UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL

INSTITUTO DE FILOSOFIA E CIÊNCIAS HUMANAS

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA POLÍTICA

FERNANDO HENRIQUE CASALUNGA

SENHORES DA REDE: as estratégias de Estados Unidos, Rússia, e China para emprego da tecnologia de informação em conflitos regionais (2007-2022)

Porto Alegre

2024

FERNANDO HENRIQUE CASALUNGA

SENHORES DA REDE: as estratégias de Estados Unidos, Rússia, e China para emprego da tecnologia de informação em conflitos regionais (2007-2022)

Tese de Doutorado em Política Internacional e Defesa, apresentada como requisito parcial para a obtenção do título de Doutor pelo Programa de Pós-Graduação em Ciência Política da Universidade Federal do Rio Grande do Sul.

Orientador: Prof. Dr. Eduardo Munhoz Svartman

Porto Alegre

2024

CIP - Catalogação na Publicação

Casalunga, Fernando
SENHORES DA REDE: as estratégias de Estados Unidos, Rússia, e China para emprego da tecnologia de informação em conflitos regionais (2007-2022) / Fernando Casalunga. -- 2024.
199 f.
Orientador: Eduardo Munhoz Svartman.

Tese (Doutorado) -- Universidade Federal do Rio Grande do Sul, , Porto Alegre, BR-RS, 2024.

1. Conflitos regionais. 2. Poder nacional. 3. Mecanismo . 4. Guerra Cibernética. 5. Guerra Híbrida. I. Svartman, Eduardo Munhoz, orient. II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica da UFRGS com os dados fornecidos pelo(a) autor(a).

Fernando Henrique Casalunga

SENHORES DA REDE: as estratégias de Estados Unidos, Rússia e China, para emprego da tecnologia de informação em conflitos regionais

Tese submetida ao Programa de Pós-Graduação em Ciência Política da Universidade Federal do Rio Grande do Sul como requisito parcial para obtenção do título de Doutor em Ciência Política.

Porto Alegre, 29 de fevereiro de 2024

Resultado: Aprovado com louvor.

BANCA EXAMINADORA:

_____

Bruno Cardoso Reis
Centro de Estudos Internacionais
Instituto Universitário de Lisboa (ISCTE)

_____

Marcos Aurélio Guedes de Oliveira
Departamento de Ciência Política
Universidade Federal de Pernambuco (UFPE)

_____

Carlos Schmidt Arturi (Examinador Interno)
Departamento de Ciência Política
Universidade Federal do Rio Grande do Sul (UFRGS)

AGRADECIMENTOS

Ao orientador e amigo, Prof. Dr. Eduardo Munhoz Svartman, pela competência e respeito com que conduziu este processo.

Ao supervisor Dr. Bruno Cardoso Reis pelo acolhimento durante passagem junto ao Centro de Estudos Internacionais de Lisboa (CEI-Iscte).

Aos examinadores Dr. Marcos Aurélio Guedes de Oliveira e Dr. Carlos Schmidt Arturi pelas valiosas contribuições oferecidas a esta pesquisa ao longo das fases de qualificação e defesa.

Aos docentes e servidores associados ao Programa de Pós-graduação em Ciência Política da Universidade Federal do Rio Grande do Sul, pelas valiosas contribuições e auxílio oportuno durante toda a minha trajetória neste departamento.

Em especial, a Cleonice Aparecida Casalunga Franco, Natália Diniz Schwether, e Heitor Schwether Casalunga que estiveram ao meu lado ao longo deste desafio, sem dúvidas vocês representam a motivação maior de sua conclusão em tempo hábil.

RESUMO

A partir do exame das estratégias empregadas pelos Estados Unidos da América, a Federação Russa e a República Popular da China em conflitos desencadeados contra seus respectivos adversários regionais, a República Islâmica do Irã (2007-2010), a República Popular da Ucrânia (2014-2015) e a República Democrática da Índia (2020-2022), esta pesquisa demonstra como e porque o ciberespaço se tornou um domínio significativo para projeção de poder nacional nesse início de século. Com base na identificação do mecanismo que conecta as mudanças pela qual passaram as instituições responsáveis pela segurança e defesa nacional das grandes potências nas últimas décadas à complexidade das operações e sofisticação das principais ameaças cibernéticas utilizadas por agentes estatais e não-estatais a serviço destes Estados para atingir seus adversários, propomos a construção de uma teoria indutiva que exprime as razões pelas quais as potências recorreram a este novo engenho de força para consecução de objetivos estratégicos. Para tanto, aplicamos as técnicas qualitativas de rastreamento de processos e análise comparativa histórica com intuito de responder ao seguinte questionamento: Por que as grandes potências utilizaram o ciberespaço para conquistarem seus objetivos estratégicos?

Palavras-chave: Guerra cibernética. Conflitos regionais. Mecanismo. Poder nacional.

ABSTRACT

From the examination of the strategies employed by the United States of America, the Russian Federation and the People's Republic of China in conflicts unleashed against their respective regional adversaries, the Islamic Republic of Iran (2007-2010), the People's Republic of Ukraine (2014- 2015) and the Democratic Republic of India (2020-2022), this research demonstrates how and why cyberspace became a significant domain for projecting national power at the beginning of this century. We propose the construction of an inductive theory that expresses the rationale behind the powers' use of this new power tool to achieve strategic objectives, based on the identification of the mechanism that links the changes that the great powers' institutions responsible for national security and defense have undergone in recent decades to the complexity of operations and sophistication of the main cyber threats used by state and non-state agents in these States' service to access their adversaries' critical infrastructure sectors and information systems. In order to do this, we used qualitative historical comparison analysis and process tracing to address the following query: Why did great powers utilize cyberspace to accomplish their geopolitical goals?

Keywords: Cyber warfare. Regional conflicts. Mechanism. National power.

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS

ADMs	Armas de Destruição em Massa
AHC	Análise Histórico Comparativa
AIEA	Agência Internacional de Energia Atômica
APAs	Ameaças Persistentes Avançadas
APC	Acordo de Parceria e Cooperação
C2	Comando e Controle
CEC	Comissão Central de Eleições
CIM	Complexo Industrial Militar
CSNU	Conselho de Segurança das Nações Unidas
DE	Departamento de Energia
DCS	Sistema de Controle Distribuído
DHS	Departamento de Segurança Interna
DM	Doutrina Militar
DoD	Departamento de Defesa
EDN	Estratégia de Defesa Nacional
ENPC	Estratégia Nacional para Proteção do Ciberespaço
ESN	Estratégia de Segurança Nacional
EUA	Estados Unidos da América
FAGCI	Agência Federal de Comunicações e Informações Governamentais
FMCs	Força de Missões Cibernéticas
FSB	Serviço Federal de Segurança
GRU	Departamento Central de Inteligência
GTC	Grupo de Trabalho Conjunto
ICSs	Sistemas de Controle Industrial
ISAC	Centro de Compartilhamento e Análise de Informações
KGB	Organização de Serviços Secretos
LAC	Linha de Controle Real
NSA	National Security Agency
ELP	Exército de Libertação Popular
MSE	Ministério de Segurança do Estado
ONU	Organização das Nações Unidas
OTAN	Organização do Tratado do Atlântico

PAPF	Polícia Armada do Povo
PC	Partido Comunista
PLCs	Controladores Lógicos Programáveis
RMA	Revolução dos Assuntos Militares
RPC	República Popular da China
SCADA	Sistemas de Supervisão e Aquisição de Dados
SCFs	Sistemas Ciber-Físicos
TNP	Tratado de Não Proliferação de Armas Nucleares
UE	União Europeia
URSS	União das Repúblicas Soviéticas
USCYBERCOM	Comando Cibernético dos Estados Unidos

APOIO DE FINANCIAMENTO CAPES

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) e do Programa de Pesquisas no Exterior em Áreas Estratégias para a Defesa (PROPEX)

SUMÁRIO

INTRODUÇÃO

O acesso à rede mundial de computadores tem aumentado consideravelmente nos últimos anos, dentre os mais de sete bilhões e oitocentos mil indivíduos que compõem a população mundial, aproximadamente cinco bilhões cento e setenta mil se conectam a Internet, parcela de usuários que representa mais de sessenta e cinco por cento do total de habitantes. As três grandes potências República Popular da China (RPC), Estados Unidos da América (EUA) e Federação Russa, objetos deste estudo, concentram em torno de vinte e cinto por centro da população mundial e dezoito por cento do total de usuários da Internet (INTERNET WORLD STATS, 2021).

Com um número cada vez maior de usuários e sistemas interconectados a segurança do fluxo de informações no domínio cibernético tornou-se um ponto nevrálgico para os Estados contemporâneos, em especial para as potências. Na medida em que os mais diversos sistemas -comunicações, financeiro, industrial e de serviços- dependem de componentes principais (*hardware*/*software* conectados ou não à Internet) para funcionar, falhas na proteção da tecnologia da informação têm potencial para causar danos sensíveis às estruturas econômicas, políticas e militares dos Estados, conferindo vantagens estratégicas aos seus adversários (WEISS, JANKAUSKAS, 2019).

À vista disso, a comunidade acadêmica, civil e militar, tem se debruçado sobre o problema fundamental da segurança cibernética, a fim de compreender os movimentos das agências estatais no que concerne às estratégias, táticas e operações utilizadas para atuar no ciberespaço com vistas à consecução de objetivos estratégicos (MOROZOV, 2009; LIBICKI, 2009; CLARKE, KNAKE, 2010; CORNISH, LIVINGSTONE, YORKE, 2010; BETZ, STEVENS, 2011; MAURER, 2011; CHOUCRI, 2012; FARWELL, ROHOZINSKI, 2012; LIFF, 2012; GILES, HAGESTAD, 2013). Na medida em que a pesquisa científica avança, novos desafios teóricos e empíricos emergem, refletindo a complexidade analítica e a dinamicidade do desafio cibernético (GARTZKE, 2013; KELLO, 2013; LINDSAY, 2013; GEERS, 2015; LIBICKI, 2015; LINDSAY, CHEUNG, REVERON, 2015; WEEDON, 2015; KJENNERUD, CULLEN, 2016; PAVLIKOVA, 2016; BAEZNER, ROBIN, 2017; NOURIAN, MADNICK, 2018; OLSZEWSKI, 2018).

Neste ensejo, é notório que a inserção do ciberespaço na conjuntura política dos Estados tem estimulado forte dinamismo no campo de estudos sobre Política Internacional e Defesa, provocando divergências sensíveis na literatura contemporânea acerca da construção de novos conceitos e das possibilidades estratégicas que advêm dos avanços no desenvolvimento da tecnologia da informação.

Em específico, no que concerne o nicho dos estudos sobre segurança cibernética, embora o debate acerca das potencialidades estratégicas do ciberespaço na qualidade de novo engenho de força à disposição dos Estados ainda esteja em estágio inicial, existem ao menos três pontos de atrito recorrentes.

A primeira zona de dissenso se preocupa em compreender se os confrontos contemporâneos refletem uma guerra cibernética já em curso (CORNISH, LIVINGSTONE, YORKE, 2010; CLARKE, KNAKE, 2010; SHAKARIAN, 2011; FARWELL, ROHOZINSKI, 2012; KELLO, 2013; WEEDON, 2015; PAVLIKOVA, 2016), ou se representam ruídos de baixa intensidade que não possuem poder disruptivo para romper com a dinâmica das relações interestatais, sejam cooperativas ou belicosas (LIBICKI, 2009, MOROZOV, 2009; WALT, 2010; BETZ, STEVENS, 2011; MAURER, 2011; LIFF, 2012; RID, 2012; LINDSAY, 2013; GARTZKE, 2013; GEERS, 2015, LINDSAY, CHEUNG, REVERON, 2015).

O segundo ponto de discussão se refere ao flagrante contraste entre as abordagens de matriz teórica liberal e realista do problema. Enquanto que a perspectiva liberal tende a buscar explicações que levam em consideração fatores éticos, relacionados à tendência de adoção de medidas de confiança mútua, incluindo a construção de instituições regulatórias capazes de restringir os movimentos dos Estados neste domínio (FRANZESE, 2009; IKENBERRY, 2010; ROWE, 2010; CHOUCRI, 2012; CHOUCRI, GOLDSMITH, 2012; JENKINS, 2013; BUTRIMAS, 2014; LILIENTHAL, AHMAD, 2015; JOSAN, 2015; MCKUNE, 2015; HAYDEN, 2016), o enfoque realista frisa a preponderância da anarquia do sistema internacional sobre a organização das relações interestatais, ressaltando que a busca por poder e riqueza continua a ocupar o centro da estratégia nacional (BETZ, STEVENS, 2011; LIFF, 2012; GARTZKE, 2013; LINDSAY, 2013).

O terceiro ponto de divergência se refere às potencialidades do uso do ciberespaço para causar danos físicos a um adversário. No tocante à magnitude dos riscos impostos pelas ameaças cibernéticas, há aqueles que as consideram altamente perigosas, enquanto outros procuram mitigar esse potencial; isto é, os primeiros

sustentam que a natureza oculta deste domínio faz dele uma ferramenta revolucionária para atenuar as distâncias que separam as potências dos demais Estados (CLARKE, KNAKE, 2010; CORNISH, LIVINGSTONE, YORKE, 2010; FARWELL, ROHOZINSKI, 2012; KELLO, 2013), já os segundos apontam para a disparidade no desenvolvimento tecnológico dos armamentos, influência diplomática e robustez econômica entre os Estados que compõem o sistema internacional, como fatores chave para o uso efetivo do ciberespaço na projeção de poder das grandes potências frente aos seus adversários (LIBICKI, 2009; BETZ, STEVENS, 2011; LIFF, 2012; LINDSAY, 2013; GARTZKE, 2013).

Frente ao contencioso, é ponto pacífico que o estudo das estratégias de atuação dos Estados, no tocante aos desafios que circundam o problema da segurança cibernética, tornou-se relevante para compreendermos como se estabelecem as disputas contemporâneas (FARWELL, ROHOZINSKI, 2012; KELLO, 2013; GEERS, 2015; LINDSAY, CHEUNG, REVERON, 2015; GALEOTTI, 2016), e, mais do que isso, o porquê o ciberespaço tornou-se fulcral para esses agentes.

Ao passo em que avança o debate acerca dos efeitos produzidos pela inserção de novas tecnologias da informação nas estratégias e modelos organizacionais adotados na dinâmica das disputas interestatais (BRENNER, 2011; 2013; DENNING, 2012; MAURER, 2013; BUTRIMAS, 2014; POLLPETER, 2015; STOKES, 2015; SHELDON, MCREYNOLDS 2015; ZHENG, 2015), cresce a demanda por pesquisas que apresentem uma compreensão apurada sobre o papel das instituições de segurança e defesa nacional e dos atores não-estatais nestes processos (MALIARCHUK, DANYK, BRIGGS, 2019; WEISS, JANKAUSKAS, 2019; DE OLIVEIRA, SVARTMAN, CASALUNGA, 2022). Uma vez que as potências têm buscado, cada vez mais, adquirir e inserir capacidades cibernéticas em seu planejamento estratégico, compreender como tais capacidades se integram à grande estratégia de ação dos Estados faz-se, igualmente, salutar (WEBER, 2018; DE OLIVEIRA, CASALUNGA, 2020; KAMINSKI, 2020; SIMONS, DANYK, MALIARCHUK, 2020; KUMAR, et al., 2022; WITHER, 2023).

Partindo da análise dos condicionantes que envolvem o processo de emprego da tecnologia da informação em conflitos regionais, esta pesquisa pretende testar a hipótese de que as operações cibernéticas são capazes de ampliar a assimetria de poder entre as grandes potências e seus adversários. Com esse intuito, o desenho de pesquisa utiliza abordagem qualitativa descritiva e explicativa para investigar a configuração de condições inerentes aos processos de emprego estratégico, operacional e tático das

tecnologias da informação para projeção de poder nacional nos conflitos desencadeados ao longo da última década entre: Estados Unidos e Irã; Rússia e Ucrânia; China e Índia com intuito de comparar os processos e construir uma teoria indutiva que indique as razões pelas quais as potências recorreram a este engenho de força durante os conflitos.

Para tanto, inicialmente, no primeiro capítulo desta tese, realizamos uma contextualização e revisão da literatura sobre o problema da segurança cibernética. Essa primeira aproximação do tema de pesquisa é sucedida, no segundo capítulo, por uma apresentação mais aprofundada das teorias que abordam o tema e da metodologia que utilizamos para embasar e suportar as inferências descritivas produzidas.

Isto posto, procedemos, nos capítulos subsequentes, com o exame de três estudos de caso-único atentos à historicidade que compõe as relações entre as potências e seus adversários; a mudança institucional nas forças de segurança e defesa nacional dos primeiros; e o uso pelos mesmos do ciberespaço em conflitos regionais. Por fim, no sexto capítulo realizamos uma comparação histórica dos resultados, seguida da explicação indutiva que responde ao questionamento central desta pesquisa.

Com a análise documental historiográfica dos principais documentos oficiais que versam sobre defesa e segurança das três potências mencionadas, verificaremos como se deu o processo de inserção do ciberespaço enquanto novo domínio de guerra na estratégia de atuação das grandes potências, mudança institucional considerada condição necessária para uso efetivo do ciberespaço com vistas à projeção de poder nacional em conflitos regionais.

Em sequência, procederemos com a análise das operações especiais desencadeadas durante os casos em destaque, com foco no exame do *modus operandi* das agências estatais e não-estatais, bem como das principais armas virtuais utilizadas. Desse modo, coletamos evidências que revelam como se deram os processos de exploração das vulnerabilidades de sistemas de informação e permitiram aos atacantes auferirem vantagens estratégicas sobre seus adversários, considerados suficientes para ampliar as capacidades de uso efetivo do ciberespaço nestes conflitos.

A mesma estratégia será aplicada a três estudos de caso distintos referentes a campanhas de reconhecimento e exploração de sistemas de informação, responsáveis pela consecução de ataques cibernéticos disruptivos, os quais atingiram setores de infraestrutura crítica no Irã (2007-2010); Ucrânia (2014-2015) e Índia (2020-2022). Em arremate, realizaremos uma análise comparativa histórica dos processos identificados para construção de uma teoria indutiva que permita oferecer uma resposta coerente e

razoável ao seguinte questionamento central: *Por que as grandes potências utilizaram o ciberespaço para conquistarem seus objetivos estratégicos?*

Nossa contribuição para o nicho de estudos sobre segurança cibernética será marcada pela identificação do funcionamento do mecanismo causal que constitui a trajetória de atuação conjunta -cinética e cibernética- de atores estatais e não-estatais, para a produção de sinergia nestes conflitos, doravante denominada simbiose -*hackers-forças armadas*-. Aspiramos, ainda, colaborar para o campo de Política Internacional e Defesa avançando o debate sobre a relevância do emprego da tecnologia da informação na estratégia da guerra híbrida, conforme aplicada pelas potências em conflitos regionais.

CAPÍTULO I

1. Contextualização e Revisão da Literatura

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, ambiente virtual composto por máquinas e usuários conectados em uma rede mundial militar e civil que lançou a humanidade na Era da Informação. Singer e Friedman (2014, p. 13-14) definem o 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.

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 revelam-se igualmente dispostas no ciberespaço. No entanto, diferentemente do mundo puramente físico, tais divisões estão em constante mutação, em larga medida, devido aos avanços produzidos pelo desenvolvimento das novas tecnologias de informação (SINGER, FRIEDMAN, 2014, p. 14-15).

Ao passo em que se transformou para além de suas características iniciais de uso, quais 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, 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, JANKAUSKAS, 2019).

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, 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 e a dissuasão com vistas à prevenção de riscos e contenção das ameaças (BETZ, 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 (APAs) (BETZ, STEVENS, 2011, WEEDON, 2015; OLSZEWSKI, 2018).

Nas últimas décadas, na medida em que reduzir os riscos e mitigar o potencial destrutivo dessas ameaças emergiu como uma das tarefas chave dos formuladores políticos, potências como a República Popular da China, os Estados Unidos da América e a Federação Russa iniciaram processos de mudança institucional com o objetivo de fortalecer as capacidades das entidades responsáveis pela defesa e a segurança nacional.

Sem embargo, documentos oficiais que tratam de aspectos relativos a estes campos, revelam que a percepção a respeito do ciberespaço difere entre ocidentais e orientais, -seja conceitos básicos e/ou questões normativas relativas à segurança cibernética- fator que gera dificuldades para a construção de medidas de confiança mútua e acordos entre os Estados (GILES, HAGESTAD, 2013; PAVLIKOVA, 2016).

As doutrinas que orientam as instituições coercitivas e acadêmicas de China e Rússia identificam desafios à segurança cibernética que são significativamente diferentes daqueles contidos nos documentos oficiais dos Estados Unidos. Além disso,

termos específicos que, a princípio se assemelham nos três idiomas, fazem alusão a conceitos distintos, o que dificulta, ainda mais, o estabelecimento de um diálogo profícuo entre as potências (GILES, HAGESTAD, 2013).

Noções como ciberespaço e guerra cibernética, por exemplo, contêm significados peculiares que variam de acordo com a percepção de cada potência acerca das dimensões que compõem este novo domínio. Enquanto, a compreensão holística Oriental classifica o ciberespaço como '*espaço da informação*'[1], zona que comporta não apenas os sistemas eletrônicos interconectados, mas, também, o nível psicossocial; o entendimento Ocidental é mais estreito e desconsidera a segunda dimensão, a definição se restringe ao aspecto mecânico no qual ocorre o intercâmbio de dados por meio de sistemas interconectados (GILES, HAGESTAD, 2013).

As idiossincrasias que permeiam a compreensão deste novo domínio levaram China, Estados Unidos e Rússia a abordarem o fenômeno da guerra cibernética de modo particular em seus documentos de segurança e defesa (PAVILKOVA, 2016). Compreendido na qualidade de campanhas militares orquestradas por Estados, grupos de Estados ou grupos políticos organizados contra alvos de infraestrutura cibernética na abordagem Oriental, o conceito dista do entendimento norte-americano que o descreve como a manifestação de ataques cibernéticos autorizados por atores estatais contra alvos de infraestrutura cibernética em conjunto com campanhas de governo (GILES, HAGESTAD, 2013).

Embora, a princípio pareçam similares, tais diferenças não são triviais se comparados o entendimento holístico mediante a incorporação de atores não-estatais, - grupos políticos organizados em campanhas militares-, permite uma combinação de forças militares e não militares em "operações nas redes de computadores; guerra eletrônica; operações psicológicas; operações de camuflagem" (PAVILKOVA, 2016, p. 5, tradução nossa) que não encontra paralelo na definição Ocidental de operações levadas à cabo por atores estatais que se utilizam, em sua totalidade, ou em partes, de meios cibernéticos para apoiar operações militares de intervenção em sistemas de informação dos adversários (GILES, HAGESTAD, 2013).

Em virtude disto, ao utilizarem o termo guerra cibernética em canais oficiais, russos e chineses o fazem em referência ao entendimento estrangeiro, uma vez que a

[1] Conforme o entendimento russo, compartilhado pela China, trata-se de um domínio "de atividade conectada com a formação, criação, conversão, transferência, uso e armazenamento de informação e que tem um efeito na consciência individual e social, na infraestrutura de informação e na própria informação" (GILES, HAGESTAD, 2013, p. 8).

ideia da guerra cibernética restrita a uma única dimensão é exígua na compreensão Oriental do fenômeno (GILES, HAGESTAD, 2013).

O quadro abaixo (Quadro 1) sumariza o entendimento das potências sobre estes conceitos:

Quadro 1. Definição dos conceitos pelas potências

	República Popular da China	Federação Russa	Estados Unidos da América
Ciberespaço	Espaço de informação onde se integram sistemas eletrônicos e o nível psicossocial (holístico).	Espaço de informação onde se integram sistemas eletrônicos e o nível psicossocial (holístico).	Espaço de integração de sistemas eletrônicos (mecânico).
Guerra cibernética	Campanhas militares orquestradas por Estados, grupos de Estados, ou grupos políticos organizados, contra alvos de infraestrutura cibernética.	Campanhas militares orquestradas por Estados, grupos de Estados, ou grupos políticos organizados, contra alvos de infraestrutura cibernética.	Ataques cibernéticos autorizados por atores estatais contra infraestrutura cibernética em conjunto com campanha de governo.

Fonte: elaborado pelo autor (2022).

Curiosamente, a despeito do caráter defensivo que o problema da segurança cibernética a priori estabeleça, as potências objeto deste estudo têm sido apontadas como protagonistas no uso do ciberespaço em ações ofensivas para projetar poder nacional. Dentre as mais diversas práticas, as ações mobilizam atores estatais e não-estatais para instalar artefatos maliciosos (*bombas lógicas*) em sistemas operacionais de Estados-alvos, para, assim, obterem vantagens estratégicas sob seus adversários em tempos de paz (CLARKE, KNAKE, 2010).

A Agência de Segurança Nacional (NSA) e o Comando Cibernético dos Estados Unidos (USCYBERCOM) são exemplos de instituições criadas com a missão de utilizar a tecnologia da informação como arma de guerra. De modo similar, novas estruturas organizacionais com semelhante missão foram constituídas a partir de instituições militares pré-existentes, respectivamente, no terceiro e no quarto departamentos do Exército de Libertação Popular (ELP), da China, e no Serviço Federal de Segurança (FSB) e Departamento Central de Inteligência (GRU), da Rússia (CLARKE, KNAKE, 2010; GEERS, 2015; LINDSAY, CHEUNG, REVERON, 2015).

> Não surpreendentemente, quando o governo dos Estados Unidos designou uma organização para fornecer a camada defensiva de nível superior contra ataques a sistemas de governantes militares e civis no final de 2007, ele escolheu não um serviço militar, mas uma agência de inteligência - NSA. Portanto, a guerra cibernética operacional deve ser realizada por agências de inteligência? Não necessariamente. Pode-se ignorar toda a questão sobre as autoridades legais. [...] basta dizer que os [agentes] militares e de inteligência podem ser bastante criativos ao permitir que ambos trabalhem juntos (LIBICKI, 2009, p. 155).

Diante desta dinâmica, compreender o papel do ciberespaço enquanto um novo engenho de força capaz de modificar os padrões tradicionais de ação das instituições estatais tornou-se uma questão relevante entre os acadêmicos e agentes responsáveis por examinar os movimentos das agências militares e civis neste novo domínio de disputa interestatal. No que tange as investigações analíticas, tal qual às diferenças presentes em documentos formais dos organismos estatais, acham-se divergências sensíveis quanto à definição do conceito de guerra cibernética entre aqueles que se dedicam a compreender sua funcionalidade e a ocorrência (CLARKE, KNAKE, 2010; LIFF, 2012).

O entendimento proposto por Liff (2012) é mais estreito e toma a guerra cibernética enquanto operações de ataque que contenham objetivos estratégicos políticos e/ou militares, excluindo campanhas de exploração de sistemas informacionais por meio de espionagem cibernética, crimes cibernéticos ou guerras psicológicas como características fundamentais. Por essa lógica, o fenômeno se manifesta pela presença de conflitos interestatais, nos quais ocorram ataques cibernéticos contra alvos de infraestrutura crítica civil ou militar com fins coercitivos, sejam eles: a consecução de objetivos estratégicos, obtenção de concessões políticas e/ou redução das capacidades de ação de um Estado-alvo mediante emprego da força física (LIFF, 2012).

Já, para Clarke e Knake (2010) a guerra cibernética se define de maneira mais ampla na qualidade de “ações de um estado-nação para penetrar nos computadores ou redes de outra nação com a finalidade de causar danos ou interrupção” (CLARKE, KNAKE 2010, p. 9). Para além da funcionalidade de seu uso como ferramenta facilitadora de ataques cinéticos mediante a inviabilização das defesas do inimigo, a definição inclui operações para subtração de informações de caráter relevante para as instituições coercitivas dos Estados.

A despeito das discordâncias, é ponto pacífico que as guerras cibernéticas atendem aos objetivos internos e externos presentes na grande estratégia dos Estados.

(CLARKE, KNAKE, 2010; LIFF, 2012). O quadro abaixo (Quadro 2) sumariza o entendimento dos autores acerca do conceito e da manifestação da guerra cibernética:

Quadro 2. Guerra cibernética e Manifestação

CONCEITO	LIFF (2012)	CLARKE, KNAKE (2010)
Guerra cibernética	Restrito: operações com objetivos estratégicos políticos e/ou militares. Não considera espionagem cibernética, crimes cibernéticos ou guerras psicológicas como características fundamentais.	Amplo: ações de um Estado para causar danos ou interrupção das redes de informação de um Estado-alvo. Considera a espionagem cibernética como parte do fenômeno.
Manifestação do fenômeno	Conflitos interestatais com ataques cibernéticos a setores de infraestrutura crítica civil ou militar, com fins coercitivos.	Conflitos interestatais com inviabilização das defesas de um Estado-alvo e/ou campanhas de subtração de informações relevantes para as instituições coercitivas dos Estados

Fonte: Elaborado pelo autor (2022)

Considerando o panorama conceitual descrito, verifica-se que as análises de casos representativos do uso do ciberespaço para obtenção de ganhos estratégicos substantivos por parte dos Estados contemporâneos, realizadas entre meados do século vinte e a primeira década do século vinte e um, foram marcadas por dissensos entre os acadêmicos no tocante à sua classificação enquanto guerra, bem como de sua inserção em um contexto estratégico mais amplo (LIBICKI, 2009, 2015; MOROZOV, 2009; CLARKE, KNAKE, 2010; CORNISH, LIVINGSTONE, YORKE, 2010; WALT, 2010; BETZ, STEVENS, 2011; MAURER, 2011; SHAKARIAN, 2011; FARWELL, ROHOZINSKI, 2012; LIFF, 2012; RID, 2012; KELLO, 2013; LINDSAY, 2013; GARTZKE, 2013; GEERS, 2015, LINDSAY, CHEUNG, REVERON, 2015; WEEDON, 2015; PAVLIKOVA, 2016).

Do início dos anos oitenta até o final da primeira década deste século o potencial da guerra cibernética para causar danos físicos ainda era pouco conhecido pelos acadêmicos, informações sobre as operações cibernéticas estavam restritas às organizações governamentais e às agências especializadas em inteligência, sendo apenas os crimes cibernéticos alvo de escrutínio público (MOROZOV, 2009).

Durante este período o insulamento de instituições governamentais especializadas em segurança cibernética foi compreendido, por alguns analistas, como

um processo de securitização com a finalidade de extrair benefícios estratégicos mediante a construção de um discurso baseado em riscos pouco prováveis de se concretizarem (MOROZOV, 2009). Essa preocupação se justificava, à época, devido à baixa ocorrência de ataques às infraestruturas críticas e a elevada frequência de ataques de espionagem via *spear phishing*[2] e *D-DoS*[3], razão pela qual as operações atribuídas às potências alvo deste estudo não puderam ser compreendidas em sua importância estratégica mais ampla.

Na ausência de evidências robustas capazes de demonstrar o potencial do ciberespaço, estabelecendo a ligação entre as operações cibernéticas e a guerra cinética interestatal, os ataques virtuais eram abordados como pouco atrativos para os Estados por não possuírem precisão calculável, sendo os efeitos colaterais de difícil previsão e sua utilização pouco estratégica, em grande medida, devido ao potencial limitado para causar danos ao adversário (MOROZOV, 2009).

Por este ângulo as operações cibernéticas atribuídas aos Estados Unidos, em 1982, que provocaram a explosão de um gasoduto da antiga União Soviética e o uso de *malwares*[4] durante a Guerra do Golfo, em 1991, para desabilitar os sistemas operacionais utilizados por militares iraquianos, não foram compreendidas por alguns analistas como atos de guerra em sentido estrito (BETZ, STEVENS, 2011).

De modo similar, os ataques atribuídos à Federação Russa com uso de *botnets*[5] que comprometeram a infraestrutura eletrônica de sistemas operacionais financeiros e de telecomunicação na Estônia, em 2007, bem como àqueles que atingiram sítios eletrônicos interrompendo a comunicação de políticos do alto escalão do governo da Geórgia, em 2008, não foram considerados atos de guerra, pois, não apresentavam danos substantivos e/ou vítimas fatais (BETZ, STEVENS, 2011).

De guisa equivalente, as campanhas atribuídas à RPC -'*Titan Rain*', '*Aurora*' e '*GhostNet*'- que atingiram alvos da rede pública e privada de diversos países do Ocidente, entre 2008 e 2010, resultando no roubo de um enorme volume de dados para

---

[2] *Spear phishing*: comunicação eletrônica direcionada a indivíduos, organização ou negócios específicos com intenção de instalar *malwares* espiões nos computadores dos alvos.

[3] *D-DoS:* negação de serviço, interrupção do tráfego normal de um servidor, serviço ou rede ao sobrecarregar o alvo ou sua infraestrutura com quantidade de tráfego acima do suportável pelo sistema.

[4] *Malware*: termo utilizado para designar um software projetado para interferir na funcionalidade do computador ou para degradar a integridade dos dados. Engloba uma gama de códigos de computador maliciosos -vírus, worms, trojan, spyware, adware, etc-. Pode ser projetado para fornecer acesso a um sistema de computador adversário, e/ou para atacá-lo (KELLO, 2013).

[5] *Botnet*: rede de computadores infectados por *malwares* que os controlam remotamente, espalhando vírus ou executando ataques cibernéticos sem ou com o consentimento de seus proprietários.

fins de inteligência militar e estratégica, foram classificadas como casos de espionagem cibernética (BETZ, STEVENS, 2011).

Em direção oposta, algumas análises sustentaram que as operações especiais norte-americanas para atingir sistemas de Comando e Controle (C2) do adversário, com vistas à obtenção de vantagens no emprego da força tradicional durante os conflitos entre norte-americanos e iraquianos (1991; 2003), deveriam ser abordadas como exemplos de guerra. Por esse prisma, consideraram, também, as campanhas russas e chinesas supracitadas, como exemplos do fenômeno, o qual não carecia, obrigatoriamente, ser ladeado por operações cinéticas (CLARKE, KNAKE, 2010)[6]. O quadro abaixo (Quadro 3) sumariza o dissenso na classificação dos casos:

Quadro 3. Classificação dos casos

CASOS	Rússia (1982) Explosão gasoduto	Iraque (1991; 2003) Sistemas operacionais militares de Defesa	Estônia (2007) Sistemas operacionais financeiros e telecomunicações	Geórgia (2008) Sistemas operacionais financeiros e telecomunicações	Estados Unidos (2008; 2010) Espionagem de instituições governamentais e empresas privadas
Consideram guerra cibernética	CLARKE, KNAKE (2010)	CLARKE, KNAKE (2010)	CLARKE, KNAKE (2010)	CLARKE, KNAKE (2010)	CLARKE, KNAKE (2010)
Não consideram guerra cibernética	BETZ, STEVENS (2011)	BETZ, STEVENS (2011)	BETZ, STEVENS (2011)	BETZ, STEVENS (2011)	BETZ, STEVENS (2011)

Fonte: Elaborado pelo autor (2022).

A despeito das divergências, por se tratar de um recurso empregado por atores estatais e/ou não-estatais com fins, formas e meios passíveis de análise objetiva mediante a descrição das operações e reações da defesa, se verificou que o fenômeno da guerra cibernética não poderia ser desconectado de sua relevância para a estratégia nacional dos Estados. Por essa perspectiva, se dispostos em um prisma analítico que

[6] As campanhas '*Titan Rain*' e '*GhostNet*' extraíram exabytes de dados de universidades, laboratórios industriais e instalações governamentais. Os segredos por trás de tudo, desde fórmulas farmacêuticas a projetos de bioengenharia, nanotecnologia, sistemas de armas e produtos industriais de uso diário, foram levados pelo ELP e por grupos de hackers privados para a China (CLARKE, KNAKE, 2010, p. 43).

levasse em consideração o contexto mais amplo, o ataque norte-americano da ‘bomba lógica’ ao gasoduto na Sibéria (1982), poderia ser compreendido como uma ação estratégica que fez uso de uma nova forma de guerra, até então sem paralelos na história, para reduzir as receitas e afetar o funcionamento da indústria militar russa, contendo o desenvolvimento tecnológico de seu adversário (CORNISH, LIVINGSTONE, YORKE, 2010).

De igual natureza, os ataques cibernéticos à Estônia (2007) e Geórgia (2008) revelavam um padrão semelhante de ação da Federação Russa para produção de retornos crescentes em seu entorno regional. Seja paralisando as capacidades de funcionamento dos sistemas de tecnologia da informação para causar danos financeiros às instituições privadas e aos indivíduos, como nos ataques à Tallinn, ou combinando a guerra cibernética com o uso de forças cinéticas para obter vantagens no campo de batalha nos confrontos pela Abkhazia e Ossétia do sul, o ciberespaço contribuiu para a grande estratégia de controle dos avanços da Organização do Tratado do Atlântico Norte (OTAN) sobre os territórios fronteiriços da Rússia (CORNISH, LIVINGSTONE, YORKE, 2010).

Outrossim, as campanhas que resultaram na decodificação de dados sigilosos subtraídos de instituições governamentais, militares e privadas, contribuíram, sobremaneira, para a produção chinesa de novas tecnologias de uso dual derivadas da apropriação indevida de propriedade intelectual norte-americana. Tais ações modificaram o jogo da espionagem interestatal possibilitando retornos estratégicos tangíveis em escala inimaginável para os padrões tradicionais que, até então, pressupunham o deslocamento de agentes em espaços físicos em suas missões (CORNISH, LIVINGSTONE, YORKE, 2010).

Destarte, o debate em torno da compreensão do fenômeno da guerra cibernética e sua relevância estratégica mais ampla, colocou em xeque o alcance explicativo dos conceitos tradicionais sobre a guerra, o papel das forças armadas e a incidência de atores não estatais capazes de atuar em conflitos interestatais via ciberespaço.

Frente às divergências, parte dos acadêmicos adere à tese de que o fenômeno da guerra cibernética não apenas é factível, como simboliza o resultado do poder disruptivo que a revolução técnica e tecnológica exerce sobre as capacidades e meios que os Estados contemporâneos dispõem para o conflito (CORNISH, LIVINGSTONE, YORKE, 2010; CLARKE, KNAKE, 2010; SHAKARIAN, 2011; FARWELL, ROHOZINSKI, 2012; KELLO, 2013), enquanto que uma segunda vertente o

compreende com ceticismo, sustentando que o emprego de tais capacidades se restringe aos Estados que dominam a tecnologia necessária para operar no ciberespaço, estando os demais entes sujeitos à lógica das consequências estratégicas impostas pelo sistema internacional, sendo, portanto, a guerra cibernética um acontecimento extraordinário (LIBICKI, 2009, 2015; WALT, 2010; MAURER, 2011; BETZ, STEVENS, 2011; LIFF, 2012; RID, 2012; GARTZKE, 2013; LINDSAY, 2013; GEERS, 2015; LINDSAY, CHEUNG, REVERON, 2015).

Considerando as definições convencionais de conflito, ao investigarem a ampla gama de possibilidades de emprego da tecnologia da informação para degradar capacidades militares, invadir redes de infraestrutura crítica, realizar crimes e espionar um adversário em relação à segurança dos sistemas que controlam as infraestruturas críticas, as abordagens céticas questionam, sobretudo, a existência da guerra cibernética (WALT, 2010; MAURER, 2011; RID, 2012).

De modo geral, os céticos identificam um potencial reduzido dos ataques cibernéticos para causar danos ao adversário, sendo assim ao utilizarem o ciberespaço para consecução de objetivos estratégicos os Estados necessitam de forças adicionais capazes de garantir efeitos duráveis. A guerra cibernética seria, portanto, insuficientemente letal para ser compreendida como tal (MAURER, 2011; BETZ, STEVENS, 2011; RID, 2012).

