Pandemônio Cibernético: o Uso do Ciberespaço para Consecução de Objetivos Estratégicos da China no Conflito Sino-Indiano (2020-2021)

Fernando Henrique Casalunga
Ph.D candidato do programa de Pós Graduação em Ciência Política da UFRGS.

Marcos Aurélio Guedes de Oliveira
Professor Titular do Departamento de Ciência Política da Universidade Federal de Pernambuco.

Eduardo Munhoz Svartman
Professor Titular do Departamento de Ciência Política da Universidade Federal do Rio Grande do Sul.

Resumo

O artigo analisa as vantagens estratégicas que o ciberespaço oferece aos Estados para projeção de poder no cenário internacional. Com intuito de demonstrar como este novo domínio é capaz de ampliar a assimetria de poder entre adversários regionais, verifica seu emprego durante o conflito desencadeado entre a República Popular da China e a Índia (2020-21). Intentamos correlacionar a mudança institucional pela qual passaram as instituições responsáveis pela defesa da China à complexidade das operações e sofisticação tática do uso de armas cibernéticas por agentes a serviço deste Estado. Buscamos identificar se as condições que sustentam a projeção do poder nacional resultam do funcionamento do mecanismo de ação tática coordenada interagencias, fator que reflete o processo de emprego do ciberespaço em disputas regionais. Para tanto, utilizamos a abordagem qualitativa, aplicando o rastreamento de processos, para responder ao seguinte questionamento: Como a China utiliza o ciberespaço para conquistar seus objetivos estratégicos?

Palavras-chave: Poder Nacional; Segurança Cibernética; Ameaças.

Abstract

Cyber Pandemonium: the Use of Cyberspace to Achieve China's Strategic Goals in the Sino-Indian Conflict (2020-2021)

The article analyzes the strategic benefits that contemporary nations' use of cyberspace offers them in terms of projecting their national power. It examines its use during the conflict trigged between the People's Republic of China and India (2020-21) to show how this new domain might heighten the power imbalance between regional rivals. We aim to correlate the institutional transformation that China's military institutions underwent to the operational complexity and tactical sophistication of the employment of cyber weapons by this State agents. Our goal is to identify whether the conditions that support the projection of national power result from the functioning of the interagency coordinated tactical action mechanism, a factor that reflects the process of employing cyberspace in regional disputes. In this vein, we employ a qualitative approach using the process tracing to address the following question: How China utilizes the internet to accomplish its strategic goals.

Keywords: *National Power; Cyber Security; Threats.*

Artigo recebido: 25.07.2022
Aprovado: 24.11.2022
https://doi.org/10.47906/ND2022.163.02

Introdução

O desenvolvimento científico técnico e tecnológico experimentado durante o período da Guerra Fria (1945-1991) resultou em diversos legados, dentre eles, destaca-se o primeiro domínio artificial inteiramente criado pela ação humana denominado ciberespaço[1], ambiente virtual composto por máquinas e usuários conectados em uma rede mundial militar e civil que lançou a humanidade na Era da Informação.

A inclusão das dimensões cognitiva, física e digital ao conceito indica a relevância das percepções humanas na construção e operação das estruturas e infraestruturas que compõem este novo domínio, de maneira que as fronteiras geográficas que orientam noções como soberania, nacionalidade e propriedade se revelam, igualmente, dispostas no ciberespaço. No entanto, diferentemente do mundo puramente físico, tais divisões estão em constante mutação, em larga medida, devido ao desenvolvimento de novas tecnologias da informação (Singer e Friedman, 2014).

O avanço no processo de digitalização de sistemas de armas e de sistemas de comando e controle tornou o espaço cibernético tema prioritário nos processos de modernização militar e de formulação de políticas de defesa nacional desde o final do século passado. Pensado inicialmente como o espaço artificial de integração dos domínios tradicionais da guerra (terrestre, naval, aéreo e, mais recentemente, espacial), o espaço cibernético configurou-se também num domínio, articulável com outras esferas de atividade humana.

Ao passo que o espaço cibernético se transformou para além de suas características iniciais de uso, qual sejam a comunicação e o comércio, novos sistemas de controle construídos para aprimorar o funcionamento das infraestruturas críticas foram sendo conectados via ciberespaço, ampliando, sobremaneira, a importância deste novo domínio para a organização das sociedades contemporâneas (Singer e Friedman, 2014).

Devido à própria natureza difusa e virtual do ciberespaço, grandes desafios foram impostos aos Estados no tocante à segurança cibernética, uma vez que o fracasso na proteção do fluxo das informações representa riscos em potencial para diferentes segmentos sociais, podendo comprometer o funcionamento de sistemas financeiros, industriais e de serviços (Weiss e Jankauskas, 2019).

1 De forma mais detalhada, entendemos ciberespaço como o "domínio das redes de computadores (e dos usuários por trás delas) em que as informações são armazenadas, compartilhadas e comunicadas on-line [...]. O ciberespaço é antes de tudo um ambiente de informação. Ele é composto de dados digitalizados que são criados, armazenados e, o mais importante, compartilhados. [...] Mas o ciberespaço não é puramente virtual. Ele compreende os computadores que armazenam dados, além dos sistemas e infraestruturas que permitem que ele flua. Isso inclui a Internet de computadores em rede, intranets fechadas, tecnologias de celulares, cabos de fibra ótica e comunicações espaciais" (Singer and Friedman, 2014, 13-14).

A dificuldade em atender a essa demanda fez com que os governos passassem a desenvolver capacidades próprias, bem como contassem com as de terceiros em prol de manter a segurança cibernética (Betz e Stevens, 2011); isto é: a "capacidade do Estado em proteger a si mesmo e as suas instituições contra ameaças, espionagem, sabotagem, crime e fraude, roubo de identidade, e outras interações e transações eletrônicas destrutivas" (Choucri, 2012, p. 39).

Verifica-se, assim, que o advento do ciberespaço inaugurou um paradoxo a partir da criação de mais oportunidades de comércio e novas formas de organização da sociedade civil, frente à abertura de um espaço que requer ações estratégicas originais para a defesa com vistas a prevenir os riscos e conter as ameaças (Betz e Stevens, 2011).

Os riscos estariam, então, associados à vulnerabilidade das infraestruturas críticas, instalações físicas, redes, serviços e bens responsáveis por proverem recursos essenciais à vida humana, sistemas altamente integrados e interconectados via ciberespaço que podem ter seu funcionamento comprometido por ameaças virtuais, dentre as quais, se destacam grupos altamente organizados que podem operar fora dos limites estatais e/ou em serviço de um Estado, com objetivos políticos específicos classificados como Ameaças Persistentes Avançadas (APA) (Betz e Stevens, 2011; Lindsay e Cheung, 2015; Olszewski, 2018).

Assim, nas últimas décadas, frente ao problema da segurança cibernética, na medida em que reduzir os riscos e mitigar o potencial destrutivo das ameaças emergiu como uma das tarefas chave dos formuladores políticos, os Estados contemporâneos deram início a processos de mudança institucional com o objetivo não apenas de fortalecer as entidades responsáveis pela defesa e a segurança dos sistemas de informação, mas de utilizar o ciberespaço como um novo engenho de força para auferir vantagens estratégicas em disputas interestatais. Este artigo analisa como se deu tal processo na República Popular da China.

A fim de compreender a estratégia chinesa de uso do ciberespaço para projeção de poder nacional, aplicamos a técnica qualitativa de rastreamento de processos com intuito de responder ao seguinte questionamento: Como a China utiliza o ciberespaço para consecução de objetivos estratégicos regionais?

