Cybersecurity* (ENISA), defende a necessidade de se engendrar esforços conjuntos entre os países no intuito de se evitar a escalada de ameaças à segurança cibernética e garantir a estabilidade mundial no ciberespaço mediante a cooperação. No que concerne ao Brasil, destaca-se o acordo de cooperação em termos de defesa cibernética firmado com a Índia em janeiro de 2020,

bem como a publicação, em fevereiro de 2020, da primeira Estratégia Nacional de Segurança Cibernética (E-Ciber), a qual possui dentre seus objetivos estratégicos aumentar a resiliência cibernética do país e fortalecer o engajamento brasileiro em segurança cibernética em nível internacional. Observa-se, assim, que tanto Brasil quanto UE comungam da mesma visão acerca necessidade de uma cooperação pacífica no ciberespaço de forma a se evitar a escalada de conflitos neste domínio.

Referências

CLARKE, R. A.; KNAKE, R. K. *The Fifth Domain: Defending our Country, Our Companies, and Ourselves in the Age of Cyber Threats*. New York. Penguin Press, 2019.

DUKE, E. J. *Cyber World War: The People's Republic Of China, Anti-American Espionage, And The Global Cyber Arms Race*. *Global Security Review. Defense & Security*, 7 de Outubro de 2020. Disponível em [Cyber World War: The People's Republic of China, Anti-American Espionage, and the Global Cyber Arms Race | Global Security Review](#) . Consultado em 15/08/21.

JINGHUA, L.; LEVITE, A. *Chinese-American Relations in Cyberspace: Toward Collaboration or Confrontation?* Carnegie Endowment for International Peace. January 24, 2019. Disponível em [Chinese-American Relations in Cyberspace: Toward Collaboration or Confrontation? - Carnegie Endowment for International Peace](#). Consultado em 18/08/21.

LEVITE, A. E.; JINGHUA, L.; PERKOVICH, G.; CHUANYING, L.; MANSHU, X.; BIN, L.; FAN, Y. *China-US Cyber-Nuclear C3 Stability*. Carnegie Endowment for International Peace / Shanghai Institute for International Studies. April 2021. Disponível em [CarnegieEndowment.org](#).

LIEBERTHAL, K.; SINGER, P. W. *Cybersecurity and US-China Relations*. 21st Century Defense Initiative/ John L. Thornton China Center. Brookings. February 2012.

RAUD, M. China and Cyber: attitudes, strategies, organisation. NATO Cooperative Cyber Defence Centre of Excellence. Tallinn, 2016.

STATISTA. China: number of internet users 2020 | Statista. Disponível em <https://www.statista.com/statistics/265140/number-of-internet-users-in-china/>. Consultado em 19/08/21.

THE UNITED STATES OF AMERICA. The Comprehensive National Cybersecurity Initiative. Disponível em The Comprehensive National Cybersecurity Initiative (fas.org) . Consultado em 13/08/21.

US DEPARTMENT OF STATE. Responding to the PRC's Destabilizing and Irresponsible Behavior in Cyberspace. Press Statement. July 19, 2021. Disponível em <https://www.state.gov/responding-to-the-prcs-destabilizing-and-irresponsible-behavior-in-cyberspace/>. Consultado em 20/08/21.

Sobre o autor

Mario Augusto dos Santos

Doutorando em Relações Internacionais pelo IRI/PUC-RIO. E-mail: mariojoplin@yahoo.com. ORCID: <http://orcid.org./0000-0001-9523-1917>.