O potencial reduzido das armas cibernéticas para causar danos aos adversários impede sua classificação como um conflito armado entre Estados ou uma guerra cibernética; isto é, ao levar em consideração a probabilidade de ocorrência de um fenômeno em função dos interesses dos agentes, com base na lógica das consequências[7], se questiona a hipótese de que os conflitos desencadeados no ciberespaço constituam, de fato, uma guerra (GARTZKE, 2013).

Visto com ceticismo, o ciberespaço é compreendido como um recurso de menor grandeza se comparado ao uso de forças convencionais para coagir e/ou dominar o adversário. Por essa perspectiva, a conexão entre a guerra cibernética e as formas tradicionais de uso da força é chave para que os Estados possam produzir força sinérgica e atingir objetivos estratégicos, sendo a guerra no ciberespaço relevante para

[7] O pessimismo cibernético se baseia fortemente nas capacidades (meios), sem se preocupar com uma lógica de consequências (fins) que o acompanhe. Muito do que poderia acontecer no mundo deixa de ocorrer, em grande parte porque aqueles que podem agir não discernem nenhum benefício significativo em iniciar um determinado ato (GARTZKE, 2013, p. 54).

entes com reconhecidas capacidades que precisam lidar com adversários mais fracos (GARTZKE, 2013).

Trata-se de um fenômeno singular e restrito aos Estados que possuem instituições robustas com capacidades para organizar campanhas cibernéticas combinadas com ações tradicionais de emprego da força para alcançar objetivos estratégicos a custos reduzidos, em grande medida, porque as potências detêm recursos pré-existentes substantivos para manejar os riscos do fracasso e sustentar os ganhos dos sucessos dessas campanhas (LINDSAY, 2013).

De modo que a concepção cética toma o ciberespaço não como um domínio revolucionário, mas evolucionário, pois, ainda que produza efeito em um conflito, os danos não serão estrategicamente decisivos para que os Estados fracos façam frente aos atores de maior poder e influência no sistema internacional (GARTZKE, 2013).

Em suma, ao abordar a guerra cibernética como uma dimensão da guerra em processo de evolução restrita às potências dominantes do sistema internacional, o entendimento cético coloca dúvidas sobre a tese do poder disruptivo da revolução técnica e tecnológica. Razão pela qual, o fenômeno precisaria cumprir as funções convencionais das forças tradicionais para ser útil aos Estados (LINDSAY, 2013; GARTZKE, 2013).

Todavia, análises aderentes à tese da revolução técnica e tecnológica contestam as premissas céticas que desconsideram as ameaças cibernéticas com base em seu baixo potencial para causar danos ao adversário, fator que impediria sua classificação enquanto ato de guerra (KELLO, 2013).

Embora reconheçam parte da explicação dada ao problema da segurança cibernética que frisa a impossibilidade de que a inclusão deste novo engenho de força altere a natureza ou os meios da guerra, Kello (2013) duvida de seu alcance para responder questões que envolvam uma perspectiva mais ampla que considere o potencial das ameaças cibernéticas para causarem danos diretos e indiretos capazes de perturbar a defesa nacional e/ou a ordem internacional.

Por este ângulo, a inserção do domínio cibernético teria potencial para afetar os padrões de competição e segurança entre os Estados, os quais precisam ser considerados pelos acadêmicos que tencionam compreender o fenômeno da guerra cibernética e explicar as razões pelas quais as potências recorrem ao ciberespaço para consecução de objetivos estratégicos (KELLO, 2013).

Em relação à análise dos conflitos recentes, ambas as perspectivas realistas convergem ao frisar as insuficiências analíticas dos modelos propostos por abordagens tecnicistas que intentam compreender o fenômeno do uso do ciberespaço por agentes estatais e não-estatais em conflitos, sem levar em conta aspectos geopolíticos fundamentais que constituem as dinâmicas de interação interestatal.

Destarte, de acordo com a perspectiva cética, por deterem expertise técnica que poucos Estados dispõem para combinar o emprego da força física às ações cibernéticas, potências como China, Estados Unidos e Rússia têm maiores incentivos a fazerem uso do ciberespaço para explorar as vulnerabilidades de sistemas de informação complexos que lhes forneçam vantagens estratégicas na consecução de seus objetivos geopolíticos (LINDSAY, 2013).

Não obstante, os aderentes à tese da revolução técnica e tecnológica ponderam que a diversidade de atores operando neste domínio têm potencial para abalar os modelos teóricos clássicos de competição entre as grandes potências, razão pela qual, as três supracitadas contam com estratégias direcionadas ao controle de ameaças cibernéticas avançadas, fator que as tornam capazes de preparar e executar operações tanto defensivas quanto ofensivas em conjunto com forças tradicionais (KELLO, 2013).

O quadro abaixo (Quadro 4) sumariza a divisão entre os realistas sobre a existência da guerra cibernética:

Quadro 4. Conflitos cibernéticos recentes

Consideram a existência do fenômeno (revolução cibernética)	CORNISH, LIVINGSTONE, YORK, 2010; CLARKE, KNAKE, 2010; SHAKARIAN, 2011; FARWELL, ROHOZINSKI, 2012; KELLO, 2013; WEEDON, 2015; PAVLIKOVA, 2016
Não consideram a existência do fenômeno (céticos)	LIBICKI, 2009; MOROZOV, 2009; WALT, 2010; BETZ, STEVENS, 2011; MAURER, 2011; LIFF, 2012; RID, 2012; LINDSAY, 2013; GARTZKE, 2013; GEERS, 2015; LINDSAY, CHEUNG, REVERON, 2015

Fonte: elaborado pelo autor (2022).

Em linhas gerais, os céticos defendem que os ataques às infraestruturas críticas são raros devido aos problemas que podem produzir ao mundo físico em termos de conflitos declarados entre os Estados. Assim sendo, ao definir a guerra cibernética como o uso de redes de computadores para atacar às infraestruturas físicas de um oponente com objetivo de auferir retornos estratégicos, os céticos sustentam que o fenômeno torna-se vantajoso somente para os entes que se encontram na vanguarda do

desenvolvimento da tecnologia da informação e contam com forças convencionais suficientes para garantir a defesa de seu território em caso de uma declaração de guerra (LIFF, 2012; GARTZKE, 2013; LINDSAY, 2013).

Já, os favoráveis a perspectiva da revolução técnica e tecnológica propõem uma interpretação holística dos fenômenos cibernéticos, pois, certificam que o menor potencial de impacto violento das armas cibernéticas é uma característica que contribui, não apenas para aumentar a gama de possibilidades de ação dos atores internacionais, mas para repensar o alcance do poder explicativo das teorias tradicionais formuladas com base em conceitos insuficientes para interpretar a realidade contemporânea (CLARKE, KNAKE, 2010; CORNISH, LIVINGSTONE, YORKE, 2010; FARWELL, ROHOZINSKI, 2012; KELLO, 2013).

Frente a este significativo debate que se insere no bojo dos estudos que abordam o problema fundamental da segurança cibernética, no que concerne às análises das ações orquestradas via ciberespaço com vistas à consecução de objetivos estratégicos, grupos com alto grau de especialização, capacidade de adaptação e recursos caracterizados como APAs[8] se destacam como objeto elementar (GARTZKE, 2013; KELLO, 2013; LINDSAY, 2015; LINDSAY, CHEUNG, REVERON, 2015; GEERS, 2015; KOVAL, 2015; WEEDON, 2015; OLSZEWSKI, 2018; WEISS, JANKAUSKAS, 2019).

Tais ameaças pertencem a uma nova geração que utilizam o ciberespaço para subtrair informações sigilosas que possam ser repassadas a terceiros ou mesmo utilizadas pelos setores de inteligência dos Estados (GARTZKE, 2013). De tal modo que, as APAs de menor potencial de impacto, como aquelas especializadas em espionagem cibernética e ataques moderados às infraestruturas críticas, despontam como estrategicamente mais atrativas aos Estados que pretendem fazer uso do ciberespaço para alcançar seus objetivos estratégicos (LINDSAY, 2015).

Frente ao cenário, análises das operações destes grupos e das armas cibernéticas utilizadas na última década têm revelado não apenas a complexidade que envolve a utilização do ciberespaço para atingir objetivos estratégicos, mas, também, o alto grau

[8] A origem do termo remete à Força Aérea norte-americana (2006), que a compreende como ataques cibernéticos realizados por atores estatais proveniente de forças militares. No entanto, essa visão passou por revisões na medida em que novos casos registrados nas últimas décadas apresentaram evidências do envolvimento, não apenas de instituições militares, mas, também, de atores não-estatais, como grupos *hackers* organizados sob as diretrizes estratégicas dos Estados (WEISS, JANKAUSKAS, 2019). Embora, "originalmente utilizada para descrever invasões cibernéticas contra organizações militares, a APA evoluiu e não está mais confinada às forças armadas" (OLSZEWSKI, 2018, p. 5).

de inteligência para acessar as vulnerabilidades das infraestruturas críticas alvo. As evidências indicam a presença de atores institucionais com maior capacidade e recursos para oferecer suporte às ações dos *hackers* (GERRS, 2015; KOVAL, 2015; WEEDON, 2015).

Por conseguinte, a construção de padrões regulatórios capazes de enquadrar as ações delas se tornou um desafio para a comunidade internacional. Ante a impossibilidade de classificá-las como vetores de iniciação de um conflito bélico nos moldes tradicionais, em grande parte, devido às implicações imediatas para a segurança internacional que resultariam dessa identificação, são descritas como atos de "espionagem cibernética, ou atividades criminosas cibernéticas mais perigosas" (BEQUEREL, 2013, *apud* OLSZEWSKI, 2018, p. 5).

As APAs encontram-se, portanto, no cerne do debate do fenômeno da guerra cibernética, são grupos que possuem vínculos estreitos com as forças armadas dos Estados, seja para aquisição de inteligência, obtenção de dados sigilosos ou comprometimento de sistemas de infraestrutura crítica (OLSZEWSKI, 2018). Representam, pois, atores estatais e não-estatais tais como: espiões, *hackers*, criminosos e terroristas cibernéticos, os quais atuam em esquemas altamente organizados, capazes de orquestrar ataques sofisticados sem que sua presença seja notada até que a ação tenha ocorrido e os danos causados (WEISS, JANKAUSKAS, 2019).

Nota-se que o potencial para contornar possíveis sanções internacionais que resultariam de ações convencionais de uso da força, fez das APAs ferramentas alternativas atraentes para os Estados perseguirem objetivos estratégicos. Razão pela qual, elas têm sido utilizadas com frequência pelas potências alvo deste estudo para impactar de modo negativo as capacidades de defesa de um Estado-alvo. Por essa lógica, as ações das APAs objetivam atingir alvos específicos via ciberespaço com intenção de subtrair dados e informações que permitem ao agressor obter vantagens sobre seus adversários.

As operações envolvem o trabalho de especialistas em tecnologia da informação capazes de explorar vulnerabilidades de sistemas de informação complexos, usando ataques multivetoriais com uma variedade de ferramentas que permitem o acesso a dados sigilosos de empresas e instituições governamentais em campanhas conduzidas por longos períodos, sem que a presença dessas ameaças possa ser detectada (OLSZEWSKI, 2018).

Contudo, na ausência de arranjos institucionais robustos capazes de coordenar as ações, mediante linhas de autoridade e comunicação bem estruturadas que impeçam que os agentes decidam atuar por conta própria, os efeitos produzidos pelas APAs podem fugir ao controle (KELLO, 2013). Nesse sentido, a mobilização efetiva de atores não-estatais via ciberespaço depende da manutenção da autoridade dos Estados sobre as operações (WEISS, JANKAUSKAS, 2019)[9].

Contudo, nas últimas décadas, as instituições necessárias para dar cabo do problema da segurança cibernética, foram vinculadas a uma série de ações cibernéticas ofensivas (MANDIANT, 2013; CROWDSTRIKE 2014; 2015; 2016; 2018; FIREEEYE 2014; 2015; 2016; 2017; F-SECURE LABS, 2014; 2016; LOOKINGGLASS, 2015; ICS-CERT, 2016; E-ISAC, 2016; RECORDED FUTURE 2017; 2021; 2022; CYFIRMA, 2020a; 2020b)[10].

Sem embargo, a guerra cibernética provocada pela estratégia de utilização de atores estatais e não-estatais em ações conjuntas que multiplicam as capacidades de projeção de poder nacional dos Estados parece estar circunscrita à grande estratégia de emprego da guerra híbrida, que delimita os espaços de conflito interestatais regionais e os insere em um contexto político mais amplo de disputas entre as potências pela hegemonia no sistema internacional.

Inicialmente formulado por Hoffman (2007), o conceito de guerra híbrida orientou o entendimento acadêmico e das organizações internacionais dedicadas ao estudo da interconexão entre as ações dos agentes estatais e não-estatais em conflitos sucedidos no início do presente século. Capaz de descrever, em parte, a composição da guerra contemporânea abordando a crescente sofisticação e complexificação da atuação dos atores não-estatais em conflitos internos, o conceito desconsiderava o papel do Estado como ator estratégico fundamental.

Kjennerud e Cullen (2016) ampliaram essa concepção e dividiram os instrumentos de poder em categorias: militar, política, econômica, civil e informacional, para identificar a relevância de sua utilização sincronizada e coordenada pelos Estados.

---

[9] A manutenção do controle hierárquico na delegação de autoridade às agências responsáveis pela contenção das ameaças cibernéticas é fundamental, sendo os arranjos de governança institucional fator chave para os Estados que pretendem se proteger dos riscos e ameaças deste novo domínio (WEISS, JANKAUSKAS, 2019).

[10] Dentre as principais instituições estatais reconhecidas por envolvimento em operações cibernéticas ofensivas, se destacam: a NSA e o USCYBERCOM norte-americanas, a FAGCI, o FSB e o GRU russas; o terceiro e quarto departamentos do ELP e o Ministério de Segurança do Estado (MSE) chinesas, atuando em conjunto com as APAs.

> A guerra híbrida do Estado envolve a plena integração dos meios militares e não-militares com o poder do Estado para alcançar objetivos políticos, nos quais o uso da força desempenha um papel central. Estados com habilidades altamente centralizadas para coordenar e sincronizar seus instrumentos de poder (governo, economia, mídia, etc.) podem criar efeitos multiplicadores de força sinérgica (KJENNERUD, CULLEN, 2016, p. 1).

Na qualidade de guarda-chuva teórico, o conceito de guerra híbrida permite considerar a guerra cibernética como um recurso que se insere em um contexto mais amplo que englobe as capacidades estratégicas dos Estados para organizar e coordenar as operações e táticas militares em conjunto com a das APAs, com vistas a atingir sistemas de informação e/ou infraestrutura crítica de seus adversários e, assim, produzir "mudanças no estado comportamental ou físico de um sistema ou elementos do sistema, de acordo com objetivos políticos" (KJENNERUD, CULLEN, 2016, p. 1).

Compreendido desta forma, o conceito de guerra híbrida pode ser operacionalizado para elucidar as razões políticas que se encontram por detrás do emprego da tecnologia da informação pelas potências nos conflitos contemporâneos, ao destacar o protagonismo dos Estados sobre as operações de guerra cibernética, marcado pela coordenação de atividades adaptáveis e flexíveis capazes de produzir força sinérgica para consecução de objetivos estratégicos a nível regional e internacional (DE OLIVEIRA, CASALUNGA, 2020).

Diante do exposto, tendo em consideração a primazia dos Estados que se encontram na vanguarda do desenvolvimento das tecnologias da informação no uso do ciberespaço para consecução de objetivos estratégicos, esta pesquisa busca operacionalizar os conceitos de guerra cibernética e da guerra híbrida para compreender como e porque o ciberespaço se tornou um domínio chave para as disputas interestatais entre potências e seus adversários regionais na última década deste século.

Com tal propósito, os três estudos de caso sobre os conflitos desencadeados nas últimas décadas entre os Estados Unidos da América e o Irã (2007-2010), a Federação Russa e a Ucrânia (2014-2015), a República Popular da China e a Índia (2020-2022) foram examinados a fim de demonstrar as condições sob as quais o fenômeno da guerra cibernética se manifesta, bem como sua relevância para a grande estratégia das potências para projetar poder sobre seus adversários em conflitos regionais.

De maneira que, ao conectarmos as implicações políticas do processo de mudança institucional, pelo qual passaram as estratégias que orientam as instituições

securitárias estatais, aos momentos críticos que levaram ao uso do ciberespaço em conflitos regionais, sustentamos que as condições de ocorrência da guerra cibernética refletem não apenas o potencial das ameaças cibernéticas para causar danos físicos, mas, fundamentalmente, as capacidades adquiridas nas últimas décadas por instituições securitárias para utilizarem um domínio de guerra com vistas à projeção de poder nacional sem incorrer no escalonamento dos conflitos.

Destarte, a partir da análise dos processos que envolveram as campanhas de reconhecimento e exploração de sistemas de informação, e de operações ofensivas que atingiram componentes responsáveis pelo funcionamento de setores de infraestrutura crítica iranianos, ucranianos e indianos, identificamos o mecanismo que proporcionou o uso efetivo da guerra cibernética para produzir retornos estratégicos crescentes[11] às potências do sistema internacional supracitadas.

Cientes de que os efeitos da conexão entre as APAs, unidades de reforço de capacidade militarizadas e os serviços de inteligência nos conflitos sob escrutínio merecem maior atenção dos estudos de Política Internacional e Defesa, em arremate, propomos uma teoria indutiva original que revela por quais razões as potências recorreram a este novo engenho de força para consecução de seus objetivos estratégicos, lacuna que escapa ao alcance analítico das teorias existentes.

Nossa análise dos processos em destaque intenta responder ao questionamento central desta pesquisa tendo por base os postulados teóricos e os pressupostos metodológicos que compõem o desenho de pesquisa apresentado no capítulo seguinte.

[11] O conceito de retornos crescentes ajuda a identificar padrões sequenciais específicos de tempo, pequenos eventos que podem ter grandes consequências, cursos de ação uma vez iniciados impõem alto custo para reversão [...] A probabilidade de ocorrer novas etapas no mesmo caminho aumenta a cada movimento nesse caminho. Isso ocorre porque os benefícios relativos da atividade atual em comparação com outras opções possíveis aumentam com o tempo (PIERSON, 2000, p. 251-252).

CAPÍTULO II

2.1. Referencial Teórico

Neste capítulo abordaremos algumas das divisões teóricas que envolvem os estudos sobre o problema da segurança cibernética, com ênfase na discussão que se estabelece no bojo da matriz teórica realista sobre as potencialidades do ciberespaço para afetar os adversários e influenciar nas dinâmicas interestatais de disputa por poder, fundamental para reforçar a pertinência de nosso teste de hipótese, bem como estabelecer um modelo teórico original que permita identificar por quais razões as potências recorreram a este engenho de força durante os conflitos desencadeados na última década.

O debate constituído em torno do problema que se dá em função da forma como os Estados contemporâneos encaram os riscos e ameaças que permeiam o ciberespaço, suscita divergências sensíveis entre teóricos realistas e liberais dedicados ao estudo das potencialidades deste novo domínio para afetar as disputas de poder interestais (IKENBERRY, 2010; CHOUCRI, 2012; GARTZKE, 2013; LINDSAY, 2013; KELLO, 2013; MCKUNE, 2015).

A matriz teórica realista se propõe a discutir os novos dilemas de segurança sob o prisma da competição interestatal por poder e influência, tendo em consideração o uso do ciberespaço como um novo engenho de força à disposição dos Estados. Já, os liberais focam no crescimento da interdependência e medidas de confiança mútua, como fatores preponderantes para a manutenção da segurança e do equilíbrio nas relações internacionais.

Se, por um lado, o argumento liberal sustenta que a robustez das instituições domésticas e internacionais produz incentivos para proteção do fluxo das informações, bem como a cooperação na construção de normas regulatórias capazes de conter não apenas as ameaças comuns, como o terrorismo e grupos transnacionais, mas, também, o ímpeto dos Estados neste domínio (FRANZESE, 2009; IKENBERRY, 2010; ROWE, 2010; BUCHAN, 2012; CHOUCRI, 2012; JENKINS, 2013; BUTRIMAS, 2014; LILIENTHAL, AHMAD, 2015; MCKUNE, 2015; HAYDEN, 2016). Por outro, os realistas sustentam que a natureza anárquica do sistema internacional impele os Estados a construir medidas individuais para garantir a segurança cibernética interna que são vistas com desconfiança por seus pares, tal dinâmica produz incentivos a uma corrida

armamentista nos moldes tradicionais que restringe as ameaças cibernéticas não em função da existência de interesses consensuais, mas da possibilidade, implícita, de retaliação em caso de reconhecimento de um ataque (GARTZKE, 2013; KELLO, 2013; LINDSAY, 2013).

Sem embargo, ao identificar que a constante recusa por parte dos Estados em admitir o envolvimento de suas instituições em campanhas cibernéticas orquestradas nas últimas décadas, tem impedido a construção de medidas de confiança mútua com base no estabelecimento de normas regulatórias internacionais, uma vez que a atividade neste domínio é "intencionalmente projetada para ser indetectável" (LINDSAY, CHEUNG, REVERON, 2015, p. 343), as abordagens realistas têm oferecido explicações mais pertinentes sobre as razões que impulsionam as potências a utilizarem o ciberespaço para consecução de uma gama de objetivos estratégicos.

Destacam-se estudos sobre o envolvimento de instituições de inteligência em campanhas de espionagem cibernética, ataques disruptivos a setores de infraestrutura crítica, desenvolvimento econômico e indústria de defesa, até medidas extremas como a anexação de territórios (GEERS, 2015; INKSTER, 2015; KOVAL, 2015; LIMNNÉL, 2015; MAURER, 2015; LINDSAY, CHEUNG, 2015; STOKES, 2015; WEEDON, 2015).

Partindo do pressuposto 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 permite um enquadramento capaz de decodificar os fenômenos recentes que envolvem o uso deste novo engenho de força por parte das potências contemporâneas (CORNISH, LIVINGSTONE, YORKE, 2010; CLARKE, KNAKE, 2010; FARWELL, ROHOZINSKI, 2012; GARTZKE, 2013; KELLO, 2013; LINDSAY, 2013; 2015; LINDSAY, CHEUNG, REVERON, 2015; GEERS, 2015; LIMNNÉL, 2015; WEEDON, 2015; PAVLIKOVA, 2016; OLSZEWSKI, 2018).

No entanto, estas abordagens são marcadas por clivagens que os levam a abordar o problema da segurança cibernética com base em pressupostos distintos. Uma importante divergência que se estabelece no bojo dessa matriz teórica refere-se à investigação das potencialidades do uso do ciberespaço para atenuar as distâncias que separam as potências dos demais Estados (CLARKE, KNAKE, 2010; CORNISH, LIVINGSTONE, YORKE, 2010; FARWELL, ROHOZINSKI, 2012; KELLO, 2013) ou

ampliá-las (LIBICKI, 2009, 2015; BETZ, STEVENS, 2011; LIFF, 2012; LINDSAY, 2013; GARTZKE, 2013).

Diante deste debate, acadêmicos aderentes às teses da revolução cibernética[12] assumem três pressupostos sobre a inserção do ciberespaço enquanto novo engenho de força a disposição dos Estados, que incentivam os agentes agressores e dificultam a defesa: i) oferece vantagens *avant la lettre* aos entes mais fracos; ii) primazia da ofensiva e conflitos de autoridade; iii) sem efeito dissuasório e ausência de mecanismos regulatórios.

O primeiro pressuposto está baseado em dois princípios basilares: i) quanto mais dependente da tecnologia da informação forem os setores militar e civil, maior será a quantidade de espaços vulneráveis passíveis de serem explorados por ataques cibernéticos; ii) dificuldades na identificação dos autores dos ataques (CLARKE, KNAKE, 2010; CORNISH, LIVINGSTONE, YORKE, 2010; KELLO 2013).

Considerando o grande número de vetores de acesso aos sistemas de informação, os teóricos da revolução cibernética frisam que as ameaças podem permanecer ocultas por longos períodos sem que seja notada qualquer alteração no funcionamento dos sistemas e/ou conhecimento sobre os alvos do ataque. De modo que a defesa tem de se preocupar com uma vasta gama de possibilidades, enquanto os atacantes podem focar em procedimentos de entrada específicos para infectar sistemas e/ou redes operacionais de infraestrutura crítica e/ou institucionais de governo, fator que eleva, consideravelmente, os custos da defesa contra um ataque cibernético (KELLO, 2013).

No entanto, a abordagem cética sustenta que um exame apurado da realidade objetiva coloca dúvidas sobre este princípio. Visto por outro ângulo, embora Estados com alto grau de desenvolvimento tecnológico possuam mais pontos de risco, é preciso levar em consideração que para atingir com sucesso sistemas de informação complexos são necessárias capacidades institucionais, técnicas e organizacionais robustas que demandam capital humano altamente especializado, fatores que não se encontram à disposição de adversários mais fracos (LIFF, 2012).

---

[12] Pontos centrais da teoria da revolução cibernética: i) favorece o mais fraco: atores mais fortes apresentam mais vulnerabilidades na medida em que possuem mais sistemas conectados ao ciberespaço, comunidades de atores fracos podem usar o domínio em anonimato evitando retaliação; ii) domínio da ofensiva: as capacidades ofensivas se modificam rapidamente, as defesas levam mais tempo para serem construídas, agencias governamentais e privadas disputam autoridade sobre o funcionamento e a segurança dos sistemas de infraestrutura crítica; iii) sem efeito dissuasório: o anonimato capacita atores fracos, identidades podem ser forjadas e os ataques podem partir de diversas jurisdições organizacionais internacionais (LINDSAY, 2013, p. 14-17).

Devido à baixa capacidade de que dispõem as instituições tradicionais de Estados tecnologicamente atrasados, sejam militares, econômicas ou diplomáticas para oferecer respaldo às ações neste domínio, estes entes precisariam vencer barreiras significativas para obter vantagens substantivas mediante o uso do ciberespaço para infringir danos efetivos a Estados mais fortes (GARTZKE, 2013).

Em referência ao segundo princípio que versa sobre o problema da atribuição (negação possível), tendo em vista que o uso de atores não-estatais pode evitar implicações diretas aos entes que as mobilizam, os teóricos da revolução cibernética sustentam que essas ameaças constituem ferramentas importantes para os Estados contemporâneos (CLARKE, KNAKE, 2010; CORNISH, LIVINGSTONE, YORKE, 2010).

Neste sentido, ao verificarem a relevância do ciberespaço enquanto substituto viável para ações táticas de difícil detecção que permitam ganhos estratégicos crescentes, os Estados passaram a mobilizar atores estatais e não-estatais organizados para atuar neste domínio, adicionando uma nova dimensão de interação entre os agentes e as instituições governamentais e privadas ao problema da segurança cibernética que escapa ao escopo analítico da abordagem cética (KELLO, 2013).

Em resposta, os céticos adicionam que a dificuldade de obtenção de retornos estratégicos de uma ação que não pode ser creditada ao seu promotor, limita o número de Estados que possam fazer uso dessas ameaças em conflitos. Logo, os defensores da teoria revolucionária falham ao desconsiderar os obstáculos que o invasor enfrenta para conseguir obter efeitos positivos de uma agressão realizada via ciberespaço, a menos que existam ações paralelas em outros domínios que lhe ofereçam respaldo (GARTZKE, 2013).

Compreendidos desta forma, os ataques cibernéticos se restringem à condição de ferramenta para romper as redes de defesa do adversário e oferecer vantagem tática e estratégica às operações convencionais. Por essa razão, somente Estados com reconhecidas capacidades para combinar ações podem transformar ganhos temporários construídos via ciberespaço em retornos crescentes e duradouros (LIFF, 2012).

O segundo pressuposto está ancorado nos seguintes princípios: i) baixo custo para adquirir e utilizar as armas cibernéticas em um ataque, se comparado à construção de defesas que garantam a segurança dos sistemas de informação e das redes críticas; ii) ataques sofisticados são difíceis de prever, sendo tarefa árdua a coordenação

interagências para conter a execução de um ataque cibernético devido à velocidade que os eventos sucedem (CORNISH, LIVINGSTONE, YORKE, 2010; KELLO, 2013).

Em relação ao primeiro princípio, os teóricos da revolução cibernética sustentam que o ciberespaço amplia o poder de atores mais fracos, pois, a exemplo daquelas empregadas em campanhas de espionagem e/ou para atingir alvos físicos causando danos significativos a sistemas de informação, as armas virtuais oferecem um retorno consideravelmente alto se comparado ao custo necessário de seu desenvolvimento e uso frente à baixa probabilidade de represálias (CORNISH, LIVINGSTONE, YORKE, 2010).

Em contraposição, os céticos consideram os custos associados à organização de um ataque cibernético efetivo: dificuldades operacionais; necessidade de pessoal com alto nível de conhecimento; grau de efemeridade das armas cibernéticas, como fatores que favorecem a defesa e desestimulam ataques realizados por atores não-estatais que não possam contar com capacidades convencionais substantivas para subsidiar as operações (LIBICKI, 2009; BETZ, STEVENS, 2010; LIFF, 2012; GARTZKE, 2013; LINDSAY, 2013).

De acordo com esta perspectiva, conhecer os pontos vulneráveis do inimigo é fundamental para o sucesso de um ataque cibernético. Razão pela qual, a fase preparatória da guerra no ciberespaço demanda recursos humanos e materiais ostensivos para obtenção de informações sobre as vulnerabilidades dos alvos e conectá-las às capacidades operacionais militares (LIBICKI, 2009).

Por este ângulo, a primazia da ofensiva é abordada em relação à ampla gama de circunstâncias que facilitam ou dificultam um ataque. Logo, se por um lado as operações cibernéticas militares têm potencial para interromper linhas de comunicação e afetar, temporariamente, a mobilização das tropas inimigas, por outro para serem bem-sucedidas necessitam de esforços de inteligência proporcionais à complexidade dos alvos. De maneira que, a propensão de ocorrência de um conflito cibernético será maior quando os impeditivos à conquista forem mais frágeis (LINDSAY, 2013).

Portanto, de acordo com os céticos se o princípio de que o equilíbrio entre ofensiva e defensiva pesa em favor dos primeiros estivesse correto, poderíamos esperar um grande número de casos de manifestação do fenômeno da guerra cibernética. Entretanto, a maior incidência de casos já registrados provém de ‘ataques irritantes’ capazes de provocar efeitos de baixa intensidade que diferem, significativamente, da magnitude predita pela teoria da revolução cibernética. Assim, a relativa ausência de

ataques disruptivos de alta intensidade indica que as defesas dos sistemas de infraestrutura crítica são menos vulneráveis do que pressupõem os adeptos da revolução cibernética (LINDSAY, 2013).

Ademais, a possibilidade de construção de armas de ataque contribui para que essas potências desenvolvam capacidades defensivas de suas redes, outra vantagem importante sobre os adversários que não se encontram no mesmo patamar de maestria em desenvolvimento e uso das tecnologias da informação (BETZ, STEVENS, 2010).

Em função da grande variabilidade e complexidade das armas cibernéticas, bem como das operações de lançamento, os céticos sustentam que a ocorrência dos ataques será proporcional ao custo relativo às fases de construção e preparação das operações e dos artefatos. Portanto, seria delicado supor que Estados tecnologicamente deficitários as pudessem empregar de modo eficaz para espionar e/ou afetar o funcionamento das infraestruturas críticas de Estados mais fortes (LINDSAY, 2013).

No tocante ao segundo princípio, de acordo com os teóricos da revolução cibernética, as defesas de sistemas de infraestrutura crítica das grandes potências ocidentais são operadas em sua maior parte por empresas privadas, um setor fragmentado que impõe dificuldades para estabelecer parâmetros capazes de coordenar a construção de defesas de modo uníssono com base em diretrizes governamentais para controle das ameaças (KELLO, 2013).

Todavia, em direção contrária os céticos ponderam que, uma vez utilizadas, as armas cibernéticas alertam o adversário sobre as vulnerabilidades existentes nos sistemas operacionais infectados, sendo a mobilização das agências securitárias, sejam nacionais e/ou internacionais, em conjunto com o setor privado, para corrigir os problemas, diretamente proporcional ao prejuízo causado. Isso faz com que o recurso cibernético de alto fator de impacto se configure numa opção efetiva apenas quando utilizado pela primeira vez (GARTZKE, 2013).

Ao considerarem que a gravidade da ação realizada via ciberespaço delimita o esforço e os investimentos que serão feitos em coordenar os movimentos interagências para encontrar as origens e os responsáveis pelos ataques, os céticos reiteram que grande parte dos ataques cibernéticos permanecem em anonimato porque não causam danos significativos que exijam esforços substantivos em investigação forense (LINDSAY, 2013).

De modo que os conflitos no ciberespaço parecem respeitar uma dinâmica de interação entre os Estados que leva em consideração, não apenas as capacidades para

causar dano ao adversário, mas a justificativa para a tomada de decisão em comparação com os custos da adoção de outros mecanismos de ação estratégica (GARTZKE, 2013). Em síntese, existem duas características que corroem a lógica do pressuposto da primazia da ofensiva: i) o dano é recuperável em curto espaço de tempo; ii) a revelação de uma arma cibernética degrada sua utilidade (LIBICKI, 2009; LIFF, 2012).

Depreende-se da primeira característica que, no longo prazo, os ataques cibernéticos já registrados não possuem grande potencial para alterar o equilíbrio de poder entre os Estados, salvo em casos em que as operações estejam associadas às formas de guerra tradicional. De modo que ataques cibernéticos isolados produzem efeitos efêmeros que podem ser recuperados em curto espaço de tempo, sendo insatisfatórios para forçar concessões sobre adversários com superior capacidade militar convencional (LIFF, 2012).

Em relação à segunda, os atacantes precisam ponderar com cautela as possibilidades de emprego das armas cibernéticas, pois, uma vez explorada a vulnerabilidade de um sistema de informação (*dia-zero*), espera-se que sejam erguidas defesas capazes de conter um novo ataque similar. Essa é uma das razões para que se espere que os ataques combinados - cibernéticos e cinéticos - sejam mais úteis para produzir efeitos sinérgicos (LIBICKI, 2009).

O último pressuposto se apoia nos seguintes princípios que dificultam a coerção das ameaças: i) ausência de acordos regulatórios que inibam as ações no ciberespaço; ii) possibilidade de lançamento de ataques cibernéticos de diferentes pontos geográficos que não necessariamente serão àqueles do agressor (CORNISH, LIVINGSTONE, YORKE, 2010; FARWELL, ROHOZINSKI, 2012).

De acordo com os teóricos da revolução cibernética, a ausência de regulação internacional que defina limites aos Estados para atuarem de modo ofensivo no ciberespaço pavimenta o caminho para que códigos maliciosos sejam utilizados de forma recorrente em disputas interestatais. Por conseguinte, o caráter enigmático das operações cibernéticas parece afetar a natureza política da guerra, na medida em que contribui para que os Estados alcancem seus objetivos estratégicos sem que para isso precisem destruir o inimigo (FARWELL, ROHOZINSKI, 2012).

> A história ensina que, uma vez que a tecnologia de armas se torna viável, os Estados a implantam. Hoje o mundo pode enfrentar uma perigosa corrida tecnológica caracterizada por armas em rápida evolução e letais [...] parece que o engajamento Estado-Estado, atendendo ou não às definições convencionais de uso da força ou ato

> de guerra, irá definir uma nova realidade e requerer novos cálculos estratégicos (FARWELL, ROHOZINSKI, 2012, p. 114-116).

Por esta perspectiva, o problema da atribuição impacta negativamente na dissuasão na medida em que os atacantes se esquivam de sanções internacionais ao emprego da força que de outro modo seriam inevitáveis. Tendo em vista, por um lado, a dificuldade de detecção das ameaças cibernéticas e, por outro, o incremento na possibilidade de construção de armas virtuais sofisticadas capazes de produzir efeitos diretos e indiretos de difícil previsão -proporcionado pelo desenvolvimento da tecnologia da informação-, o domínio cibernético cria complicações importantes para a defesa que não podem ser compreendidas com ceticismo (KELLO, 2013).

Frente a este desafio, os céticos apresentam fatores que reduzem a probabilidade da proliferação de ataques cibernéticos, tais como: a incerteza sobre as ramificações do ataque que podem sair do controle e ferir os interesses do atacante e a dificuldade em conhecer o real potencial da defesa adversária. Logo, a eficácia da dissuasão depende menos de marcos regulatórios que contenham as ameaças virtuais, do que das incertezas quanto às capacidades de que dispõem os Estados para retaliar seus agressores em caso de danos severos aos sistemas de informação (LIFF, 2012).

Em relação ao segundo princípio, os teóricos da revolução cibernética sustentam que devido à transcendência dos limites geográficos que a rede mundial de computadores alcançou nas últimas décadas, tornou-se impossível para os Estados exercer controle total sobre este espaço. Em razão disso, a possibilidade de lançamento de ataques multivetoriais via ciberespaço não apenas elimina as fronteiras geográficas que separam os adversários, como, também, amplia os pontos de contato entre o agressor e os alvos. Outrossim, o uso de *proxies* como as redes privadas virtuais podem acobertar atacantes criando uma zona cinzenta que dificulta a identificação das origens do ataque (CORNISH, LIVINGSTONE, YORKE, 2010; KELLO, 2013).

Em resposta ao problema da atribuição, devido às inúmeras possibilidades que o ciberespaço oferece para mascarar as ações dos atacantes, seja pelo uso de identidades e/ou credenciais falsificadas, arquivos corrompidos, redes privadas e criptografia que permitem o lançamento de ataques cibernéticos de diversas áreas geográficas, os céticos reforçam que as medidas para encontrar as causas desses ataques serão proporcionais à gravidade do dano causado. Por essa lógica, ataques disruptivos que conduzam à interrupção de sistemas de infraestrutura crítica devem atrair substancial atenção dos organismos internacionais e setores da iniciativa privada, entidades com recursos

suficientes para conduzir investigações minuciosas capazes de classificar a origem, o modo de operação das ameaças e as armas utilizadas com alto nível de precisão (GARTZKE, 2013; LINDSAY, 2013).

Não obstante, a compreensão abrangente das causas e consequências estratégicas que envolvem um ataque cibernético capaz de comprometer setores de infraestrutura crítica industrial revela a importância da dissuasão não apenas para inibir um adversário mais fraco de realizar um ataque cibernético disruptivo, conforme estabelecido pela teoria da revolução cibernética, mas, principalmente, para conter ações desproporcionais de uso da força por parte de atacantes com poderio bélico robusto. Por esse prisma, ataques cibernéticos disruptivos podem, inclusive, impedir o escalonamento de conflitos, uma vez que os atores políticos ponderem seu uso de modo discreto e efetivo *vis-à-vis* operações cinéticas convencionais de maior risco (GARTZKE, 2013; LINDSAY, 2013).

Novamente os céticos ponderam que, se a dissuasão não fosse possível, casos de ataques cibernéticos efetivos empregados por adversários com capacidades militares inferiores contra setores de infraestruturas críticas de grandes potências seriam recorrentes. No entanto, ocorre o inverso, a grande maioria dos ataques já registrados produziram efeitos modestos, salvo nos casos em que foram utilizados por potências contra adversários tecnologicamente vulneráveis, nenhum deles foi capaz de comprometer o funcionamento de setores de infraestrutura crítica (LINDSAY, 2013).

O quadro abaixo (Quadro 5) sumariza a divisão entre os teóricos realistas sobre as potencialidades do uso do ciberespaço nos conflitos contemporâneos.

Quadro 5. Potencialidades do uso do ciberespaço

Reduz a assimetria de Poder entre os Estados (revolução cibernética)	CLARKE, KNAKE, 2010; CORNISH, LIVINGSTONE, YORKE, 2010; FARWELL, ROHOZINSKI, 2012; KELLO, 2013
Amplia a assimetria de Poder entre os Estados (céticos)	LIBICKI, 2009, 2015; BETZ, STEVENS, 2011; LIFF, 2012; LINDSAY, 2013; GARTZKE, 2013

Fonte: elaborado pelo autor (2022).