Com base em fontes primárias e secundárias – documentos oficiais, acadêmicas, jornalísticas, e de relatórios produzidos por instituições governamentais e empresas especializadas em segurança cibernética –, realizamos uma investigação das condições necessária e suficiente inerentes ao processo de emprego das tecnologias da informação no conflito regional sino-indiano (2020-21).[2]

2 A técnica do rastreamento de processos ajuda a revelar como os processos observáveis que compõem o mecanismo causal investigado conectam o fenômeno observado (Y/*assimetria de poder*) à causa inicial (X/*mudança institucional*). As observações do processo causal são usadas

Partindo do pressuposto de que os Estados contam com meios técnicos e experiência para conduzir ações estratégicas via ciberespaço, bem como, encontram poucas restrições legais que os impeçam de agir neste domínio em função de seus interesses, a teoria realista tem permitido um enquadramento capaz de decodificar os fenômenos recentes que envolvem o uso deste novo engenho de força por parte das potências contemporâneas. No entanto, essas abordagens são marcadas por clivagens que nos levam a abordar o problema da segurança cibernética com base em pressupostos distintos.[3]

Com intuito de avançar o debate sobre a relevância do uso estratégico do ciberespaço em conflitos regionais, tema ainda pouco explorado pela literatura ocidental, aspiramos, mediante a identificação do funcionamento do mecanismo de simbiose entre as agências estatal e não-estatal para emprego do ciberespaço na produção de vantagens estratégica, contribuir para preencher as lacunas e desatar os nós analíticos presentes nos estudos de Política Internacional e Defesa que buscam compreender o fenômeno da guerra cibernética. A contribuição de nossa análise consiste em abordar em profundidade os procedimentos e as razões que se encontram por detrás das campanhas de reconhecimento, exploração e dos ataques para demonstrar como este domínio contribuiu para causar um pandemônio cibernético[4] que ampliou a assimetria de poder regional entre China e Índia (2020-2021).

Para tanto, o artigo conta com três seções nas quais coletamos evidências que demonstram a relevância estratégica do ciberespaço contida: i) no pensamento militar formulado pelos teóricos do Exército de Libertação Popular (ELP) para realizar a guerra cibernética; ii) na mudança pela qual passaram as instituições responsáveis pela defesa e segurança nacional; e, iii) na complexidade das operações e sofisticação tática das principais ameaças cibernéticas utilizadas por forças convencionais e não-convencionais a serviço da China.

em conjunto com uma generalização mais ampla relevante para os casos em análise (Collier, 2011; Mahoney, 2012).

3 Para um aprofundamento do debate entre adeptos e céticos realistas sobre as teses da revolução cibernética ver: Libicki, 2009; Betz and Stevens, 2009; Clarke, Knake, 2010; Cornish, Livingstone and Yorke, 2010; Farwell, Rohozinski, 2012, Liff, 2012; Gartzke, 2013; Kello, 2013, Lindsay, 2013; 2015; Pollperter, 2015 Hjortdal, 2011; Lindsay, 2015; Lindsay, Cheung and Reveron, 2015; Pollpeter, 2015; Stokes, 2015; Nurkolov, 2017.

4 Definição: conceito alinhado com a categorização dada pelas referências consultadas que remete às atuações das APA RedEcho (APA41), Stone Panda (APA10) e Gothic Panda (APA3) identificadas neste artigo.

1. Guerra Cibernética: o Pensamento Militar Estratégico do Exército de Libertação Popular (ELP)

Nesta seção destacamos nuances no pensamento militar estratégico do Exército de Libertação Popular (ELP) que ajudam a observar o contorno que assumem as instituições. Cientes de que a constituição deste pensamento representa um dos principais fatores que orientam as mudanças institucionais civis e militares da China, sendo, portanto, relevante para explicar o comportamento cibernético do país quando confrontado com evidências que indiquem "como as instituições produzem esses trajetos, como elas estruturam a resposta de uma dada nação a novos desafios" (Hall, Taylor, 2003, p. 200).

Ao conectarmos as implicações do processo de mudança institucional pelo qual passaram as regras formais que estruturam o ELP aos momentos críticos posteriores à eclosão do conflito regional sino-indiano (2020-2021), pretendemos avaliar como a estratégia chinesa se adaptou às mudanças nas diretrizes oficiais que organizam essas agências, padrões que "podem fossilizar-se ao longo do tempo e tornar-se visões de mundo, que são propagadas por organizações oficiais e terminam por moldar a imagem de si e as preferências dos interessados" (Hall, Taylor, 2003, p. 199).

Com base nos principais documentos que orientam as instituições civis e militares da China verifica-se que a combinação entre segurança e desenvolvimento nacional é considerada o principal objetivo estratégico do Estado. Em função disso, sua grande estratégia se organiza em torno dos seguintes princípios: projeção de poder nacional; pontos estratégicos focais; vencer sem guerrear; unidade dos objetivos e caminhos; estabilidade relativa (Thomas, 2014; Pollpeter, 2015; Stokes, 2015; Lindsay, Cheung e Reveron, 2015).

De acordo com os teóricos do pensamento estratégico militar do ELP da ativa e reserva, o êxito na projeção do poder nacional depende da capacidade das instituições para compreender e manipular a realidade objetiva (Bingyan, 2004; Desjardins, 2005; Jijun, 2006; Zheng e Bao, 2007; Xue Guo'an, 2010).

Tomando o crescimento do poder nacional como fio condutor, as instituições militares da China adotaram, desde a guerra sino-japonesa (1937-45), uma postura de 'defesa ativa' que, a depender da conjuntura, podia se modificar rapidamente e assumir caráter ofensivo (Zedong, 1936). Ponto chave para construir e exercer o poder militar com vistas à proteção da soberania e segurança nacional, este princípio se manteve no bojo dessas instituições como característica fundamental que orienta, ainda hoje, a ciência da estratégia militar no desenvolvimento de mecanismos que possibilitem alcançar êxito em conflitos sob condições de alta tecnologia (Desjardins, 2005).

No entanto, embora fundamental, os teóricos do ELP não consideram a aquisição de recursos materiais suficiente para sustentar a projeção do poder nacional, é

necessário que os líderes políticos e militares consigam controlar a iniciativa para alcançar vitórias sem guerrear, tal condição pressupõe que os agentes institucionais sejam capazes de aplicar estratagemas para sincronizar o processo de tomada de decisão do adversário com os interesses nacionais chineses, induzindo, assim, o alvo a tomar decisões de modo previsível (Zheng e Bao, 2007).

A estratégia militar da China se constitui, portanto, com o intuito de alcançar controle na aquisição e uso da informação sobre um adversário que permita obter vantagem sobre o mesmo. Para tanto, o uso dos estratagemas é considerado um dos componentes chave para causar impacto no desempenho dos alvos em um conflito (Qi, 2002) [5]. Nesse sentido, processo de uso da inteligência para aplicação desses estratagemas deve considerar o sistema de crenças e os mecanismos que organizam a tomada de decisão para inserir informação de interesse dos alvos e/ou pressionar os líderes políticos, aproveitando de sua posição na hierarquia organizacional das burocracias administrativas, com vistas a manipular as ações do adversário (Thomas, 2014).

Em síntese, os teóricos do ELP consideram o emprego de tecnologia da informação em ações estratégicas representa um recurso significativo para amplificar as chances de vitória da China em conflitos contemporâneos se, e somente se, combinados à aplicação de estratagemas condizentes com as capacidades objetivas disponíveis (Bingyan, 2004; Jijun, 2006; Xue Guo'an, 2010). Consequentemente, as instituições militares e políticas assumiram o pressuposto de que o resultado de um conflito depende das condições materiais militares, políticas, econômicas e naturais, somadas *à* percepção subjetiva dos tomadores de decisão, ou seja, as operações estratégicas se encontram circunscritas por limitações impostas pelas condições materiais e capacidades de ação dos atores (Thomas, 2014; Pollpeter, 2015; Stokes, 2015).