De acordo com os teóricos da revolução cibernética, a ausência de regularidade intencional e de lógicas de interação estáveis ou conhecidas faz com que as ações cibernéticas se desviem dos padrões rotineiros de competição que caracterizam a anarquia internacional. Por conseguinte, a interpretação cética estaria restrita às dificuldades impostas ao enquadramento dos danos e dos resultados produzidos através

do domínio cibernético, sob a luz de conceitos limitados de guerra e paz (KELLO, 2013).

> Embora a revolução cibernética não tenha alterado fundamentalmente a natureza da guerra, ela tem consequências para questões importantes no campo dos estudos de segurança, incluindo ameaças estrangeiras não militares e a capacidade de atores não tradicionais de infligir danos econômicos e sociais (KELLO, 2013, p. 8).

Partindo do entendimento de que em um sistema anárquico a segurança dos Estados depende da capacidade de organizar suas interações, com base em regras e princípios de conduta que ofereçam um grau razoável de previsibilidade das ações, estes teóricos defendem o caráter revolucionário da tecnologia da informação sobre a ordem das relações interestatais, devido ao impacto causado pela inserção de atores não-estatais nesta dinâmica (CLARKE, KNAKE, 2010; CORNISH, LIVINGSTONE, YORKE, 2010; FARWELL, ROHOZINSKI, 2012; KELLO, 2013).

De modo que, os modelos da vertente revolucionária consideram a magnitude dos efeitos produzidos pelo impacto das armas cibernéticas não apenas em alvos físicos, mas, fundamentalmente, nas estratégias de atuação dos Estados contemporâneos. Por essa lógica, o ciberespaço é compreendido como um domínio que pode introduzir instabilidade nas relações internacionais (KELLO, 2013).

Em contrapartida, ao encararem com desconfiança a identificação das capacidades destes atores, bem como dos efeitos que podem ser produzidos mediante o emprego do ciberespaço nos conflitos interestatais, realistas céticos questionam as premissas dedutivas da teoria da revolução cibernética que restam ancoradas em inferências construídas a partir de uma compreensão peculiar da natureza da tecnologia da informação que expõe vulnerabilidades da defesa e superdimensionam o potencial destrutivo das ameaças (BETZ, STEVENS, 2011; LIFF, 2012; GARTZKE, 2013, LINDSAY, 2013).

Os pilares que sustentam a teoria da revolução cibernética foram erigidos sobre a ideia equivocada de que o ciberespaço e as tecnologias da informação utilizadas para operar sistemas interconectados são permeáveis e permissivas, porém, quando consideradas as consequências lógicas que circundam as ações neste domínio, a trajetória percorrida entre as fases de preparação, operação e coleta dos benefícios de um ataque cibernético disruptivo pode ser mais complexa do que supõem os teóricos da revolução cibernética. Em virtude disso, o alto custo das operações capazes de atingir

alvos estratégicos de modo discreto e efetivo, é considerado fator chave para limitar a possibilidade de uso deste domínio por Estados tecnologicamente desprivilegiados (LIBICKI, 2009; LIFF, 2012; GARTZKE, 2013; LINDSAY, 2013).

Tomando por base a discussão exposta, podemos observar que o problema da segurança cibernética tem provocado inconsistências e divergências teóricas significativas entre os realistas partidários e céticos da tese da revolução cibernética.

No que tangencia aos propósitos analíticos desta pesquisa, que se estabelecem em consonância com as discussões que se encontram na fronteira dos estudos sobre o problema em destaque, depreende-se que a inserção de atores não-estatais nas disputas interestatais via ciberespaço suscita alterações no comportamento das instituições securitárias, civis e militares, que extrapolam as explicações tradicionais calcadas em concepções tradicionais dos fenômenos de guerra e paz (CLARKE, KNAKE, 2010; KELLO, 2013).

Não obstante, é improvável supor que esta nova dinâmica contorne as consequências lógicas que compõem as disputas interestatais, restando o entendimento que se comprova por evidências de que o ciberespaço, até então, não se mostrou capaz de reduzir as assimetrias de poder entre as potências e os adversários mais fracos, muito pelo contrário, antes de tudo tem se demonstrado um domínio reservado aos poderosos, útil para ampliá-las (GARTZKE, 2013; LINDSAY, 2013).

Todavia, ambas as abordagens teóricas falham ao desconsiderarem a relevância de um exame aprofundado das condições que permitem o uso do ciberespaço para projeção de poder nacional, bem como da identificação do mecanismo que permite a constituição das operações cibernéticas ofensivas capazes de produzir efeitos cinéticos disruptivos no mundo físico. Diante dessa lacuna, faz-se *mister* a produção de estudos de caso empíricos capazes de explorar em profundidade o seu funcionamento, revelando os procedimentos e as razões que se encontram por detrás dos processos de sua utilização em conflitos regionais.

Frente ao desafio, nossa análise comparativa descritiva e explicativa propõe a construção de uma teoria indutiva que tem por objetivo desatar os nós analíticos presentes nos estudos de Política Internacional e Defesa, que buscam compreender os fenômenos da guerra cibernética e da guerra híbrida, com base nos procedimentos metodológicos que serão detalhados na seção seguinte.

2.2. Metodologia

O desenho de pesquisa descrito nesta seção tem por objetivo fornecer as ferramentas substanciais para que possamos responder ao questionamento central: Por que as grandes potências -China, Estados Unidos e Rússia- utilizaram o ciberespaço para conquistar seus objetivos estratégicos?

Fundamentados pela literatura que será apresentada, testaremos a hipótese de que as operações de emprego da tecnologia da informação nos conflitos sob escrutínio ampliam a assimetria de poder entre as potências e seus adversários regionais.

Nossa análise do fenômeno da guerra cibernética lança luz sobre o funcionamento do mecanismo que conecta o uso da tecnologia da informação ao processo de mudança pelo qual passaram as instituições responsáveis pela segurança e defesa nacional de Estados Unidos, China e Rússia nas últimas décadas, denominado simbiose *hackers-forças armadas*.

A partir do exame de documentos oficiais[13] e relatórios produzidos por empresas especializadas em segurança cibernética[14], de modo específico, objetivamos: i) demonstrar como o processo de mudança permitiu a incorporação do ciberespaço na qualidade de novo domínio de guerra às estratégias de atuação das instituições securitárias a serviço das potências em destaque; ii) verificar como estes processos proporcionaram a constituição de operações especiais que envolveram a ação de atores estatais e não-estatais em campanhas de reconhecimento e exploração de sistemas de informação que culminaram em ataques cibernéticos disruptivos sobre setores de infraestrutura crítica durante os conflitos desencadeados entre os Estados Unidos e o Irã (2007-2010); Rússia e Ucrânia (2014-2015); e China e Índia (2020-2022); Estados Unidos e Irã (2010; 2019); Rússia e Ucrânia (2014-2015); iii) construir uma teoria indutiva original, à luz dos estudos dos casos supracitados, que permita identificar as

[13] Fontes primárias examinadas: **Estados Unidos da América**: Estratégia Nacional para Proteção do Ciberespaço (2003); Estratégia de Segurança Nacional (2006; 2010; 2015) Estratégia Nacional de Defesa (2008; 2011; 2015); Estratégia Cibernética do Departamento de Defesa (2015); **Federação Russa**: Doutrina Militar (2010; 2014); Estratégia de Segurança Nacional (2009; 2015); **República Popular da China**: Estratégia de Defesa Nacional (2009; 2011); Emprego Diversificado das Forças Armadas (2013); Estratégia Militar (2015); Defesa Nacional na Nova Era (2019). Todos os documentos originais em língua nativa, mandarim, russo e inglês estão disponíveis *on-line* e foram traduzidos para o português com ajuda da ferramenta 'Google Tradutor'.

[14] Fontes secundárias examinadas: MANDIANT (2013); CROWDSTRIKE (2014; 2015; 2016; 2018); FIREEEYE (2014; 2015; 2016; 2017); F-SECURE LABS (2014; 2016); LOOKINGGLASS (2015); SISTEMA DE CONTROLE INDUSTRIAL PARA CIBER EMERGÊNCIAS (ICS-CERT) (2016); CENTRO DE ANÁLISE E COMPARTILHAMENTO DE INFORMAÇÕES (E-ISAC) (2016); RECORDED FUTURE (2017; 2021; 2022); CYFIRMA (2020a; 2020b).

razões pelas quais a guerra cibernética tornou-se parte substantiva do empenho da grande estratégia de guerra híbrida dessas potências em disputas por poder e influência regional.

Para tanto, utilizamos em conjunto às técnicas qualitativas de análise comparativa histórica e rastreamento de processos para coletar e agrupar evidências que permitam verificar como se constitui o fenômeno de nosso interesse (HALL, 2006; 2012; BENNET, 2010; COLLIER, 2011; MAHONEY, 2012; BENNET, CHECKEL, 2014; FALLETI, MAHONEY, 2015; FALLETI, 2016)[15].

Inicialmente, a aplicação do rastreamento de processos requer a especificação da estrutura conceitual, sob a qual operacionalizamos nosso entendimento da guerra cibernética conforme descrito no capítulo 1, somada à identificação de regularidades empíricas resultantes de sua observação que permitam estabelecer a conexão causal entre as condições que serão verificadas. Desse modo, o componente descritivo da série de momentos específicos que marcaram as principais etapas do processo é o ponto angular que robustece a análise da mudança e sequência dos eventos sob investigação.

> Os testes nem sempre são fáceis de aplicar. Portanto, pode ser produtivo começar com uma boa narrativa ou com um tempo que lista a sequência de eventos. Pode-se, então, explorar as ideias causais embutidas nas narrativas, considerar os tipos de evidência que podem confirmar ou desconfirmar essas ideias e identificar os testes apropriados para avaliar essas evidências (COLLIER, 2011, p. 828-829).

Nesse sentido, delimitamos duas condições, uma necessária e outra suficiente, envolvendo inferência descritiva com base, respectivamente, nos princípios de singularidade e certeza[16].

No tocante à condição de necessidade, com base nos documentos oficiais verificaremos a mudança realizada nas instituições militares mediante a observância de fatores como: crescimento dos investimentos em pesquisa e desenvolvimento de novas tecnologias da informação, fomento à constituição de novas agências de comando

[15] O rastreamento de processos sistematiza a análise qualitativa a partir de uma perspectiva capaz de explicar relações causais mediante a observação de como determinadas condições produzem um fenômeno social (CDIPP, 2015). Trata-se de uma ferramenta útil para extrair inferências descritivas e causais a partir de evidências compreendidas como parte de uma sequência temporal de eventos ou fenômenos (COLLIER, 2011).

[16] Esses princípios indicam se a evidência coletada é necessariamente sólida para confirmar a hipótese de singularidade (*uniqueness*) fomentada; e, se a evidência é suficiente para sustentar a certeza (*certainty*) da hipótese levantada, sendo então possível descartar explicações alternativas (BEACH; PEDERSEN 2013; BEFANI; MAYNE 2014, *apud* CDIPP, 2015, p. 4).

especializadas em segurança cibernética e a incorporação da iniciativa privada ao conjunto de setores responsáveis pela segurança no ciberespaço.

O teste de necessidade pressupõe que uma evidência ou observação específica do processo causal deve estar presente para que uma hipótese seja válida, entretanto, a confirmação por si só não é suficiente para confirmar o argumento hipotético dedutivo que orienta a investigação empírica. Para tanto, é preciso identificar os processos causais observáveis (PCOs), embora falhar no teste de suficiência não a elimine como ocorre com o teste de necessidade (MAHONEY, 2012).

> Em resumo, os testes de rastreamento de processo baseiam-se em informações sobre o mecanismo como base para inferência causal. Embora os testes geralmente não sejam realizados de forma explícita, eles geralmente são usados implicitamente por analistas que trabalham na pesquisa de histórico comparativa e de estudo de caso [...] Os testes de rastreamento de processo projetados para inferência causal sempre exigem que o analista localize e utilize mecanismos. Sem localizar PCOs que incorporam informações sobre mecanismo, não se pode usar testes de rastreamento de processo para ajudar a estabelecer se um evento causa outro (MAHONEY, 2012, p. 583-586).

Em relação à condição de suficiência, verificaremos o *modus operandis* das principais ameaças cibernéticas em operações conjuntas, orquestradas por forças de segurança e defesa nacional, para atingir setores críticos de seus adversários. Concomitantemente, mediante a identificação do funcionamento do mecanismo causal que conecta a mudança institucional às operações em tela, pontuamos os efeitos do uso deste novo domínio da guerra nas capacidades de projeção de poder nacional das potências em conflitos regionais.

Em síntese, através da análise das fontes secundárias descreveremos estes processos com atenção ao funcionamento do mecanismo que conecta o fenômeno observado (Y: *guerra cibernética*) à causa inicial (X: *mudança institucional*). Desse modo, "as observações do processo causal (PCOs) são usadas em conjunto com uma generalização mais ampla relevante para o caso em análise" (COLLIER; BRADY; SEAWRIGHT, 2010, *apud* MAHONEY, 2012, p. 571).

De acordo com a lógica inferencial construída, se a mudança no modo de operação das forças militares das três potências for suficiente para produzir o fenômeno de nosso interesse, igualmente o será para o funcionamento do mecanismo em destaque, vetor observável do impacto da tecnologia da informação para consecução de objetivos estratégicos das potências nestes conflitos. Logo, ao avaliarmos a plausibilidade do

mecanismo “a suposição é que se X realmente é suficiente para Y, também deve ser (de acordo com a lógica elementar) suficiente para todos os mecanismos intervenientes necessários para Y” (MAHONEY, 2012, p. 580).

O quadro abaixo (Quadro 6) sumariza os testes que serão aplicados para construção de nosso argumento hipotético-dedutivo:

Quadro 6. Testes de Hipótese Condicional

Condição Necessária Mudança institucional (*estratégia nacional de defesa e segurança*)	Investimentos em programas de desenvolvimento de tecnologia da informação; criação de novas agências especializadas em segurança cibernética; incorporação da iniciativa privada aos setores responsáveis pela segurança do ciberespaço.
Condição Suficiente Simbiose (*hackers-forças armadas*)	Campanhas estratégicas, operações e táticas de uso do ciberespaço para ataques coordenados entre atores estatais e não-estatais aos setores de infraestrutura crítica e alvos institucionais.
Hipótese Configuração de condições (*necessária e suficiente*)	Vantagens estratégicas que ampliam a assimetria de poder entre as potências frente a seus adversários regionais

Fonte: Elaborado pelo autor (2022).

No que concerne à consecução dos objetivos estratégicos regionais, consideramos que o conceito da dependência da trajetória[17], ajuda a compreender como se deram os processos de incorporação da dimensão cibernética nos documentos oficiais que regulam a ação das instituições militares especializadas em segurança cibernética destes Estados, bem como da simbiose *hackers-forças armadas* (atuação conjunta - cinética e cibernética- de atores estatais e não-estatais) para a produção da dinâmica de retornos crescente, a partir do uso do ciberespaço nestes conflitos.

Por este prisma, mediante a explicação de como as instituições “produzem esses trajetos, como elas estruturam a resposta de uma dada nação a novos desafios” (HALL; TAYLOR, 2003, p. 200) intentamos demonstrar que o processo causal observado é dependente da trajetória de emprego da guerra híbrida, por parte das potências que recorrem ao ciberespaço para atuar em seu entorno regional.

[17] O conceito delimita que “[...] uma vez que o Estado começa um movimento os custos de reversão são altos, existem outros pontos de escolha, mas o novo arranjo institucional impede um retorno fácil para o ponto inicial” (PIERSON, 2000, p. 252).

O ponto chave para compreensão destes processos resta, portanto, na relação que se estabelece através da interdependência da matriz institucional observada e a concepção de produção de retornos crescentes (PIERSON, 2000) aplicadas ao campo da Política Internacional e Defesa. De maneira que, a mudança institucional juntamente à simbiose configurem as condições que permitem a identificação do impacto exercido pelo emprego da tecnologia da informação nos conflitos (COLLIER, 2011; MAHONEY, 2012).

A partir da verificação destas condições, realizaremos, por fim, uma análise comparativa histórica dos casos em tela para construção de uma teoria indutiva capaz de responder ao questionamento central desta pesquisa (FALLETI, MAHONEY, 2015).

À vista disso, ao avaliar como as estratégias de ação do Estado são induzidas por mudanças nas diretrizes oficiais que organizam os parâmetros estratégicos, táticos e operacionais das agências responsáveis pela segurança e defesa das potências analisadas esta pesquisa se vincula ao quadro analítico do institucionalismo histórico[18].

Combinadas as técnicas de análise qualitativa proporcionam elementos fundamentais à construção da explicação indutiva que deverá contribuir para o campo de estudos sobre Política Internacional e Defesa avançando o debate sobre a relevância da guerra cibernética para a estratégia de guerra híbrida aplicada pelas potências em conflitos regionais.

[18] No mesmo espírito, numerosos teóricos dessa escola tendem a distinguir no fluxo dos eventos históricos períodos de continuidade e "situações críticas", vale dizer, momentos nos quais mudanças institucionais importantes se produzem, criando desse modo "bifurcações" que conduzem o desenvolvimento por um novo trajeto. O principal problema consiste evidentemente em explicar o que provoca as situações críticas, e em geral os teóricos insistem no impacto das crises econômicas e dos conflitos militares (HALL, TAYLOR, 2003, p. 201).

CAPÍTULO III

O capítulo considera as nuances da relação américo-irananiana em torno do conflito desencadeado por conta do programa nuclear do Irã, como ponto de partida para explicar o fenômeno da guerra cibernética. Com intuito de verificar "como as instituições produzem esses trajetos, como elas estruturam a resposta de uma dada nação a novos desafios" (HALL, TAYLOR, 2003, p. 200) procuramos responder ao seguinte questionamento: Como os Estados Unidos utilizaram o ciberespaço para consecução de objetivos estratégicos regionais?

Ao conectarmos as implicações do processo de mudança institucional pelo qual passaram as forças de segurança e defesa dos Estados Unidos, aos momentos críticos que culminaram na eclosão do conflito regional américo-iraniano (2006-2010), nossa análise identifica as condições que proporcionaram o uso efetivo e discreto do ciberespaço para consecução de objetivos estratégicos. Consideramos, pois, necessárias alterações nas diretrizes que orientam as instituições securitárias para constituição de operações especiais que, por sua vez, são suficientes para maximizar as capacidades de projeção do poder nacional frente a um adversário estratégico[19].

Conter o programa nuclear iraniano e, assim, evitar que o país consiga obter acesso a armas de destruição em massa (ADMs) que poderiam abalar o equilíbrio estratégico securitário no Oriente Médio se converteu em objetivo estratégico declarado nos EUA na primeira década deste século (DE FALCO, 2012; ISIS, 2012; SANGER, 2012; NAKASHIMA, WARRICK, 2012; JOLLEY, 2013; BAEZNER, ROBIN, 2017).

Frente à dinâmica, a espionagem cibernética emerge como opção valiosa para promover os interesses nacionais. Conforme veremos, a criação de incentivos a constituição de operações conjuntas, envolvendo campanhas de reconhecimento e exploração de redes de computadores e ataques cibernéticos disruptivos, indica não somente o nível de desenvolvimento do aparato científico e tecnológico norte americano, mas, sobretudo, a eficiência institucional em utilizar novos domínios de guerra para ampliar a assimetria de poder em conflitos regionais.

[19] Nosso exame das condições inerentes ao emprego da tecnologia de informação em operações ofensivas para atingir setores de infraestrutura crítica dá-se com base em fontes primárias (documentos oficiais) e secundárias (acadêmico-científicas, relatórios, jornais).

3.1. Conflito américo-iraniano: contexto político
[Conteúdo indisponível, divulgação no Lume prevista para 29/11/2024]

3.2. Mudança institucional: a transformação das forças de segurança e defesa norte americanas para incorporar o ciberespaço como novo domínio de guerra
[Conteúdo indisponível, divulgação no Lume prevista para 29/11/2024]

3.3. Guerra Cibernética: o emprego da tecnologia da informação no conflito Estados Unidos - Irã (2007-2010)
[Conteúdo indisponível, divulgação no Lume prevista para 29/11/2024]

3.4. Considerações Finais
[Conteúdo indisponível, divulgação no Lume prevista para 29/11/2024]

CAPÍTULO IV

O capítulo considera as nuances da relação russo-ucraniana em torno do conflito desencadeado após o movimento Euromaidan organizado na praça central de Kiev contra o governo Yanukovych, como ponto de partida para explicar o fenômeno da guerra cibernética. Com intuito de verificar "como as instituições produzem esses trajetos, como elas estruturam a resposta de uma dada nação a novos desafios" (HALL, TAYLOR, 2003, p. 200) procuramos responder ao seguinte questionamento: Como a Rússia utilizou o ciberespaço para consecução de objetivos estratégicos regionais?

Conter o processo de alargamento das instituições securitárias e comerciais promovidos pela UE e a OTAN e, assim, manter parte da Ucrânia sob sua esfera de influência regional se converteu em objetivo estratégico declarado da Federação Russa na segunda década deste século (MATUSZAK, 2012; BARATA, 2014; MEARSHEIMER, 2014; MIELNICZUK, 2014; GEERS, 2015; MAURER, 2015; WEEDON, 2015; MEYERS, 2016).

Frente à dinâmica, a espionagem cibernética emerge como opção valiosa para promover os interesses nacionais. Conforme veremos, a criação de incentivos a constituição de operações conjuntas, envolvendo campanhas de reconhecimento e exploração de redes de computadores e ataques cibernéticos disruptivos, indica não somente o nível de desenvolvimento do aparato científico e tecnológico russo, mas, sobretudo, a eficiência institucional em utilizar novos domínios de guerra para ampliar a assimetria de poder em conflitos regionais.

4.1. Conflito russo-ucraniano: contexto político

A presente seção tem a pretensão de compreender, de modo breve, a dinâmica política que colocou os interesses russos e ucranianos em rota de colisão, para isso são consideradas as nuances que constituem a historicidade das relações entre estes dois Estados, frente a um panorama mais amplo da Política Internacional.

Sem embargo, em 1985, com a nomeação de Mikhail Gorbachev ao cargo de Secretário-Geral do Partido Comunista da URSS, dá-se o início de uma série de

reformas estruturais promovidas com o intuito de recuperar a economia soviética dos efeitos da disputa geopolítica do período da Guerra Fria (NUNES, 2021).

A implementação destas reformas provocou, entretanto, atritos entre os setores conservadores e os liberais do Partido Comunista (PC), em parte, devido aos incentivos que as políticas da '*perestroika*' (reestruturação) e '*glasnost*' (transparência) exerciam para descentralização do poder administrativo e abertura da econômica (REMPEL, 1996; PONS, 2014).

Boris Yeltsin, que havia liderado setores da indústria soviética por mais de dez anos, foi nomeado, em 1986, primeiro-secretário do PC, vindo a integrar o Politburo, comitê executivo do PC. Yeltsin se transformou em uma das principais referências da ala liberal do Partido. Sua rápida ascensão o conduziu ao cargo de deputado por Moscou, em 1989, e a uma cadeira no *Soviete Supremo*[20]. Figura controversa, exerceu papel de destaque na desintegração da URSS, dentre suas principais ações políticas defendeu a implementação de reformas estruturais para impulsionar a economia russa, as quais, por vezes, iam de encontro às diretrizes do Secretário-Geral (BRZEZINSKI, 1997; PONS, 2014).

> Gorbachev aproveitou isto como uma oportunidade para abrir negociações com os líderes das repúblicas constituintes e, no Verão, tinha elaborado um acordo que teria transformado a URSS, de fato, de um império, numa verdadeira federação. [...] A era do domínio do Partido Comunista teria acabado, o enorme Exército Vermelho seria reduzido e a tão temida KGB, que unia o controle político, a segurança interna e a inteligência estrangeira, seria dividida em grupos (GALLEOTI, 2022, p. 35).

Em 29 de maio de 1990, a revelia de Gorbachev, Yeltsin foi eleito chefe de Estado da Rússia Soviética e, em 12 de junho, declarou a soberania das instituições russas, dando início ao processo formal e contínuo de desintegração do bloco (BULAU, 2004). Na esteira destes acontecimentos, o Conselho Supremo da República Socialista Soviética da Ucrânia instituía, em 5 de julho de 1991, o cargo de presidente, num movimento que sinalizava o interesse da classe política em organizar seu próprio processo de independência nacional, caminho trilhado por países como Estônia, Letônia, Lituânia e Geórgia que, naquele mesmo ano, haviam se emancipado do bloco.

A eclosão de movimentos independentistas em parte das repúblicas soviéticas amplificou a tensão política dentro do PC culminando em uma tentativa de golpe de

[20] Última instância do poder legislativo da URSS, única capaz de realizar alterações constitucionais e indicar a formação do Conselho de Ministros e da Suprema Corte.

Estado, orquestrada pela ala conservadora e parte da organização de serviços secretos (KGB), em agosto daquele ano. Entretanto, incapazes de retirar a toque de caixa Gorbachev e Yeltsin do poder e, assim, reestabelecer o controle do partido sobre a URSS, o movimento malogrou. Muito em virtude da incapacidade dos conservadores em cooptar setores representativos do oficialato, bem como, da atuação de uma legião de apoiadores convocados por Yeltsin para ocupar o parlamento e resistir (BONNEL, COOPER, FREIDIN, 1994; GALEOTTI, 2022).

Com efeito, ao passo em que o fracasso do golpe incidiu positivamente sobre o capital político de Yeltsin, por outro lado, reduziu, significativamente, a influência de Gorbachev sobre a política da Rússia Soviética independente, acelerando o processo de desmantelamento da URSS. Por conseguinte, naquele mesmo ano, as atividades do PC em solo russo foram proibidas (VISSENTINI, 2021). Em meio a esse cenário, em 24 de agosto, o parlamento ucraniano declarou a independência do país, ação referendada por cerca de noventa por cento da população que chancelou a decisão legislativa (FILHO, 2022).

Á nível internacional, meses depois, em dezembro de 1991, as autoproclamadas repúblicas da Rússia e da Ucrânia assinaram o Pacto de Belaveja, o qual deu andamento à formação da Comunidade de Estados Independentes, composta por outras doze repúblicas[21] que se mantiveram sob a órbita de influência russo-ucraniana, manobra que na prática mitigou por completo o poder do chefe de Estado da URSS (VISSENTINI, 2021).

Dessa forma, grosso modo, em 26 de dezembro de 1991, ao reconhecer a legitimidade das independências dos seus antigos satélites, o *Soviete Supremo* conclui o processo de desmanche do bloco, sendo este o último ato de Gorbachev antes de sua renúncia e transferência do controle político ao presidente Yeltsin (SEBESTYEN, 2011; GALEOTTI, 2022).

Embora o fim do bloco soviético tenha provocado efeitos diversos sobre as antigas repúblicas que o compunham, chama a atenção o fato de que embora os processos emancipatórios concretizados na Rússia e na Ucrânia tenham ocorrido sob condições idiossincráticas, havia um desejo comum entre as classes políticas e sociais por reformar o Estado sob a égide normativa liberal, incorporando diretrizes institucionais democráticas, tais como: separação de poderes; liberdade de imprensa;

[21] Aceitaram fazer parte da comunidade as repúblicas do Azerbaijão, Bielorrússia, Cazaquistão, Quirguiztão, Moldávia, Tajiquistão, Turcomenistão e Uzbequistão.

eleições diretas; e, abertura econômica, fatores que os distanciassem da matriz soviética (TSYGANKOV, 2010).

Não obstante, em ambos as disputas intraelites minaram a coesão doméstica, tornando o equacionamento das relações externas tarefa árdua, de maneira que os efeitos dessa dinâmica impossibilitaram a promoção equilibrada dos interesses de cada qual na região e acabaram os colocando em rota de colisão.

Em específico, na Ucrânia, o primeiro presidente eleito por voto direto Leonid Kravchuk (1991-1994) teve sua administração marcada por um extremo autoritarismo, sob um forte sistema oligárquico. De modo similar, o seu sucessor Leonid Kushma (1994-2004) manteve o caráter centralizador das estruturas de poder, sob um regime semi-autoritário que caminhou *pari passu* à promoção de interesses econômicos e financeiros das elites nacionais (MATUSZAK, 2012) [22].

Os regimes de governo adotados colocavam em dúvida os rumos do processo de democratização e impediam um maior aprofundamento das relações externas com a Europa e com os Estados Unidos. Em uma tentativa de reverter o impasse, em 1998, a administração Kushma aderiu ao Acordo de Parceria e Cooperação (APC)[23] com a UE, ato que afrontou diretamente os interesses do Kremlin na região (FREIRE, 2008).

Por outro ângulo, na Rússia, embora as reformas liberais encabeçadas pela administração Yeltsin (1991-1999) tenham assegurado a liberdade de imprensa e consolidado o federalismo, igualmente, não foram capazes de mitigar a influência das redes de patronagem e clientelismo oligárquico, as quais, durante o seu governo, sustentaram uma maior autonomia política, promovendo disputas internas que se prolongaram, mesmo após a dissolução do parlamento, em 1993 (CASALUNGA, 2020).

Com efeito, o contraste entre as políticas implementadas e os altos níveis de corrupção, inflação, restrição ao crédito e subsídios à indústria, elevou as taxas de

[22] Constituída por membros da *nomenklatura* que assumiram o controle de setores industriais utilizando recursos acumulados nos últimos anos da URSS, dentre os quais, se destacam àqueles que passaram a controlar indústrias pesadas de setores energéticos, concentradas predominantemente em Donetsk, Lugansk e Zaporizhia. Tais 'clãs' fortaleceram seus laços com a classe política após a independência, por intermédio de um procedimento de dupla troca que permitia o fluxo de capital necessário para assegurar a manutenção das lideranças políticas no controle da máquina estatal, em troca do necessário suporte aos processos de privatização que tomaram fôlego com a queda da URSS. Entretanto, a solidificação dos laços intraelites só viria a ocorrer ao longo da administração Kuchma que cristalizou o sistema de dependência mútua no bojo das instituições estatais (MATUSZAK, 2012, p. 13-14).

[23] O acordo sinaliza o interesse da UE em promover valores e interesses comuns que reforcem a segurança das fronteiras e assegurem o desenvolvimento e a estabilidade dos membros do bloco, dessa forma, a Europa buscou apoiar o processo de transição econômica e democrática na Ucrânia, porém o documento carecia de compromissos com aplicação direta ou metas definidas (FREIRE, 2008).

desemprego, marcando um longo período de declínio na qualidade de vida dos russos. Destarte, em 14 de março de 2000, a candidatura vitoriosa de Vladmir Putin - ex-oficial de inteligência da KGB - à presidência, representou uma tentativa de estabilizar as disputas internas, e, por conseguinte, mitigar a crise que assolava a Federação (GALEOTTI, 2022).

A primeira administração Putin (2000-2009) procurou acomodar os interesses conflitantes, imprimindo um forte caráter personalista que permitiu a constituição de um partido político hegemônico - Rússia Unida -, capaz de cooptar as elites políticas regionais. Dessa forma, as máquinas administrativas, outrora controladas pelos governadores, se uniram sob sua liderança, em torno de um projeto de desenvolvimento que buscava retomar a grandeza internacional da Rússia (CASALUNGA, 2020).

Assim, o Kremlin acompanhava com atenção o andamento dos processos políticos na Ucrânia, considerados vitais para salvaguardar os interesses estratégicos do país, pois, se tratava de um importante aliado regional[24]. Logo, a adesão da Ucrânia, de Kushma, à Política Europeia de Vizinhança[25], iniciativa que representava o esforço da comunidade europeia em promover seu alargamento, somada ao APC, promoveu o distanciamento das relações russo-ucranianas (FREIRE, 2006).

A decisão não se deu por unanimidade, parte da classe política ucraniana pró-rússia se mostrou cética quanto à abertura de espaço para intervenção europeia na dinâmica política interna do país, denunciavam, pois, a deterioração das relações com a Federação Russa em função da adoção de uma política regional que consideravam carecer de propostas objetivas e coerentes, capazes de promover a integração do país ao bloco europeu (FREIRE, 2008).

Com vistas a esse cenário que parte dos estudos realistas que se debruçaram sobre o conflito russo-ucraniano desencadeado em 2013, considera os Estados Unidos e os seus aliados europeus como responsáveis pela crise na região (MEARSHEIMER, 2014). Por essa lógica, o programa de alargamento das instituições políticas e de

[24] Dentre as variadas razões pelas quais os russos a consideravam um importante parceiro regional, destacamos: i) os laços dos setores de produção de energia, em específico da exportação de gás natural à Europa, uma vez que, até 2014, quase oitenta por cento do recurso destinado ao mercado europeu transitava necessariamente pela Ucrânia (FÂNZERES, 2014, p. 55); ii) posição geoestratégica do território que permite acesso ao Mar Negro via Novorossiysk, Odessa e Sevastopol, para escoamento da produção industrial e agrícola aos mercados internacionais (BARATA, 2014, p. 34).

[25] Um plano de ação para reforma institucional da Ucrânia com intuito de promover a democratização do país, concepção normativa que prevê o estabelecimento do estado de direito e proteção a direitos humanos fundamentais como princípios basilares para integração às instituições ocidentais (FREIRE, 2008).

segurança ocidentais é apontado como fator que colocou os interesses russos e ucranianos em antagonismo, resultando em abalos frequentes no tênue equilíbrio que constituía suas relações exteriores (BARATA, 2014; MIELNICZUK, 2014).

Considerando o processo de alargamento sob o prisma da política de contenção da URSS durante a Guerra Fria, se verifica um aumento do sentimento antiocidental na população de origem russa que se sentiu prejudicada com os novos arranjos institucionais propostos pela Europa, os quais afrontavam os interesses da Rússia, fator chave para se entender a "legitimidade de iniciativas antagônicas aos interesses ocidentais" (LYNCH, 2001 *apud* MIELNICZUK, 2014, p. 4) tomadas pela Federação.

É neste cenário que, em 2004, eclode a chamada 'Revolução Laranja' na Ucrânia, um dos elementos críticos para o aumento da preocupação russa com a tentativa de ingerência da Europa na região. Esse movimento tomou forma após a divulgação dos resultados das eleições para presidência, realizadas em dezembro daquele ano, pleito que dispôs frente a frente ambições regionais distintas.

A disputa entre o partido 'Nossa Ucrânia' do antigo primeiro-ministro da administração Kushma, Viktor Yushchenko (1999-2001), com inclinação pró-ocidente, e o partido das 'Regiões' do primeiro-ministro Viktor Yanukovych (2002-2005), pró-Moscou, explicitou a cisão irreconciliável entre forças sociais rivais que se cristalizava na Ucrânia. Ao passo em que o partido desafiante representava o interesse da classe política ucraniana pró-ocidental em dar prosseguimento ao processo de democratização e integração às instituições ocidentais, o governista, por sua vez, promovia a confluência de interesses de parte das oligarquias locais, ávidas em manter o *status quo* político (BARATA, 2014).

Com a divulgação do resultado das eleições e a vitória de Yanukovych, o movimento se pôs em marcha alegando fraude no processo, aos protestos, organizados junto à praça central de Kiev, se uniram organismos contrários à manutenção das estruturas de poder vinculadas ao antigo sistema soviético, com destaque para o partido 'Pátria', liderado por Yulia Tymoshenko (FREIRE, 2006).

Passados dois meses de protestos, a classe política e as instituições judiciais ucranianas foram compelidas a reconsiderarem o resultado das urnas, em reflexo, um novo pleito foi realizado, em 23 de janeiro de 2005, consagrando a candidatura de Yushchenko (2005-2010) que, por conseguinte, indicou Tymoshenko ao cargo de primeiro-ministro, numa tentativa de consolidar a implementação das reformas liberais (FREIRE, 2008).

Longe do escopo de nossa análise verificar em profundidade os efeitos da dita ‘Revolução Laranja’, vale ponderar que, embora tenha fomentado mudanças, produziu efeitos marginais e insuficientes para assegurar a consecução do processo de democratização e abertura econômica. Tymoshenko perdurou no cargo por apenas nove meses, incapaz de equacionar as disputas internas de poder, e, imersa em escândalos de corrupção que aplacaram a sua legitimidade, foi forçada a renunciar, dando lugar ao pragmático primeiro-ministro Yuriy Yekhanrov (2005-2006) (FREIRE, 2006).

O denso entrelaçamento de interesses conflitantes entre as oligarquias russas e ucranianas manteve a Ucrânia dividida, por conta disso, a administração Yuschenko procurava manter uma política externa *multi vetorial* com intuito de equacionar o processo de integração com a Europa *vis-à-vis* a manutenção da cooperação estratégica com a Federação Russa (FREIRE, 2008).

Em tal conjuntura, em 26 de março de 2006, com o apoio russo, o partido das ‘Regiões’ conquista as eleições legislativas. Contudo, o número insuficiente de cadeiras para governar sem coligação com partidos opositores, resultou num longo período de paralisia decisória. Diante do impasse, a primeira coligação proposta procurou unir os partidos de oposição e governista, reduzindo a influencia dos últimos, em uma tentativa dos liberais de nomearem Tymoshenko, novamente, ao cargo de primeiro-ministro. Porém a manobra malogrou, provocando uma nova onda de protestos nas ruas de Kiev, dessa vez, em defesa de Yanukovych. Em resposta, em julho, Yushchenko considerou a coligação inconstitucional (FREIRE, 2006).

> Esta luta para conseguir a formação de um novo governo mostra [claramente] a dificuldade que qualquer governo que venha a ser formado terá em conduzir uma agenda política e econômica nacional [...] parece que a sociedade civil efetivamente mudou com a Revolução Laranja e as eleições de 2006. Mas em termos de consolidação interna a Ucrânia ainda tem um longo percurso a percorrer, é também clara a influência de atores externos neste processo de transição (FREIRE, 2006).

Somente após a aprovação de uma nova coligação que, na prática, mitigava o poder da oposição, Viktor Yanukovych foi eleito primeiro-ministro, sendo prontamente felicitado por Putin (BARATA, 2014). No entanto, sua ascensão esteve condicionada a assinatura da Declaração de Unidade Nacional que firmou o compromisso do governo com a implementação das reformas necessárias para integração da Ucrânia às estruturas econômicas e de defesa ocidentais (FREIRE, 2006).

Em âmbito internacional, a administração Yushchenko-Yanukovych assentou sobre uma política conciliatória, a qual procurava harmonizar os interesses ucranianos aos europeus e russos. Sem embargo, com a adesão ao Tratado de Lisboa[26], em outubro de 2007, a Ucrânia assinalava seu compromisso com a implementação de mecanismos institucionais de segurança requeridos para entrada do país na UE e na OTAN, entrando, mais uma vez, em rota de colisão com os interesses do Kremlin que, por sua vez, passou a pressionar Kiev com ameaças de desabastecimento de suprimentos e energia (FREIRE, 2008).

> Desde meados da década de 1990, os líderes russos se opuseram firmemente ao alargamento da OTAN e, nos últimos anos, deixaram claro que não permaneceriam sentados enquanto seu vizinho estrategicamente importante se transformasse em um bastião ocidental (MEARSHEIMER, 2014, p. 1).

Frente a difícil conciliação entre os interesses ucranianos e russos, Yushchenko opta pela dissolução do parlamento, convocando novas eleições legislativas, vencidas pela oposição, em 30 de setembro de 2007. Dois meses depois, Tymoshenko reassume o cargo de primeiro-ministro dando novo fôlego ao processo de aprovação das reformas liberais, nesse ínterim, a Rússia realiza cortes pontuais no suprimento de gás destinado à Ucrânia (FREIRE, 2008).

Enquanto isso, na Federação Russa, Putin deixa o cargo de presidente e assume como primeiro-ministro, em seu lugar Dmitry Medvedev (2008-2012) é eleito, o empresário que até então, ocupava a presidência da Gazprom, principal exportadora de gás da Rússia, com forte inserção no mercado ucraniano. A administração Medvedev continuou a exercer pressão econômica e política sobre Kiev, a fim de conter o processo de aproximação com a UE e a OTAN (FREIRE, 2008).

Diante disso, a UE rejeita o Plano de Ação para Adesão da Ucrânia, a justificativa reiterava a premência de se promover a estabilidade interna e o combate à corrupção para adesão ao bloco. Conquanto, a implementação das reformas não surtiu o efeito desejado na economia que, em movimento contrário, entrou em recessão,

---

[26] Reformador → novos mecanismos institucionais e operacionais com base na segurança e estabilidade (principios a liberdade e direitos fundamentais, democratização e economia de mercado). Modelo normativo: Tratado de Lisboa → paz sustentável, democracia, direitos humanos, Estado de direito, liberdade, solidariedade social, boa governança (diplomacia transformativa). UE: interesse em apoiar uma comunidade alargada de segurança na sua vizinhança pouco estável (FREIRE, 2008, p. 10).

elevando vertiginosamente a taxa de desemprego no país, fatores que levaram a administração Tymoshenko, novamente, ao colapso (BARATA, 2014).

Um breve período de coesão da política interna só seria alcançado após a vitória Yanukovych à presidência do país, em 2010. De imediato os rumos da política externa ucraniana foram parcialmente alterados, sua administração passou a considerar apenas o estreitamento dos laços econômicos com a UE, negando, assim, o interesse em integrar a OTAN. Em suas declarações iniciais o presidente declarou a intenção de tornar a Ucrânia um Estado neutro, interessado em cooperar nas questões de segurança com a OTAN e com a Rússia (ESTADOS UNIDOS, 2015).

Yanukovych que mantinha laços estreitos com o Kremlin teve sua administração marcada por forte conflito de interesses entre seus correligionários pró-rússia e os oligarcas ucranianos pró-ocidente, em razão disso, o partido das 'Regiões' procurou reencontrar um equilíbrio que promovesse de modo equânime os interesses divergentes. Neste sentido, em 2012, o partido ampliou sua influencia unindo-se ao partido 'Ucrânia Forte' apoiado por importantes oligarcas transnacionais, entretanto, os esforços para aumentar a coesão interna sucumbiram frente à pressão econômica e diplomática exercida pelo Kremlin que minava os interesses do grupo pró-ocidental (ESTADOS UNIDOS, 2015).

A situação se agravou quando, em novembro de 2013, o presidente rejeitou um grande acordo econômico que estava sendo negociando com a UE para aceitar o aporte financeiro russo de quinze bilhões de dólares, ação que sinalizava uma nova guinada na política externa ao encontro dos interesses russos (MEARSHEIMER, 2015). A decisão desencadeou protestos da oposição que resultaram na organização de novas manifestações na praça central de Kiev, movimento que ficou conhecido como Euromaidan, os protestos tiveram início em 21 de novembro de 2013 de forma pacífica e se prolongaram por três meses, chegando a reunir mais de duzentos e cinquenta mil pessoas (ESTADOS UNIDOS, 2015).

Entretanto, em fevereiro de 2014, dado a ocupação de prédios públicos e a resistência do governo, a violência eclodiu, ocasionando em uma contra ofensiva de tropas policiais que resultou na morte de ao menos oitenta e oito manifestantes, além de centenas de feridos entre os dias 18 e 20. Na manhã seguinte, as tentativas de costurar um acordo às pressas que mantivesse a legitimidade do presidente até a realização de novas eleições foram, veementemente, refutadas pelo parlamento, culminando na fuga de Yanukovych e de vários deputados do partido das 'Regiões' da capital (BBC, 2015).

Em 22 daquele mês, o parlamento decidiu dissolver a Berkut, unidade de elite da polícia envolvida na morte dos manifestantes, proibir o idioma russo como segunda língua oficial do país e, remover Yanukovych do cargo, em seu lugar assumia como presidente interino Oleksandr Turchynov (ESTADOS UNIDOS, 2015).

Contudo, a resolução do caso estava longe de ser positivada, pelo contrário, a queda de Yanukovych representou o estopim de um dos mais intrigantes conflitos contemporâneos (2013-2015). Se por um lado sua saída amplificou o sentimento de aversão à Rússia no oeste ucraniano, por outro, fomentou a aversão da região leste ao governo central, dividindo o país em duas metades separadas pelo rio Dnieper, "a crise mostra que a *realpolitik* permanece relevante e os Estados que a ignoram o fazem por sua própria conta e risco" (MEARSHEIMER, 2015, p. 1).

A queda do presidente ucraniano democraticamente eleito forneceu a narrativa adequada àquilo que Putin, eleito à presidência em 2012, classificou como golpe de Estado. Imediatamente, veículos de imprensa russos passaram a transmitir informações que identificavam a UE e os Estados Unidos como pivôs do golpe que ameaçava os interesses regionais da Federação, e colocava em risco a vida de russos que habitavam a região leste do país (MEARSHEIMER, 2015).

Com base nestes argumentos, apenas três dias depois do fato, a península da Crimea, onde mais de dois milhões de habitantes eram falantes da língua e se identificam com a etnia russa, foi anexada pelas Forças Armadas da Rússia (BBC, 2015). Na ocasião, o líder da força paramilitar ucraniana na península Sergei Aksyonov, solicitou à Putin que intervisse com apoio militar para garantir que a cidade de Sevastopol, base histórica da marinha russa no Mar Negro, se mantivesse dentro da jurisdição da Federação (ESTADOS UNIDOS, 2015).

Mais tarde, se verificou que tais grupos armados e agentes de inteligência sem identificação faziam parte de tropas mercenárias, as quais atuavam em conjunto com forças de operações especiais russas, atores estatais e não-estatais, com emprego de equipamentos fornecidos pelas Forças Armadas russas (GILES, 2015). Embora o Kremlin tenha, inicialmente, negado envolvimento nas operações, pouco tempo depois, a sede da frota russa do Mar Negro admitiu ter movimentado efetivo para a Crimeia a fim de assegurar o controle do porto de Sevastopol (ESTADOS UNIDOS, 2015).

Após a intervenção, o parlamento da Crimeia decidiu unir o território à Rússia e convocou um referendo para consulta popular, organizado por governos locais da península, em 16 de março de 2014, com aprovação de mais de noventa por cento da

população. Dois dias depois, um tratado para anexação foi assinado e a Crimea passou a pertencer, formalmente, ao território russo (ESTADOS UNIDOS, 2015). À altura, a tensão em torno da presença de militares ucranianos em bases localizadas na península foi dissipada por meio de acordos que garantiram sua retirada da região em segurança (MIELNICZUK, 2014).

Os Estados Unidos e a UE reagiram aplicando sanções econômicas à Rússia[27], medidas insuficientes para conter o sentimento antiocidental que tomou corpo nas regiões do leste ucraniano. Desse modo, em 7 de abril, grupos separatistas que classificavam o governo de Kiev como símbolo do fascismo, organizaram um movimento para desvincular a região de Donbass, onde estão localizadas as cidades de Donetsk, Luhansk e Kharkiv, da Ucrânia (BBC, 2015).

Os separatistas ocuparam prédios públicos e exigiram a realização de referendos regionais semelhantes ao da Crimeia, com a recusa do governo central em reconhecer a legitimidade do movimento, os referendos foram organizados de modo informal e, em 11 de maio de 2014, foram declaradas a independência da República Popular de Donetsk e a autonomia de Luhansk e Kharkiv. Por conseguinte, em 22 de maio, estes grupos declararam o estabelecimento da Nova Rússia, uma área que incluía os territórios ao sul e a leste do rio Dnieper (ESTADOS UNIDOS, 2015).

Em resposta, o parlamento organizou novas eleições presidenciais que deram a vitória ao oligarca pró-ocidente Petro Poroshenko (2014-2019), o qual, rapidamente, anunciou medidas para um cessar-fogo. No entanto, o plano de Poroshenko durou apenas uma semana, quando um helicóptero militar ucraniano foi abatido ao sobrevoar o território do leste (BBC, 2015).

Não obstante, a administração Poroshenko assinou o Acordo de Associação com a UE que havia sido rejeitado por seu antecessor, concluindo, assim, o estreitamento dos laços da política externa ucraniana com a Europa. Concomitantemente, os países membros da aliança do norte decidiram que a aliança permaneceria aberta a novos membros, ‘Nenhum país terceiro veta o alargamento da OTAN’ (MEARSHEIMER, 2015).

Em sequência, as tropas militares ucranianas iniciaram uma contraofensiva para retomar os territórios ocupados pelos separatistas em Donetsk e Luhansk. Os combates

[27] Em 17 de Março 2014 a UE e os EUA impõem restrições de visto e congelamento de vistos de oficiais russos e ucranianos atingindo cargos de alto escalão como o chefe do conselho Federal, o Primeiro Ministro e o assessor presidencial (IVAN, 2018).

se intensificaram com as forças do governo avançando e acuando os separatistas que, em 17 de julho, disparam um míssil contra o voo MH17 da Malaysian Airlines, provocando a morte de duzentos e oitenta e três passageiros e quinze tripulantes civis (BBC, 2015). A tragédia conduziu a novas sanções econômicas à Rússia por parte dos Estados Unidos e da UE que atingiram setores controlados pelas oligarquias russas (IVAN, 2018).[28]

Em agosto daquele ano, com apoio militar de norte-americanos e europeus, os ucranianos conseguiram recuperar cerca de dois terços do território ocupado pelos separatistas (ESTADOS UNIDOS, 2015). A contraofensiva causou fortes baixas no movimento separatista, abrindo espaço para a negociação de outro cessar-fogo, estabelecido em 5 setembro com a chancela da Rússia e da UE (BBC, 2015). A Organização para Segurança e Cooperação na Europa coordenou as negociações de paz na cidade de Minsk, na Bielorússia, na ocasião Poroshenko conseguiu a aprovação plena dos quinze pontos do plano de paz que havia sido proposto em junho.

Dentre os pontos principais do plano, Kiev se comprometia a conceder maior autonomia para a região de Donbass e proteger os russos que habitavam estes territórios, como contrapartida, equipamentos de combate seriam removidos das áreas de conflito e os prisioneiros deveriam ser libertos (ESTADOS UNIDOS, 2015). Contudo, a trégua durou apenas dois meses, em 12 de novembro, as hostilidades foram retomadas nos territórios a leste, à época, sob controle de Kiev. Com apoio de tropas russas, os separatistas voltaram a declarar a autonomia da região (BBC, 2015).

As hostilidades se prolongaram, até que, em 12 de fevereiro um novo cessar-fogo foi acordado em Minsk, entre Rússia, Ucrânia, Alemanha e França. A medida previa a retirada de armas, a troca de prisioneiros e a redução de armamento pesado entre as forças de artilharia envolvidas no conflito. Entretanto, mesmo com a assinatura do acordo os conflitos não cessaram e o movimento separatista continuou a avançar, a fim de unir as regiões de Donetsk e Luhansk, ato consumado nos meses seguintes.

Doravante, um novo *status quo* geopolítico constituído na região promoveu um tênue equilíbrio nas relações entre russos e ucranianos, sustentado por quase cinco anos, em parte, devido à manutenção dos territórios a leste sob controle dos separatistas, da

[28] Em 18 de julho o Banco Europeu de Investimento suspendeu o financiamento de projetos de infraestrutura na Rússia. No dia 29 daquele mês os Estados Unidos impõem sanções destinadas a setores da economia russa, incluindo armamentos, energia e finanças, em sequência, a UE restringe o acesso ao mercado de capitais aos bancos estatais russos, e impõe um embargo comercial restringiu exportações de armas, bens de uso dual e tecnologias, especialmente no setor de petróleo (IVAN, 2018).

anexação da Crimea ao território da Federação e da livre promoção dos interesses de Kiev (CASALUNGA, 2022).

Contudo, a fratura nas relações entre russos e ucranianos continuou irreparável, uma vez que a Federação Russa se manteve inflexível quanto à união comercial e militar da Ucrânia às alianças ocidentais. Nesse sentido, chama a atenção o fato de que o processo de alargamento das instituições securitárias e comerciais promovidos pela UE e a OTAN não tenha sofrido quaisquer alterações, mesmo diante de evidências irrefutáveis do ímpeto russo em manter parte da Ucrânia sob sua esfera de influência regional (CASALUNGA, 2022).

Frente ao exposto, naquilo que tangencia a relevância acadêmica e securitária das operações que atingiram a Ucrânia, se faz *mister* compreender como se deu o processo de mudança institucional nas forças de segurança nacional da Rússia que promoveu incentivos seletivos para o seu desenvolvimento e posterior execução. Com base na análise de fontes primárias, a próxima seção destaca os meandros institucionais que permitiram à Federação incorporar o domínio cibernético à estrutura segurança e defesa com vistas à projeção de poder nacional na região da Eurásia.

4.2. Mudança Institucional: a transformação das forças de segurança e defesa russas para incorporar o ciberespaço como novo domínio de guerra

Nesta seção verificamos os efeitos da mudança institucionais pela qual passaram as principais agências responsáveis pela segurança e defesa nacional da Federação Russa para uso efetivo das operações especiais orquestradas durante a anexação da Crimeia e eclosão dos movimentos separatistas na fronteira leste. Com base na análise de documentos oficiais[29], coletamos evidências da mudança que permitiu incorporar o ciberespaço como um novo domínio da guerra, considerada condição necessária para seu uso efetivo com vistas à projeção de poder nacional em conflitos regionais.

Nossa análise ordenou o conteúdo das fontes em três fatores considerados significativos para explicar a mudança institucional: i) desafios geopolíticos; ii) definição e integração entre fins e meios; e, iii) construção de narrativa estratégica, aspectos basilares para a orientação estratégica das instituições responsáveis pela segurança nacional russa. O material examinado registra os incentivos que permitiram a

[29] Fontes primárias: Estratégia de Segurança Nacional (2009; 2015); Doutrina Militar (2010; 2014).

articulação entre setores de defesa, inteligência, iniciativa privada e parceiros internacionais, para incorporar o ciberespaço como um novo recurso do poder nacional.

À luz das mudanças implementadas ao longo das administrações Medvedev (2008-2012) e Putin (2001-2008; 2012-2016), o ciberespaço passou a ser considerado um domínio de guerra fundamental para a consecução dos objetivos estratégicos da Federação, representando uma alternativa capaz de oferecer vantagens assimétricas em operações ofensivas.

Sem embargo, desde a década de sessenta, pensadores soviéticos chamavam a atenção para as implicações da chamada Revolução dos Assuntos Militares (RMA) ou a 'revolução técnica científica', a qual estabeleceu a necessidade de profissionalização das forças de segurança. Já na década de oitenta, a árdua tarefa de acompanhar a corrida armamentista fez com que a União Soviética tivesse de responder aos desafios securitários por vias distintas, assim, considerando a atuação das instituições securitárias em conflitos regionais, procurou promover o desenvolvimento do Complexo Industrial Militar (CIM) e a profissionalização militar, a fim de que pudessem operar em múltiplos domínios, com destaque para o espaço da informação (HALPIN et al., 2006).

> A guerra regional [...] será caracterizada por [...] guerra em todas as esferas; operações de coalizão; utilização em massa de PGM's, formas eletrônicas e outras formas novas de combate; ataques em todo o território dos lados opostos [...] Um sistema de tecnologia (S&T) independente e produtivo deve ser desenvolvido para atender às necessidades militares, especialmente para uma nova geração de armamentos (HALPIN et al., p. 159, 2006).

Ao longo da primeira década deste século, na esteira do pensamento militar soviético, a mudança que incidiu sobre as agências securitárias procurou alavancar os incentivos à pesquisa e ao desenvolvimento tecnológico-científico, dentre outras razões, com intuito de assegurar o funcionamento conjunto de sistemas de inteligência, capazes de reduzir a incerteza e aumentar a eficiência operacional (CARVALHO, SILVA, 2006).

A transformação marcada por tensões geográficas, antecedentes ideológicos, padrões tecnológicos e a relação das instituições com seus líderes (HEICKERO, 2010), produziu efeitos sobre diversas agências, dentre as quais destacamos: o Serviço de Proteção Federal, o Serviço Federal de Segurança Federal, o Serviço de Inteligência Estrangeira e o GRU.

Promulgada em 13 de maio de 2009, a Estratégia de Segurança Nacional registra a percepção sobre os desafios geopolíticos que ameaçam os interesses da Federação, bem como oficializa as diretrizes que deverão ser perseguidas para robustecer as instituições responsáveis pela segurança nacional. Nesse sentido, o eixo narrativo da ESN (2009) assinala a superação do processo histórico que conduziu ao esfacelamento da URSS, e reforça a imagem de uma Rússia independente que superou a crise política e socioeconômica que, ao final do século vinte e um, havia reduzido, consideravelmente, a qualidade de vida de seus cidadãos. Frente ao cenário, manifesta o interesse da Federação em sua reinserção na ordem global, enquanto potência com peso significativo nos processos decisórios internacionais (RÚSSIA, 2009, p. 1).

Outrossim, chama atenção para os efeitos da interdependência na dinâmica geopolítica, ao passo em que denuncia o desenvolvimento desigual entre os países e o fortalecimento de novos centros de crescimento econômico e influência política, desafios para os quais a Federação demonstra interesse em "encontrar a solução para os problemas existentes e resolver situações de crise em uma base regional sem a participação de forças não regionais" (RÚSSIA, 2009, p. 4).

A ESN (2009) registra que a instalação, nas regiões fronteiriças, de um sistema de defesa antimísseis da OTAN representa um fator de instabilidade que pode conduzir ao emprego de força militar (RÚSSIA, 2009, p. 5). Por essa lógica, o avanço da infraestrutura militar ocidental sobre os antigos satélites soviéticos, desconsiderando os interesses legítimos da Rússia, é considerado chave para a insegurança na região euro-atlântica (RÚSSIA, 2009, p. 7).

Frente ao contexto, frisa que o desenvolvimento e uso por parte dos Estados de equipamentos militares - armas de alta precisão, guerra de informação, armas químicas, armas nucleares e a formação do sistema global unilateral de defesa antimíssil -, para desestabilizar países estrangeiros, pode estar produzindo uma nova corrida armamentista, em grande parte, devido a crescente militarização das adjacentes à Rússia (RÚSSIA, 2009, p. 10-11).

No que concerne às ameaças identificadas, assinala o potencial de "atividades de inteligência e serviços especiais de Estados estrangeiros, [...] grupos e organizações terroristas, [...] atividades extremistas [...] e de grupos de criminosos transnacionais" (RÚSSIA, 2009, p. 12) para desorganizar o funcionamento da esfera pública, prejudicar o funcionamento de infraestruturas críticas e causar instabilidade social. Nesse sentido, os conflitos desencadeados nas regiões fronteiriças por "organizações terroristas e

extremistas internacionais" (RÚSSIA, 2009, p. 14), representam desafios que deverão ser enfrentados com o auxílio de estruturas multifuncionais de alta tecnologia a serem instaladas nestas zonas, mediante a cooperação com a Ucrânia, a Geórgia, o Cazaquistão e o Azerbaijão.

Não obstante, no que concerne aos meios para enfrentar tais desafios e assegurar o retorno da Federação ao patamar de potência internacional, prevê a constituição de incentivos institucionais que permitam incrementar as capacidades de projeção de poder nacional para atuar em conflitos regionais, por intermédio de operações dissuasórias, orquestradas em cooperação interagências "políticas, diplomáticas, militares, econômicas, informacionais" (RÚSSIA, 2009, p. 10). Em razão disso, em âmbito político, considera *mister* o apoio a medidas que ofereçam respaldo ao processo, promovendo a transformação qualitativa das forças militares, mediante a implementação de programas de fomento ao "desenvolvimento, criação e modernização de armas e equipamentos militares especiais, incluindo comunicações, inteligência, guerra eletrônica e gestão" (RÚSSIA, 2009, p. 11).

Ainda no tocante aos meios que tangenciam as metas estratégicas, os campos da ciência e educação recebem destaque dado o potencial para produção de "tecnologias como meios técnicos, de software, linguísticos, legais, organizacionais, incluindo canais de telecomunicações usados no sistema de segurança nacional para coletar, formar, processar, transmitir ou receber informações" (RÚSSIA, 2009, p. 3).

No médio prazo, sublinha que a eficiência destes campos, na qualidade de vetores do desenvolvimento e inovação industrial, depende do treinamento de especialistas e trabalhadores qualificados e da construção de parcerias público-privadas que permitam integrar os campos da ciência, inovação e indústria em prol da consecução dos objetivos estratégicos da "defesa nacional, estadual e da segurança pública, bem como o desenvolvimento sustentável do país" (RÚSSIA, 2009, p. 22). Enquanto que, no longo prazo, sublinha a necessidade de aproximar as instituições de segurança às redes de ensino superior, federais e nacionais, para desenvolver tecnologia de ponta a ser aplicada em produtos de uso dual (RÚSSIA, 2009, art. 70, p. 22).

Por este ângulo, o ciberespaço é percebido como um domínio estratégico capaz de ampliar as capacidades de projeção do poder nacional, razão pela qual, prevê a construção e uso de tipos modernos de armas e equipamentos especiais, não apenas pelas Forças Armadas da Federação, como também por outras tropas, unidades e órgãos paramilitares (RÚSSIA, 2009, p. 12) que os permitam atuarem neste domínio.

Conquanto, atividades cibernéticas maliciosas são descritas como entraves aos interesses da Federação, que denuncia o crescimento de conflitos envolvendo o espaço de informação como ponto fulcral na desestabilização de territórios nacionais, mediante a promoção de "sentimentos nacionalistas, xenofobia, separatismo e extremismo violento, inclusive sob os slogans de radicalismo religioso" (RÚSSIA, 2009, p. 5).

Com intuito de controlar as ameaças provenientes do ciberespaço, a ESN (2009) registra o interesse em investir na segurança do funcionamento dos sistemas de informação e telecomunicações e infraestruturas críticas. Para tanto, prevê a criação de um "sistema unificado de suporte à informação e telecomunicações que atenta as necessidades do sistema de segurança nacional" (RÚSSIA, 2009, p. 31).

Em que pese se tratar de um documento produzido em período anterior ao início do conflito com a Ucrânia, considera a possibilidade de "construir uma parceria estratégica igual e de pleno direito com os EUA" (RÚSSIA, 2009, p. 7) para controle da proliferação de ADMs e resolução de conflitos regionais, com intenção de concentrar "esforços necessários ao nível menos oneroso para manter a paridade com os EUA no campo das armas ofensivas estratégicas, no contexto da implantação de um sistema global de defesa antimísseis" (RÚSSIA, 2009, p. 29).

Em 2010, a Federação Russa torna pública uma nova Doutrina Militar (DM), o documento registra evidências do processo de transformação em curso nas instituições responsáveis pela segurança nacional, transformações realizadas com intuito de desenvolver capacidades que assegurem a efetividade das operações.

A DM (2010) estabelece o compromisso com "o uso de instrumentos políticos, diplomáticos, legais, econômicos, ambientais, de informação, militares e outros instrumentos" para proteger os interesses estratégicos da Federação e de seus aliados (RÚSSIA, 2010, p. 1-2). Nesse sentido, aponta para a redução da polarização ideológica na conjuntura internacional, em razão da emergência de uma multipolaridade, a qual fragmenta o nível de influência econômica, política e militar de alguns Estados (RÚSSIA, 2010, p. 3-4).

Não obstante, mostra preocupação com o aumento das guerras regionais em curso, descritas como efeitos da insuficiência de mecanismos regulatórios internacionais com poder para inibi-los, fator que representa uma ameaça de escalonamento, com possibilidade de envolvimento de armas convencionais e nucleares. Em razão disso, o avanço da infraestrutura militar da OTAN sobre as fronteiras da Federação é descrito

como um dos principais desafios geopolíticos que fomentam a desestabilização estratégica regional (RÚSSIA, 2010, p. 3-4).

Frente ao cenário, estes conflitos são percebidos como produto da combinação entre forças militares e outros meios de natureza não militar, operando sistemas de armas e equipamentos de alta tecnologia, comparáveis, em termos de eficácia, às armas nucleares. Por essa lógica, considera a guerra de informação como um recurso significativo para as operações militares, ampliando, consideravelmente, a eficiência da rede de sistemas de C2 de tropas e armas (RÚSSIA, 2010, p. 6-7). Mais do que isso, pode oferecer vantagens assimétricas aos Estados que pretendem "atingir objetivos políticos sem o uso de força militar" (RÚSSIA, 2010, p. 7) ao passo em que constroem "uma reação favorável da comunidade mundial" (RÚSSIA, 2010, p. 7).

No tocante a finalidade das forças de segurança nacional, registra a necessidade de "avaliar e prever o desenvolvimento da situação político-militar em nível global e regional [...] utilizando sistemas técnicos modernos e tecnologias da informação [...] e neutralizar possíveis perigos e ameaças militares usando meios políticos, diplomáticos e outros meios não militares" (RÚSSIA, 2010, p. 8).

Para tanto, assinala a relevância da transformação institucional que assegure o desenvolvimento de capacidades que permitam as forças de segurança nacional lidar com sofisticação das ameaças externas. Por esse prisma, prevê a construção de "modelos modernos de armas, equipamentos militares e especiais de alta qualidade", bem como "a integração e o desenvolvimento coordenado de sistemas de apoio técnico, logístico e outras formas de apoio às forças armadas e outras tropas" (RÚSSIA, 2010. 15-16).

No que concerne às medidas a serem adotadas, destaca o interesse em constituir parcerias entre instituições de ensino militares e federais para formação de profissionais de nível superior em programas de treinamento militar, equipados com material atualizado e base técnica (RÚSSIA, 2010, p. 16-17), além da criação de condições que ofereçam suporte ao desenvolvimento militar, mediante a integração dos setores civil e militar em esferas específicas de produção e coordenação das atividades estratégicas do Estado (RÚSSIA, 2010, p. 19). Por essa lógica, o fortalecimento da base industrial de defesa passa, necessariamente, pela construção de armas modernas, dentre as quais, se destacam os "meios de guerra de informação" (RÚSSIA, 2010, p. 20).

Neste contexto, o desenvolvimento do CIM é considerado a pedra angular capaz de "atender às necessidades das Forças Armadas e de outras tropas por armamentos

modernos e equipamentos militares especiais" (RÚSSIA, 2010, p. 21) que empreguem alta tecnologia. Em razão disso, prevê a construção de estruturas que assegurem a "independência tecnológica [...] na esfera da produção de modelos estratégicos e outros de armamentos [...] possibilitando a renovação qualitativa da base científica, técnica, manufatureira, e da base tecnológica" (RÚSSIA, 2010, p. 22), nesse sentido, a tecnologia da informação é apontada como recurso significativo no "desenvolvimento, produção e manutenção de modelos de armamentos e equipamentos militares especiais" (RÚSSIA, 2010, p. 22).

Com a eclosão do conflito russo-ucraniano (2013-2015) que contou com o envolvimento direto das instituições de segurança nacional russas, a percepção acerca da magnitude dos desafios geopolíticos regionais, bem como das diretrizes necessárias para assegurar a efetividade das agencias sofreu alterações significativas, conforme apontam os documentos oficiais publicados entre 2014 e 2015.

Em 2014, a Federação Russa promulgou uma nova Doutrina Militar, o documento reitera a crescente preocupação com o avanço das estruturas de defesa militar da aliança do norte ocidental sobre territórios pertencentes as antigas repúblicas soviéticas da Eurásia, fator que impõe a necessidade de dar continuidade ao processo de fortalecimento das capacidades operacionais das forças de segurança nacional, a fim de assegurar a soberania e o território do povo russo.

Neste sentido, considera primordial o aprimoramento do sistema de C2 de fluxo de informação e a construção de armas de alta precisão que permitam o combate às ameaças que promovem a instabilidade regional do entorno estratégico russo, reforçando o compromisso com a proteção militar dos interesses nacionais em caso de esgotamento das "possibilidades de usar instrumentos políticos, diplomáticos, legais, econômicos, informacionais e outros instrumentos não violentos" (RÚSSIA, 2014, p. 2).

Embora, destaque a instabilidade regional como produto do avanço militar da aliança do norte ocidental sobre as regiões fronteiriças, a DM (2014) assinala uma mudança significativa na percepção da guerra regional, retirando a possibilidade de escalonamento envolvendo armas nucleares empregadas por forças militares ou de coalizão, prevista no documento antecessor (RÚSSIA, 2014, p. 3).

A percepção do contexto internacional, também, sofreu alterações em função do conflito com a Ucrânia, ao reforçar a preocupação com a eclosão de conflitos regionais que permanecem sem solução devido à insuficiência do sistema de segurança internacional em prover proteção equitativa aos Estados, assinala a "tendência de

transferir perigos e ameaças militares para o espaço de informação e a esfera interna da Federação Russa" (RÚSSIA, 2014, p. 4).

Sinalizando a importância estratégica crescente do espaço de informação, identifica uma nova natureza dos conflitos regionais, marcados pelo emprego integrado de tropas militares e não militares em conjunto com ações políticas, econômicas e informativas, "implementadas com amplo uso do potencial de protesto da população e das forças de operações especiais" (RÚSSIA, 2014, p. 7).

Mais do que isso, indica que o uso de sistemas de armas e equipamentos militares, tais como "armas hipersônicas de alta precisão, armas de guerra eletrônica [...] sistemas de controle de informações, veículos marítimos, e aéreos autônomos não tripulados" (RÚSSIA, 2014, p. 7), pode produzir impacto significativo sobre um adversário. Por essa lógica, apresenta forte preocupação com o uso da guerra de informação para atingir a estabilidade interna de um Estado mediante a "participação nas hostilidades de grupos armados irregulares e empresas militares privadas [...] método de ação indireto e assimétrico" que envolve "políticas e movimentos sociais financiados e controlados externamente" (RÚSSIA, 2014, p. 7).

As principais formas de dissuasão e prevenção de conflitos militares foram mantidas, com o acréscimo de trechos que indicam a necessidade de garantir a segurança da Federação em tempo de guerra, razão pela qual, pondera que a preparação dos quadros do serviço militar depende da ampliação dos investimentos em tecnologia que ofereçam respaldo às operações de enfrentamento aos desafios geopolíticos.

> [...] neutralizar tentativas de estados individuais (grupos de estados) de alcançar superioridade militar, implantando sistemas estratégicos de defesa antimísseis, armas no espaço sideral e sistemas não nucleares estratégicos de armas de alta precisão; reduzir o risco do uso de tecnologias da informação e comunicação para fins militares e políticos para a implementação de ações dirigidas contra a soberania, independência política, integridade territorial dos Estados (RÚSSIA, 2014, p. 9-10).

No que tange ao uso legítimo das Forças Armadas e outras tropas para dissuasão estratégica e/ou conter ataques realizados contra a Federação, a doutrina (2014, p. 10-12) mantém na íntegra o posicionamento do documento anterior. Entretanto, as tarefas das forças de segurança nacional em tempos de paz receberam inserções que, dentre outros pontos, destacam a construção de "novas instalações de infraestrutura militar e modernização das existentes [...] bem como a seleção de instalações de uso dual pelas

tropas para fins de defesa" (RÚSSIA, 2014, p. 12). Por conta disso, reforça o interesse em assegurar o funcionamento do sistema de C2, e manter a segurança do fluxo de informação entre os órgãos públicos federais e estaduais em nível que permita solucionar problemas de forma eficiente e dinâmica (RÚSSIA, 2014, p. 14).

Não obstante, as prioridades para o desenvolvimento da estrutura e organização militar para enfrentar os desafios geopolíticos foram preservadas, com a inserção da necessidade de alinhamento entre a estrutura de segurança e os modelos modernos de armas e equipamentos militares especiais, capacidades que permitam o combate a ameaças em tempos de paz ou guerra, assim, prevê o aprimoramento contínuo das "capacidades políticas, socioeconômicas, demográficas e técnico-militares" (RÚSSIA, 2014, p. 15-16).

No tocante às ameaças cibernéticas, prevê a formação de quadros capazes de prover a defesa das instalações militares e assegurar a segurança da informação e o funcionamento das infraestruturas críticas de setores como transportes, comunicação e energia (RÚSSIA, 2014, p. 17).

A significância da mudança institucional para contenção de novos conflitos é marcada pela reformulação dos principais objetivos relativos ao treinamento para mobilização, diretriz que difere diametralmente das contidas na doutrina (2010). Neste ponto, todos os itens foram revistos para contemplar a necessidade de preparação para mobilização em tempos de guerra, nesse sentido, a fim de assegurar a capacidade operacional das forças de segurança, prevê a formação de unidades especiais que possam organizar a mobilização, fornecendo "recursos humanos e materiais técnicos das próprias Forças Armadas, outras tropas e órgãos para resolver problemas em condição de guerra" (RÚSSIA, 2014, p. 19).

Os pontos centrais que tratam das condições para oferecer suporte ao desenvolvimento militar foram mantidos, no entanto, o conteúdo foi reformulado e incorporado a um texto conciso que adiciona aos principais meios a manutenção do investimento em "equipamentos militares e especiais baseados no desenvolvimento do potencial científico militar do país" (RÚSSIA, 2014, p. 19-20) que permitam ampliar a eficiência das operações militares.

Outrossim, reforça a primazia organizacional do CIM no que tenciona o "treinamento operacional, de combate e mobilização de tropas [...] desenvolvimento do complexo industrial militar" em nível que permita a coordenação das atividades das Forças Armadas, outras tropas e órgãos, garantindo a "integração das áreas de produção

dos setores civil e militar da economia, a proteção legal dos resultados da atividade militar intelectual, especial, e de uso dual" (RÚSSIA, 2014, p. 20).

No que concerne à tecnologia empregada para equipar as forças de segurança nacional e outras tropas, acrescenta a necessidade de construir "novos modelos de armas de alta precisão e meios de combatê-las" (RÚSSIA, 2014, p. 21), em específico, pontua sua significância para "sistemas de defesa aeroespacial, sistemas de comunicação, reconhecimento e controle, guerra eletrônica, complexos de veículos aéreos não tripulados, sistemas de ataque robótico" (RÚSSIA, 2014, p. 21).

Os principais objetivos a serem perseguidos para desenvolvimento da estrutura do CIM foram mantidos com acréscimo de um item que pontua o interesse na "produção e prontidão tecnológica das organizações do complexo para o desenvolvimento e produção de tipos prioritários de armas e equipamentos militares especiais" (RÚSSIA, 2014, p. 23). Manifesta, ainda, a intenção em estabelecer o diálogo com parceiros interessados pelas "abordagens nacionais para combater os perigos e ameaças militares decorrentes do uso em larga escala de tecnologias de informação e comunicação para fins político-militares" (RÚSSIA, 2014, p. 24).

Em 31 de dezembro de 2015, a Federação promulga uma nova Estratégia de Segurança Nacional com a qual procura reforçar o compromisso do Estado em dar continuidade ao processo de mudança institucional em curso, por intermédio de ações "políticas, militares, organizacionais, socioeconômicas, informacionais, legais e outras" (RÚSSIA, 2015, p. 3). Mais concisa e direta, a ESN (2015) conta com alterações que registram a preocupação russa com os conflitos desencadeados na região da Eurásia, bem como, a significância da cooperação em operações especiais.

Alguns conceitos basilares para atuação das forças de segurança nacional sofreram alterações na ESN (2015), trechos que faziam alusão direta a presença de atores não-estatais –outras tropas- atuando em conjunto com as forças de segurança nacionais foram retirados, igualmente, não menciona a tecnologia da informação enquanto meio significativo para controle de ameaças (RÚSSIA, 2015, art. 6, p. 3).

No que tange à percepção russa das relações interestatais, a descrição do avanço do processo de interdependência foi substituída por dois artigos objetivos que se referem às capacidades demonstradas pela Federação para ampliar seu potencial econômico, político, militar e espiritual, e, assim, contribuir para assegurar a estabilidade estratégica regional, participando ativamente nos processos de resolução de conflitos militares (RÚSSIA, 2015, p. 3-4).

Face à imposição de sanções econômicas por parte da UE e os Estados Unidos à Federação Russa pós-anexação da Crimea, trechos que descreviam as intenções de inserção da Rússia entre os principais países da economia mundial foram retirados para ressaltar a importância em "manter e fortalecer seu potencial em condições de instabilidade na economia mundial" (RÚSSIA, 2015, p. 4).

Igualmente, a identificação de desafios geopolíticos que apresentam risco de escalonamento, tais como a instalação do sistema de defesa antimíssil norte-americano, cedeu lugar à descrição de um confronto de interesses no qual a Federação assinala intenção de atuar de modo independente, em contrapartida à "pressão política, econômica, militar e de informações" (RÚSSIA, 2015, p. 4) imposta por seus adversários. Outrossim, o trecho que sublinhava a preocupação com o avanço regional da OTAN foi substituído por artigos que denunciam as manobras efetuadas com intuito de conter o processo de integração da Ucrânia à Federação, ações que culminaram em um 'golpe inconstitucional', apoiado por norte americanos e europeus, que produziu o caos na sociedade ucraniana (RÚSSIA, 2015, p. 5).

Diante deste cenário, a ESN (2015) promove alterações que incidem sobre o eixo narrativo ao frisar que o "fortalecimento da ideologia nacionalista de extrema direita e a formação intencional da imagem da Rússia como inimiga da população ucraniana" (RÚSSIA, 2015, p. 5-6) transformou a Ucrânia em um vetor de instabilidade na Europa, dando início às operações de uso da força por parte dos envolvidos. Por conseguinte, o interesse em promover acordos para controle da proliferação de ADMs e contenção de conflitos regionais cedeu lugar à preocupação com as capacidades manifestadas por Estados para desestabilizar regimes políticos legítimos, a partir do fomento ao "ódio étnico, ódio religioso e outras manifestações de extremismo" (RÚSSIA, 2015, p. 6).

No tocante a finalidade da tecnologia da informação em conflitos regionais, a descrição de operações capazes de afetar os interesses nacionais através do espaço de informação foi omitida, em seu lugar destacou as ações implementadas para melhorar a vida dos cidadãos russos, dentre as quais, medidas para sustentar o crescimento demográfico e aumentar a expectativa de vida (RÚSSIA, 2015, p. 4). Conquanto, identifica o impacto do espaço de informação por Estados que buscam desestabilizar territórios por meio do uso de "tecnologias da informação e comunicação" para "manipulação da consciência pública e falsificação da história" (RÚSSIA, 2015, p. 6).

Com intuito de responder aos desafios identificados e, assim, se consolidar como potência global, prevê a alocação de recursos em programas que deem continuidade a implementação das transformações que visam incrementar as instituições de segurança nacional (RÚSSIA, 2015, p. 8). Algumas diretrizes foram profundamente alteradas, a fim de assegurar o funcionamento de mecanismos que promovam a eficiência da "organização militar do estado, formas e métodos de uso das forças armadas, outras tropas, unidades e órgãos militares" (RÚSSIA, 2015, p. 9).

Nesse ensejo, pontua que a eficiência das instituições de segurança depende da "identificação oportuna dos perigos e ameaças militares existentes e futuras" (RÚSSIA, 2015, p. 9). Contudo, não apresenta uma descrição detalhada de tais ameaças, como estabelecido anteriormente, ao invés, destaca o papel do CIM, enquanto ponto nevrálgico do desenvolvimento e emprego da tecnologia no "fortalecimento das capacidades de defesa e equipamentos das forças armadas da Federação Russa, outras tropas, unidades e corpos militares especiais com equipamentos modernos" (RÚSSIA, 2015, p. 9).