Por esta lógica, a espionagem cibernética emerge como opção valiosa para promover os interesses políticos, econômicos e diplomáticos da China. Razão pela qual, as campanhas de reconhecimento e exploração de redes de computadores são orquestradas não apenas com intenção de desenvolver o aparato científico e tecnológico, considerados estratégicos pelo Estado e forças armadas, mas, sobretudo, para testar a eficiência institucional em produzir vantagens estratégicas nos conflitos (Thomas, 2014).

Em termos operacionais, a premissa básica é que as instituições militares modernas devem ser capazes de realizar ataques precisos de longo alcance capazes de parali-

5 Oficiais do instituto de comunicação e comando da China definem os estratagemas aplicados à guerra de informação (cibernética) como 'esquemas e métodos utilizados pelos comandantes e corpos institucionais para garantir a supremacia da informação com base no uso de métodos inteligentes para vencer os conflitos a custos reduzidos' (Li, Jiangzou and Dehui, pp. 115-122).

sar o adversário e alcançar a vitória em curto espaço de tempo com custo humano e econômico menor do que o necessário em ataques cinéticos (Zhang 2006).

Neste contexto, o ciberespaço é compreendido pelos teóricos do ELP como um recurso de potencial decisivo para conflitos futuros. Consideram que a guerra cibernética pode ser utilizada para oferecer suporte aos interesses de projeção nacional do país ao passo em que permita: i) identificar vulnerabilidades em redes de computadores que possam ser exploradas para aquisição de informação; ii) comprometer o funcionamento de redes logísticas, de comunicação e comercial; iii) retardar o tempo de resposta de um adversário frente a uma ação ofensiva; iv) servir como multiplicador de força em operações cinéticas; v) ser útil em ações coercitivas (Pollpeter, 2015).

Ao considerarem a primazia da ofensiva no domínio cibernético como fator preponderante para adquirir vantagens assimétricas contra adversários poderosos (Qingmin, 2002), os teóricos do ELP compreendem as operações em redes de computadores como revolucionárias, pois, capazes de impactar não apenas os sistemas de informação, mas, conceitos operacionais tradicionais do pensamento e método da esfera militar, a política e a economia dos adversários (Pollpeter, 2015).

Ao enfatizarem a importância da integração das operações cinéticas e cibernéticas para atingir alvos civis e militares em tempos de guerra e/ou paz, os militares chineses assinalam que ataques cibernéticos contra sistemas C4ISR[6] e/ou outros centros de gravidade presentes em níveis estratégicos, de campanha, e táticos, com intenção de coletar informações de acesso que possam ser úteis para causar paralisia e/ou comprometer o processo de tomada de decisão e a economia nacional, têm potencial para causar a derrota de um poder militar superior frente a um adversário mais fraco (Pollpeter, 2015).

Frente a este cenário, parte da literatura ocidental[7] se dispôs a analisar os movimentos estratégicos da China via ciberespaço com foco nas possibilidades de uso deste domínio para reduzir a assimetria de poder entre o país e adversários militarmente mais poderosos como os Estados Unidos da América (Hjortdal, 2011; Lindsay, 2015; Lindsay, Cheung e Reveron, 2015; Pollpeter, 2015; Stokes, 2015; Nurkolov, 2017),

6 Definição de C4ISR (comando, controle, comunicação, computadores, inteligência, vigilância e reconhecimento): sistemas de informação que possuem tecnologia avançada e representam o centro nervoso dos sistemas militares (Qingmin, 2002).

7 A divisão entre literatura ocidental e não ocidental dá-se em virtude da necessidade de sublinhar os limites analíticos das referências mobilizadas para identificação do mecanismo de ação das instituições para uso do ciberespaço com vistas à consecução de objetivos estratégicos. Nossa opção por fontes acadêmicas, jornalísticas, e de relatórios produzidos por instituições governamentais e empresas especializadas em segurança cibernética de origem ocidental ocorre em função das restrições linguísticas que implicam o uso de fontes não-ocidentais.

desconsiderando seu provável emprego em conflitos regionais contra adversários mais fracos (Guedes de Oliveira e Casalunga, 2020).

Sem embargo, estes estudos verificam que o progresso da China na aplicação do pensamento estratégico militar em campanhas de reconhecimento e exploração para intrusão em sistemas de rede de instituições governamentais e empresas tem sido célere. Dentre as razões pelas quais o Estado chinês sustenta uma postura agressiva no ciberespaço, se destacam: a espionagem de tecnologia estrangeira militar e industrial; a dissuasão por comprometimento de sistemas operacionais de infraestrutura crítica (Hjordtal, 2011; Lindsay, 2015; Nurkolov, 2017).

Ademais, identificam que a construção do pensamento militar estratégico do ELP com base em uma pretensa primazia da ofensiva do domínio cibernético desconsidera aspectos impeditivos significativos associados aos custos da organização de um ataque cibernético disruptivo efetivo, tais como: dificuldades operacionais; necessidade de pessoal com alto nível de conhecimento; e, grau de efemeridade das armas cibernéticas, fatores que favorecem a defesa e desestimulam ataques que não possam contar com capacidades convencionais substantivas para subsidiar as operações (Libicki, 2009; Betz e Stevens, 2009; Liff, 2012; Gartzke, 2013; Lindsay, 2013; 2015; Pollperter, 2015).

A *lógica das consequências* relativas à disparidade entre as forças militares de potências como Estados Unidos e China faz com que o potencial destrutivo das ameaças cibernéticas se mantenha abaixo da linha de uma possível escalada do uso da força cinética entre elas (Gartzke, 2013).

De modo que os teóricos realistas ocidentais[8] sustentam que para cada ameaça ativa no ciberespaço para exploração de vulnerabilidades em sistemas e redes de computador, existe uma contramedida de força reforçada pela superioridade tecnológica Ocidental frente a adversários de modesto desenvolvimento tecnológico que permite considerar a guerra cibernética entre norte-americanos e chineses como um evento altamente improvável (Lindsay, 2015).

Conforme indica a literatura há, portanto, uma forte estabilidade no domínio cibernético das operações que são levadas a cabo, embora ataques irritantes e moderados possam ser frequentes, os disruptivos capazes de afetar setores estratégicos (críticos) representam exceções. Ainda que a exploração cibernética ultrapasse as barreiras operacionais, ainda haverá incentivos para moderar a intensidade das ações e, assim, preservar os benefícios que fazem da exploração algo útil para os atacantes a princípio (Libicki, 2009; Liff, 2012; Lindsay, 2015).

Em função disto, parte dos que se debruçam sobre o problema da segurança cibernética é cética ao considerar a espionagem industrial e militar como forma de

8 Literatura circunscrita à esfera de análise de matriz fundamentalmente euro-americana, para mais sobre esta vertente ver: Liff, 2012; Gartzke, 2013; Lindsay, 2013.

guerra cibernética (Libicki, 2009; Morosov, 2009; Walt, 2010; Ball, 2011; Betz, Stevens, 2011; Maurer, 2011; Liff, 2012; Rid, 2012; Lindsay, 2013; Gartzke, 2013; Geers, 2015; Lindsay, Cheung e Reveron, 2015). A posição se justifica, pois, na primeira década do século vinte e um, as campanhas de exploração e reconhecimento registradas indicavam que a China ainda não possuía capacidade para sistematicamente atingir setores de comando e controle, defesa aérea e redes de inteligência e fontes de dados de adversários avançados, ou mesmo conduzir operações secretas de manipulação de dados nestas redes. Uma defasagem significativa existente entre os softwares de defesa contra vírus e segurança de rede disponíveis na China frente aos disponíveis em sociedades de tecnologia da informação avançada, impede a realização de ataques disruptivos provenientes do lado tecnologicamente menos avançado (Ball, 2011).