Naquilo que corresponde às forças de segurança, o interesse pela transformação qualitativa foi reformulado para realçar a necessidade de que o aprimoramento das "formas e os métodos de uso das forças armadas da Federação Russa, outras tropas, unidades e órgãos militares" (RÚSSIA, 2015, p. 10), caminhe *pari passu* às novas "tendências da natureza das guerras modernas e dos conflitos armados" (RÚSSIA, 2015, p. 10), uma vez que a preparação do terreno, mediante a "realização das capacidades de combate das tropas (forças), o desenvolvimento de requisitos para formações promissoras e novos meios de luta armada" (RÚSSIA, 2015, p. 10) é percebida como chave para a consecução dos objetivos estratégicos nacionais.

As ameaças à segurança nacional, também, sofreram alterações, com acréscimo de trechos que sublinham ações envolvendo o "uso de tecnologias de informação e comunicação para divulgação e propaganda da ideologia do fascismo, extremismo, terrorismo e separatismo, causando danos à paz civil, instabilidade política e social" (RÚSSIA, 2015, p. 11).

Em relação ao meios necessários para responder aos desafios impostos pelo "impacto destrutivo das informações de organizações extremistas e terroristas, serviços especiais estrangeiros e estruturas de propaganda" (RÚSSIA, 2015, p. 13), e, assim, consolidar a segurança nas regiões adjacentes à Federação, foram acrescidos ao interesse em implantar sistemas multifuncionais de alta tecnologia nas áreas

fronteiriças, o aprimoramento do sistema de identificação, análise e combate de ameaças na esfera da informação; e o aperfeiçoamento da cooperação interagencias.

Aos fatores reconhecidos como ameaças à qualidade de vida dos cidadãos russos, acrescenta trechos que denunciam a "introdução de medidas econômicas restritivas" (RÚSSIA, 2015, p. 14) por adversários da Federação. Dentre as ações previstas para combatê-las, assinala a necessidade de manter o desenvolvimento e o acesso a "infraestrutura de rede, incluindo o uso de tecnologias de informação e comunicação" (RÚSSIA, 2015, p. 15). Por essa lógica, considera a modernização da produção industrial, com base no desenvolvimento de novas indústrias de alta tecnologia e investimentos no CIM, o ponto fulcral da estratégia (RÚSSIA, 2015, p. 19)

A segurança tecnológica é apontada como fator preponderante no desenvolvimento sustentável da Federação que registra o compromisso em investir na "segurança nacional no campo da ciência, tecnologia e educação, inclusive na esfera da informação" (RÚSSIA, 2015, p. 21). Sobre este ponto o documento é mais específico que seu antecessor, embora mantenha o interesse no desenvolvimento de alta tecnologia, sublinha o papel de suporte do Estado na "interação entre organizações educacionais e centros de pesquisa com empresas industriais", bem como na melhoria da "qualidade do treinamento de cientistas, engenheiros e especialistas técnicos" (RÚSSIA, 2015, p. 22).

Não obstante, reforça o compromisso com o cumprimento dos acordos estabelecidos em tratados de direito internacional dos quais é signatária, e aponta as organizações internacionais como a ONU e o CSNU como peças centrais do sistema de resolução de conflitos (RÚSSIA, 2015, p. 30). Neste ponto, os militares deixam de serem considerados atores nestes processos, de maneira que a estabilidade regional é percebida como subproduto do "fortalecimento da cooperação mutuamente benéfica com os estados europeus" (RÚSSIA, 2015, p. 32,).

Em função disto, manifesta o interesse em construir um "sistema aberto de segurança coletiva na região euro-atlântica" (RÚSSIA, 2015, p. 32). Para tanto, propõe um acordo de "parceria completa com os EUA com base em interesses coincidentes, inclusive na esfera econômica, levando em consideração a influencia fundamental das relações russo-americanas no estado da situação internacional como um todo" (RÚSSIA, 2015, p. 32).

No entanto, embora sustente o compromisso em cooperar para "manter o potencial de dissuasão menos dispendioso no campo de armas ofensivas estratégicas"

(RÚSSIA, 2015, p. 33-34), a ESN (2015) insere dois artigos que sublinham a preocupação com a aproximação da infraestrutura militar da OTAN de suas zonas fronteiriças. À vista disto, frisa que a intenção da aliança do norte em adquirir funções globais que contradizem os tratados de direito internacional, representa o grande fator de desestabilização das relações entre a Federação e as potências ocidentais (RÚSSIA, 2015, p. 34).

Conquanto, reintera o interesse em fortalecer a segurança da Eurásia mediante a aproximação das relações com seus adversários, desde que efetuadas com base no respeito aos "interesses legítimos da Federação Russa na implementação do planejamento político-militar" (RÚSSIA, 2015, p. 34).

Ademais, a preocupação com o funcionamento dos sistemas de informação e a construção de um sistema unificado de suporte foi mantida. No entanto, a diretriz se tornou abstrata, estabelecendo como fundamental à sua efetiva implementação o investimento em segurança da informação, sem, contudo, apresentar uma descrição detalhada das ações a serem implementadas neste campo (RÚSSIA, 2015, p. 35).

A ESN (2015) oferece uma resposta clara ao confronto de interesses posto entre a Federação e os Estados Unidos e seus aliados no que se refere aos conflitos regionais na Eurásia, na medida em que reforça sua intenção de atuar de modo independente nas esferas da política externa e doméstica. Nesse sentido, o desafio geopolítico imposto pela expansão da infraestrutura militar da OTAN, ignorando os interesses legítimos da Rússia foi contraposto de modo objetivo na nova estratégia.

Destarte, a análise documental realizada identificou diretrizes e orientações normativas, as quais promoveram transformações institucionais para incorporar o ciberespaço como um novo domínio da guerra, condição necessária para atender aos anseios estratégicos do poder nacional russo.

Conforme veremos, o conflito que resultou da irreparável equalização dos interesses das elites políticas e econômicas de Rússia e Ucrânia na região da Eurásia, somado ao robustecimento das capacidades de emprego da força por parte das instituições de segurança e defesa da Federação Russa, representa o segundo caso excepcional do uso do ciberespaço em ações ofensivas para auferir vantagens estratégicas em um conflito regional. Nesse ensejo, a seção seguinte, apresenta destaca as operações militares deflagradas pelos russos, com foco na identificação do mecanismo que regula o uso do ciberespaço para consecução de objetivos estratégicos do Estado.

4.3. Guerra Cibernética: o emprego da tecnologia da informação no conflito Rússia-Ucrânia (2014-2015).

A fim de compreender de forma substantiva os efeitos do fenômeno da guerra cibernética esta seção pretende examinar os ataques cibernéticos que atingiram setores de infraestrutura crítica na Ucrânia em seu contexto mais amplo que se constitui numa cadeia de eventos interconectados que aproximam campanhas de reconhecimento e exploração de sistemas de informação ao uso da força militar (BRENNER, 2011; LILIENTHAL, AHMAD, 2015), considerada condição suficiente para o uso efetivo do ciberespaço para projeção de poder nacional.

A partir da coleta de evidências que revelam o *modus operandi* das instituições civis e militares russas via ciberespaço, bem como as principais ameaças e armas utilizadas, identificamos o funcionamento do mecanismo de ação conjunta entre os atores estatais e não-estatais nas operações, simbiose que amplifica a assimetria de poder entre Rússia e Ucrânia em contexto regional. Por essa lógica, a ligação entre a campanha de espionagem cibernética e atores estatais russos - Serviço Federal de Segurança e Agência Federal de Comunicações e Informações Governamentais (FAGCI) - pode ser tomada como a pedra angular do processo.

Ao passo em que verificamos a dinâmica das operações, nossa análise do conflito frisa a congruência entre os ataques cibernéticos e as ações convencionais de uso da força como indicativo da relevância estratégica do ciberespaço para consecução de objetivos do Estado em conflitos regionais.

Sem embargo, relatórios de agências especializadas em segurança cibernética e de instituições governamentais contêm uma série de evidências que indicam a ligação entre as atividades de atores não-estatais em conjunto com as forças Spetsnaz.[30] Este material registra uma série de ataques de infiltração, que fizeram uso de *spear phishing e-mails*[31] para instalar armas cibernéticas capazes de subtrair informações sigilosas de setores de comunicação, bancários e eleitorais, bem como ataques disruptivos que causaram danos cinéticos ao paralisarem sistemas operacionais de infraestrutura crítica

[30] Spetsnaz (Спецназ): grupos especiais de intervenção da polícia, dos ministérios de justiça e assuntos internos russos, FSB, Serviço de Inteligência Estrangeira, Agência Federal de Comunicações e Informações Governamentais (FAGCI), bem como do exército russo.

[31] *Spear phishing*: comunicação eletrônica direcionada a indivíduos, organização ou negócios específicos com intenção de instalar *malwares* espiões nos computadores dos alvos.

elétrica (CROWDSTRIKE, 2014; 2015; 2016; FIREEYE, 2014; 2016; F-SECURE LABS 2016; LOOKINGGLASS, 2015; ICS-CERT 2016; E-ISAC 2016).[32]

O relatório emitido pelo Grupo de Inteligência sobre Ameaças Cibernéticas (CTIG) classificou as operações como "uma mistura alarmante entre espionagem cibernética, guerra física e as forças políticas por trás delas" (LOOKINGLASS, 2015, p. 3). Nesse sentido, ao confrontarmos as motivações políticas e militares com a análise da linha do tempo dos ataques, o não envolvimento da Rússia nas operações se torna de difícil sustentação.

Dentre os efeitos observados, a 'Operação Armadegon', envolvendo a 16ª divisão da FAGCI e do 18º Centro do FSB em conjunto com *hackers* altamente qualificados, se destaca devido às capacidades demonstradas pelos invasores para subtrair informações do governo, polícia e militares que permitiram aos russos anteciparem os planos formulados em Kiev para conter o avanço de suas tropas (LOOKINGLASS, 2015).

Os ciberataques foram realizados mediante o envio de correios eletrônicos contendo arquivos de extração automática (SFX) maliciosos que, ao serem abertos, permitiam aos invasores coletarem informações valiosas dos alvos. A análise da infraestrutura de rede identificou nomes de arquivos similares e períodos de maior volume de ataques cibernéticos que coincidiam com o horário de trabalho em Kiev, fatores que facilitaram o rastreamento das atividades dessas ameaças (LOOKINGLASS, 2015, p. 18).

O quadro abaixo (Quadro 7) sumariza as informações do relatório que apontam os efeitos da campanha de espionagem cibernética com base na ligação entre os ataques cibernéticos e os principais eventos políticos e militares que ocorreram durante o conflito.

Quadro 7. Cronograma da operação "Armadegon"

2014	Ação física	2014	Ação cibernética
15 Abril	Após separatistas tomarem o controle das cidades de Luhansk e Donetsk, o governo ucraniano anuncia uma "operação antiterrorista" para retomada dos territórios	16 abril	"install_flashplayer_aih.exe" dropper SFX instalado em arquivo formato Microsoft Word disparado via spear phising para alvos militares, mídia e org. governamentais
14	Separatistas derrubam avião militar	14	Novos ciberataques são detectados

[32] Os relatórios analisados representam fontes secundárias que contêm informações produzidas por especialistas em segurança cibernética reconhecidos mundialmente. Tratam-se, pois, de um recurso central para coleta de evidências sobre as operações envolvendo atores estatais e ameaças cibernéticas.

Junho	ucraniano com 49 oficiais	Junho	utilizando o mesmo malware e portas de entrada TTPs para buscar informações sobre como a Ucrânia iria responder ao ocorrido
20 Junho	Primeiro cessar-fogo (1 semana)	20 Junho	Os ataques cibernéticos cessam (1 semana)
17 Julho	Queda do voo MH17 Malaysian Airlines (298 civis mortos), as forças armadas russas auxiliam a retomada das cidades ucranianas do leste que haviam sido tomadas pelas tropas do governo central	17 julho	"install.flashplayer_aih.exe" nova versão, o 123.cmd não inclui mais uma senha necessária para abrir o arquivo SFX de "sex.exe". Direcionado para alvos militares, mídia e org. governamentais. Arquivo contém relatório legítimo para notificação diária da Administração do Presidente da Ucrânia sobre as operações antiterroristas na Ucrânia, dados sobre ataques terroristas contra o exército ucraniano e suas perdas
24 Agosto	Após invasões das forças armadas russas nos territórios do leste, as forças ucranianas são forçadas a se retirar	26 agosto	Os ataques cibernéticos cessam na região leste, início da retomada da operação de espionagem
12 Setembro	SBU anuncia que identificaram movimento de forças especiais russas programando novos ataques cibernéticos contra a Ucrânia	30 outubro 26 novembro	Spear phising com dois arquivos datados de 21 de agosto endereçados via email para contas pessoais e do Tribunal Internacional de Arbitragem Comercial da Câmara de Comércio e Indústria da Ucrânia são encontrados com links para páginas falsas de acesso ao Google Chrome
2015	Ação física	2015	Ação cibernética
15 janeiro 29 janeiro	Após um longo combate as tropas ucranianas perdem o controle do aeroporto de Donetsk para os separatistas	25 janeiro	Execução de arquivo SFX contendo malware indexado a documento oficial escrito em ucraniano com dados sobre equipamentos e batalhões de reconhecimento envolvidos no conflito em julho de 2014
8 fevereiro	Segundo cessar-fogo Chefe do centro antiterrorista da SBU divulga informações sobre os ataques das forças especiais russas	15 fevereiro 16 fevereiro	Os ataques cibernéticos não param até a retirada das tropas ucranianas do Debaltaseve, só então os ataques cibernéticos cessaram. As ameaças foram movidas para servidores de uma transportadora internacional de logística de carne e uma loja de eletrônicos Dropper com relatório do centro antiterrorista da SBU sobre os territórios do leste é utilizado em novos ataques spear phising contra alvos militares
13 março	SBU divulga comunicado oficial sobre atividade cibernética russa atribuída à 16ª antiga FAGCI e 18º FSB da Rússia	25 março	Novos ataques spear phising são identificados, dessa vez com as entradas de servidor TTPs monitoradas pela SBU modificadas. Dois arquivos SFX com novos códigos "tron.cmd" contendo malwares identificados

Fonte: Elaborado pelo autor com base em LookingGlass (2015).

Não obstante, ao longo da operação, distintas APAs utilizaram táticas de intrusão sofisticadas para comprometer sistemas de informação do governo, mídia e infraestrutura crítica da Ucrânia, com ataques cibernéticos de negação de serviço e espionagem. Destacamos as APAs28: CyberBerkut; FancyBear/Sofacy/Pawn Storm e Sandworm (CROWDSTRIKE, 2015; 2016).

> O uso do ciberespaço no conflito ucraniano é particularmente interessante porque combina táticas cibernéticas e de guerra de informação. Isso inclui adulteração de cabos de fibra ótica e telefones celulares de parlamentares ucranianos, além de ferramentas maliciosas mais comuns, como ataques DDoS e falhas na web. O alcance dessa atividade ilustra como a guerra cibernética pode ser diferenciada da guerra de informação e sugere que as ações cinéticas futuras provavelmente serão acompanhadas por ambas (MAURER, JANZ, 2014).

Destarte, uma das armas cibernéticas mais utilizadas na Ucrânia foi o '*BlackEnergy'* (BE)[33]. Ao longo do conflito diversas variações deste código malicioso foram identificadas, capazes de atingir alvos políticos, ocasionando a queda de diversos sítios eletrônicos do governo, incluindo o do gabinete presidencial ucraniano (BERGEN, MAURER, 2018); em sua versão mais sofisticada, este código malicioso foi utilizado para comprometer o funcionamento de sistemas operacionais de infraestrutura crítica (ICS 2016; E-ISAC 2016).

Em fevereiro de 2014, diversos ataques envolvendo o uso de variantes do código malicioso BE foram registrados, dentre os efeitos das operações de reconhecimento e exploração os invasores obtiveram acesso aos serviços de telefonia celular de membros do parlamento ucraniano, interferindo na comunicação entre os envolvidos no processo decisório de resposta à invasão do território da Crimeia (MAURER, 2015).

A sabotagem das redes de comunicação evitou que o poder público tomasse uma atitude com relação ao movimento das forças russas (WEEDON, 2015). Apenas quatro dias após a anexação da península ucraniana, instalações da empresa de comunicações Ukrtelecom foram invadidas e os cabos de fibra ótica adulterados, inviabilizando a conexão entre a península e o restante da Ucrânia (MAURER, 2015).

---

[33] A evolução deste malware tem sido acompanhada por diversas empresas especializadas em segurança cibernética que apontam a convergência entre as atividades criminosas e a espionagem russa através do ciberespaço (FIREEYE, 2014; F-SECURE LABS, 2016).

Vale ressaltar que os ataques cibernéticos ocorreram em sincronia com as ações das forças militares russas e grupos mercenários, os chamados “homens de verde” (Spetsnaz), representam grupos armados e agentes de inteligência sem identificação, responsáveis pelas operações militares que tomaram controle da península e apoiaram os movimentos separatistas do Leste (GILES, 2015, p. 20).

> Grupos de homens armados não identificados começaram a aparecer em toda a região, frequentemente em coordenação com milícias pró-russas locais. Tanto o governo ucraniano quanto a maioria das fontes de inteligência ocidentais alegaram que os “homenzinhos verdes” eram agentes russos. As milícias da “autodefesa” da Crimeia apreenderam prédios do governo, bases aéreas e instalações militares, e o governo de Kiev, desejando evitar derramamento de sangue e outras provocações, ordenou que suas forças militares não resistissem (ESTADOS UNIDOS, 2015, p. 31).

As tropas especiais empregaram equipamentos das Forças Armadas da Federação Russa que incluíam veículos blindados de transporte de pessoal e helicópteros. Embora, o Kremlin tenha, inicialmente, negado envolvimento nas operações, pouco tempo depois a sede da frota russa do Mar Negro em Sevastopol admitiu que a península havia sido ocupada para garantir o controle do porto (ESTADOS UNIDOS, 2015, p. 56).

Em março, a APA CyberBerkut atingiu a página da rede do governo da Ucrânia, que ficou fechada por três dias, além dos sites oficiais, telefones celulares dos parlamentares ucranianos também foram invadidos (WEEDON, 2015). Na ocasião, o grupo composto por dissidentes das forças policiais ucranianas, passou a vincular notícias na Internet com informações que condenavam como ilegítimo o governo ucraniano formado após a expulsão do ex-presidente Viktor (CROWDSTRIKE, 2014).

A CyberBerkut utilizou as variações ‘*BE.lite’*[34] e ‘*BlackEnergy2’* (BB2)[35] para subtrair informações sigilosas como códigos de execução e senhas de acesso remoto de seus alvos, em geral compostos por políticos ucranianos do alto escalão do governo. O vazamento periódico de documentos sigilosos prosseguiu durante os primeiros meses do conflito “foram mais de 50 itens exclusivos, emails, relatórios, acordos, propostas, imagens aéreas e identificação pessoal” (CROWDSTRIKE, 2015, p. 29).

[34] Arma cibernética que utiliza diretórios temporários para executar arquivos iscas infectados com o *malware* que são carregados por comandos “rundll32.exe”, a variante não utiliza *rootkit* para ocultar objetos no sistema ou *driver kernel* para descarregar os arquivos (LIPOVSKY, 2014, p. 3).

[35] Arma cibernética capaz de esconder os processamentos de rotina utilizados nos ataques, mantém uma lista codificada de *offsets* em estruturas de *driver kernel* que oferece acesso total às informações dos sistemas contaminados (F-SECURE LABS, 2014b, p. 1).

Em abril de 2014, quando o conflito eclodiu por toda região leste, as operações cibernéticas para coleta de informações vitais aos setores de inteligência aumentaram exponencialmente, oferecendo vantagem significativa às tropas russas no campo de batalha cinético (LOOKINGGLASS, 2015).

Naquele mês a CyberBerkut atingiu empresas militares privadas que operavam no conflito, o grupo assumiu a autoria dos ataques que atingiram a rede da Comissão Central de Eleições (CEC), na ocasião, os invasores assumiram o controle da página que exibia os resultados da apuração eleitoral em tempo real, minutos antes do encerramento da contagem, o grupo publica uma foto anunciando a vitória do conservador Dmitry Yarosh no sítio eletrônico oficial da CEC, a notícia falsa foi imediatamente compartilhada pelos canais de televisão russos (KOVAL, 2015, p. 56).

No dia seguinte, quando o sistema da CEC teve seu funcionamento reestabelecido pelo serviço de segurança ucraniano, a comissão confirmou a invasão, e só então declarou a vitória do social-democrata Petro Poroshenko à presidência.

Sem embargo, o grau de alinhamento das operações com as prioridades estratégicas das instituições securitárias russas chamou a atenção de especialistas do setor de segurança cibernética que, à altura, sublinharam o apoio técnico e tático dado pela Federação aos movimentos que declararam a independência dos territórios de Donbass da Ucrânia, em 21 de maio. O volume e a magnitude dos ataques cibernéticos aumentaram juntamente aos eventos políticos em andamento, por conta disso, a coordenação entre a propaganda distribuída e as informações vinculadas pela grande mídia foi apontada como evidência do *modus operandi* dos serviços de inteligência da Federação através do espaço de informação (CROWDSTRIKE, 2014; KOVAL, 2015).

Igualmente identificada nas operações, a APA FancyBear/Sofacy/PawnStorm é apontada como responsável por atingir diversas organizações políticas com armas cibernéticas multifuncionais. A APA vinculada ao GRU (CROWDSTRIKE, 2016) foi identificada como responsável pela campanha de espionagem cibernética orquestrada para usurpar credenciais de acesso corporativo a sistemas de informação de importantes organizações governamentais da Ucrânia, como Forças Armadas, Ministério da Defesa, indústria de Defesa, partidos políticos, mídia e governos (HACQUEBORD, 2015).

Em agosto, uma série de e-mails *spear phishing* contendo uma lista com nomes de membros do parlamento ucraniano que supostamente estariam oferecendo apoio aos separatistas do leste foram enviados em nome do primeiro ministro da Ucrânia Arzeniy Yatsenyuk a diversos órgãos de investigação ucranianos –dentre os quais, Ministério

Público, Serviço de Segurança, Ministério de Assuntos Internos e o Ministério da Justiça-, a isca continha diretrizes oficiais para que essas instituições verificassem a veracidade das informações contidas nos documentos, conquanto, o arquivo em anexo estava infectado com um arquivo malicioso que, ao ser aberto, oferecia acesso às contas destes servidores aos invasores (LIPOSVKY, 2014, p. 2–3).

As amostras dos códigos maliciosos coletados contêm informações escritas em idioma russo, além disso, a APA registrava suas atividades em horário comercial, de acordo com o fuso horário das principais cidades da Federação Russa, "evidências de operações focadas e de longa data que indicam um patrocinador do governo — especificamente, um governo com sede em Moscou" (FIREEYE, 2014, p. 3).

> Mais de 96% das amostras de malware que atribuímos ao APA28 foram compiladas entre segunda e sexta-feira. Mais de 89% foram compilados entre 8h e 18h no fuso horário UTC+4, que é paralelo ao horário de trabalho em Moscou e São Petersburgo. Essas amostras tiveram datas de compilação que variaram de meados de 2007 a setembro de 2014 (FIREEYE, 2014, p. 5).

O relatório registra que as amostras "utilizam a mesma sequência de descriptografia e algoritmos semelhantes para codificação e decodificação" (FIREEYE, 2014, p. 21), ademais, há um padrão identificável nos códigos maliciosos, "arquivos com nomes específicos, hashes MD5, carimbos de data e hora, funções personalizadas e algoritmos de criptografia, backdoors com endereços de IP e Comando e Controle similares e nomes de domínios incorporados" (FIREEYE, 2014, p. 29).

As ações cibernéticas das APAs Pawn Storm e CyberBerkut estar conectadas a fim de facilitar o intercâmbio de informações roubadas e o vazamento de documentos confidenciais. Embora a relação entre elas ainda tenha sido pouco explorada, analistas sublinham que a "CyberBerkut publicou informações roubadas durante as campanhas do Pawn Storm" (HACQUEBORD, 2017, p. 8).

Outra arma cibernética associada a esta APA, o '*X-Agent*'[36], desenvolvido em formato de aplicativo pelo oficial ucraniano Yaroslav Shertuk, com a promessa de oferecer maior eficiência aos sistemas de artilharia do Exército, reduzindo o tempo de disparo de minutos para segundos, foi introduzida em fóruns militares ocorridos na Ucrânia, e chegou a ser utilizada por quase nove mil usuários. Uma vez instalada, a

[36] Arma cibernética de acesso remoto capaz de infectar sistemas operacionais como Windowns, iOS e plataformas móveis. Possui arquitetura modular que combina a funcionalidade de implante necessária de acordo com o equipamento utilizado pelo alvo escolhido (CROWDSTRIKE, 2014, p. 59).

ferramenta implantava de modo sigiloso um código malicioso nos sistemas operacionais de telefonia celular dos alvos que, em grande parte, integravam a artilharia ucraniana (MEYERS, 2016).

Os aparelhos infectados forneciam aos invasores a localização exata, e em tempo real, das tropas inimigas, por sua vez os dados eram repassados aos setores de inteligência russos permitindo às tropas anteciparem os movimentos do adversário no campo de batalha. A análise código apresentou uma série de artefatos em língua russa de natureza militar que indicam uma correlação entre o grupo e o setor de inteligência militar russa que operava em apoio aos separatistas do leste (MEYERS, 2016).

Figura 2. Área sob controle dos separatistas 2014-2015

Fonte: BBC (2015)

A última APA identificada no conflito é o Sandworm, apontada como responsável pelos ataques a setores de infraestrutura crítica elétrica da Ucrânia, em dezembro de 2015, os principais malwares utilizados nos ataques cibernéticos disruptivos foram o '*BlackEnergy 3'* (BB3)[37] e o '*KillDisk'* (KD)[38] (LIPOVSKY, 2014).

Sem embargo, o DHS em conjunto com a Equipe de Resposta a Emergências Cibernéticas de Sistema de Controle Industrial (ICS-CERT), e, em parceria com o instituto SysAdmin, Auditoria, Rede, Segurança (SANS) e o Centro de Análise e Compartilhamento de Informações de Eletricidade (E-ISAC), emitiram relatórios sobre

[37] Arma cibernética utilizada para infiltração e roubo de informações que não utiliza componente de *driver kernel*, invade diretamente a pasta de dados do aplicativo local e instala um arquivo LNK para executar o malware usando o "*rundll32.exe*" (F-SECURE LABS, 2016, p. 11).
[38] Arma cibernética desenvolvida para apagar o rastro dos processos de infiltração conectados via *serial-to-ethernet* e substituir o arquivo executável por dados aleatórios (E-ISAC 2016, p. 6).

o envolvimento da Federação Russa nos ataques cibernéticos que causaram a interrupção no fornecimento de energia elétrica na região ucraniana Ivano-Frankvisk (E-ISAC, 2016; ICS-CERT, 2016).

O incidente, reportado em 24 de dezembro pela Kyivoblenergo (companhia regional de distribuição de energia elétrica), revelou que terceiros obtiveram acesso ilegal ao sistema de tecnologia de informação da rede elétrica, desconectando sete subestações 110kV e 23 35kV, por três horas. O relatório confirma o envolvimento de uma rede de planejamento e coordenação de difícil detecção, capaz de ocultar os rastros contidos nos dispositivos atingidos (ICS-CERT, 2016, 1-2).

Com alto grau de complexidade técnica, esta representa uma operação especial, de longo prazo, que se estimou ter levado aproximadamente seis meses, entre o reconhecimento do sistema e o ataque disruptivo. Uma operação que só poderia ser efetuada por agentes especializados em táticas de intrusão, com acesso a recursos externos e treinamento profissional, capazes de subtrair credenciais e informações privadas para obter acesso aos sistemas operacionais que controlavam a distribuição de energia, sem que sua presença pudesse ser notada pelos operadores de segurança.

> Os atores demonstraram experiência, não apenas em redes e infraestrutura online, como Fontes de Alimentação Ininterrupta (UPSs), mas também em operar os ICSs através de um sistema de controle de supervisão, como a Interface Homem Máquina (HMI) [...] A capacidade mais forte dos atacantes não estava na escolha das ferramentas ou na sua perícia, mas na capacidade de realizar operações de reconhecimento para aprender sobre o ambiente e executar um ataque múltiplo altamente sincronizado (E-ISAC, 2016, p. 1–2).

As etapas de planejamento e execução dos ataques seguiram o modelo apresentado por Assant e Lee (2015). Composta por diversos estágios, a operação envolveu em seu primeiro estágio as fases de preparação e execução da intrusão cibernética, mediante o reconhecimento do sistema e armazenamento do código malicioso (E-ISAC 2016).

Durante a fase de planejamento, os computadores da companhia regional de distribuição de energia elétrica foram infectados com o uso de *spear phising* e-mails enviados aos usuários que possuíam acesso à rede administrativa. Estes correios eletrônicos continham arquivos em formato Microsoft Office Excel e Word infectados com a variante BB3, que permitiram aos invasores extraírem os códigos de informação e senhas de acesso aos sistemas operacionais das instalações. Uma vez sob controle dos

alvos, a APA atuava no ambiente infectado com as credenciais de usuários autorizados; o acesso irrestrito e indetectável permitiu descobrir as vulnerabilidades do sistema e extrair os dados necessários para um ataque disruptivo efetivo e sigiloso (E-ISAC, 2016).

Com acesso ao sistema de C2, os invasores puderam utilizar a própria rede privada virtual (VPN) das estações para obter acesso aos dados administrativos das empresas e lançar comandos destrutivos à distância. Desse modo, a APA conseguiu atingir os alvos físicos sem que fossem detectados pelo sistema de segurança (E-ISAC, 2016).

A fase seguinte resultou no desenvolvimento e execução do ataque cibernético que danificou os sistemas operacionais das estações e subestações elétricas de modo simultâneo. Após o feito, para evitar o rastreamento, os invasores utilizaram o código KD para destruir os arquivos corrompidos do sistema e apagar vestígios da invasão. Em arremate, promoveram um ataque do tipo de negação de serviço (D-DoS) no sistema de comunicação telefônica, para congestionar o serviço da central de atendimento ao cliente da empresa de energia e assegurar que os usuários atingidos não conseguissem relatar as interrupções (E-ISAC, 2016).

A ação, imperceptível no curto prazo, envolveu o uso de códigos maliciosos capazes de atingir dispositivos *serial-to-ethernet* e danificar não apenas os disjuntores das subestações elétricas conectadas através dos sistemas operacionais SCADA, mas, também, evitar que as estações fossem recuperadas com uso de comandos remotos (E-ISAC, 2016).

Figura 3. Área afetada pelos ataques cibernéticos

Fonte: Enciclopédia Livre (2024)

Contudo, os códigos maliciosos utilizados nesta operação não foram os reais causadores da interrupção do funcionamento dos sistemas operacionais SCADA, neste caso apenas serviram como ferramentas sofisticadas para exploração e obtenção de informações de acesso privilegiado da administração aos sistemas operacionais dessas infraestruturas que foram atingidas por comandos externos enviados pelos invasores (E-ISAC, 2016). Em suma, a execução do ataque utilizou o controle do próprio sistema para afetar o funcionamento de uma infraestrutura crítica.

Todavia, desde o ano anterior à operação, as atividades do Sandworm já estavam sendo monitoradas pelo FireEye (2014), que alertou sobre uma invasão em curso aos sistemas de energia de empresas polonesas e agências do governo ucraniano: "[...] o grupo parecia estar desenvolvendo métodos para atingir as arquiteturas especializadas de computadores usadas para gerenciar remotamente os equipamentos industriais físicos" (GREENBERG, 2017, p. 11).

Não obstante, ao utilizarem ataques para atingir alvos dessa natureza, a APA inaugurou uma nova fase no conflito que se desenrolava via ciberespaço, a operação demonstrou a alta capacidade de penetração dos invasores para atingir alvos operacionais de sistemas críticos, aumentando os riscos à segurança dessas infraestruturas.

Em função do elevado grau de sofisticação que envolve os ataques cibernéticos, somada a capacidade de transformação das armas cibernética utilizadas, se torna difícil refutar a suspeita de que estas operações tenham sido impulsionadas por uma agente institucional robusto, com recursos para alavancar, consideravelmente, campanhas de longo prazo dessa natureza. Uma vez que para ser efetiva, estas operações requerem largo investimento no desenvolvimento de tecnologia da informação e amplo conhecimento do funcionamento de sistemas operacionais de infraestrutura crítica (WEEDON, 2015).

Apesar de a Federação Russa negar, veementemente, o apoio às APAs, as evidências contidas nos relatórios apresentados nesta seção revelam como a atuação conjunta entre atores estatais e não-estatais contribuiu para ampliar a capacidade de projeção do poder nacional russo sobre um adversário regional. Nossa análise destaca, portanto, as seguintes evidências: a coincidência cronológica entre os ataques cibernéticos e as invasões por terra; os horários de funcionamento das APAs; a

engenharia da informação por detrás dos códigos das armas identificadas; e, o alto grau de sofisticação e complexidade das operações realizadas.

Conforme demonstrado, o funcionamento do mecanismo que permite a conexão entre atores estatais e não-estatais a serviço da Federação Russa para projeção de poder nacional via ciberespaço depende da cooperação interagências, interdepartamentos e iniciativa privada, bem como parceiros externos que promovam o intercâmbio de informações e expertise técnica suficientes para uso do poder cibernético com vistas à consecução de objetivos estratégicos nacionais.

4.4 Considerações Finais

Ao considerarmos as nuances que permeiam o equilíbrio das relações entre russos e ucranianos, verificamos indícios de que o conflito desencadeado em 2013, resulta de uma série de acontecimentos políticos que incidiram sobre a classe política e social de ambos os Estados, na tentativa de acomodar interesses dissonantes, mormente, devido aos efeitos provocados pelos processos de emancipação dos territórios da antiga URSS e o alargamento das instituições econômicas e securitárias ocidentais, capitaneadas por Estados Unidos e os seus aliados europeus.

Como descrito, tanto na Rússia quanto na Ucrânia, a orientação ideológica dos movimentos de libertação cedeu lugar às disputas políticas domésticas intraelites que não se furtaram em manter o caráter centralizador das estruturas da administração pública de matriz soviética, por essa lógica, a falta de coesão dificultou o equacionamento das relações externas que permitissem a promoção equilibrada dos interesses de cada qual na região. Como agravante, o processo de expansão das instituições de segurança e comércio ocidentais, foi incorporado ao eixo narrativo utilizado pela Federação Russa para justificar as operações de suas forças de segurança.

Nossa análise identifica duas condições, suficiente e necessária, que permitiram à Federação Russa utilizar o ciberespaço para projetar poder sobre a região da Eurásia. Nesse ensejo, com base em relatórios produzidos por empresas e instituições especializadas em segurança cibernética, verificamos um aumento das capacidades operacionais, manifesta em função da atuação interagencias, com vistas à consecução de objetivos estratégicos.

Dentre as principais agências estatais e não-estatais envolvidas destacamos: o FSB; a FAGCI e o GRU, órgão ao qual estão subordinadas as forças especiais russas (Spetsnaz); bem como as ameaças: CyberBerkut, FancyBear/PawnStorm/Sofacy e Sandworm.

Já a análise das fontes oficiais, aponta para a mudança institucional promovida no cerne das forças de segurança russas como a pedra angular do desenvolvimento tecnológico-científico, considerada condição necessária para assegurar seu uso efetivo e discreto em conflitos regionais. Para atingir tal meta, a Federação Russa promoveu a constituição de incentivos seletivos que permitiram a incorporação do ciberespaço como um novo domínio da guerra.

Por fim, as operações ora examinadas envolveram diretamente o uso de informações coletadas em campanhas de reconhecimento e exploração de sistemas computacionais que demonstram a significância da tecnologia da informação, da cooperação interagências e do ciberespaço para ampliar a assimetria de poder entre a Federação Russa e a Ucrânia durante o conflito (2013-2015).

CAPÍTULO V

O capítulo considera as nuances da relação sino-indiana em torno dos conflitos desencadeados por disputas territoriais em zonas fronteiriças que separam estes Estados, como ponto de partida para explicar o fenômeno da guerra cibernética. Com intuito de verificar "como as instituições produzem esses trajetos, como elas estruturam a resposta de uma dada nação a novos desafios" (HALL, TAYLOR, 2003, p. 200) procuramos responder ao seguinte questionamento: Como a China utiliza o ciberespaço para consecução de objetivos estratégicos regionais?

Ao conectarmos as implicações do processo de mudança institucional pelo qual passaram as forças de segurança e defesa da China, aos momentos críticos posteriores à eclosão do conflito regional sino-indiano (2020-2022), nossa análise identifica as condições que proporcionaram o uso efetivo e discreto do ciberespaço para consecução de objetivos estratégicos. Consideramos, pois, necessárias alterações nas diretrizes que orientam as instituições securitárias para constituição de operações especiais que, por sua vez, são suficientes para maximizar as capacidades de projeção do poder nacional frente a um adversário estratégico[39].

Tendo em conta a combinação entre segurança e desenvolvimento nacional como principal meta do Estado, a China organiza sua grande estratégia 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, REVERON, 2015).

Frente à dinâmica, a espionagem cibernética emerge como opção valiosa para promover os interesses nacionais. Conforme veremos, a criação de incentivos a constituição de operações conjuntas, envolvendo campanhas de reconhecimento e exploração de redes de computadores e ataques cibernéticos disruptivos, indica não somente o nível de desenvolvimento do aparato científico e tecnológico chinês, mas, sobretudo, a eficiência institucional em utilizar novos domínios de guerra para ampliar a assimetria de poder em conflitos regionais.

[39] Nosso exame das condições inerentes ao emprego da tecnologia de informação em operações ofensivas para atingir setores de infraestrutura crítica dá-se com base em fontes primárias (documentos oficiais) e secundárias (acadêmicas, relatórios de empresas especializadas na temática, jornais).

5.1. Conflito sino-indiano: contexto político

Nesta seção consideramos brevemente a historicidade das relações sino-indianas, de modo a compreender como se constituíram as disputas territoriais nas áreas de fronteira e quais efeitos produziram sobre o equilíbrio securitário regional.

A República Popular da China e a República da Índia compartilham uma das fronteiras interestaduais não demarcadas mais longas do mundo, com cerca de quatro mil quilômetros de distância, divididas em três setores que, atualmente, compõe a Linha de Controle Real (LCR) (WESTCOTT, 2017; MURATBEKOVA, 2018; BASHIR, TAJ, 2022)[40].

Sem embargo, a disputa fronteiriça sino-indiana pode ser considerada produto do processo histórico que, ao longo do século dezenove, envolveu a competição entre os impérios britânico e russo pela hegemonia no sistema internacional (MAXWELL, 2013). O legado deste período envolve, pois, a tradição e os costumes que, ao longo de séculos de ocupação e controle administrativo da região se cristalizaram em territórios chave como Aksai Chin e Arunachal Pradesh controlados, respectivamente, por China e a Índia (DEEPAK, 2005; MEHRA, 2007; MALIK, 2011; GARVER, 2011; SCOTT, 2011; ZHANG, LI, 2013; CHANGSHENG, BEZERRA, 2014; MOREIRA, 2016)[41].

Com a percepção de que o expansionismo russo ameaçava suas possessões os britânicos adotaram uma estratégia de fortalecimento de ‘estados tampão’ em regiões de fronteiras que incidiu diretamente sobre a dinâmica política interna de territórios como Tibete, Nepal e Butão, considerados ideais para salvaguardar os interesses da coroa (SCOTT, 2011; ZHANG, LI, 2013; 2021; BASHIR, TAJ, 2022).

No setor ocidental, o confronto com o Império Sikh (1845-1846) o qual, desde 1799, controlava os territórios de Jammu[42] e Caxemira (J&C) -atualmente localizados na Índia e no Paquistão-, envolveu a cooperação entre a Companhia Britânica das Índias

[40]Setor Oriental: Linha McMahon (India, China e Butão) parte do estado indiano de Arunachal Pradesh; Setor Médio: junção Ngari, Tibete, Las Dwags e Punjab até a trijunção China, India e Nepal; Setor Ocidental: Karakoram até Ngari, no Tibete, La Dwags e Himachal Pradesh (SCOTT, 2011; ZHANG, LI, 2013; WESTCOTT, 2017; BASHIR, TAJ, 2022).

[41] Aksai Chin: região de difícil acesso e praticamente inabitada, planalto árido e desolado com valor estratégico para a China, conecta as províncias do Tibete e Xinjiang através da Estrada Nacional 219 (ZHANG, LI, 2013). Arunachal Pradesh possui mais de um milhão de cidadãos indianos, centros budistas importantes, como Tawang, outros territórios referentes ao setor médio como Himachal Pradesh e Uttar Pradesh possuem menor valor estratégico para ambos, embora também representem áreas de disputa significativa (SCOTT, 2011).

[42] O Tratado de Chushul que reconhece o Reino de Jammu ou Ladakh, vagamente demarcado, já foi citado por chineses e indianos para reivindicar o território (WESTCOTT, 2017).

Orientais (CBIO) e o marajá Gulab Singh para libertar a região da influência administrativa chinesa, através de Lhasa no Tibete oriental (WESTCOTT, 2017).

Com o fim do conflito, Gulab Singh se tornou governante de J&C, sob o mando da Índia britânica que, por sua vez, deu início a um processo contínuo de demarcação unilateral das fronteiras, formalizando tratados que modulavam os limites territoriais da região de acordo com a posição que melhor atendesse aos interesses da coroa, manobras consideradas ilegítimas pelos chineses (DEEPAK, 2005; MEHRA, 2007; BASHIR, TAJ, 2022)[43].

De modo similar, no setor oriental, com intuito de dominar as rotas comerciais que cortavam o Tibete, o avanço britânico se deu em 1904 com a ocupação de Lhasa. A fim de assegurar sua presença na região, dois anos depois, a China retomou o controle do Tibete e quatro anos mais tarde o 13º Dalai Lama se refugiou na Índia (WESTCOTT, 2017).

A disputa entre britânicos e chineses se intensificou com a eclosão da Revolução de 1911 que destituiu a Dinastia Qing e pôs fim à monarquia, a turbulência minou a capacidade chinesa de exercer o controle efetivo das regiões fronteiriças, com isso os britânicos passaram a controlar a fronteira nordeste, anexando Lhasa e o Tibete, em 1912 (DEEPAK, 2005). No ano seguinte, Dalai Lama, que havia regressado ao Tibete, declarou a autonomia do território e da província de Lhasa, dando início as hostilidades entre separatistas tibetanos e militares chineses (WESTCOTT, 2017)[44].

Frente ao contencioso, os britânicos organizaram a conferência de Simla (1913-14) para promover um acordo de delimitação das fronteiras no setor. Ao final das tratativas, a proposta Linha McMahon[45], que na prática empurrava a fronteira indo-tibetana sessenta milhas para o norte, foi aceita formalmente por líderes políticos tibetanos, mas rejeitada pelos chineses que não reconheciam a autonomia do Tibete (MALIK, 2011; MURATBEKOVA, 2018; BASHIR, TAJ, 2022).

---

[43] Em 1885 os britânicos consideraram Aksai Chin parte da Caxemira, e quatro anos depois propuseram um acordo reconhecendo o controle dos chineses de parte do setor ocidental, em específico, sobre Aksai Chin, já as possessões sobre Lingzitang e o Vale Chip Chap deveriam ser mantidas sob os auspícios da coroa (SCOTT, 2011; CHANGSHENG, BEZERRA, 2014).

[44] Os chineses consideravam Tawang e Lhasa como parte do Tibete do Sul, pois, cumpriam obrigações fiscais com a China desde 1720, quando a Dinastia Qing estabeleceu a ligação administrativa e demográfica na região (BASHIR, TAJ, 2022). Já os indianos compreendiam estes territórios como um dos espaços estratégicos vitais para a Índia, pois, oferecem acesso ao Vale do Brahmaputra e a outros estados do Nordeste; proteção ao flanco oriental com o Butão; e o menor trajeto para chegar ao Tibete e/ou à China em caso de confronto militar (SCOTT, 2011).

[45] A demarcação passa por Butão e Mianmar, separando o Tibete de Siquim e Arunachal Pradesh, representa, pois, um marco temporal significativo para defesa da região nordeste da Índia (BASHIR, TAJ, 2022).

Ao longo das duas décadas seguintes, um equilíbrio tênue nas relações entre a Índia britânica e a China manteve o setor oriental livre de conflitos, situação que começou a se modificar em 1937, quando os britânicos reafirmaram, unilateralmente, a legitimidade da fronteira demarcada pela Linha McMahon (MEHRA, 2007).

Neste ínterim, na China a eclosão da guerra civil (1927-37), produto do prolongamento da instabilidade doméstica provocada por disputas entre comunistas e nacionalistas pelo controle político e administrativo do Estado, impediu qualquer tomada de decisão assertiva nas regiões fronteiriças, que porventura viesse a ameaçar a legitimidade das lideranças (MAXWELL, 2013). Conquanto, a percepção de insegurança no ambiente regional foi considerada pela classe política como efeito temporário do imperialismo britânico o qual, desconsiderando a soberania estabelecida desde o século treze pela Dinastia Mongol Yuan (1271-1368), pretendia criar um Tibete independente na região (SCOTT, 2011).

Em meados da década de quarenta, com o fim da segunda Guerra Mundial (1939-1945) e a consequente erosão da hegemonia britânica ao final do conflito, movimentos separatistas tomaram fôlego nas possessões coloniais (MAXWELL, 2013). Diante do cenário, em 1947, a coroa reconheceu a independência da República da Índia que passou ao controle político e administrativo da União Indiana, sob a liderança de Nehru como primeiro-ministro (WESTCOTT, 2017)[46].

Por outro ângulo, em 1949, o processo revolucionário liderado por Mao Zedong que retirou o nacionalista Chiang Kai-shek do poder e estabeleceu o regime comunista, deu origem à República Popular da China. Daí em diante, Mao passou a organizar a política externa de forma personalista e pragmática, razão pela qual, nos anos cinquenta, os chineses não adotaram o irridentismo em matéria de disputas territoriais em áreas de fronteira (CHANGSHENG, BEZERRA, 2014).

Neste período, ambos os líderes políticos em ascensão encaravam a unidade e a integridade territorial como símbolos do poder nacional, logo as disputas em região de fronteira eram consideradas estratégicas, pois, capazes de produzir efeitos significativos sobre o capital político em âmbito doméstico. A conta disso, a narrativa adotada para atuarem nestas áreas guarda certa similaridade, enquanto que os chineses procuravam

[46] Desde o final da Grande Guerra (1914-18), o enfraquecimento paulatino da influência do império britânico havia permitido a articulação entre setores das oligarquias agrárias e a classe política indiana que, sob a liderança de Jawaharlal Nehru, deram origem ao processo de independência do país (MEHRA, 2007; MAXWELL, 2013).

reaver territórios governados por dinastias seculares, os indianos intentavam assegurar as possessões conquistadas pelo império britânico (MURATBEKOVA, 2018).

A despeito disso, em que pese o fato de as fronteiras ao longo do Himalaia nunca terem sido oficialmente demarcadas com reconhecimento de ambos os lados, entre 1949-1957 as relações sino-indianas fluíam de modo satisfatório (MAXWELL, 2013).

A conta disto, apesar do compromisso firmado pela classe política em dar continuidade à estratégia expansionista britânica - '*Forward Policy'* -[47], a Índia reconheceu o Tibete como parte integral do território da China, em 1950. Em contrapartida, no ano seguinte, a administração Nehru criou a Agência da Fronteira Nordeste (AFN) no setor oriental e organizou expedições que ocuparam o mosteiro de Tawang (ZHANG, LI, 2013).

Com os ruídos nas relações sino-indianas aumentando, entre 1951 e 1954 foram propostos acordos de confiança mútua que registraram a relevância estratégica do setor oriental, considerado por indianos uma região autônoma e por chineses como parte integral de seu território. Diante do quadro, as lideranças acordaram em cumprir com os 'Cinco Princípios de Coexistência Pacífica', os quais preconizavam o respeito mútuo pela integridade territorial e soberania, bem como a não interferência nos assuntos internos de cada qual (ZHANG, LI, 2013)[48].

Não obstante, na Índia mapas oficiais que registravam as fronteiras demarcadas de acordo com o entendimento do governo começaram a ser amplamente divulgados[49], em resposta, os chineses fizeram o mesmo, mas na direção oposta. Paralelamente, ambos mantiveram projetos para construção de infraestrutura civil e militar nas regiões de fronteira contestada (MURATBEKOVA, 2018)[50].

Ao final dos anos cinquenta a névoa que envolvia as relações sino-indianas começou a se dissipar, ao passo em que atritos cada vez mais frequentes entre forças militares na zona fronteiriça desgastavam seu tênue equilíbrio (BASHIR, TAJ, 2022).

---

[47] Estratégia britânica de avanço de tropas para ocupar s territórios considerados legítimos que foi readaptada pela Índia para avançar sobre regiões fronteiriças (MAXWELL, 2013).

[48] No ano seguinte, na Conferência de Bandung, a China reforçou compromisso com a política de coexistência pacífica, e a promoção de incentivos a construção de mecanismos de cooperação capazes de mitigar os efeitos perversos da descolonização (CHANGSHENG, BEZERRA, 2014).

[49] Com base no acordo de Panchsheel a Índia alterou os mapas incorporando Aksai Chin ao seu território (WESTCOTT, 2017).

[50] No setor ocidental, entre 1953-57 a China finaliza a autoestrada NH 219 conectando a província de Xinjiang ao Tibete através de Aksai Chin; já no setor oriental passou a reivindicar o território de Assam como parte do Tibete, contestando a demarcação da Linha McMahon (ZHANG, LI, 2013; BASHIR, TAJ, 2022).

Frente ao cenário, em 1959, os laços culturais e históricos que mantinham as relações em patamares amistosos foram desfeitos, em parte, devido à decisão da administração Zedong em realizar as reformas social e agrária no Tibete, movimento que provocou a reação da teocracia tibetana apoiada pela Índia (CHANGSHENG, BEZERRA, 2014).

Como resultado da repressão aos separatistas por tropas chinesas, novamente, o Dalai Lama se refugiou em solo indiano, onde declarou um novo governo. Por conseguinte, a administração Nehru reforçou o compromisso com a política externa expansionista, tornando os embates entre as forças militares inevitáveis (CHANGSHENG, BEZERRA, 2014; BASHIR, TAJ, 2022). Nesse ínterim, setores da inteligência do ELP da China acusaram os indianos de subsidiarem a revolta no Tibete com intuito de forçar a negociação de territórios em disputa nas fronteiras (WESTCOTT, 2017).

Frente ao contencioso, os primeiros enfrentamentos entre forças militares ocorreram em 25 de agosto de 1959, na região de Aksai Chin, mais precisamente no território de Longjiu, lado chinês da Linha McMahon. Naquele mesmo ano, um novo confronto eclodiu na região de Kongka, divisa entre a Caxemira e Aksai Chin, provocando a morte de nove policiais indianos e outros sete detidos (CHANGSHENG, BEZERRA, 2014).

A percepção de insegurança na região fez com que os chineses tomassem a iniciativa de promover negociações em torno dos territórios em disputa, em um ano notas, cartas e memorandos sobre a questão foram trocados com os indianos (FANG, 2014). Nesse cenário, em 1960, o então Ministro das Relações Exteriores Zhou Enlai, em visita a Índia, demonstrou interesse em reconhecer as fronteiras conforme a demarcação britânica, porém com os ajustes que se fizessem necessários (FRAVEL, 2008; KALHA, 2014).

A proposta de acordo apontava que os chineses abdicariam de reivindicar territórios abaixo da linha McMahon se, em contrapartida, os indianos abandonassem qualquer aspiração sobre Aksai Chin. Entretanto, diante da recusa de Nehru em aderir aos termos, a fim de assegurar o controle de Aksai Chin, no ano seguinte tropas do Exército do ELP substituíram as forças de segurança (PAPF) no setor ocidental (WESTCOTT, 2017).

A operação militar preparada pelo Estado-Maior do ELP para controlar a região fronteiriça de Thag La, a norte da Linha McMahon, ocupou postos controlados por tropas indianas em Dhola sem que houvesse enfrentamento militar. Três dias depois a

situação se modificou com a decisão da classe política indiana de reprimir com uso da força qualquer nova incursão chinesa ao seu território (CHANGSHENG, BEZERRA, 2014).

O fomento aos movimentos separatistas no Tibete, a fuga do Dalai Lama e a constante recusa de Nehru em negociar a resolução do contencioso nos termos propostos pela China, bem como os confrontos sucessivos na região fronteiriça entre forças militares contribuíram, sobremaneira, para a deterioração nas relações sino-indianas que acabaram se rompendo.

Consequentemente, no mês seguinte, mesmo após as tropas chinesas terem desocupado o posto de Dhola, as hostilidades não cessaram. Diante do impasse, em 18 de outubro os chineses lançaram a contraofensiva que deu origem à guerra sino-indiana, em 1962 (DEEPAK, 2005; KALHA, 2014).

As operações do ELP tiveram início em 20 de outubro, com a retomada de postos estratégicos em Ladakh e Arunachal Pradesh, seguidas por um cessar-fogo por vinte dias. Nesse ínterim, Nehru rejeitou as propostas chinesas de negociação, e, em 14 de novembro, lançou uma nova operação para retomar postos de controle militares. Porém, dessa vez, o contra-ataque chinês foi assertivo e eliminou a presença indiana na região em 22 de novembro. Após a vitória a China declarou cessar-fogo unilateral e recuou suas tropas para a posição ocupada, em 1959 (BASHIR, TAJ, 2022)[51].

Em âmbito doméstico, as disputas territoriais na fronteira foram consideradas positivas para o capital político de Mao não apenas por terem recuperado postos estratégicos de modo célere e efetivo em Ladakh e Arunachal Pradesh, mas, sobretudo, por terem imposto uma derrota cabal às forças indianas (CHANGSHENG, BEZERRA, 2014)[52].

Após o fim das hostilidades na fronteira, as relações sino-indianas permaneceram congeladas por quase uma década, com o agravante de que o teste nuclear promovido pela China, em 1964, ampliou, ainda mais, a preocupação da Índia com a segurança regional (MURATBEKOVA, 2018). Frente à ameaça, em 1967, um novo conflito letal entre forças militares na região disputada de Nathu La, fronteira entre Índia, Tibete e Butão, resultou em baixas de ambos os lados (FRAVEL, 2015).

[51] Os chineses optaram por manter o controle em Aksai Chin, considerando Arunachal Pradesh como de menor importância para a posição da China no Tibete. Com isso, pretendiam assegurar o controle apenas das áreas estratégicas necessárias (SCOTT, 2011).

[52] Com o fim das hostilidades quase cinco mil soldados indianos foram mortos, e outros quatro mil capturados, já no lado chinês poucas baixas e nenhum soldado capturado (MAXWELL, 2013).

Não obstante, no início da década de setenta, as políticas implementadas pelo regime comunista e as ações militares do ELP provocaram novas revoltas no Tibete, por sua vez, a Índia interveio no Paquistão Oriental, em 1971, transformado em Bangladesh durante a administração de Indira Gandhi (MURATBEKOVA, 2018).

Somente a partir de meados da década de setenta com a despersonalização da política externa e das reformas estruturais promovidas por Gandhi e Xiaoping, líderes que assumiram o controle político-administrativo em seus respectivos Estados, a restauração do equilíbrio securitário regional voltou a ser discutida (HOLSLAG, 2009)[53].

De tal que, a despeito dos embates em torno da cisão do território do Paquistão, e a exploração sócio econômica do Tibete, aos poucos as relações sino-indianas foram sendo reestabelecidas (BASHIR, TAJ, 2022). Nesse ensejo, em 1979, as lideranças concordaram em constituir uma comissão para tratar a questão das fronteiras, com o objetivo de firmarem medidas de confiança significativas para promoção da segurança e manutenção das relações bilaterais em patamares que possibilitassem o desenvolvimento econômico e social (MURATBEKOVA, 2018).

O diálogo profícuo entre os vizinhos proporcionou a construção de diversos acordos, firmados ao longo da década de oitenta e noventa com vistas a encerrar as disputas em torno da possessão de territórios-chave como Aksai Chin e Arunachal Pradesh (ZHANG, LI, 2013)[54].

Todavia, as negociações, embora, tenham registrado enquadramentos variados sobre o problema, malograram em atingir consenso (ZHANG, LI, 2013), em parte, devido aos novos embates entre forças militares desencadeados na região de fronteira ao longo do vale de Sumdorong Chu, ao sul de Thag La (GARVER, 2016)[55]. Para majorar, em fevereiro de 1987, a Índia concedeu ao NEFA a condição de estado, renomeado como Arunachal Pradesh, doravante considerado parte de seu território nacional (ZHANG, LI, 2013).

---

[53] Na China, em 1976, a morte de Mao Zedong permitiu a ascensão de setores reformistas liderados por Deng Xiaoping que, em 1978, deram início a abertura econômica. De modo similar, Indira Gandhi, reeleita em 1971, procurava criar incentivos a implementação de políticas públicas voltadas para redução de desigualdades (DEEPAK, 2005).

[54] Em 1981, o Ministro de Negócios Estrangeiros da China Huang Hua, em visita a Índia, inicia a primeira de três rodadas de negociação sobre as disputas fronteiriças registradas entre 1982-83. Com efeito, em 1984, na quarta rodada, ambos concordaram em mudar sua posição original sobre os limites fronteiriços, a fim de alcançarem um acordo final abrangente (CHUNG, 2004; KALHA, 2014).

[55] O impasse envolveu mais de cinquenta mil soldados colocados sob prontidão para agir em caso de escalonamento do conflito (FRAVEL, 2008).

A tensão só voltou a arrefecer, em 1988, quando ambos concordaram em retirar as forças militares de áreas críticas ao longo da fronteira oriental (CHUNG, 2004). Concomitantemente, celebraram a criação de um Grupo de Trabalho Conjunto (GTC) para resolução do contencioso nas fronteiras, grupo que promoveu a assinatura de tratados de cooperação mútua entre 1988 e 2003 (FANG, 2002).

Tendo como pano de fundo o fim da Guerra Fria e o desmoronamento da URSS, as relações sino-indianas se mantiveram em equilíbrio. Assim, em 1993, China e Índia firmaram os acordos Sobre a Manutenção da Paz e da Tranquilidade ao longo da LAC que reconheceu a demarcação como fronteira funcional e de Medidas de Fortalecimento da Confiança no Campo Militar ao longo da LCR, em 1996, que pretendiam obstar novos confrontos militares (SCOTT, 2011; ZHANG, LI, 2013).

Conquanto os compromissos assumidos demonstrassem o interesse mútuo em considerar o equilíbrio securitário fulcral para o desenvolvimento econômico e social (MURATBEKOVA, 2018), eram documentos pouco objetivos em matéria de demarcação das áreas sob contestação (BASHIR, TAJ, 2022). Mais do que isso, não impediram o retorno das disputas e a crescente militarização em territórios chave como o Tibete, fatores que, somados a realização de testes nucleares pela Índia, congelaram, uma vez mais, os movimentos na esfera diplomática (MOREIRA, 2016).

Com intuito de retomar o diálogo, ambos concordaram em aderir a Declaração Conjunta sobre Princípios para Relações e Cooperação Abrangente que convocou representantes especiais, civis e militares, para auxiliar o GTC, num esforço para retomar as negociações sobre os territórios disputados nos setores de fronteira (WESTCOTT, 2017; MURATBEKOVA, 2018) [56].

Destarte, entre 2003 e 2009, foram realizadas treze rodadas de conversações entre os representantes especiais e o GTC. Com efeito, em 2005, China e Índia assinaram o Tratado sobre Parâmetros Políticos e Princípios Orientadores para a Resolução da Questão da Fronteira Índia-China se comprometendo com a construção de um ‘pacote de resolução’ para demarcação dos territórios que considerasse a história, os interesses estratégicos, a geografia e a população estabelecida na região como parâmetros decisórios (SCOTT, 2011).

[56] Com o acordo a China reconheceu o território de Siquim como parte da India, reabrindo a passagem de Nathu La Pass na fronteira com o Tibete, fechada desde a guerra de 1962. Não houve reconhecimento do território indiano Arunachal Pradesh, apenas do Tibete como parte do território chinês (SCOTT, 2011).

Novamente, os produtos da esfera diplomática, embora necessários para tentar reaver o tênue equilíbrio securitário na região das fronteiras, não foram suficientes para evitar o retorno das hostilidades que abalaram, mais uma vez, as relações sino-indianas (WESTCOTT, 2017).

Senão vejamos, em 2006, a China voltou a reivindicar territórios no setor oriental, a considerar Tawang parte de seu território. Em contrapartida, o Dalai Lama erradicado na Índia, reforçou a legitimidade do Acordo de Simla (1914) para demarcação da fronteira, pondo em dúvida a soberania chinesa sobre o Tibete (SCOTT, 2011).

Numa tentativa de desarmar a tensão provocada pelo retorno dos movimentos militares em ambos os lados da LCR, China e Índia aderiram ao Acordo de Visão Compartilhada para o Século 21, em 2008 (BASHIR, TAJ, 2022). Porém, no ano seguinte, a visita do Dalai Lama, em companhia de líderes políticos indianos, ao setor oriental da fronteira reacendeu a rivalidade com os chineses (SCOTT, 2011).

Não obstante, entre 2012 e 2013, novas rodadas de diálogo sobre a disputa nas fronteiras deram origem a dois acordos firmados para o Estabelecimento de um Mecanismo de Trabalho para a Consulta e Coordenação nas Áreas Fronteiriças Índia-China e Sobre Cooperação em Defesa Fronteiriça, os compromissos previam, ainda, a criação de uma linha ‘direta’ de comunicação entre generais para resolução de conflitos ao longo da LAC (ZHANG, LI, 2013; MOREIRA, 2016; MURATBEKOVA, 2018).

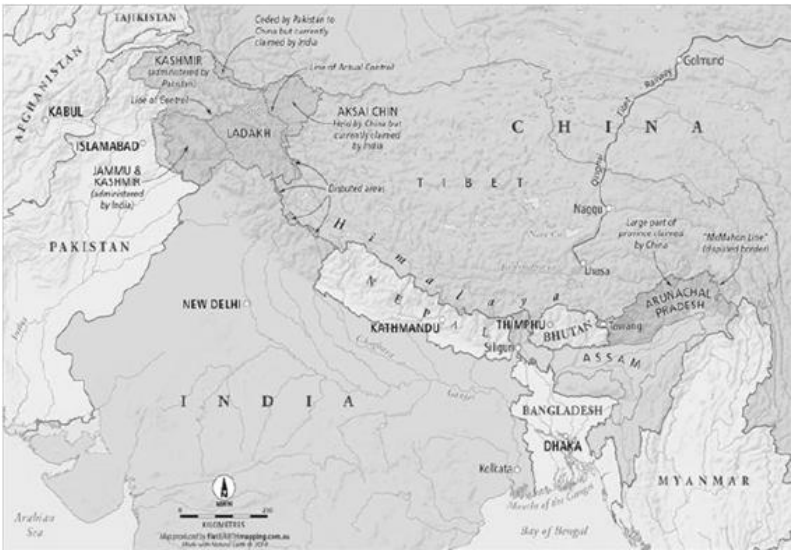
No entanto, os movimentos da esfera diplomática continuavam a contrastar com o avanço de projetos para construção de obras de infraestrutura promovidos por ambos os lados nas regiões sob disputa (EDFAC, 2013)[57].

Com a crescente percepção de insegurança nas fronteiras, novos encontros entre tropas militares se tornaram inevitáveis, a exemplo dos impasses, sem vítimas registradas, na passagem de Karakorum, em 2013; Chumar, na cidade de Demchok, lado indiano de Ladakh, em 2014; Donglang, fronteira entre o Butão, Siquim e o Tibete, e Pangong, lado chinês de Ladakh, em 2017 (DUTTA 2014; LAU, 2017).

[57] A PAPF e o Exército participaram na construção de centenas de projetos de infraestrutura energética e de transportes nas regiões de fronteira em territórios-chave tais como: “Nuozhadu (Yunnan), Jinpnig (Sichuan) e Pangduo (Tibete). Além disso, as unidades de transporte da PAPF empreenderam a construção de 172 projetos, incluindo rodovias nas montanhas de Tianshan, na Região Autônoma Uigur de Xinjiang, a ponte viaduto de dois andares sobre o rio Luotang, na província de Gansu, e o túnel Galungla, ao longo da rodovia Medog, na província de Gansu. Região Autônoma do Tibete, com extensão total de 3.250 km” (EDFAC, 2013, p. 21-22).

Curiosamente, mesmo após a retirada das tropas, a tensão entre as forças militares não arrefeceu, o patrulhamento e a prontidão para confrontos em áreas disputadas continuaram de modo ostensivo. Em contraste, as lideranças políticas intentaram promover incentivos ao reestabelecimento do equilíbrio securitário regional, uma vez mais sem sucesso (SCOTT, 2021).

Figura 4. Demarcação de Fronteiras em 2017



Fonte: Westcott (2017)

A catarse ocorreu em 5 de agosto de 2019, quando a classe política decidiu revogar o Artigo 370 que reconhecia a autonomia dos territórios de Jammu, Caxemira e Ladakh, desconsiderando a coletânea de medidas de confiança mútua acordadas com a China no pós-guerra (1972-2013). Com a alteração no texto constitucional, a Índia passou a considerar Ladakh, em sua totalidade, como parte do território indiano, assim, novamente, mapas com a nova demarcação das fronteiras foram publicados (BASHIR, TAJ, 2022).

Tais provocações foram percebidas pelos chineses como ameaças de adoção do irredentismo para resolução da questão fronteiriça, movimento que provocou forte abalo no equilíbrio securitário regional (SCOTT, 2021). A conta disso, em maio de 2020, em resposta a crescente militarização da LCR, tropas chinesas e indianas voltaram a entrar em confronto na região leste de Ladakh, numa área de entroncamento na zona

fronteiriça do Vale de Galwan[58], próximo à Aksai Chin, local onde os indianos haviam construído uma rodovia para conectar a região à base aérea militar reativada de Daulat beg Oldi, em 2019 (BBC, 2020)[59].

Com o agravamento da tensão, em 15 de junho de 2020 um novo confronto violento eclodiu no setor ocidental, o embate foi considerado o mais grave na fronteira em quase meio século, e resultou em baixas de ambos os lados. Embora, o número preciso permaneça sob escrutínio, é inegável que o retorno das hostilidades abalou severamente as relações sino-indianas (BBC, 2020; THE PRINT, 2021). Uma vez mais, a decisão de retirar as tropas dos locais de conflito em fevereiro de 2021, não foi suficiente para arrefecer os ânimos, assim, em agosto daquele ano, um alto volume de tropas foi mobilizado para atuar em Ladakh (SCOTT, 2021; BASHIR, TAJ, 2022).

Contudo, chama atenção o fato de que mesmo à luz da relevância estratégica que possuem as relações sino-indianas para o desenvolvimento econômico e social de ambos (MURATBEKOVA, 2018), tanto a China quanto a Índia, após diversas tentativas de resolução diplomática das disputas territoriais em áreas fronteiriças, tenham dado continuidade a projetos para construção de infraestrutura civil e militar ao longo da LAC com intuito de responder aos desafios securitários regionais sob o argumento de proteção à soberania e à integridade territorial de seus respectivos Estados (SCOTT, 2021; BASHIR, TAJ, 2022)[60].

Frente ao exposto, naquilo que tangencia a relevância acadêmica e securitária das operações que atingiram a Índia, se faz *mister* compreender como se deu o processo de mudança institucional nas forças de segurança e defesa nacional da China que promoveu incentivos seletivos para o seu desenvolvimento e posterior execução. Com base na análise de fontes primárias, a próxima seção destaca os meandros institucionais que permitiram à China incorporar o domínio cibernético à estrutura segurança e defesa com vistas à projeção de poder nacional na região da Ásia.

---

[58] 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 (BBC, 2020).

[59] Na prática, a obra ampliou a capacidade de transporte de militares e materiais da Índia no setor ocidental, medida que despertou a atenção da China em relação aos interesses da Índia em avanças sobre as fronteiras (BASHIR, TAJ, 2022).

[60] Com a reestruturação da Força Especial de Fronteira (SFF) composta por tibetanos étnicos, a Índia movimenta efetivos do Paquistão para Ladakh e cria uma nova divisão no setor central; o 17º batalhão foi ampliado e concentrado em Arunachal Pradesh (SCOTT, 2021). Já a China investiu em efetivos para atuar grandes altitudes e nos outros setores de fronteira, com foco na construção de estruturas militares nas regiões de Galwan, Depsang e Hot Springs (BASHIR, TAJ, 2022).

5.2. Mudança institucional: a transformação das forças de segurança e defesa chinesas para incorporar o ciberespaço como novo domínio de guerra

Nesta seção verificamos os efeitos institucionais das operações especiais orquestradas pela China para atingir sistemas de informação na Índia via ciberespaço. A partir do exame de documentos oficiais que regulam os movimentos das agências de segurança e defesa da China, coletamos evidências do processo de mudança pela qual tais instituições passaram ao incorporarem a tecnologia da informação como vetor da modernização, considerada condição necessária para mobilizar novas estratégias de projeção do poder nacional em conflitos regionais[61].

Nossa análise ordenou o conteúdo das fontes em três fatores considerados significativos para explicar a mudança institucional: i) desafios geopolíticos; ii) definição e integração entre fins e meios; e, iii) construção de narrativa estratégica, aspectos basilares para a orientação estratégica das instituições responsáveis pela segurança e defesa nacional. O material registra os incentivos que permitiram a articulação entre os setores de defesa, inteligência, iniciativa privada e parceiros internacionais, para incorporar o ciberespaço como um novo domínio de guerra.

Em síntese, o ELP passou a considerar o emprego de tecnologia da informação em ações estratégicas como um recurso significativo para amplificar as chances de vitória da China em conflitos regionais quando combinados à aplicação de estratagemas condizentes com as capacidades objetivas das forças, um dos componentes chave para causar impacto no desempenho dos alvos (LI, 2002)[62]. Por essa lógica, de acordo com teóricos do pensamento estratégico militar da ativa e da reserva, o êxito na projeção do poder nacional depende da capacidade das instituições em compreender e manipular a realidade objetiva (BINGYAN, 2004; JIJUN, 2006; ZHENG, BAO, 2007; XUE GUO'AN, 2010).

Tendo em vista o crescimento do poder nacional como fio condutor, as instituições militares adotaram, desde a guerra sino-japonesa (1937-1945), uma postura de 'defesa ativa' que, a depender da conjuntura, podia se modificar rapidamente e

[61] Documentos oficiais analisados: Estratégia de Defesa Nacional (2009); Defesa Nacional da China (2011); O Emprego Diversificado das Forças Armadas da China (2013); Estratégia Militar da China (2015); Defesa Nacional da China na Nova Era (2019).

[62] Embora suficiente para produzir o fenômeno da guerra cibernética, a aplicação efetiva das operações ofensivas via ciberespaço depende da capacidade dos atores institucionais em controlar a iniciativa para alcançar vitórias sem guerrear, tal condição pressupõe que consigam aplicar estratagemas para sincronizar o processo de tomada de decisão do adversário com os interesses nacionais, induzindo o alvo a tomar decisões de modo previsível (ZHENG, BAO, 2007).

assumir caráter ofensivo (ZEDONG, 1936). Ponto chave para construir e exercer o poder militar com vistas à proteção da soberania e da segurança nacional, tal princípio se manteve no bojo dessas agências como característica fundamental que orienta, ainda hoje, a ciência da estratégia militar no desenvolvimento de meios que as permitam vencer conflitos sob condições de alta tecnologia (DESJARDINS, 2005).

Em termos operacionais, a premissa básica rege que as instituições militares modernas devem ser capazes de realizar ataques precisos de longo alcance que paralisem o adversário, obtendo vitórias em curto espaço de tempo, com custo humano e econômico menor ao de ataques tradicionais cinéticos (ZHANG, SIHAI, CHENGXIAO, 2010)[63]. Por essa lógica, constataram que as operações cibernéticas se encontravam circunscritas por limitações impostas pelas condições materiais e capacidades de ação dos atores (THOMAS, 2014; POLLPETER, 2015; STOKES, 2015).

Todavia o processo organizado pelo Partido Comunista (PC) para incorporar a tecnologia como vetor de desenvolvimento das operações de forças de segurança e defesa teve início somente no último quartil do século passado (EDN, 2009; EMC, 2015).

Desde 1983, quando incidiu sobre instituições políticas tradicionais, como no Instituto de Defesa (ID) dando origem ao MSE e, quinze anos depois, ao Centro de Avaliação de Segurança de Tecnologia da Informação da China (CASTI), órgão responsável por coordenar centros regionais de avaliação de segurança e tecnologia da informação (STOKES, 2015). Outrossim, foram criados o Grupo de Líderes do Estado para Informatização (GLEI) e o Escritório do Conselho do Estado para Informatização, dirigidos por representantes do PC e organizações militares para implementação da estratégia nacional de defesa (LINDSAY, CHEUNG, REVERON, 2015)[64].

Frente ao contexto, a Estratégia de Defesa Nacional da China (EDN) promulgada em janeiro de 2009, pode ser considerada o primeiro de uma série de documentos oficiais que ratificam o andamento do processo de criação de incentivos ao

[63] 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’ (NU, JIANGZHOU, DEHUI, 2000).

[64] Em 2003, a instituição deu origem ao Pequeno Grupo de Coordenação em Rede de Segurança do Estado e Informação (SNISCSG) voltado ao desenvolvimento de novas tecnologias informacionais (AVERSA, 2018).

desenvolvimento de novas tecnologias que permitam a efetiva implementação da defesa ativa, principal objetivo a ser perseguido pelas forças de segurança nacional[65].

A narrativa estratégica destaca a crescente importância da China no sistema internacional, em parte, devido ao forte crescimento econômico sustentado nas últimas décadas; e, condena a expansão militar como produto da pretensão hegemônica de alguns Estados. Considera, pois, que tais fatores impõem a necessidade da construção de novos arranjos institucionais que permitam mitigar a presença de ameaças ao equilíbrio securitário.

No tocante a esfera internacional, ao passo que assume o compromisso em exercer uma política externa "independente e de paz e uma política de defesa nacional destinada exclusivamente a proteger o seu território e o seu povo" (EDN, 2009, p. 3), registra preocupação com o elevado volume de investimentos de grandes potências internacionais nas últimas décadas para produção e emprego de novas tecnologias de armamento, sublinha que para estes Estados "(...) As forças nucleares estratégicas, a astronáutica militar, os sistemas de defesa antimísseis e o reconhecimento e vigilância global e nos campos de batalha tornaram-se prioridades máximas" (EDN, 2009, p. 4) do processo de RMA, considerado símbolo do desenvolvimento técnico-científico de que dispõem para projeção de poder nacional.

Nesta direção, destaca o interesse em perseguir "um caminho de informatização militar com características chinesas" (EDN, 2009, p. 16) tendo o desenvolvimento da tecnologia informacional como pedra angular das operações em múltiplos domínios (EDN, 2009)[66]. Por essa lógica, a informatização é descrita como parâmetro para mensurar a efetividade das forças e a tecnologia de informação o aspecto central para alcançarem "a mecanização e grandes avanços na informatização até 2020 (...) e a modernização da defesa nacional e das forças armadas até meados do século XXI" (EDN, 2009, p. 12).

Com a finalidade de atingir as metas traçadas, prevê a criação de incentivos à indústria de ciência e tecnologia voltada para a defesa, a fim de promover não apenas o

---

[65] Desde a década de noventa, "o ELP estabeleceu a diretriz estratégica militar de defesa ativa baseada na vitória de guerras locais em condições de tecnologia moderna, particularmente de alta tecnologia. (...) uma estratégia de fortalecimento das forças armadas através da ciência e da tecnologia (...) para modernização da defesa nacional e das forças armadas" (EDN, 2009, p. 11).

[66] Desse modo, o ELP assume o compromisso com o fortalecimento das capacidades institucionais que permitam o desenvolvimento técnico-científico em patamares significativos, orientados para "salvaguardar a soberania, a segurança e o desenvolvimento nacionais, tomando a reforma e a inovação como a sua força motriz fundamental, e avançando na modernização da sua defesa nacional e das suas forças armadas" (EDN, 2009, p. 3).

desenvolvimento de equipamentos e armas eficientes, mas o aprimoramento da expertise técnica e tática das forças. Razão pela qual, considera necessária a assimilação por militares e civis das novas tendências de "guerra de informação, particularmente da guerra eletrônica. (...) aprimorando o treinamento sobre como operar e usar armas e equipamentos de informação" (EDN, 2009, p. 12)[67].

No tocante aos desafios estratégicos representados por guerras locais, enfatiza que a eclosão recorrente de conflitos dessa natureza ocorre em função da política expansionista incorporada por Estados que, ao instarem movimentos separatistas em territórios estratégicos, ameaçam a soberania e a integridade territorial da China[68]. À vista disso, frisa os efeitos negativos para o equilíbrio securitário regional do entrelaçamento de "ameaças tradicionais e não tradicionais" (EDN, 2009, p. 6).

No que se refere à estrutura de força para a defesa de regiões de fronteira com a finalidade de assegurar a soberania nacional e a integridade territorial, prevê a implementação de medidas para reforçar a "prontidão para o combate, aprimorando de forma abrangente suas capacidades de reconhecimento e vigilância, comando e controle, resposta rápida e operações defensivas" (EDN, 2009, p. 22).

Cientes de que tais conflitos se desenrolam sob condições que favorecem o uso da tecnologia da informação, destaca o potencial do domínio cibernético para aprimorar as capacidades de emprego da força com o intuito de obter vantagens estratégicas que permitam explorar e "aproveitar ao máximo nossos pontos fortes para atacar os pontos fracos do inimigo" (EDN, 2009, p. 9). Outrossim, salienta a relevância de operações que não envolvam declaração formal de guerra, como "forma importante de aplicação das forças militares nacionais" (EDN, 2009, p. 9).

Diante do cenário prospectivo, cresce a relevância dos esforços conjuntos entre instituições nacionais e a iniciativa privada. Nesse sentido, prevê fomentar parcerias entre institutos de pesquisa e a indústria de defesa para produção de tecnologia para uso dual, a exemplo da estrutura de rede integrada de informação, em vigor desde 2006, que promoveu avanços na "construção de sistemas de comando e controle para operações conjuntas integradas, que ampliaram significativamente a capacidade de apoio à informação no campo de batalha" (EDN, 2009, p. 16).

---

[67] As novas diretrizes, orientadas por teorias que sustentam a significância da tecnologia da informação para uso em conflitos modernos, vêm sendo paulatinamente aplicadas em "planos e orientações de médio e longo prazo para a informatização das forças armadas foram formulados e promulgados, normas técnicas foram revistas e refinadas, e a educação institucional e a formação de pessoal (...) reforçados" (EDN, 2009, p. 17).

[68] Destaca a presença de ameaças desta natureza organizadas no Tibete (EDN, 2009).

> A China está a acelerar a transformação das estruturas e mecanismos das empresas da indústria de defesa e está na fase inicial de estabelecimento de um novo sistema de ciência, tecnologia e indústria relacionados com a defesa [...] As contradições estruturais na ciência, tecnologia e indústria relacionadas com a defesa foram gradual e fundamentalmente resolvidas através da reestruturação estratégica e da consolidação do corpo principal da indústria de defesa (EDN, 2009, p. 43).