No início deste século as análises céticas não relevaram nenhum caso de ataque disruptivo a sistemas de comando e controle por parte do ELP, somente operações de negação de serviço orquestradas por hackers nacionalistas haviam sido registradas, sendo a maioria delas atribuídas às instituições militares e civis da China casos de exploração e reconhecimento de rede para inteligência (Libicki, 2009; 2015; Morosov; 2009; Liff, 2012)

Por conseguinte, a utilidade da guerra cibernética seria mais limitada do que acreditam os teóricos do ELP, as considerações sobre a efetividade militar convencional, o balanço de poder e a habilidade para combinar armas em operações conjuntas, continuava tendo preponderância no calculo estratégico e operacional aplicados aos conflitos (Lindsay, 2015).

Não obstante a evidente fragilidade da compreensão dos teóricos do ELP sobre o potencial do ciberespaço para reduzir a disparidade de forças entre adversários militarmente mais poderosos, o pensamento militar estratégico gestado orientou uma série de mudanças realizadas em instituições civis e militares da China que estiveram envolvidas em campanhas de uso do ciberespaço para projeção de poder nacional, estruturas militares e civis constituídas na tentativa de obter novos arranjos de comando e controle, incluindo especializações funcionais e formação de unidades para coordenar esforços interagencias (linhas da burocracia) com intuito de auferir retornos estratégicos com a guerra cibernética, conforme veremos na seção seguinte.

2. Mudança Institucional: como a China se Preparou para Utilizar o Ciberespaço com Vistas à Consecução de Objetivos Estratégicos

Nesta seção verificamos como os chineses se tornaram aptos a utilizar o ciberespaço para amplificar as capacidades de projeção do poder nacional mediante descrição da mudança pela qual passaram algumas das principais instituições civis e

militares da China, considerada condição necessária para utilização do ciberespaço com vistas à consecução de objetivos estratégicos do Estado. Tais modificações almejavam não apenas construir políticas cibernéticas para fortalecer a segurança e assegurar o crescimento econômico do país, mas garantir a eficiência das campanhas cibernéticas (Lavender, 2013; Lindsay, Cheung e Reveron, 2015; Stokes, 2015; Inkster, 2015; Nurkolov, 2017; Aversa, 2018).

> Com intuito de transformar o *modus operandi* e amplificar a eficiência das agencias de inteligência para coleta de informação estrangeira, a postura cautelosa e de aversão ao risco foi, gradualmente, substituída por uma de autoconfiança operacional que acompanhava o surgimento da China como ator com status e influencia crescente no sistema internacional (Inkster, 2015, p. 34).

O processo organizado pelo Partido Comunista e os líderes do Estado teve início ao final do século passado, em instituições políticas tradicionais como no Instituto de Defesa (ID) que, em 1983, deu origem ao Ministério da Segurança do Estado (MSE), e da constituição de outras como o Centro de Avaliação de Segurança de Tecnologia da Informação da China (CASTI), em 1998, que passou a coordenar uma vasta rede de centros regionais de avaliação de segurança e tecnologia da informação no país (Stokes, 2015).

Na esfera militar, a mudança teve implicações diretas para a dinâmica de distribuição de poder regional, transformando as forças armadas chinesas de uma instituição militar tradicional, composta por conscritos, em uma força moderna, menor e mais profissional, como se verifica, em específico, nas forças especiais[9], e, no geral, nas estruturas do terceiro e quarto departamento do ELP (Lavender, 2013).[10]

Houve um forte impacto da transformação das capacidades de coleção de informação externa do ELP por vias de exploração cibernética (espionagem e sabotagem) (Inkster, 2015). Embora as organizações do ELP responsáveis por realizar ataques disruptivos permaneçam uma questão aberta, o quarto departamento, organização voltada para planejamento relacionado a radares e operações de contramedidas eletrônicas, é visto como o provável responsável (Stokes, 2015).

9 As forças especiais realizam missões de: reconhecimento; ataques e sabotagem; ações integradas com terra, mar, ar, espaço e eletrônica, combates assimétricos, combate de larga escala e ataques cirúrgicos. Para uma análise aprofundada sobre o processo ver: Wamqiam. Guohua (2000); Blakso (2005); Fisher Jr (2012).

10 Conforme indica o Reporte Anual do Ministério da Defesa ao Congresso (2012), o Partido Comunista declara a intenção em utilizar uma estratégia de longo prazo para estabelecer um programa de modernização militar abrangente visando melhorar as capacidades das forças da China para lugar guerras locais em condições de informação, ou alta intensidade, e, operações militares regionais de curta duração centrada na informação (Lavender, 2013)

Outrossim, a China criou o Grupo de Líderes do Estado para Informatização (GLEI) e o Escritório do Conselho do Estado para Informatização, dirigidos por representantes mais velhos do Partido Comunista e organizações militares, que ficou responsável pela implementação das políticas de informatização. Em 2003, a instituição deu origem ao Pequeno Grupo de Coordenação em Rede de Segurança do Estado e Informação (SNISCSG) para desenvolvimento de novas tecnologias da informação com vistas robustecer a segurança nacional (Lindsay, Cheung e Reveron, 2015; Aversa, 2018).

Em 2014, o GLEI passou a ser dirigido pelo chefe de Estado Xi Jinping através da Comissão Central Militar que incluía entre seus membros o Chefe do Estado-Maior do ELP, General Fang Fenghui, responsável pelas políticas relacionadas com operações cibernéticas nacionais e segurança da internet (Stokes, 2015).

Daí em diante, o ELP se tornou a instituição central do sistema de segurança cibernética da China com responsabilidade por operações de inteligência militar, guerra eletrônica e espionagem. Os militares passaram a administrar um dos maiores centros de coleta de inteligência e infraestrutura de segurança da informação do mundo, com competência para atuar nas áreas de sinais de inteligência (SIGINT), computação avançada de alto desempenho e capacidades técnicas para criptografia e descriptografia (Lindsay, Cheung, Reveron, 2015).

As operações cibernéticas se tornaram vitais para que a China pudesse aplicar o pensamento estratégico do ELP de lutar guerras limitadas sob condições de alta tecnologia com vistas à projeção do poder nacional (Pollpeter, 2015). Dentre os objetivos das campanhas de espionagem destacam-se a aquisição de propriedade intelectual para desenvolvimento de tecnologia de ponta, e, de informação política com fins dissuasórios (Lavender, 2013).

Entretanto a efetividade das operações cibernéticas da China para controle da informação e invasão de sistemas de informação de seus adversários não se deveu apenas a transformação efetuada nas instituições basilares civis e militares, mas também, em larga medida, a cooperação com outras estruturas governamentais e privadas (Nurkolov, 2017).

Diversas instituições civis e empresas privadas foram associadas às campanhas de reconhecimento e exploração de redes associadas ao terceiro e quarto departamentos do ELP, dentre elas, universidades e institutos de pesquisa e desenvolvimento de tecnologia para a guerra de informação, e, gigantes do setor de tecnologia da informação como a Boyu Information Technology Company (Boyusec) e a Huawei Technologies (Hjortdal, 2011; Stokes, 2015).[11]

11 Dentre os subdepartamentos e instituições de ensino superior ligados a essa instituição destacam-se: as universidades de engenharia de Hefei; de engenharia da informação de Zhengzou; de defesa e tecnologia de Chagsha; academia de comunicações e comando de Wuhann; os

Admitindo que a exploração cibernética represente um primeiro passo para a construção de medidas mais incisivas, é plausível supor que a China detenha potencial para realizar operações ofensivas que resultem em ataques disruptivos, embora o caminho que conecta a exploração a um ataque dessa natureza seja longo e difícil de percorrer (Lindsay, 2015).[12] Acreditamos que esta lacuna na literatura possa ser preenchida pelo estudo das capacidades cibernéticas empregadas pela China para projeção de poder nacional em seu entorno regional após o conflito desencadeado no Vale de Galwan (2020).

Ao conectarmos a estratégia militar elaborada pelos teóricos do ELP para realizar a guerra cibernética à mudança institucional que deu origem a departamentos civis e militares especializados em reconhecimento e exploração de redes, somada à ampla gama de especialistas universitários e hackers civis aptos a atuar no campo da segurança da informação, consideramos que as instituições chinesas dispõem dos atributos necessários para utilizar ataques cibernéticos disruptivos de modo efetivo com vistas à consecução de objetivos estratégicos.

Embora ataques disruptivos entre potências continuem uma possibilidade remota, o mesmo não mais se verifica em relação a seu uso contra adversários militarmente mais frágeis em disputas regionais, pelo contrário, operações dessa natureza têm se tornado cada vez mais frequentes, conforme revelam estudos sobre ataques aos sistemas de infraestrutura crítica do Irã (2010-12) e da Ucrânia (2014-5), respectivamente, por potências como Estados Unidos e Rússia (Lindsay, 2013; Guedes de Oliveira e Casalunga, 2020). A próxima seção destaca o caso sino-indiano (2020-21) como a mais recente manifestação deste fenômeno.

3. O Conflito Sino-Indiano (2020-21): o Ciberespaço Utilizado para Projeção de Poder Nacional

Nesta seção coletamos evidências que revelam o *modus operandi* das instituições civis e militares chinesas via ciberespaço, bem como as principais ameaças e armas utilizadas. Ademais, identificamos o funcionamento do mecanismo de ação conjunta entre os atores estatais e não-estatais para realizar campanhas de reconhecimento, exploração e ataques disruptivos, simbiose considerada condição suficiente para ampliar a assimetria de poder entre China e Índia.

institutos 58º de Pesquisa e Desenvolvimento em criptologia e segurança da tecnologia da informação; Pesquisa em Segurança da Informação; e o Centro de computador do Norte de Beijing: responsável pelo desenho da arquitetura de reconhecimento cibernético, desenvolvimento de tecnologia, engenharia de sistemas e aquisição (Hjortdal, 2011; Stokes, 2015).

12 Para uma análise da dificuldade de passar da exploração de redes para ataques cibernéticos disruptivos ver: Owens, Dam, Lin, (2009); Sanger, Schmidt, (2013).

Nas últimas décadas, análises acadêmicas e relatórios de empresas especializadas em segurança cibernética identificaram um padrão de ação institucional resultante da conexão entre instituições civis e a infraestrutura organizacional dos setores de inteligência, redes de defesa e guerra eletrônica do ELP (Stokes, Lin, e Hsiao, 2011; Stokes e Hsiao, 2012; Krekel, Adams e Bakos, 2012; Mandiant, 2013; FireEye, 2015; 2017; Crowdstrike, 2018; FCW, 2018; Cyfirma 2020a; Cyfirma, 2020b; Recorded Future, 2021).

Do amálgama entre as instituições civis e militares resulta a simbiose entre atores estatais e não estatais para uso do ciberespaço com vistas à consecução de objetivos estratégicos que se verifica na atuação das Ameaças Persistentes Avançadas (APA) em fases de preparação para penetrar em alvos específicos, subtrair dados úteis, e, posteriormente, realizar ataques disruptivos. Mais especificamente, essas ameaças invadem sistemas de rede para coletar informação sobre tecnologia de defesa; governos estrangeiros; atividade de dissidentes chineses; e segredos de produção industrial civil e militar (Lindsay e Cheung, 2015).

Ao acessarem as redes dos alvos, as APA podem permanecer indetectáveis por longos períodos de tempo, os agentes contam com procedimentos operacionais padronizados, infraestrutura técnica reutilizável, divisão de trabalho e inteligência para operar em sistemas de rede complexos, fatores que indicam a presença de estruturas organizacionais robustas capazes de subsidiar as operações (Mandiant, 2013). [13]

A análise do conflito sino-indiano (2020-21) revela como o pensamento estratégico militar associado à mudança institucional pela qual passaram as forças armadas da China resultou no aprimoramento das técnicas de intrusão para espionagem militar e industrial utilizadas para inserção de programas maliciosos (códigos) em controles sensíveis de rede que ofereceram suporte aos ataques cibernéticos disruptivos verificados após a eclosão do conflito no Vale de Galwan (2020).

Na medida em que os dois Estados mais populosos do globo, China e Índia, se desenvolvem, aumentam também suas ambições geoestratégicas para projeção de poder nacional. Separados por uma zona de fronteira que se estende por 3.440km, esses gigantes estiveram envolvidos em disputas territoriais durante boa parte do século passado que só arrefeceram com a assinatura de um acordo, em 1996, o qual estabeleceu medidas de confiança para manutenção pacífica das áreas controladas pelos dois países.

13 As APA comprometem as redes dos alvos utilizando engenharia social ou truques de confiança que exploram as interações dos usuários humanos. Ao ganhar acesso aos sistemas, o atacante amplia seus privilégios para reconhecer toda a rede e conseguir subtrair informação dos servidores de comando e controle via internet (Mandiant, 2013).

No entanto, recentemente a escalada de tensão na região do Himalaia reavivou os embates, culminando em um confronto físico rudimentar desencadeado dentro do território indiano, numa área de entroncamento na zona fronteiriça do Vale de Galwan, em Ladakh, que se localiza ao longo do setor oeste da Linha de Controle Atual (LCA), perto de Aksai Chin, área reivindicada pela Índia, mas controlada pela China (BBC, 2020).

O território de Galwan é considerado estratégico por ambos os Estados, trata-se do local de pouso para aeronaves militares mais alto do mundo, uma área com cumes de até 14.000 pés, na qual, em 2019, a Índia construiu uma estrada para conectar a base aérea militar reativada de Daulat beg Oldi à região de Ladakh, ampliando as capacidades de transporte de militares e materiais de modo eficaz e rápido para a zona fronteiriça em caso de conflito, a ação despertou a vigilância das forças chinesas (BBC, 2020)

Frente a este cenário, o confronto que se iniciou na noite de 15 de junho de 2020 e ocasionou baixas entre soldados indianos e chineses, pode ser considerado o mais grave na fronteira terrestre instável mais longa do mundo em quase meio século. Embora, o número preciso de baixas permaneça sob escrutínio, é inegável que o retorno das hostilidades entre chineses e indianos abalou as relações diplomáticas e econômicas entre os países (The Print, 2021).

Logo após o confronto, ambos os Estados iniciaram tratativas diplomáticas para reestabelecer as relações de confiança mútua na região. Sem embargo, medidas coercitivas foram tomadas em diversos segmentos econômicos, dentre as quais, se destacam o banimento de mais de duzentos aplicativos de origem chinesa, sob a alegação do governo de que estariam sendo utilizados para coletar dados dos cidadãos indianos (Recorded Future, 2021).

A resposta chinesa foi dada em 13 de outubro de 2020 via ciberespaço, com ataques disruptivos que causaram danos ao sistema financeiro e de transporte ferroviário deixando vinte milhões de indianos sem energia elétrica em suas casas, e outros milhares impedidos de se locomover (The New York Times, 2021).

As tentativas da China para utilizar o ciberespaço e atingir sistemas de energia já haviam sido registradas na primeira década deste século contra alvos de sistemas operacionais dos Estados Unidos (HJORTDAL, 2011). Quase uma década depois, o Estado parece ter adquirido capacidade para realizar um ataque disruptivo contra redes de sistemas de infraestrutura crítica (Recorded Future, 2021).