Em linha com o documento antecessor, a estratégia de Defesa Nacional da China (EDN), promulgada em 2011, reforçou o compromisso com o desenvolvimento de novas tecnologias da informação para fortalecer as capacidades das forças em implementar a defesa ativa, pilar da soberania e integridade territorial.

Com poucas alterações no eixo narrativo, destaca a relevância da China em um sistema internacional marcado pela existência de uma multiplicidade de centros de poder que impõem a necessidade de promover medidas de confiança mútua e cooperação que contribuam para o equilíbrio securitário e o enfrentamento de "ameaças integradas, complexas e voláteis" (EDN, 2011, p. 4).

Naquilo que tange à esfera internacional, reforça o compromisso com a orientação de uma política externa independente, voltada à promoção da cooperação interestatal que permita erigir "relação amigável e de parceria com os seus vizinhos" (EDN, 2011, p. 66)[69].

Não obstante, acrescenta trechos que reiteram a preocupação com os efeitos do processo de implementação de mudanças nas estratégias de atuação promovidas por Estados fortes com o intuito de aprimorar a produção e o uso de tecnologias informacionais, "algumas potências elaboraram estratégias, (...) desenvolveram meios para uma rápida resposta global a ataques, (...) aprimoraram as capacidades de uso das operações cibernéticas para ocupar novos patamares de comando estratégico" (EDN, 2011, p. 5).

Em resposta, assinala o compromisso em impulsionar a estratégia da RMA com características chinesas com base no fomento ao desenvolvimento técnico-científico que permita alterar "gradualmente o foco da quantidade e escala para a qualidade e

[69] Considera os acordos firmados entre China e Índia (1993; 1996; 2005) produtos do diálogo profícuo interinstitucional para estabelecimento de medidas que promovam a segurança regional em territórios fronteiriços disputados. E registra a constituição do 'sistema representativo de fronteira' como iniciativa das instituições responsáveis pela segurança nacional para acelerar a resolução de eventuais conflitos nas regiões de fronteira (EDN, 2011).

eficiência, de um modelo intensivo em mão-de-obra para um modelo intensivo em tecnologia" (EDN, 2011, p. 15).

Dentre as finalidades da política de defesa nacional, destaca a continuidade do processo de desenvolvimento da tecnologia de informação para a modernização das forças de segurança, que promoverá a mecanização das forças, até 2020, com base no "desenvolvimento de armamentos e equipamentos de alta tecnologia, e novos tipos de forças de combate" (EDN, 2011, p. 12). Outrossim, prevê incentivos ao processo de transformação das capacidades de uso da tecnologia da informação para alcançar a vitória em guerras locais travadas sob condições de informatização, com efeito, sublinha avanços consideráveis alcançados na "construção de sistemas de informação para reconhecimento e inteligência, comando e controle e preparação do campo de batalha (...) [e] formação de comandantes para operações conjuntas" (EDN, 2011, p. 20).

No que concerne aos desafios estratégicos, mantém a preocupação com os abalos no equilíbrio securitário regional, provocados pelo aumento da influência de grandes potências em conflitos envolvendo territórios disputados em zonas de fronteira. Mais do que isso, em específico, insiste em denunciar como fator preponderante o suporte técnico e tático oferecido às ameaças domésticas provenientes de movimentos separatistas organizados no Tibete (END, 2011).

A fim de mitigar o problema, por um lado reforça a intenção de: i) organizar sua política de defesa nacional com base no princípio da prudência estratégica, "atacar apenas depois de ser atacado"; ii) jamais "procurar a hegemonia, nem adotar a abordagem da expansão militar agora ou no futuro" (EDN, 2011, p. 9); e, iii) fomentar a criação de incentivos à resolução de conflitos com base na construção de medidas de confiança mútua[70]. Por outro, orientado pela revisão das estratégicas de uso da força, reitera a necessidade de produzir incentivos à constituição de operações conjuntas que permitam o uso de recursos de informação para auferir vantagens estratégicas em conflitos regionais (EDN, 2011)[71].

No tocante à estrutura das forças de segurança pública e do Exército do ELP, responsáveis pela patrulha de regiões disputadas, destaca a missão de salvaguardar o equilíbrio securitário regional com base nas diretrizes da política de consolidação da

[70] De acordo com o documento: "a força de defesa fronteiriça do ELP criou ao longo das fronteiras mais de sessenta estações para conversações e reuniões fronteiriças, e todos os anos participa em milhares de conversações e reuniões com países vizinhos" (EDN, 2011, p. 67).

[71] "Uma nova geração de doutrinas de comando em campanhas e operações conjuntas, e outras doutrinas de apoio relevantes foram emitidas e implementadas, e uma série de trabalhos teóricos e livros de treinamento em campanhas conjuntas foram compilados" (EDN, 2011, p. 20-21)

defesa fronteiriça "de manutenção da estabilidade e de promoção do desenvolvimento" (EDN, 2011, p. 30)[72].

Conquanto, mantém forte interesse em aprimorar sistemas de C2, reconhecimento e inteligência, que permitam amplificar as capacidades de uso da tecnologia da informação em sistemas de apoio integrado (EDN, 2011). Já no tocante à formação dos quadros para lidar com os desafios, prevê "o cultivo de comandantes de operações conjuntas, profissionais de informação, especialistas em tecnologia da informação e especialistas em operação e manutenção de novos tipos de equipamentos" (EDN, 2011, p. 25)[73].

Já no que diz respeito aos meios para alcançar os objetivos, reforça a relevância das parcerias entre o setor público e o privado com intuito de aprimorar as capacidades técnico-científicas aplicadas à defesa, projetos que nas últimas décadas têm se destacado por "avanços significativos registrados em técnicas de reconhecimento e exploração, processamento de dados, produção de armamento e equipamento" (EDN, 2011, p. 55).

Na esteira da mudança institucional sob escrutínio, a China promulgou O Emprego Diversificado das Forças Armadas da China (EDFAC), em 2013, documento chave para a orientação estratégica militar do ELP.

O eixo narrativo mantém o compromisso com a construção de medidas de cooperação e confiança interestatal que promovam o equilíbrio securitário com base na implementação da defesa ativa. Nesse ensejo, frisa que a robustez das forças deve ser proporcional à posição internacional ocupada pelo Estado, dessa forma, prevê alavancar o processo de modernização mediante à construção de sistemas informacionais que ampliem a efetividade das operações de combate a ameaças tradicionais e não tradicionais (EDFAC, 2013).

Em termos de desafios geopolíticos, reforça o registro sobre as mudanças na dinâmica dos conflitos interestatais provocadas pelo uso de tecnologias informacionais por grandes potências com intuito de assegurar "superioridades estratégicas na

[72] "A Comissão Estatal de Defesa Fronteiriça e Costeira, sob a dupla liderança do Conselho de Estado e da Comissão Militar Central (CMC), coordena as defesas fronteiriças e costeiras da China. Todos os comandos das áreas militares, bem como as províncias fronteiriças e costeiras, cidades e condados, têm comissões para coordenar as defesas fronteiriças e costeiras com as suas respectivas jurisdições" (EDN, 2011, p. 30).

[73] "Para formar oficiais comandantes para operações conjuntas, o ELP também reformou o modelo de formação de graduados para o seu Mestrado em Ciências Militares. Após a promulgação das Medidas de Implementação do Projeto de Pessoal Militar de Alto Nível em Inovação Científica e Tecnológica, a cada dois anos o PLA, seleciona duzentos cientistas líderes e talentos de alto desempenho de diferentes disciplinas para treinamento especial, a fim de melhorar sua aptidão para a inovação em ciência e tecnologia" (EDN, 2011, p. 25).

concorrência internacional em áreas como o espaço exterior e o ciberespaço" (EDFAC, 2013, p. 4). Em resposta, sublinha que a efetiva implementação da defesa ativa se orienta, dentre outras finalidades, a: i) salvaguardar os interesses da segurança nacional no ciberespaço; ii) combater movimentos separatistas que ameacem a soberania e a integridade territorial do Estado; iii) aprimorar as capacidades das forças para atuarem em conflitos travados sob condições de informatização (EDFAC, 2013, p. 5)[74].

Não obstante, registra evidências de como a mudança institucional impulsiona a cooperação interagências para desenvolvimento tecnológico e organizacional das instituições de defesa e segurança. A exemplo das reformas administrativas que incidiram sobre Comissão Militar Central (CMC) e deram origem ao Departamento de Planejamento Estratégico (DPE) do ELP e à reorganização de departamentos chave do Estado-Maior, dentre os quais, se destacam os de comunicações; informação; treinamento e armas, num esforço para "tornar as forças operacionais enxutas, conjuntas, multifuncionais e eficientes" (EDFAC, 2013, p. 8).

Seguindo as diretrizes, o Exército modificou a orientação da defesa estática para um modelo de mobilidade eficiente, tendo por base a informatização como vetor do "desenvolvimento de tropas de aviação do exército, unidades mecanizadas ligeiras e forças de operações especiais (...), tornando gradualmente as suas unidades pequenas, modulares e multifuncionais" (EDFAC, 2013, p. 8).

Dentre os princípios que orientam as operações de combate, a dissuasão é considerada fulcral, consequentemente, o domínio cibernético desponta como opção estratégica para assegurar a efetividade das operações. Por essa lógica, reforça o compromisso em dar continuidade ao processo de aprimoramento de armas, equipamentos e dos efetivos "treinamento de conceitos operacionais em condições de informatização como domínio da informação, confronto entre diferentes sistemas, ataque de precisão, fusão, integração e articulação (...) e treinamento em ambientes complexos de campo de batalha" (EDFAC, 2013, p. 18).

Tendo em consideração o exposto, fica evidente que as operações cibernéticas se tornaram vitais para que a China pudesse incorporar uma estratégia de defesa ativa que permitisse vencer guerras limitadas sob condições de alta tecnologia (POLLPETER, 2015). Dentre os efeitos registrados das campanhas de reconhecimento e exploração

[74] "As forças armadas da China baseiam firmemente a sua preparação militar na vitória de guerras locais sob condições de informatização, fazem planos globais e coordenados para promover a preparação militar em todas as direções estratégicas, intensificam o emprego conjunto de diferentes serviços e armas e melhoram as capacidades de combate com base em sistemas de informação" (EDFAC, 2013, p. 5).

organizadas, registradas na primeira década deste século, se destacam a aquisição de propriedade intelectual para desenvolvimento de tecnologia de ponta e de informação política com fins dissuasórios (LAVENDER, 2013).

Diante do cenário, o GLEI passou a ser dirigido pelo chefe de Estado Xi Jinping, em 2014, através da Comissão Central Militar (CCM) que incluía entre seus membros o Chefe do Estado-Maior do ELP, General Fang Fenghui, responsável pelas políticas relacionadas as operações cibernéticas nacionais e segurança da internet. Com isso, o Exército do ELP se tornou a instituição central do sistema de segurança cibernética da China, responsável por operações de inteligência militar, guerra eletrônica e espionagem (STOKES, 2015)[75].

A Estratégia Militar da China (EMC), publicada em 2015, contém parâmetros e mecanismos de ação adotados para implementação da defesa ativa que registram a significância do ciberespaço para a consecução de objetivos estratégicos nacionais (EMC, 2015)[76].

A narrativa estratégica permanece similar aos documentos antecessores, descreve o andamento do processo de transformação internacional provocado por mudanças e reformas na estrutura de governança global e, em específico, na região Ásia-Pacífico, que tornaram ainda mais complexa a dinâmica das relações internacionais. Ante a dinâmica, frisa o interesse em alcançar o 'rejuvenescimento' da nação e reafirma o compromisso com a política externa contra hegemônica e de defesa ativa (EMC, 2015).

Com relação aos desafios geopolíticos, mantém a atenção aos impactos provocados por alterações nas estratégias de segurança e defesa das grandes potências, com intuito de avançar a construção de armas e equipamentos para uso em novos domínios de guerra, com destaque para o ciberespaço. Embora, ressalte que tais mudanças na tecnologia e na configuração dos domínios não afetem significativamente o ambiente político e militar internacional, a nível regional tais fatores são identificados como "novos e graves desafios à segurança militar da China" (EMC, 2015, p. 5).

---

[75] O Exército do ELP passou 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).

[76] Considerando a experiência histórica das guerras revolucionárias, na década de cinquenta a estratégia da CMC promoveu alterações nas diretrizes de implementação da defesa ativa em paralelo aos processos de disputa territorial que abalaram o equilíbrio securitário regional ao longo de décadas (EMC, 2015).

Igualmente, manifesta preocupação com o potencial entrelaçamento de ameaças tradicionais e não tradicionais para abalar o equilíbrio securitário, em específico, insere trechos que sublinham a relevância estratégica de combatê-las em territórios chave como o Tibete, onde se verifica a necessidade de se "intensificar os esforços nas operações contra a infiltração, o separatismo e o terrorismo, de modo a manter a segurança política e a estabilidade social da China" (EMC, 2015, p. 7).

Afim de preparar as forças de segurança e defesa para superar os desafios, reforça o interesse em dar continuidade ao processo de modernização, tornando-as aptas para vencer guerras locais sob condições de informatização. À vista disso, aborda o problema sob perspectiva holística com base em diretrizes inovadoras que orientam as forças a "prestarem muita atenção aos desafios nos novos domínios de segurança e trabalharem arduamente para tomar a iniciativa estratégica na competição militar" (EMC, 2015, p. 6)[77].

Considerando o ciberespaço como domínio promissor, no qual os Estados têm se orientado para construção de capacidades operacionais ofensivas e defensivas com potencial para atingir setores e sistemas de informação de alvos estratégicos, o ELP "(...) acelerará o desenvolvimento de uma força cibernética e aumentará as suas capacidades de consciência situacional do ciberespaço, defesa cibernética, apoio aos esforços do país no ciberespaço e participação na cooperação cibernética internacional" (EMC, 2015, p. 14).

Não obstante, sustenta que a efetiva implementação da defesa ativa depende de ajustes no modelo de preparação das forças que permitam a distribuição eficiente das forças para atuarem em operações especiais de combate as "(...) ameaças provenientes de novos domínios de segurança, como o espaço exterior e o espaço cibernético" (EMC, 2015, p. 10)[78]. Nesse sentido, prevê a criação de incentivos a construção de sistemas

[77] "A abordagem holística procura equilibrar a preparação e a prevenção da guerra, a proteção dos direitos e a manutenção da estabilidade, a dissuasão e o combate à guerra, as operações em tempos de guerra e o emprego de forças militares em tempos de paz" (EMC, 2015, p. 9).

[78] Dentre os meios a serem implementados para tornar as forças de segurança e defesa aptas a combater ameaças provenientes do uso de novas tecnologias da informação em conflitos interestatais, destacamos: i) o desenvolvimento e produção de armas e equipamentos sofisticados e inovadores que possam contribuir para robustecer as capacidades do ELP em confrontos travados sob condições de informatização; ii) formação de quadros qualificados para formular e implementar teorias militares inovadoras que indiquem mecanismos operacionais efetivos e compatíveis com o emprego da tecnologia da informação em conflitos atuais e futuros; iii) incrementar as instituições militares ligadas ao CMC, promovendo ajustes no sistema de liderança e gestão de serviços e armas que permitam o uso planejado de recursos estratégicos em caso de confronto; iv) aprimorar a integração civil-militar em âmbito da segurança nacional em novos domínios operacionais (EMC, 2015, p. 16-17).

informacionais integrados e funcionalmente independentes, sistemas de reconhecimento e exploração para identificação precoce de ameaças e desenvolvimento de armas capazes de atingir alvos distantes com precisão e discrição (EMC, 2015, p. 19).

Como se nota, o processo de mudança institucional persegue o propósito de permitir a atuação das forças nos mais diversos domínios de conflito, haja vista a percepção da complexidade dos desafios estratégicos que ameaçam a soberania e a integridade nacional. Em virtude disso, se torna *mister* a transformação nos padrões operacionais das forças com intuito de maximizar "ainda mais a disposição do campo de batalha e fortalecer o pré-posicionamento estratégico" (EMC, 2015, p. 20).

> [...] aproveitar a iniciativa estratégica na luta militar, planejar proativamente a luta militar em todas as direções e domínios e aproveitar as oportunidades para acelerar a construção, reforma e desenvolvimento militar [...] aproveitar ao máximo a eficácia global das operações conjuntas, concentrar forças superiores e fazer uso integrado de todos os meios e métodos operacionais (EMC, 2015, p 10).

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 militar, da política e da economia dos adversários (THOMAS, 2014).

> Com intuito de transformar o *modus operandi* e amplificar a eficiência das agências 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 influência crescente no sistema internacional (INKSTER, 2015, p. 34).

A mudança causou um forte impacto na capacidade de coleta de informação do adversário, seja por via da espionagem ou sabotagem (INKSTER, 2015). Embora, as organizações do ELP responsáveis por realizar ataques disruptivos permaneçam não reveladas, o quarto departamento dedicado ao planejamento de operações e contramedidas eletrônicas, é visto como o provável responsável (STOKES, 2015).

Ademais, 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[79], e, no geral, nas estruturas do terceiro e quarto departamento do ELP (LAVENDER, 2013).

Igualmente, ao enfatizarem a importância da integração das operações cinéticas e cibernéticas para atingir alvos civis e militares em tempos de guerra e/ou paz, destacam o potencial de novos domínios da guerra capazes de ampliar a assimetria de poder entre adversários estratégicos. A exemplo daquelas capazes de atingir sistemas C4ISR[80] e/ou outros centros de gravidade presentes em níveis estratégicos e táticos, com intenção de coletar informações para subsidiar ações ofensivas que possam vir a causar paralisia e/ou comprometer o funcionamento destas estruturas (POLLPETER, 2015).

O ciberespaço conforme compreendido pelos chineses representa, pois, um recurso de potencial decisivo para conflitos futuros. Por essa lógica, a guerra cibernética pode ser utilizada para oferecer suporte aos interesses de projeção nacional 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).

Tendo em vista os apontamentos, a Defesa Nacional da China na Nova Era (DNCNE), divulgada em 2019, último documento geral antes do confronto no Vale de Galwan, registra sinais da consolidação do processo de incorporação da tecnologia de informação às capacidades operacionais das forças de defesa e segurança. Nesse ensejo, enfatiza a eminente mecanização das forças em 2020, e a necessidade de manter atualizados os modelos teóricos de emprego da força, como fatores que incidem sobre o processo de modernização da defesa nacional e das forças armadas com previsão para término em 2035 (DNCNE, 2019).

Sem embargo, a narrativa estratégica sofre ligeiras alterações ao descrever uma China estável dos pontos de vista político, étnico e social, que nas últimas décadas

---

[79] 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: Wanquan, Guohua (2000); Fisher Jr (2008).

[80] 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).

ampliou, sobremaneira, sua influencia no sistema internacional em função dos altos índices de desenvolvimento econômico apresentado (DNCNE, 2019).

A preocupação com os desafios geopolíticos impostos por mudanças nas estratégias militares de Estados fortes permanece em evidencia, transformações que deram origem a novas estruturas de força e combate em domínios estratégicos, tais como o ciberespaço. Nesse ensejo, salienta que avanços no desenvolvimento técnico-científico têm permitido o surgimento de novas tecnologias militares baseadas em sistemas informacionais, tendência que se reflete na construção de incentivos ao desenvolvimento e uso de "armas e equipamentos de precisão de longo alcance, inteligentes, furtivos ou não tripulados" em conflitos regionais (DNCNE, 2019, p. 6)[81].

Em resposta, ressalta avanços na RMA em curso na China e reforça o compromisso em promover incentivos para que a informatização alcance patamares que concretizem a modernização das forças armadas, a ponto de "satisfazer as exigências da segurança nacional" (DNCNE, 2019, p. 16).

Ainda a respeito dos desafios ao equilíbrio securitário, promovidos por potências com pretensões hegemônicas que buscam intervir em disputas regionais, e criam entraves ao desenvolvimento de Estados emergentes, mantém a preocupação com a ligação entre estas e movimentos separatistas que ameaçam a segurança nacional e a estabilidade social da China (DNCNE, 2019).

Tendo em vista a percepção do cenário, insere trechos que manifestam a intenção em resolver tais disputas por via diplomática, restrita aos Estados envolvidos. Em particular, marca o interesse em "promover a estabilidade e a segurança ao longo da fronteira com a Índia, e buscar medidas eficazes para criar condições favoráveis para a resolução pacífica do impasse de Donglang (Doklam)" (DNCNE, 2019, p. 11).

Todavia, em contrapartida, outros dois tópicos originais sublinham a necessidade de combater ameaças provenientes de movimentos separatistas organizados no Tibete, bem como de assegurar os interesses nacionais em novos domínios de guerra, com destaque para o ciberespaço (DNCNE, 2019, p. 6-7)[82]. Em específico, denuncia a

[81] "Impulsionada pela nova onda de revolução tecnológica e industrial, a aplicação de tecnologias de ponta, como a inteligência artificial, a informação quântica, os grandes volumes de dados, a computação em nuvem e a Internet das Coisas, está a ganhar ritmo no domínio militar" (DNCNE, 2019, p. 6).

[82] Compreendido como domínio significativo da segurança nacional, por um lado o ciberespaço é descrito como um vetor do desenvolvimento econômico e social, e por outro como ambiente pretenso a proliferação de ameaças à segurança cibernética, fator que impõe a necessidade de mudanças nas instituições de defesa que permitam alavancar o processo de estruturação de capacidades operacionais ofensivas e defensivas "consistentes com a posição internacional da China e o seu estatuto como um importante país cibernético" (DNCNE, 2019, p. 14).

presença de ameaças não tradicionais neste domínio como fator que impõe a necessidade de atualização constante das capacidades das instituições de defesa nacional "A guerra está evoluindo em direção à guerra informatizada, e a guerra inteligente está no horizonte" (DNCNE, 2019, p. 6).

Tendo em consideração as vantagens estratégicas do uso da tecnologia de informação nas guerras modernas e a preparação robusta das forças de segurança, a defesa continua a ser posta em evidência como produto do imperioso desenvolvimento técnico-científico aplicado em projetos de construção e uso de armas inteligentes em múltiplos domínios (DNCNE, 2019).

Ante ao contexto, registra evidências das transformações pela qual passaram as forças de segurança e defesa para facilitar a atuação em conflitos travados sob condições de informatização. Por essa lógica, sob o comando da Comissão Militar Central (CMC) e dos Teatros Comando (TC) foram implementadas medidas que produziram melhorias significativas nas capacidades funcionais e de gestão operacional das forças (DNCNE, 2019)[83]. Outrossim, mudanças realizadas no nível doutrinário permitiram incorporar a informatização como pilar das operações conjuntas

Destarte, os incentivos criados para impulsionar o processo de modernização no Exército do ELP ampliaram as capacidades das "operações de manobra, bem como do ataque e da defesa multidimensionais", a orientação regional deu lugar à primazia da movimentação entre teatros considerado o modo mais eficiente de combate na nova era (DNCNE, 2019)[84]. Igualmente, incidiram sobre as instituições de ensino e pesquisa, civis e militares, que passaram a compor importantes núcleos de pesquisa e desenvolvimento teórico e técnico-científico, dedicados à indústria e à defesa (DNCNE, 2019) [85].

---

[83] No tocante a mudança institucional: "o Quartel-General, Departamento Político Geral, Departamento Geral de Logística e Departamento Geral de Armamentos foram reorganizados em 15 órgãos sob a liderança centralizada da CMC (...) o ELP estabeleceu um sistema de comando de operações conjuntas simples e eficiente, composto por estabelecimentos de comando permanentes e especializados tanto para operações em tempos de paz como em tempos de guerra" (DNCNE, 2019, p. 16-17).

[84] As estruturas militares em Shenyang, Pequim, Lanzhou, Jinan, Nanjing, Guangzhou e Chengdu foram reorganizados em 5 Teatros de Comando: Oriental (ETC), Sul (STC), Ocidental (WTC), Norte (NTC) e Central (CTC) (...) foi estabelecido um sistema de comando de operações CMC-TCs-Tropas (...) [e] o número de pessoal nos órgãos dirigentes ao nível do regimento e acima dele foi reduzido em cerca de 25%, e o das unidades não combatentes em quase 50% (DNCNE, 2019, p. 17-18).

[85] Ao todo foram reestruturadas 77 universidades e 44 faculdades. A Universidade de Defesa Nacional (NDU) e a Universidade Nacional de Tecnologia de Defesa (NUDT) foram reorganizadas. As forças armadas da China criaram o Comitê Diretor da CMC para a Investigação Científica Militar e reorganizaram a Academia de Ciências Militares (AMS) e os institutos de investigação das forças (DNCNE, 2019, p. 19).

> Foram tomadas medidas de reforma para reforçar a capacidade de combate das armas, reduzir as hierarquias de comando e combinar as tropas em níveis inferiores. Novos tipos de forças de combate foram aprimorados para conduzir operações especiais, ataque e defesa em todas as dimensões, [...] com o objetivo de tornar a composição da força completa, combinada, multifuncional e flexível (DNCNE, 2019, p. 19).

As transformações nas agências responsáveis pela defesa e segurança conduziram à priorização da eficácia no uso da força, com vistas a consecução de objetivos estratégicos nacionais. De tal que as tropas da PAPF foram reorganizadas, com isso cinco comandos, dentre eles o de Xinjiang e o do Tibete ficaram sob responsabilidade dos militares (DNCNE, 2019)[86].

No que concerne às novas estruturas construídas, vale destacar a força PLASSF criada para alavancar as capacidades organizacionais das operações conjuntas orquestradas em múltiplos domínios, responsáveis, dentre outras funções, por oferecer suporte operacional para aquisição e uso de "informação, comunicações, segurança da informação e testes de novas tecnologias" em conflitos (DNCNE, 2019, p. 21).

Diante do exposto, consideramos axiomático que ao longo das últimas duas décadas as mudanças estruturais e organizacionais levadas à cabo no ceio das agências de defesa e segurança, as tornaram aptas para utilizar o ciberespaço como novo domínio de guerra.

Conforme veremos, o conflito que resultou da irreparável equalização dos relações sino-indianas, somado ao robustecimento das capacidades de emprego da força por parte das instituições de segurança e defesa da China, representa o terceiro caso excepcional do uso do ciberespaço em ações ofensivas para auferir vantagens estratégicas em um conflito regional. Nesse ensejo, a seção seguinte, apresenta destaca as operações militares deflagradas pelos chineses, com foco na identificação do mecanismo que regula o uso do ciberespaço para consecução de objetivos estratégicos do Estado.

[86] Em 2019 o Exército do ELP contava com cinco comandos, dentre eles o de Xinjiang e o do Tibete.

5.3. Guerra Cibernética: o emprego da tecnologia da informação no conflito China-Índia (2020-2022)

A fim de compreender de forma substantiva os efeitos do fenômeno da guerra cibernética esta seção pretende examinar os ataques cibernéticos que atingiram setores de infraestrutura crítica na Índia em seu contexto mais amplo. Na qualidade de operação especial que se constitui numa cadeia de eventos interconectados que aproximam campanhas de reconhecimento e exploração de sistemas de informação ao uso da força militar (BRENNER, 2011; LILIENTHAL AND AHMAD, 2015), considerada condição suficiente para o uso efetivo do ciberespaço para projeção de poder nacional.

A partir da coleta de evidências que revelam o *modus operandi* das instituições civis e militares chinesas via ciberespaço, bem como as principais ameaças e armas utilizadas, identificamos o funcionamento do mecanismo de ação conjunta entre os atores estatais e não-estatais nas operações do ELP, simbiose que amplifica a assimetria de poder entre China e Índia em contexto regional.

Os relatórios examinados apresentam evidências de que as operações cibernéticas ofensivas que atingiram as redes de infraestrutura crítica indiana foram orquestradas pela China, através de campanhas de reconhecimento e exploração de longo prazo, que proporcionam as condições para a consecução de operações cibernéticas ofensivas. No que se refere à sua configuração, o material contém registros do funcionamento do mecanismo de atuação conjunta entre atores estatais e não-estatais a serviço da República Popular da China para projeção de poder nacional via ciberespaço (CYFIRMA 2020a; CYFIRMA, 2020b; RECORDED FUTURE, 2021; 2022).

Do amálgama entre instituições vinculadas ao setor público e ao privado, resultam operações conjuntas que permitiram o uso efetivo do ciberespaço com vistas à consecução de objetivos estratégicos, fenômeno que se verifica com base no rastreamento do processo de atuação conjunta entre as forças de segurança e defesa nacional e das APAs. Mais especificamente, através da identificação dos caminhos percorridos entre as fases de preparação para penetrar em alvos específicos e subtrair

informações úteis e os ataques cibernéticos aos sistemas operacionais de infraestrutura crítica (MANDIANT, 2013; RECORDED FUTURE, 2021; 2022)[87].

Sem embargo, nas últimas décadas, as operações cibernéticas envolvendo atores não-estatais privados e órgãos institucionais atribuídas à China têm despertado a atenção da comunidade internacional de segurança. Em virtude disso, análises acadêmicas e relatórios produzidos por 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, HSIAO, 2011; KREKEL, PATTON, BAKOS, 2012; MANDIANT, 2013; FIREEYE, 2015; 2017; CROWDSTRIKE, 2018; JOHNSON, 2018; CYFIRMA 2020a; 2020 b; RECORDED FUTURE, 2017; 2021; 2022).

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

Diversas instituições civis e empresas privadas se associaram às campanhas de reconhecimento e exploração de redes vinculadas ao terceiro e ao quarto departamentos do ELP. Dentre as quais, universidades e institutos de pesquisa e desenvolvimento de tecnologia para a guerra de informação e gigantes do setor de tecnologia da informação, como as empresas Boyu Information Technology Company (Boyusec) e a Huawei Technologies (HJORTDAL, 2011; STOKES, 2015)[88].

Frente ao problema, em 2016, o setor de inteligência do Departamento de Defesa norte-americano reportou uma possível ligação entre as empresas de segurança cibernética e o serviço de inteligência do MSE, em operações de espionagem

[87] Ao acessarem as redes dos alvos, as ameaças podem permanecer indetectáveis por longos períodos de tempo, pois, contam com procedimentos operacionais padronizados, infraestrutura técnica reutilizável, divisão de trabalho e inteligência para operar em sistemas de rede complexos, fatores que não apenas amplificam a efetividade das operações, mas indicam a presença de estruturas organizacionais robustas capazes de subsidiar as operações (MANDIANT, 2013).

[88] 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 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).

cibernética que tinham como objetivo favorecer empresas chinesas, as quais estariam atuando em conjunto com as instituições militares para a produção de tecnologias de uso dual (THE WASHINGTON FREE BEACON, 2016).

A denominada APA3 ou Gothic Panda envolvida nestes ataques era monitorada desde 2010, seu envolvimento com o MSE e a 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, foi identificado como catalisador do desenvolvimento de produtos de defesa para emprego em operações de inteligência cibernética nas últimas décadas (RECORDED FUTURE, 2017). Em 2015, a empresa e o escritório de segurança da informação chinês criaram um laboratório conjunto para teste de *softwares* para desenvolvimento de defesas cibernéticas[89].

As evidências da ligação entre a APA3, instituições civis, militares, a Boyusec e seus parceiros registram o funcionamento de um modelo de ação orquestrado pelo Estado 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, técnicas tradicionais, como o uso de *spear phishings* e de ferramentas de acesso remoto, bem como de ferramentas mais sofisticadas capazes de causar ataques disruptivos contra sistemas operacionais de setores estratégicos, como defesa, transporte, telecomunicações e departamentos governamentais foram empregadas (FIREEYE, 2015).

Cientes de que já haviam sido registradas, na primeira metade deste século, tentativas chinesas de uso do ciberespaço para atingir sistemas de energia nos Estados Unidos (HJORTDAL, 2011). Quase uma década depois, agências especializadas em segurança cibernético apontaram evidências de que os chineses haviam adquirido a capacidade de realizar um ataque cibernético disruptivo contra redes de sistemas de infraestrutura crítica (RECORDED FUTURE, 2021).

Destarte, logo após o término do confronto no Vale de Galwan, em 2020, China e Índia iniciaram tratativas diplomáticas para reestabelecer as relações de confiança mútua na região. Conquanto, medidas coercitivas foram tomadas em diversos

[89] 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).

segmentos econômicos, com destaque para o banimento de mais de duzentos aplicativos de origem chinesa, sob a alegação de que estariam sendo utilizados para coletar dados dos cidadãos indianos (RECORDED FUTURE, 2021).

A resposta chinesa foi dada pelo ciberespaço, em 13 de outubro de 2020, com ataques disruptivos que causaram danos aos sistemas financeiro, elétrico e de transporte ferroviário indiano, afetando mais de vinte milhões de usuários (THE NEW YORK TIMES, 2021).

Em fevereiro de 2021, na medida em que as investidas cibernéticas sobre a Índia continuaram a ganhar relevo, agentes responsáveis por uma série de operações de infiltração foram identificados, bem como os códigos maliciosos utilizados para afetar o funcionamento de quatro centros regionais de distribuição de energia e dois portos marítimos. De acordo com o relatório, as operações foram conduzidas pela APA41 ou RedEcho, especializada em espionagem cibernética (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 C2 das infraestruturas críticas indianas (RECORDED FUTURE, 2021).

Embora, a ligação entre a interrupção de energia e o código malicioso ainda não tenha sido admitida por fontes oficiais, existem fortes evidências que apontam para o envolvimento da China neste evento "[...] 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).

As operações demonstraram capacidades chinesas para utilização deste domínio para causar danos físicos, inéditas até então, tais ações representam movimentos estratégicos do Estado e visam ampliar a magnitude do poder nacional "[...] 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).

Conforme registrado, as incursões da China contra alvos indianos cresceram exponencialmente. Em dezembro de 2020, uma série de ataques cibernéticos utilizando *spear phishing*, e-mails com informações sobre os soldados feridos no conflito foram disparados para atrair a atenção de usuários com acesso aos sistemas operacionais de infraestrutura crítica, dentre os alvos setores de energia, refinarias de petróleo e uma usina nuclear (THE NEW YORK TIMES, 2021).

As operações foram atribuídas à organização Fang Xiao Qing, grupo proveniente dos territórios de Guangdong e Henan na China, e reportadas 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).

Entre 2020-2021, a APA10 ou Stone Panda/MenuPass, outra ameaça vinculada à China, foi detectada tentando acessar as redes de infraestrutura crítica na Índia. Foram registradas operações cibernéticas em escala, com intuito de subtrair dados comerciais e informações sobre cadeia de suprimentos de empresas indianas, invadir sistemas de informação de setores diversos (automotivo, aviação, energia, finanças, produtos farmacêuticos e telecomunicações) e redes corporativas, todos foram alvos de tentativa de extração de dados de propriedade intelectual vinculadas a projetos de pesquisa e desenvolvimento de tecnologia com alto valor agregado (CYFIRMA, 2020a; 2020b).

Em 2021, o grupo atingiu o setor 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 da APA10 estavam sendo monitoradas há mais de uma década por empresas especializadas em cibersegurança, as quais indicaram sua associação com o MSE e a CASTI (FIREEYE, 2017)[90]. Os relatórios contêm uma série de evidências dos

[90] 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

movimentos de membros vinculados a este grupo, coletadas em 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; JOHNSON, 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).

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 comunicação entre os servidores 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).

Em 2022, novas operações cibernéticas identificadas indicaram o envolvimento de grupos hackers e instituições de Estado da China, o ELP e do MSE foram apontados como os principais articuladores dos ataques que atingiram: o Centros de Despacho de Cargas Estaduais (CDCE), responsável pela distribuição de energia elétrica em Ladakh, no setor ocidental de fronteira com a Índia, o sistema nacional de resposta a emergências e uma empresa privada de logística (RECORDED FUTURE, 2022) [91].

Dentre as armas utilizadas, o '*ShadowPad*' foi identificado, porém as atividades não foram atribuídas ao grupo RedEcho por ausência de evidências que corroborem a ligação, em razão disso, o grupo foi classificado temporariamente como Grupo de Atividades e Ameaças 38 (GAA38). Contudo, os alvos atingidos foram similares àqueles em que o RedEcho esteve envolvido, são mantenedores de frequência e

'*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).

[91] Os alvos identificados estão localizados próximos a área de fronteira disputada em Ladakh, alguns deles já haviam sido atingidos por atividades anteriores da RedEcho (RECORDED FUTURE, 2022).

estabilidade de rede, responsáveis por garantir o acesso aos SCADA (RECORDED FUTURE, 2022)[92].

As operações do grupo buscavam acesso a dispositivos interconectados, como câmeras de vigilância para coleta de informações que pudessem viabilizar as atividades de intrusão. Diante da complexidade dos ICSs que operam infraestruturas críticas, a aquisição de informações sobre o funcionamento interno destes alvos é fundamental para assegurar a efetividade, por essa lógica, a identificação de campanhas de intrusão lenta e gradual, direcionadas a monitorar o fluxo de redes operacionais, aumentam a probabilidade de uma ação ofensiva ocorrer num próximo confronto na região fronteiriça (RECORDED FUTURE, 2022).

Logo, conforme o exposto, o fenômeno da guerra cibernética resulta dos insumos coletados através de campanhas de reconhecimento e exploração, somados à presença de ataques disruptivos. Nossa análise demonstra que sua efetividade decorre do funcionamento da interação entre as instituições securitárias, os setores da iniciativa privada e as ameaças avançadas - Gothic Panda (APA3), Stone Panda (APA10), RedEcho (APA41) e GAA (APA38) -, para uso de novos domínios da guerra que permitam ampliar as capacidades de projeção de poder nacional da China.

5.4. Considerações Finais

Ao considerarmos as nuances que permeiam o equilíbrio das relações entre chineses e indianos, verificamos indícios de que o conflito sucedido, em 2020, resulta de uma série histórica de disputas territoriais envolvendo o uso da força e de vias diplomáticas, com intuito de acomodar os interesses estratégicos de China e Índia nas regiões da LAC.

Conforme apresentado, chineses e indianos passaram por processos políticos internos e externos que produziram efeitos sobre o equilíbrio securitário regional, provocando a eclosão de movimentos separatistas e a anexação de territórios-chave ao longo da região de fronteiras, por essa razão, as reivindicações em torno da possessão destes locais, nos setores ocidental e oriental, continuam em aberto. Como agravante, o

[92] Embora a GCC38 atue de modo similar ao RedEcho, no que tange aos alvos e armas utilizadas, os peritos identificaram diferenças significativas nos TTPs de infraestrutura utilizados durante a operação, diante da ausência provas técnicas suficientes a conexão entre os grupos não foi considerada neste relatório (RECORDED FUTURE, 2022).

processo de interação entre grandes potências e os separatistas foi incorporado ao eixo narrativo utilizado pela República Popular da China para justificar as operações das forças de segurança e defesa.

Nossa análise identifica duas condições, suficiente e necessária, que permitiram à China utilizar o ciberespaço para projetar poder sobre a região da Ásia-Pacífico. Com base em relatórios produzidos por empresas e instituições especializadas em segurança cibernética, verificamos um aumento das capacidades operacionais, manifesta em função da atuação interagências, com vistas à consecução de objetivos estratégicos.

Dentre as principais agências estatais e não-estatais envolvidas destacamos: o MSE, CASTI, GLEI e Terceiro e Quarto Departamentos do Exército do ELP, empresas de tecnologia Boyusec e Huawei e as ameaças Gothic Panda, Stone Panda, RedEcho e GAA.

A análise das fontes oficiais, demonstra que a magnitude para coordenar esforços em um patamar que proporcione a utilização do domínio cibernético em operações ofensivas depende das condições institucionais adequadas, bem como do funcionamento da atuação conjunta de atores estatais e não-estatais, para uso de novas tecnologias da informação em conflitos regionais de modo discreto e efetivo.