Em fevereiro de 2021, na medida em que as investidas cibernéticas sobre a Índia continuaram a ganhar relevo, analistas identificaram os agentes responsáveis pela série de operações de infiltração aos setores de infraestrutura crítica da Índia, foram detectados *malwares* em quatro centros regionais de distribuição de energia e dois portos marítimos. De acordo com o relatório, esta operação foi conduzida por uma

APA especializada em espionagem cibernética denominada RedEcho ou APT41 (Recorded Future, 2021).

Utilizando técnicas de verificação de registro de domínio, tráfego de redes automatizadas e de componentes, e código aberto, os analistas identificaram o *modus operandi* das ameaças e estabeleceram a ligação entre os hackers e as instituições civis e militares chinesas, revelando o envolvimento do MSE e de departamentos ligados ao ELP "[...] fomos capazes de determinar um padrão claro e consistente das organizações indianas visadas nesta campanha por meio do perfil comportamental do tráfego de rede para atingir a infraestrutura do adversário" (Recorded Future, 2021, p. 6).

A análise identificou que a APA41 utilizou programas maliciosos como o '*PlugX*' e '*ShadowPad*' para invadir sites do governo, setor público e organizações de defesa e do setor privado indianos, se movendo lateralmente nesses sistemas por cerca de nove meses antes do ataque disruptivo que comprometeu setores de comando e controle (C2) das infraestruturas críticas indianas. As ações via ciberespaço representam uma forte evidência das capacidades chinesas de utilização deste domínio para causar danos físicos, inéditas até então "[...] à medida que as tensões bilaterais continuam a aumentar, esperamos ver um aumento contínuo nas operações cibernéticas conduzidas por grupos vinculados à China, como a RedEcho, de acordo com os interesses estratégicos nacionais" (Recorded Future, 2021, p. 11).

Embora se reconheça que a ligação entre a interrupção de energia e o *malware* ainda não tenha sido admitida por fontes oficiais, existem fortes evidências que apontam para o envolvimento da China neste evento. Razão pela qual, especialistas em segurança cibernética foram enfáticos ao afirmar: "[...] a sinalização está sendo feita [pela China] para indicar que podemos e temos a capacidade de fazer isso em tempos de crise [...] é como enviar um aviso à Índia de que temos [chineses] essa capacidade" (The New York Times, 2021, p. 4).

Se considerarmos as orientações estratégicas dos teóricos do ELP sobre as vantagens do uso da guerra cibernética descritas na primeira seção, podemos afirmar com alguma precisão que os ataques disruptivos fizeram parte de uma campanha cibernética que serviu de alerta para os indianos sobre as capacidades chinesas de utilização do ciberespaço para conter as divergências territoriais entre os dois países.

A despeito de que ambos os Estados possam recorrer ao domínio cibernético, as capacidades institucionais da China para utilizá-lo são desproporcionalmente superiores às da Índia, parte da infraestrutura de rede indiana tem origem chinesa, a exemplo dos *hardwares* utilizados nos setores de energia e ferroviário, é pouco provável que os indianos conseguirão eliminar a dependência de tecnologia de sistemas estrangeira em um curto espaço de tempo (The New York, 2021).

As incursões da China contra alvos indianos cresceram exponencialmente após o conflito no Vale de Galwan. Em dezembro de 2020, foi verificada outra tentativa de

ataque cibernético que utilizou *spear phishing* e-mails contendo informações sobre os soldados feridos no conflito para atrair a atenção dos usuários e subtrair senhas de acesso ao setor de energia, refinarias de petróleo e uma usina nuclear (The New York Times, 2021).

As operações cibernéticas, provenientes do território chinês de Guangdong e Henan, foram atribuídas à organização Fang Xiao Qing, e, reportados como tentativa de infiltração para ataques disruptivos futuros "Até agora, o foco da China era o roubo de informações. Mas Pequim está cada vez mais ativa na inserção de códigos em sistemas de infraestrutura, sabendo que, quando descoberto, o medo de um ataque poder ser uma ferramenta tão poderosa quanto o próprio ataque" (The New York Times, 2021, p. 2).

Em 2021, outra ameaça vinculada à China, denominada APA10 ou Stone Panda/ MenuPass, foi detectada tentando acessar as redes de infraestrutura de tecnologia de informação da empresa Bharat Biotech e do Instituto Serum da Índia (SII), em uma tentativa de obter dados de propriedade intelectual vinculada à produção da vacina AstraZeneca, desenvolvida para tratamento do novo coronavírus (COVID-19) (Reuters, 2021).

As atividades cibernéticas da APA10 estavam sendo monitoradas há mais de uma década por empresas especializadas em cibersegurança que indicaram sua associação com o MSE e a CASTI (FireEye, 2017; Cyfirma, 2020a; 2020b). As evidências foram registradas por imagens fotográficas, de satélite, e, recibos de aplicativos de transporte utilizados pelos hackers que viajavam regularmente para o complexo do MSE, em Tianjin (Crowdstrike, 2018; FCW, 2018).

As operações cibernéticas tinham por objetivo coletar informações militares e de inteligência, bem como subtrair dados comerciais, que pudessem contribuir com o desenvolvimento tecnológico das forças armadas e corporações chinesas. Dentre os principais alvos atingidos inicialmente, figuravam empresas de construção e engenharia aeroespacial, telecomunicações e instituições dos governos norte americano, europeu e japonês (FireEye, 2017).

Em 2016 a APA10 atingiu setores de tecnologia da informação em diversos países, incluindo empresas de manufatura da Índia. As principais armas cibernéticas identificadas para invasão dos sistemas foram o '*Haymaker*' e o '*Snugride*' utilizados na primeira fase de intrusão e o '*Bugjuice*' e '*QuasarRat*' na segunda fase de aquisição, por fim, o '*SOGU*' na terceira fase, estes programas maliciosos são '*backdoors*' altamente sofisticados que demandam forte investimento para seu desenvolvimento, fator que indica a presença de um ente com alta capacidade para oferecer recursos para sua construção (FireEye, 2017).

O *modus operandi* da Stone Panda inclui ataques *spear phising* e o uso de provedores de serviços globais para acesso às redes de sistemas corporativos. De tal modo que ao se movimentar lateralmente pelos sistemas infectados, estabelecendo comunica-

ção entre servidores de Comando e Controle (C2) dos alvos e um provedor de serviços remoto – utilizado como um '*proxy*' para instalação dos programas maliciosos –, o grupo obtinha acesso a dados confidenciais sem ser detectado (FireEye, 2017).

A APA10 realizou uma série de operações cibernéticas para subtrair dados comerciais e informações sobre cadeia de suprimentos de empresas indianas (Cyfirma, 2020a), e invadir sistemas de informação de setores diversos (automotivo, aviação, educação, energia, finanças, saúde, manufatura de alta tecnologia, produtos farmacêuticos e telecomunicações) de adversários comerciais, sendo as redes corporativas indianas alvo de tentativa de extração de dados de propriedade intelectual vinculadas a projetos de pesquisa e desenvolvimento de tecnologia com alto valor agregado (Cyfirma, 2020b).

Há pelo menos uma década as operações cibernéticas da China envolvendo atores não-estatais privados e órgãos institucionais vem sendo motivo de preocupação da comunidade internacional de segurança. Em 2016, o setor de inteligência do Departamento de Defesa norte-americano reportou uma possível ligação entre empresas de segurança cibernética e o serviço de inteligência do MSE em operações de espionagem cibernética que tinham como objetivo favorecer empresas chinesas do setor de telecomunicações que atuam como vetores para produção de produtos de segurança alta tecnologia de uso dual que seriam empregados no setor privado e pelas forças militares chinesas (The Washington Free Beacon, 2016).

A denominada APA3 ou Gothic Panda envolvida nestes ataques vinha sendo monitorada desde 2010. As ações dessa ameaça foram atribuídas ao MSE em associação com a empresa Boyusec que, desde 2014, atuava em parceria com a Huawei e a rede nacional de centros de avaliação de segurança de Guangdong administrados pelo CASTI, instituição vinculada ao MSE, no desenvolvimento de produtos de defesa e comando de operações de inteligência cibernética (Recorded Future, 2017).

Em 2015, a empresa e o escritório de segurança da informação da China criaram um laboratório conjunto para teste de *softwares* para desenvolvimento de defesas cibernéticas[14]. As evidencias indicaram a ligação entre a APA3, instituições civis e militares, a Boyusec e seus parceiros, em um modelo de ação orquestrado pelo Estado da China para mobilizar agentes não-estatais em missões de espionagem cibernética que serviram de cobertura para as operações de inteligência do MSE (Recorded Future, 2017).

No tocante às táticas de infiltração se verificam técnicas tradicionais como uso de *spear phishings* e ferramentas de acesso remoto, bem como de ferramentas mais

14 Boyusec e Huawei estão trabalhando juntos para produzir produtos de segurança que serão carregados em computadores e equipamentos telefônicos de fabricação chinesa. Os produtos adulterados permitirão que a inteligência chinesa capture dados e controle computadores e equipamentos de telecomunicações (The Washington Free Beacon, 2016, p. 1).

sofisticadas capazes de causar ataques de '*dia-zero*' contra sistemas de empresas do setor de defesa, transporte, alta tecnologia, telecomunicações e departamentos governamentais em diversos países ao redor do mundo (FireEye, 2015).

Conforme exposto, o rastreamento do processo que resulta nas campanhas de reconhecimento e exploração e ataques disruptivos orquestrados pela China revela evidências do funcionamento do mecanismo de simbiose entre instituições civis, militares e as APA: RedEcho (APA41), Stone Panda (APA10) e Gothic Panda (APA3) para consecução de objetivos estratégicos regionais, demonstrando a relevância do ciberespaço para projeção de poder nacional da China, em conformidade com os parâmetros estabelecidos pelos teóricos do pensamento militar do ELP.

Considerações Finais

Neste artigo elucidamos duas condições em que ocorre o processo de uso do ciberespaço para projeção de poder nacional. Com base na análise da atuação de instituições civis, militares e das APA em campanhas de reconhecimento, exploração e ataques disruptivos orquestradas pela República Popular da China, consideramos que a mudança institucional e a simbiose entre agentes estatais e não-estatais permeadas pelas nuances do pensamento estratégico militar do ELP representam fatores chave para explicar o comportamento cibernético da República Popular da China nas últimas décadas.

Inicialmente, demonstramos como os teóricos do ELP abordam o fenômeno da guerra cibernética e orientam a aplicação de estratagemas em campanhas que utilizam o ciberespaço como engenho de força para projeção de poder nacional. Em seguida, verificamos como a mudança pela qual passaram as instituições políticas e militares contribuiu para robustecer as estruturas responsáveis por estas campanhas, considerada condição necessária para uso do ciberespaço com vistas à consecução de objetivos estratégicos.

Partindo do pressuposto de que o ciberespaço é um domínio que oferece vantagens assimétricas aos Estados militar e tecnologicamente mais avançados frente a adversários mais fracos, nossa análise do caso sino-indiano (2020-21) averiguou que o desenvolvimento das capacidades alcançado pela China para atuar neste domínio permitiu o uso efetivo de ataques disruptivos como forma de dissuasão e/ou coerção, considerada condição suficiente para ampliar a capacidade de projeção de poder regional da China.

Finalmente, identificamos evidências que revelam o funcionamento da simbiose atores estatais e não-estatais nas campanhas via ciberespaço, considerado o mecanismo que impacta na produção de vantagens estratégicas para uma potência em um conflito regional. Sem deixar de considerar o impacto que as campanhas de

reconhecimento e exploração de sistemas exercem sobre o fenômeno da guerra cibernética, nossa análise robustece a hipótese de que o ciberespaço tem se constituído como domínio relevante para ampliar a assimetria de poder entre potências e adversários regionais, sendo assim, potências médias estariam mais vulneráveis e suscetíveis a terem seus sistemas críticos atingidos por este tipo de ataque.

Referências

Aversa, 2018. *China: An evolutionary analysis of its cyber strategy*. Center for cyber security and international relations studies, CSSII, 2-14.

BBC, 2020. Galwan Valley: China and India clash on freezing and inhospitable battlefield [Online]. London, *BBC News*. Available: https://theprint.in/defence/4-9-or-14-even-china-isnt-sure-how-many-pla-soldiers-died-in-galwan-valley/613372/ [Accessed, 15. March 2021].

Betz, D., Stevens, T., 2011. Cyberspace and the State: Toward a Strategy for Cyber-Power, London, IISS Adelphi Paper.

Bingyan, L., 2004. *Stratagem and Transformation*, Beijing, Beijing University Press.

Blakso, D., 2005. Chinese Army Modernization: An Overview, *Military Review*, 85, 1-68.

Choucri, N., 2012. *Cyberpolitics in international relations*, London, MIT Press.

Clark, R., Knake, R., 2010. *Cyber War: The Next Threat to National Security and What to Do about It*. New York, NY: Harpercollins.

Collier, D., 2011. Understanding Process Tracing. Political Science and Politics, 4, 823-830.

Cornish, P., Livingstone, D., e Yorke, C., 2010. *On Cyber Warfare*. Royal Institute of International Affairs, Chatham House Report.

Crowdstrike, 2018. Two Birds, One Stone Panda [Online]. UK, CrowdstrikeBlog. Available: https://www.crowdstrike.com/blog/two-birds-one-stone-panda/ [Accessed 08 September 2019].

Cyfirma, 2020a. Cyber espionage and the Asia Threat Landscape. [Online]. Tokyo, *Cyfirma News*. Available: https://www.cyfirma.com/news/cyber-espionage-and-the-asia-threat-landscape/ [Accessed 02 November 2019].

Cyfirma, 2020b. Rising cyber attacks due to China-India border conflict [Online]. Tokyo, *Cyfirma News*. Available: https://www.cyfirma.com/early-warning/rising-cyber-attacks-due-to-china-india-border-conflict/ [Accessed 13 July 2020].

Desjardins, R., 2005. The Science of Military Strategy. In: Guangdqian, P. Youzhi, Yao., ed, Beijing, Military Science Publishing House.

Farwell. J., Rohozinski, R., 2012. The New Reality of Cyber War, *Survival*, 54, 107-120.

FCW, 2018. Chinese hacker group targets tech supply chain, report says [Online]. Washington, Government Media Executive Group LLC. Available: https://fcw.com/articles/2018/08/31/china-supply-chain-hack.aspx [Accessed 10 September 2019].

FireEye 2017. APT10 (MenuPass Group): New Tools, Global Campaign Latest Manifestation of Longstanding Threat [Online]. Virginie, Mandiant Inc. Available: https:// https://www.mandiant.com/resources/apt10-menupass-group [Accessed 26 October 2019].

Fisher Jr., Richard, D., 2012. *China's Modernization: Building for Regional and Global Reach*, Santa Barbara, Praeger Security International.

Gartzke, E., 2013. E. The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. *International Security*, 38, 41-73.

Geers, K., 2014. *Cyber war in Perspective* [e-book] NATO CCD COE/Atlantic Council/Taras Shevchenko National University of Kyiv [Online]. Available: https://ccdcoe.org/uploads/2018/10/CyberWarinPerspective_full_book.pdf [Accessed 13 November 2020].

Guedes, O., Casalunga, F. H. Guerra Híbrida: o emprego da tecnologia da informação no conflito Rússia-Ucrânia (2014-2015). *Revista Brasileira de Estudos de Defesa*, 7, 13-36.

Guo'an, X., 2010. Characteristics of China's Traditional Strategic Thought. *China Military Science*, 3, 116-122.

Hall, P., Taylor, R., 2003. The Three Versions of Neo-Institutionalism. *Revista de Cultura e Política*, 58, 193-223.

Hjortdal, M., 2011. China's Use of cyber warfare: espionage meets strategic deterrence. *Journal of Strategic Security*, 4, 1-23.

Inkster, N., 2015. The Chinese Intelligence Agencies: evolution and empowerment in Cyberspace. In: Lindsay, J. Cheung, T. Reveron, D., 2015, *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, London, Oxford University Press.

Jijun, L., 2006. Military Strategic Thinking and Scientific Decision-making. *China Military Science*, 1, 28-38.

Kello, L., 2013. The meaning of the Cyber Revolution Perils to Theory and Statecraft. *International Security*, 8, 7-40.

Krekel, B., Patton, A., e Bakos, G., 2012. *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*. Washington DC, Northrop Grumman Corporation.

Krekel, B., 2009. *G. Capability of the People's Republic of China to Conduct Cyberwarfare and Computer Network Exploitation*, Washington, Northrop Grumman Corporation.

Li, N., Jiangzhou, L., e Dehui, X., 2000. Xu. Planning Strategies of Information Operations in High Tech Local Wars. *China Military Science Review*, 54, 115-22.

Libicki, M., 2009. *Cyberdeterrence and Cyberwar*, Santa Monica, RAND Corporation.

Libicki, M., 2015. *The Cyber War That Wasn't In: Cyber war in Perspective* [e-book] NATO CCD COE / Atlantic Council / Taras Shevchenko National University of Kyiv. Available: https://ccdcoe.org/uploads/2018/10/CyberWarinPerspective_full_book.pdf [Accessed 13 November 2020].

Liff, A., 2012. Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War. *Journal of Strategic Studies*, 35, 401-428.

Li, N., Jifeng, W., 2003. On the New Concept of Chinese Military Strategy in the 21st Century. *China Military Science*, 2, 85-90.

Lindsay, J., 2013. Stuxnet and the Limits of Cyber Warfare. *Security Studies*, 22, 365-404.

Lindsay, J., 2015. The impact of China on Cybersecurity: Fiction and Friction. *International Security*, 39, 7-47.

Lindsay, J., Cheung, T. e Reveron, D., 2015. *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, London, Oxford University Press.

Lindsay, J., Cheung, T., 2015. From Exploitation to Innovation. In: Lindsay, J., Cheung, T e Reveron, D., 2015. *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, London, Oxford University Press.

Lavender, D., 2013. *China's Special Operations Forces Modernization, Professionalization and Regional Implications*, U.S. Army War College, Master of Strategic Studies Degree, Philadelphia, Report Strategy Research Project.

Mandiant, 2013. APT1 Exposing One of China's Cyber Espionage Units [Online]. Virginie, Mandiant Inc. Available: https://www.mandiant.com/resources/apt1-exposing-one-of-chinas-cyber-espionage-units [Accessed: 02 September 2019].

Mahoney, J., 2012. The logic of Process Tracing Tests in the Social Sciences. *Sociological Methods & Research*, 41, 570-597.

Morozov, E., 2009. Cyber-Scare: The Exaggerated Fears over Digital Warfare. [Online]. Cambridge, *Boston Review*. Available: https://bostonreview.net/articles/cyber-scare-evgeny-morozov/ [Accessed 20 November 2020].

Nurkolov, N., 2017. New Cyber Strategy of China and the Alterations in the Field. *Journal of Political Science & Public Affairs*, 5(4), 1-6.

Olszewski, B., 2018. Advanced Persistent Threats as a Manifestations of State Military Activity in Cyber Space. Institute of International Studies, 189, 57-71.

Pollpeter, K., 2015. Chinese Writing on Cyberwarfare and Coercion. In: Lindsay, J., Cheung, T e Reveron, D., 2015. *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, London, Oxford University Press.

Qi, L., 2002. Campaign Stratagem Application under High-Tech Conditions. In: Zhang, X., Zhang, L. 2002. *Campaign Stratagems*, Beijing, National Defense University.

Qingmin, D., 2002. *On Integrating Network Warfare and Electronic Warfare*. Beijing, PLA Press.

Recorded Future, 2017. Recorded Future research concludes Chinese Ministry of State Security Behind APT3 [Online]. Boston, *Recorded Future*. Available: https://www.informationispower.com/explore/papers/APT/APT_CyberCriminal_Campaign/2017/Recorded Future_Chinese-Ministry-State-APT3(05-17-2017).pdf [Accessed 20 August 2019].

Recorded Future, 2021. China-lined Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions [Online]. Boston, *Recorded Future*. Available: https://go.recordedfuture.com/redecho-insikt-group-report [Accessed 03 March 2021].

Reuters, 2021. Chinese hackers target Indian vaccine makers SII, Bharat Biotech, says security firm [Online]. City: publisher. Available: https://www.reuters.com/article/health-coronavirus-india-china-idINKCN2AT21O [Accessed 09 March 2021].

Rid, T., 2012. Cyber War Will Not Take Blace. *Journal of Strategic Studies*, 35, 5-32.

Singer, P., Friedman, A., 2014. *Cybersecurity and cyberwar: What everyone needs to know*, Oxford, Oxford University Press.

Stokes, M., Lin, J. e Hsiao, L., 2011. The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure [Online]. Arlington, The Project 2049 Institute. Available: https://project2049.net/wp-content/uploads/2018/05/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf [Accessed 24 March 2021].

Stokes, M., Hsiao, L., 2012. Countering Chinese Cyber Operations: Opportunities and Challenges for U. S. *The Project 2049 Institute* [Online]. Available: https://project2049.net/2012/10/29/countering-chinese-cyber-operations-opportunities-and-challenges-for-u-s-interests/ [Accessed 04 June 2021].

Stokes, M., 2015. The Chinese People's Liberation Army Computer Network Operations Infrastructure. In: Lindsay, J., Cheung, T e Reveron, D., 2015. *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, London, Oxford University Press.

The New York Times, 2021. China Appears to Warn India: Push Too Hard and the Lights Could go out [Online]. City: Publisher. Available: https://www.nytimes.com/2021/02/28/us/politics/china-india-hacking-electricity.html [Accessed 12 March 2021].

The Washington Free Beacon, 2016. Pentagon Links Chinese Cyber Security Firm to Beijin Spy Service [Online]. Washington, *WFB News*. Available: https://freebeacon.com/national-security/pentagon-links-chinese-cyber-security-firm-beijing-spy-service/ [Accessed 08 August 2019].

The Print, 2021. 4, 9 or 14? Even China 'isn't sure' how many PLA soldiers died in Galwan Valley [Online]. Karnataka, *P News*. Available: https://theprint.in/defence/4-9-or-14-even-china-isnt-sure-how-many-pla-soldiers-died-in-galwan-valley/613372/ [Accessed 12 March 2021].

Thomas, T., 2014. *Military Strategy: Basic Concepts and Examples of its Use*, Kansas, Foreign Military Studies Office.

Walt, S., 2010. Is the Cyber Threat Overblown? [Online]. Pennsylvania, *Foreign Policy*. Available: https://foreignpolicy.com/2010/03/30/is-the-cyber-threat-overblown/ [Accessed 27 September 2020].

Wanquan, C., Guohua, Y., 2005. PRC PLA Analysis of 20th Century Combat Theory. Peoples Liberation Army Daily. Beijing, PLA Press.

Youzhi, Y., Debao, M., 2004. Sun Tzu's Art of War and Mainstream Contemporary Chinese Theories of War. *China Military Science*, 6, 9-16.

Zhang, Y., 2006. *In Their Own Words: Foreign Military Thought Science of Campaigns*, Montgomery, China Aerospace Studies Institute.

Zhang, Y., Zhang, L., 2002. *Campaign Stratagems*, Beijing, National Defense University.