Por fim, as operações ora examinadas envolveram diretamente o uso de informações coletadas em campanhas de reconhecimento e exploração de sistemas computacionais, isto é, revelam a significância da tecnologia da informação, da cooperação interagências e do ciberespaço para ampliar a assimetria de poder entre a República Popular da China e a Índia durante o conflito (2020-2022).

CAPÍTULO VI

6.1. Considerações Metodológicas
[Conteúdo indisponível, divulgação no Lume prevista para 29/11/2024]

6.2. Análise Histórico-Comparativa: diferenças e similitudes
[Conteúdo indisponível, divulgação no Lume prevista para 29/11/2024]

6.3. Guerra Híbrida: uma teoria indutiva
[Conteúdo indisponível, divulgação no Lume prevista para 29/11/2024]

CONCLUSÃO

Ao tratarmos do problema fundamental da segurança cibernética, esta pesquisa demonstrou como e porque potências como Estados Unidos, Rússia e China passaram a incorporar a tecnologia da informação com vista à projeção de poder nacional. Ao longo deste percurso, nossa análise dos conflitos desencadeados nas últimas décadas contra adversários como Irã, Ucrânia e Índia, identificou as condições e o mecanismo causal que fizeram do ciberespaço um domínio de guerra fulcral para consecução dos objetivos estratégicos das potências à nível regional.

Nossa atenção à historicidade dos casos destaca os interesses das potências em intervir na dinâmica interna de seus adversários, razões ditadas pelas nuances nas relações entre eles. Por conseguinte, o ciberespaço foi considerado uma alternativa viável para que pudessem atingi-los de modo discreto e efetivo.

Frente ao contexto, realizamos inferências descritivas lógico-dedutivas por meio da aplicação de testes qualitativos que tiveram por finalidade indicar a conexão das cadeias causais que permitiram a produção do fenômeno da guerra cibernética, lastreados pela identificação de evidências que confirmaram as condições hipotéticas previstas em nosso modelo.

Neste ensejo, verificamos que a mudança institucional pela qual passaram as forças de segurança e defesa nacional para incorporar este domínio à estratégia nacional produziu novas estruturas institucionais e mobilizou outras já existentes para oferecer respaldo à construção de operações especiais que utilizaram o ciberespaço para explorar as vulnerabilidades em sistemas informacionais de seus adversários.

Ao examinarmos a ligação entre campanhas de reconhecimento e exploração e ataques disruptivos a setores de infraestrutura crítica, sublinhamos a existência da guerra cibernética e seus efeitos cinéticos. Frente aos achados resta explícito o caráter auto reprodutivo deste fenômeno, os casos subsequentes à operação ‘Jogos Olímpicos’ foram registrados como produto de processos similares pelos quais passaram as instituições securitárias de Rússia e China.

No tocante às zonas de divergências que se constituem na literatura recente sobre o tema, verificamos que as explicações realistas possuem lacunas que, por um lado, desconsideram a concretude da guerra cibernética e, por outro, quando a reconhecem, pouco atestam sobre seus mecanismos de ação conforme empregados por Estados fortes. Diante das lacunas, nossos achados tornam inconteste a existência do

fenômeno, porém nos parece pouco plausível desconsiderar o grau de desenvolvimento tecnológico e eficiência institucional das potências como chave para seu uso efetivo e discreto.

Com base nos resultados desta pesquisa, resta claro que a sofisticação necessária para coordenar campanhas de reconhecimento e exploração de sistemas a fim de empreender ataques cibernéticos capazes de causar danos físicos às infraestruturas críticas, torna imperativa a robustez institucional que balize a constituição de operações especiais sofisticadas. Tais movimentos envolvem expertise técnica, capacidades militares avançadas e estruturas de suporte consolidadas, restritas a poucos Estados do sistema internacional, restando pouco provável que àqueles tecnologicamente menos avançados possam causar danos de modo similar contra as potências, invertendo a lógica das consequências, em caso de escalonamento indesejável dos conflitos.

Nosso exame da simbiose que representa a interação entre atores estatais e não estatais atuando via ciberespaço revela como a guerra cibernética afeta a disparidade de forças entre as potências e seus adversários mediante o uso de um novo domínio, para o qual os segundos não possuíam capacidades de combate satisfatórias. Por intermédio da abordagem qualitativa descritiva e explicativa identificamos este mecanismo como a pedra angular que conecta a mudança institucional ao uso do ciberespaço para explorar vulnerabilidades em infraestruturas críticas e causar danos cinéticos.

Diante do exposto, podemos afirmar com parcimônia que os condicionantes que envolvem o processo de emprego da tecnologia da informação em conflitos regionais confirmam a hipótese de que as operações cibernéticas ampliam a assimetria de poder entre as grandes potências e seus adversários regionais.

Sem embargo, a explicação deste fenômeno aponta algumas das razões pelas quais o ciberespaço se tornou relevante para Estados Unidos, Rússia e China no século vinte e um. Ao buscarmos oferecer a resposta ao questionamento central que orientou esta tese retomamos o debate liberal sobre a necessidade de construção de mecanismos regulatórios das atividades dos Estados no ciberespaço para averiguar quais incentivos as potências supracitadas possuem para levar à cabo esta agenda, uma vez que a inserção deste domínio nas estratégias nacionais das potências afeta noções tradicionais sobre a guerra e a paz consolidadas no campo de estudos sobre Política Internacional e Defesa.

Nossa teoria aponta para o *cinismo* em matéria de política internacional como fator chave para explicar não apenas as razões que conduziram as potências a recorrer

ao ciberespaço para alcançar objetivos estratégicos, mas, sobretudo, tornar evidente a ausência de incentivos para alterar a atual dinâmica da guerra cibernética, uma vez que são elas as principais beneficiárias do atual *status quo* dos mecanismos de regulação das atividades ofensivas neste domínio.

Frente ao cenário consideramos que ao utilizarem a guerra híbrida para exercer pressão sobre seus alvos, as potências levantaram dúvidas sobre a capacidade do poder público em prover a segurança interna de seu território e população. Por essa lógica, demonstraram a posição de vulnerabilidade em que encontravam seus adversários ao infringir-lhes danos cinéticos, através de operações que se mantiveram abaixo do limiar da guerra convencional, conflitos perenes que não produziram efeitos negativos dada atribuição tardia dos ataques.

Consideramos que nossa teoria indutiva, ainda que restrita ao universo de poucos casos analisados possa alcançar validade externa na medida em que casos semelhantes, nos quais a mudança institucional para incorporação da tecnologia da informação às estratégias de segurança e defesa nacional dos Estados não resulte em ataques a infraestruturas críticas como alternativas para consecução de objetivos estratégicos nacionais, possam ser examinados. A relevância do estudo de casos negativos pode vir a se constituir numa agenda de pesquisa útil para testar nossas explicações ou refutá-las com uso de métodos de avaliação mais sofisticados como Qualitative Comparative Analysis (QCA), indicado para pesquisas com número médio de casos que se dispõem a testar sua consistência.

Finalmente, ao atestarmos a relevância do emprego da tecnologia da informação na estratégia da guerra híbrida, conforme aplicada pelas potências em conflitos regionais acreditamos que esta tese possa contribuir para o avanço das pesquisas neste campo ainda pouco explorado pela literatura acadêmico-científica.

REFERÊNCIAS

ALBRIGHT, David; BRANNAN, Paul; WALROND, Christina. Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment. **Institute for Science and International Security**, dez. 2010. Disponível em: https://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/. Acesso em: 26 mar. 2023.

ALBRIGHT, David et al. Preventing Iran From Obtaining Nuclear Weapons: Restricting its Future Nuclear Options. **Institute for Science and International Security**, mar. 2012. Disponível em: https://isis-online.org/uploads/isis-reports/documents/USIP_Template_5March2012-1.pdf. Acesso em: 27 mar. 2023.

ALBRIGHT, David; BURKHARD, Sarah. Entering Dangerous, Uncharted Waters: Iran's 60 Percent Highly Enriched Uranium**. Institute For Science and International Security**, abr. 2022. Disponível em: https://isis-online.org/isis-reports/detail/entering-uncharted-waters-irans-60-percent-highly-enriched-uranium. Acesso em: 12 ago. 2023.

AVERSA, Tullio. China: An Evolutionary Analysis of its Cyber Strategy. **Center for Cyber Security and International Relations Studies**, Florença, p. 1-13, 2018. Disponível em: https://www.researchgate.net/publication/335798514_China_An_Evolutionary_Analysis_of_its_Cyber_Strategy. Acesso em: 23 nov. 2022.

AZENHA, Pedro Jorge de Oliveira. **A estratégia Nuclear Iraniana e os Desafios Colocados à Comunidade Internacional**. 2010. Trabalho de Investigação Individual -Instituto de Estudos Superiores Militares, Lisboa, 2010.

ASSANT, Michael J; LEE, Robert M. The Industrial Control System Cyber Kill Chain. **SANS Institute Information Security Reading Room**, p. 1–23, out. 2015. Disponível em: https://sansorg.egnyte.com/dl/HHa9fCekmc. Acesso em: 20 abr. 2020.

BAEZNER, Marie; ROBIN, Patrice. Hotspot Analysis: Stuxnet. **Centre for Security Studies**, p. 1-16, out. 2017 Zurich: ETH. 2017. Disponível em: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-04.pdf. Acesso em: 18 jun. 2023.

BARATA, Pedro. A Ucrânia, a UE e a Rússia: Softpower versus Realpolitik?. **Observatório da Universidade Autônoma de Lisboa**, Lisboa, v.5, n.1, p. 33-50, mai./out. 2014. Disponível em: https://repositorio.ual.pt/bitstream/11144/573/5/pt_vol5_n1_art3.pdf. Acesso em: 12 abr. 2020.

BASHIR, Sadaf; TAJ, Shaista. An Assessment of Drivers and Dynamics of 2020 Sino-Indian Border Conflict. **Multicultural Education**, v. 8, n. 6, jun. 2022. Disponível em: http://ijdri.com/me/wp-content/uploads/2022/06/28.pdf. Acesso em: 18 mai. 2022.

BBC. Ukraine Crisis in Maps. **BBC NEWS**, fev. 2015. Disponível em http://www.bbc.com/news/world-europe-27308526. Acesso em: 18 abr. 2020.

BBC. Galwan Valley: China and India Clash on Freezing and Inhospitable Battlefield. **BBC NEWS**, jun. 2020. Disponível em: https://theprint.in/defence/4-9-or-14-even-china-isnt-sure-how-many-pla-soldiers-died-in-galwan-valley/613372/. Acesso em: 15 mai. 2022.

BENCSÁTH, Boldizsár et al. The Cousins of Stuxnet: Duqu, Flame, and Gaus. **Future Internet**, n. 4, p. 971-1003, 2012. Disponível em: https://www.mdpi.com/1999-5903/4/4/971. Acesso em 19 jun. 2023.

BENNET, Andrew; CHECKEL, Jeffrey T. **Process Tracing from metaphor to analytic tool**. 1º ed. New York: Cambridge University Press, 2014.

BERGEN, Peter; MAURER, Tim. Cyberwar Hits Ukraine. **CNN NEWS**, mar. 2018. Disponível em: https://edition.cnn.com/2014/03/07/opinion/bergen-ukraine-cyber-attacks/index.html. Acesso em: 28 mai. 2020.

BERMÚDEZ, Ángel. Programa Nuclear do Irã: Como EUA Ajudaram o País a Iniciar Polêmico Plano Atômico. **BBC NEWS Brasil**, dez. 2021. Disponível em: https://www.bbc.com/portuguese/geral-59491973. Acesso em: 15 abr. 2023.

BETZ, David J.; STEVENS, Tim. **Cyberspace and the State: Toward a Strategy for Cyber-Power**. 1.º ed. UK : IISS Routledge, 2011. 153 p.

BLINDER, Caio. Discurso do 'Eixo do Mal' Assombra Bush. **BBC NEWS Brasil**, out. 2006. Disponível em: https://www.bbc.com/portuguese/reporterbbc/story/2006/10/061012_caioblinderaw. Acesso em: 20 fev. 2023.

BINGYAN, Li. **Stratagem and Transformation**. Beijing: New China Press, 2004.

BONNEL, Victoria; COOPER, Ann; FREIDIN, Gregory. **Russia at the barricades: eyewitness accounts of the 1991 Coup**. 1.º ed. New York: Routledge, 1994. 384 p.

BRENNER, Joel. **America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare**. Penguin. 1.º ed. England : Penguin Press, 2011. 431 p.

BRENNER, Joel. Eyes Wide Shut: The Growing Threat of Cyber Attacks on Industrial Control Systems. **Bulletin of the Atomic Scientists**, v. 69, n. 5, p. 16-20, 2013. Disponível em: https://www.ingentaconnect.com/content/routledg/rbul20/2013/00000069/00000005. Acesso em: 12 jul. 2023.

BRZEZINSKI, Zbigniew. **The Grand Chessboard: American Primacy and Its Geostrategic Imperatives**. 1º ed. Washington D.C: Basic Books, 1997. 240 p. E-book.

BUCHAN, Russel. Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?. **Journal of Conflict and Security Law**, v. 17, n.2, p. 211-227, 2012. Disponível em: https://www.jstor.org/stable/26296227. Acesso em: 21 mai. 2021.

BULAU, Doris. 1990: Rússia Declara Independência da URSS. Deutche Welle História. **DW NEWS**, 2004.

Disponível em: https://www.dw.com/pt-br/1990-r%C3%BAssia-declarava-independ%C3%AAncia-da-urss/a-314494. Acesso em: 19 mai. 2020.

BUTRIMAS, Vytautas. National Security and International Policy Challenges in a Post Stuxnet World. **Lithuanian Annual Strategic Review**, v. 12, p. 11-31, 2014. Disponível em: https://kam.lt/wp-content/uploads/2022/03/lithuanian-annual-strategic-review-2013-2014-vol-12.pdf. Acesso em 08 mai. 2023.

CARVALHO, Fernando Duarte; SILVA, Eduardo Mateus. **Cyberwar-Netwar: Security in the Information Age**. Amsterdam: IOS Press, 2006. 176 p.

CASALUNGA, F. H. Entre Amigos: A Consolidação do Autoritarismo Competitivo na Rússia Pós-Soviética (1990-2009). **Política Hoje**, v. 29, n.2, p. 8-29, 2020. Disponível em: https://periodicos.ufpe.br/revistas/index.php/politicahoje/article/view/246563. Acesso em 13 jul. 2021.

CASALUNGA, F. H. Guerra Russo-Ucraniana: Uma Tragédia Anunciada?. **ESTADÃO Gestão, Política e Sociedade**, fev. 2022. Disponível em: https://www.estadao.com.br/politica/gestao-politica-e-sociedade/guerra-russo-ucraniana-uma-tragedia-anunciada/. Acesso em: 28 mar. 2022.

CENTER FOR DEVELOPMENT IMPACT PRACTICE PAPER. Straws-in-the-Wind, Hoops and Smoking Guns: What can Process Tracing Offer to Impact Evaluation? **Institute of Development Studies**, n. 10, abr, p. 1-8, 2015. Disponível em: https://www.ids.ac.uk/publications/straws-in-the-wind-hoops-and-smoking-guns-what-can-process-tracing-offer-to-impact-evaluation/. Acesso em: 29 jun. 2020.

CHEN, Thomas. Stuxnet, the Real Start of Cyber Warfare?. **IEEE Network**, v. 24, n. 6, nov./dez, p. 2-3, 2010. Disponível em: https://ieeexplore.ieee.org/abstract/document/5634434. Acesso em: 19 jun. 2023.

CHEN, Thomas; ABU-NIMEH, Saeed. Lessons from Stuxnet. **IEEE Network**, v. 44, n. 4, abr, p. 91-93, 2011. Disponível em: https://ieeexplore.ieee.org/document/5742014. Acesso em: 16 jun. 2023.

CHOUCRI, Nazli.; GOLDSMITH, Daniel. Lost in cyberspace Harnessing the Internet, international relations, and global security. **Bulletin of the Atomic Scientists**, v. 68, n.2, p. 372-385, 2012. Disponível em: https://journals.sagepub.com/doi/full/10.1177/0096340212438696. Acesso em: 05 jul. 2023.

CLARKE, Richard. The Comming Cyber Wars: Obama's Cyber Strategy is Missing the Point. **Boston Globe**, jul, 2011. Disponível em: https://archive.boston.com/bostonglobe/editorial_opinion/oped/articles/2011/07/31/the_coming_cyber_wars/. Acesso em: 26 mar. 2023.

CLARK, Richard; KNAKE, Robert. **Cyber War: The Next Threat to National Security and What to Do about It**. New York: Harpercollins, 2010. 306 p.

CLAYTON, M. Stuxnet Malware is 'Weapon' Out to Destroy…Iran's Bushehr Nuclear Plant? **Christian Science Monitor**, set. 2010. Disponível em:

https://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant. Acesso em: 18 jun. 2023.

COLLIER, David. Understanding Process Tracing. **Political Science and Politics, Berkley**, v. 44, n. 4, p. 823-830, out, 2011. Disponível em: https://polisci.berkeley.edu/sites/default/files/people/u3827/Understanding%20Process%20Tracing.pdf. Acesso em 08 mai. 2020.

COLLIER, David; BRADY, Henry. E.; SEAWRIGHT, Jason. Sources of Leverage in Causal Inference: Toward an Alternative View of Methodology. *In:* COLLIER, David; BRADY, Henry E. **Rethinking Social Inquiry: Diverse Tools, Shared Standards**. 2.º ed. Lanham: Rowman and Littlefield, 2010. p. 161-199.

COLLINS, Sean; MCCOMBIE, Stephen. Stuxnet: The Emergence of a New Cyber Weapon and Its Implications. Journal of Policing. **Intelligence and Counter Terrorism**, v. 7, n. 1, p. 80-91, 2012. Disponível em: https://www.tandfonline.com/doi/full/10.1080/18335330.2012.653198. Acesso em: 23 jul. 2023.

CORNISH, Paul.; LIVINGSTONE, Dave Clemente.; YORKE, Claire. On Cyber Warfare. **Royal Institute of International Affairs**, nov, 2010. Disponível em: https://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r1110_cyberwarfare.pdf. Acesso em: 16 mar. 2023.

CHANGSHENG, S.; MENEZES JR. A. B. A Guerra Sino-Indiana de 1962: Contornos de um Conflito Inevitável. **Revista da Escola Superior de Guerra**, v. 29, n. 58, p. 180-198, 2014. Disponível em: https://revista.esg.br/index.php/revistadaesg/article/view/186. Acesso em: 23 jun. 2022.

CHOUCRI, Nazli. **Cyberpolitics in international relations**. Cambridge: MIT Press, 2012. 320 p. E-book.

CHUNG, Chien-peng. **Domestic Politics, International Bargining and China's Territorial Disputes**. UK: Routledge, 2004. 240 p.

CROWDSTRIKE, Global Threat Intel Report. **Crowdstrike**, p. 4-76, 2014. Disponível em: https://www.crowdstrike.com/2014-global-threat-report. Acesso em: 06 abr. 2020.

CROWDSTRIKE. Global Threat Intel Report. **Crowdstrike**, p. 3–89, 2015. Disponível em: https://go.crowdstrike.com/rs/281-OBQ-266/images/15GlobalThreatReport.pdf. Acesso em: 06 mai. 2020.

CROWDSTRIKE. Cyber Intrusion Services Casebook. **Crowdstrike**, p. 2–25, 2016. Disponível em: https://www.crowdstrike.com/resources/reports/crowdstrike-cyber-intrusion-services-casebook-2016/. Acesso em: 07 jun. 2020.

CROWDSTRIKE. Two Birds, One Stone Panda, **Crowdstrike**, 2018. Disponível em: https://www.crowdstrike.com/blog/two-birds-one-stone-panda/. Acesso em: 21 jun. 2022.

CYFIRMA. Cyber Espionage and the Asia Threat Landscape**. Cyfirma News**, 2020a. Disponível em: https://www.cyfirma.com/news/cyber-espionage-and-the-asia-threat-landscape/. Acesso em: 17 jun. 2022.

CYFIRMA. Rising Cyber Attacks Due to China-India Border Conflict Tokyo, **Cyfirma News**, 2020b. Disponível em: https://www.cyfirma.com/early-warning/rising-cyber-attacks-due-to-china-india-border-conflict/. Acesso em: 17 jun. 2023.

DANYK, Yuriy; BRIGGS, Chad; MALIARCHUK, Tamara. Hitting Home: Cyber-Hybrid Warfare in Ukraine and its Impact on the United States. **Georgetown Journal of International Affairs**, fev, 2020. Disponível em: https://gjia.georgetown.edu/2020/02/18/cyber-hybrid-warfare-in-ukraine-and-impact-on-united-states/. Acesso em: 17 jan. 2024.

DE FALCO, Marco. **Stuxnet Facts Report: A Technical and Strategic Review**. Estônia: Tallinn, NATO Cooperative Cyber Defense Center of Excellence, 2012. Disponível em: https://ccdcoe.org/library/publications/stuxnet-facts-report-a-technical-and-strategic-analysis-2/. Acesso em: 08 jun. 2023.

DE OLIVEIRA, Marcos Aurélio Guedes; CASALUNGA, Fernando Henrique. Guerra Híbrida: O Emprego da Tecnologia da Informação no Conflito Rússia-Ucrânia (2014-2015). **Revista Brasileira de Estudos de Defesa**, v. 7, n. 2, p. 13-36, 2020. Disponível em: https://rbed.abedef.org/rbed/article/view/75208/42129. Acesso em: 07 jan. 2021.

DE OLIVEIRA, Marcos Aurélio Guedes, SVARTMAN, Eduardo Munhoz; CASALUNGA, Fernando Henrique. Pandemônio Cibernético: O Uso do Ciberespaço para Consecução de Objetivos Estratégicos da China no Conflito Sino-Indiano (2020-2021). **Revista Nação e Defesa**, n. 163, p. 27-50, 2022. Disponível em: https://www.idn.gov.pt/pt/publicacoes/nacao/Documents/NeD163/2.pdf. Acesso em: 29 jan. 2023.

DEEPAK, B. R. **India and China 1904-2004: A Century of Peace and Conflict**. 1.º ed. NewDelhi: Manak Publications, 2005. 508 p.

DENNING, Dorothy. Stuxnet: What Has Changed?. **Future Internet Journal**, v. 4, n. 3, 672-687, 2012. Disponível em: https://www.mdpi.com/1999-5903/4/3/672. Acesso em: 08 mai. 2023.

DESJARDINS, Richard. The Science of Military Strategy. *In*: GUANGQIAN, Peng. YOUZHI, Yao. **The China Quarterly**. Beijing: Military Science Publishing House, 2005. p. 194-196.

DUGGAN, Patrick M. Why Special Operations Forces in US Cyber-Warfare?. **The Cyber Defense Review**, jan, 2016. Disponível em: https://cyberdefensereview.army.mil/DesktopModules/ArticleCS/Print.aspx?PortalId=6&ModuleId=1233&Article=1136057. Acesso em: 12 mar. 2023.

DUGGAN, Patrick M.; OREN, Elizabeth. U.S. Special Operations Forces in Cyberspace. **The Cyber Defense Review**, v. 1, n. 2, p. 73-81, 2016. [Online] Disponível em: https://cyberdefensereview.army.mil/Portals/6/Documents/CDR-FALL2016.pdf?ver=2017-03-27-130219-357. Acesso em: 24 mar. 2023.

DUTTA, Sujan. Eyeball to Eyeball in Southern Ladakh – Fresh border row erupts between Indian and China patrols ahead of Xi visit. **The Telegraph**, mar, 2014. Disponível em: https://www.telegraphindia.com/india/eyeball-to-eyeball-in-southern-ladakh-fresh-border-row-erupts-between-indian-chinese-patrols-ahead-of-xi-visit/cid/1578313. Acesso em: 11 mai. 2022.

ELETRICITY INFORMATION SHARING AND ANALYSIS CENTER. Analysis of the Cyber Attack on the Ukranian Power Grid. **SANS Industrial Control Systems**, mar, 2016. Disponível em: https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf. Acesso em: 05.07.2023.

ESTADOS UNIDOS DA AMÉRICA. **Estratégia Nacional de Segurança Cibernética**. America's Cyber Defense Agency, 2003. Disponível em: https://www.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf. Acesso em: 08 ago. 2023.

ESTADOS UNIDOS DA AMÉRICA. **Estratégia de Segurança Nacional**. Washington DC: Office of the Secretary of Defense, 2006. Disponível em: https://history.defense.gov/Historical-Sources/National-Security-Strategy/. Acesso em: 10 jul. 2023.

ESTADOS UNIDOS DA AMÉRICA. **Estratégia de Segurança Nacional**. Washington DC: Office of the Secretary of Defense, 2010. Disponível em: <https://history.defense.gov/Historical-Sources/National-Security-Strategy/. Acesso em: 12 jul. 2023.

ESTADOS UNIDOS DA AMÉRICA. **Estratégia de Segurança Nacional**. . Washington DC: Office of the Secretary of Defense, 2015. Disponível em: https://history.defense.gov/Historical-Sources/National-Security-Strategy/. Acesso em: 18 jul. 2023.

ESTADOS UNIDOS DA AMÉRICA. **Estratégia de Defesa Nacional**. Washington DC: Office of the Secretary of Defense, 2008. Disponível em: https://history.defense.gov/Historical-Sources/National-Defense-Strategy/. Acesso em: 11 jul. 2023.

ESTADOS UNIDOS DA AMÉRICA. **Estratégia de Defesa Nacional**. Washington DC: Office of the Secretary of Defense, 2011. Disponível em: https://history.defense.gov/Historical-Sources/National-Military-Strategy/. Acesso em: 15 jul. 2023.

ESTADOS UNIDOS DA AMÉRICA. **Estratégia de Defesa Nacional**. Washington DC: Office of the Secretary of Defense, 2015. Disponível em: https://history.defense.gov/Historical-Sources/National-Military-Strategy/. Acesso em: 19 jul. 2023.

ESTADOS UNIDOS DA AMÉRICA. **Estratégia Ciber do Departamento de Defesa**. Washington DC: Office of the Secretary of Defense, 2015. Disponível em: https://nsarchive.gwu.edu/document/21384-document-25. Acesso em: 20 jul. 2023.

ESTADOS UNIDOS DA AMÉRICA. **'Little Green Men': a primer on Modern Russian Unconventional Warfare, Ukraine 2013-2014**. North Carolina: The United States Army Special Operations Command, 2015. Disponível em: https://www.jhuapl.edu/sites/default/files/2022-12/ARIS_LittleGreenMen.pdf. Acesso em: 29 abr. 2020.

FALLETI, Tulia. G. Process Tracing of Extensive and Intensive Processes. **New Political Economy**, v. 21, n. 5, p. 455-462, 2016. Disponível em: https://www.tandfonline.com/doi/full/10.1080/13563467.2015.1135550. Acesso em: 27 abr. 2023.

FALLETI, Tulia G.; MAHONEY, James. The comparative sequential method. *In:* MAHONEY, James; THELEN, Kathleen. **Advances in Comparative-Historical Analysis**. UK: Cambridge University Press, 2015. p. 211-239. Disponível em: https://www.cambridge.org/core/books/abs/advances-in-comparativehistorical-analysis/comparative-sequential-method/4EA22A74E138226321803CDBDE27618E. Acesso em: 02 jan. 2023.

FALLIERE, Nicolas; OMURCHU, L.; CHIEN, E. W32. Stuxnet Dossier. **Symantec Security Response**. USA: Symantec Corporation World Headquarters, fev, 2011. Disponível em: https://nsarchive.gwu.edu/document/21440-document-44 . Acesso em: 26 jan. 2023.

FANG, T. The Sino-Indian Border Talks Under the Joint Working Group. Issues & Studies, n.38, p. 150-183, 2002.

FANG, Tien-sze. **Asymmetrical Threat Perceptions in India-China Relations**. UK: New Delhi: Oxford University Press, 2014. 266 p. E-book.

FÂNZERES, José Manuel Ferreira. Geopolítica e Geoestratégia da Federação Russa: A Força da Vontade, a Arte do Possível. **Instituto de Defesa Nacional**, n. 14, 2014. Disponível em: https://comum.rcaap.pt/bitstream/10400.26/7758/1/idncaderno_14.pdf. Acesso em: 11 mar. 2020.

FARWELL, J.; ROHOZINSKI, R. The New Reality of Cyber War. **Survival : Global Politics and Strategy**, v. 54, n. 4, p. 107-120, 2012. Disponível em: https://www.tandfonline.com/doi/abs/10.1080/00396338.2012.709391. Acesso em: 19 jun. 2023.

FEDERAÇÃO RUSSA. **Doutrina Militar da Federação Russa**. Moscou: Presidência da República, 2010. Disponível em: http://kremlin.ru/supplement/461. Acesso em: 28 abr. 2020.

FEDERAÇÃO RUSSA. **Doutrina Militar da Federação Russa**. Moscou: Presidência da República, 2014. Disponível em: <https://rg.ru/2014/12/30/doktrina-dok.html>. Acesso em: Acesso em: 29 abr. 2020.

FEDERAÇÃO RUSSA. **Estratégia de Segurança Nacional da Federação Russa até 2020**. Moscou: Presidência da República, 2009. Disponível: em: http://kremlin.ru/supplement/424. Acesso em: 02 mai. 2020.

FEDERAÇÃO RUSSA. **Estratégia de Segurança Nacional da Federação Russa**. Moscou: Presidência da República, 2015. Disponível em: https://rg.ru/2015/12/31/nac-bezopasnost-site-dok.html. Acesso em: 03 mai. 2020.

FILHO, Willian Helal. O Referendo que Decretou a Independência da Ucrânia, Com Apoio de 92% do Povo. **O GLOBO**, fev, 2022. Disponível em: https://blogs.oglobo.globo.com/blog-do-acervo/post/ucrania-o-referendo-que-consolidou-independencia-apoiada-por-92-da-populacao.html. Acesso em: 29 mar 2022.

FIREEYE. APA28: A Window Into Russia's Cyber Espionage Operations? **FireEye**, p. 3–44, 2014. Disponível em: https://cyber-peace.org/wp-content/uploads/2018/11/rpt-apt28.pdf. Acesso em: 06 abr. 2020.

FIREEYE. APT30 and the Mechanics of A Long-Running Cyber Espionage Operation. **FireEye**, p. 3-67, 2015. Disponível em: < https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf. Acesso em: 20 abr 2020.

FIREEYE. Overload Critical Lessons From 15 Years of ICS Vulnerabilities. Industrial Control Systems (ICS) Vulnerability Trend Report, p. 3–11, 2016. Disponível em: https://vulners.com/fireeye/FIREEYE:4E09F4331A15A963A4DBE2EB3FF5EC20. Acesso em: 10 abr. 2020.

FIREEYE. APT10 (MenuPass Group): New Tools, Global Campaign Latest Manifestation of Longstanding Threat. **MANDIANT**, 2017. Disponível em: <https:// https:// www.mandiant.com/resources/apt10-menupass-group. Acesso em: 20 mai. 2022.

FISHER Jr., Richard. **China's Modernization: Building for Regional and Global Reach**. Santa Barbara: Praeger Security International, 2008. 344 p. E-book.

FRANZESE, Patrick. Sovereignty in Cyberspace: Can It Exist?. **Air Force Law Review**, v. 68, n.1, p. 1-42, 2009. Disponível em: https://www.afjag.af.mil/Portals/77/documents/AFD-091026-024.pdf. Acesso em: 04 ago. 2023.

FRAVEL, Taylor. **Strong Borders, Secure Nation: Cooperation and Conflict in China's Territorial Disputes**. USA: Princeton University Press, 2008. 408 p. E-book.

FRAVEL, Taylor. The PLA and National Security Decision Making: Insights from China's Territorial and Maritime Disputes. *In:* SAUNDERS, Phillip C.; SCOBELL, Andrew. **PLA Influence on China's National Security Policymaking**. USA: Stanford University Press, 2015. p. 249–73.

FREIRE, Maria. A Revolução Laranja na Ucrânia: Uma Democracia a Consolidar. **Instituto Português de Relações Internacionais**, n. 12, dez, p. 49-64, 2006. Disponível em: https://ipri.unl.pt/images/publicacoes/revista_ri/pdf/ri12/RI12_03MRFreire.pdf. Acesso em: 26 abr. 2020.

FREIRE, Maria. Relações UE-Ucrânia: A complexa Gestão de Objetivos, Motivações e Expectativas. **Instituto Português de Relações Internacionais**, jun, p. 2-36 2008. Disponível em: http://www.ces.uc.pt/myces/UserFiles/livros/877_IPRI%20Working%20Paper%2037.pdf. Acesso em 28 abr. 2020.

F-SECURE LABS. BlackEnergy Rootkit, Sort of. **F-Secure Labs**, 2014. Disponível em: https://www.f-secure.com/weblog/archives/00002715.html. Acesso em: 20 mai. 2020.

F-SECURE LABS. Blackenergy & Quedagh: The Convergence of Crimeware and APA Attacks. **F-Secure Labs**, p. 1–16, 2016. Disponível em: https://blog-assets.f-secure.com/wp-content/uploads/2019/10/15163408/BlackEnergy_Quedagh.pdf. Acesso em: 22 abr. 2020.

GALEOTTI, Mark. Russia's Hybrid Wars as A Byproduc of Hybrid State. **War on The Rocks**, 2016. Disponível em: https://warontherocks.com/2016/12/russias-hybrid-war-as-a-byproduct-of-a-hybrid-state/. Acesso em: 16 mar. 2020.

GALEOTTI, Mark. **Putin's Wars: From Chechnya to Ukraine**. UK: Bloomsbury Puslishinng Plc, 2022.

GARTZKE, Erik. The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. **International Security**, v. 38, n. 2, p. 41-73, 2013. Disponível em: https://www.jstor.org/stable/24480930. Acesso em: 12 jul. 2020.

GARVER, John. The Unresolved Sino-Indian Border Dispute: An Interpretation. **Journal of East Asian Studies**, v. 47, n.2, p. 99–113, 2011. Disponível em: https://journals.sagepub.com/doi/abs/10.1177/000944551104700204. Acesso em: 25 mai. 2022.

GARVER, John. **China's Quest: The History of the Foreign Relations of the People's Republic of China**. 1.º ed. New York: Oxford University Press, 2016.

GEERS, Kenneth. Introduction: Cyber War in Perspective. *In:* GEERS, Kenneth. **Cyber War in Perspective: Russian Aggression against Ukraine.** . NATO Cooperative Cyber Defense Centre of Excellence. EST: Tallinn, 2015. p. 13-18.

GILES, Keir. Russia and its Neighbours: Old Attitudes, New Capabilities. Conflict Studies Research Centre. *In:* GEERS, Kenneth. **Cyber War in Perspective: Russian Aggression against Ukraine.** 2015. p. 19-28.

GILES, Keir; HAGESTAD. William. Divided By a Common Language: Cyber definitions in Chinese, Russian and English. *In:* PODINS, K; STINISSEN, J; MAYBAUM, M. **5th International Conference on Cyber Conflict**. Cooperative Cyber Defense Centre of Excellence. EST: Tallinn 2013. p. 413-431.

GOSTEV, Alexander; KUZNETSOV, Igor. Stuxnet/Duqu: The Evolution of Drivers. **Kaspersky**, 2011. Disponível em: https://securelist.com/stuxnetduqu-the-evolution-of-drivers/36462/. Acesso em: 14 abr. 2020.

GREENBERG, Andy. Your Guide to Russia's Infrastructure Hacking Teams. **Wired Security**, jul, 2017. Disponível em: https://www.wired.com/story/russian-hacking-teams-infrastructure/. Acesso em: 20 abr. 2020.

HACQUEBORD, Feike. Pawn Storm's Domestic Spying Campaign Revealed: Ukraine and US Top Global Targets. **Trendmicro Security Intelligence**, 2015. Disponível em: http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storms-domestic-spying-campaign-revealed-ukraine-and-us-top-global-targets/. Acesso em: 22 abr. 2020.

HACQUEBORD, Feike. Two Years of Pawn Storm Examing and Incresingly Relevant Threat. **Trendmicro Security Intelligence**, 2017. Disponível em: https://documents.trendmicro.com/assets/wp/wp-two-years-of-pawn-storm.pdf. Acesso em: 12 mai. 2020.

HALL, Peter A. Systematic Process Analysis: When and How To Use It. **European Management Review**, n. 3, p. 24-31, 2006. Disponível em: https://scholar.harvard.edu/sites/scholar.harvard.edu/files/hall/files/emr.pdf. Acesso em: 05 jan. 2020.

HALL, P. A. Tracing the Progress of Process Tracing. Center for European Studies, Harvard University, Cambridge, p. 20-30, 2012. *In:* Center for European Studies, mar. 2012, Massachusetts. **Symposium**. USA: European Consortium for Political Research. 2012. p. 1-11. Disponível em: https://scholar.harvard.edu/files/hall/files/hall2012_eps.pdf. Acesso em: 06 jan. 2023

HALL, Peter A.; TAYLOR, Rosemary. C. As Três Versões do Neo-Institucionalismo. **Lua Nova**, n. 58, p. 193-224, 2003. Disponível em: https://ria.ufrn.br/handle/123456789/1883. Acesso em: 09 jan. 2020.

HALPIN, Edward et al. **Cyberwar, Netwar and the Revolution in Military Affairs**. UK: Palgrave Macmillian, 2006. 268 p. E-book.

HAYDEN, Michael. **Playing to the Edge: American Intelligence in the Age of Terror**. Nova York: Penguin Press, 2016. 460 p. E-book.

HEICKERO, Roland. Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations. **Swedish Defence Research Agency**, 2010. Disponível em: https://www.foi.se/rest-api/report/FOI-R%E2%80%932970%E2%80%93SE. Acesso em: 10 abr. 2020.

HJORTDAL, Magnus. China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence. Journal of Strategic Security, v. 4, n. 2, p.1-23, 2011. Disponível em: https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1101&context=jss. Acesso em: 29 abr. 2022.

HOFFMAN, Frank. **Conflict in the 21 Century The Rise of Hybrid Wars**. Virginia: Potomac Institute for Policy Studies, 2007. 72 p. E-book.

HOJNACKI, Daniel. Prescient Warnings For a Post-Stuxnet World. **Project Muse**, v. 41, n. 2, p. 143-145, 2021. Disponível em: https://muse.jhu.edu/article/852332. Acesso em: 21 jul. 2023.

HOLSLAG, Jonathan. The Persistent Military Security Dilemma Between China and India. **Journal of Strategic Studies**, v. 32, p. 811–840, 2009. Disponível em: https://www.tandfonline.com/doi/full/10.1080/01402390903189592. Acesso em: 18 mai. 2022.

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM. Cyber-Attack Against Ukrainian Critical Infrastructure. **Cybersecurity and Infrastructure Security Agency**, jun. p. 1–5, 2016. Disponível em: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01. Acesso em: 20 mai. 2020.

INSTITUTE FOR SCIENCE AND INTERNATIONAL SECURITY. Basic Attack Strategy of Stuxnet 0.5. rev .1. **Institute for Science and International Security**, fev. 2013. Disponível em: <https://isis-online.org/isis-reports/detail/basic-attack-strategy-of-stuxnet-0.5/. Acesso em: 24.06.2023.

IKENBERRY, John G. The Liberal International Order and Its Discontents. **Millennium: Journal of International Studies**, v. 38, n. 3, p. 509-521, 2010. Disponível em: https://collaborate.princeton.edu/en/publications/the-liberal-international-order-and-its-discontents. Acesso em: 27 mai. 2020.

INKSTER, Nigel. The Chinese Intelligence Agencies: Evolution and Empowerment in Cyberspace. *In:* LINDSAY, Jon; CHEUNG, Tai Ming; REVERON, Derek S. China and **Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain**. New York: Oxford University Press, 2015. p. 29-50.

IVAN, Gutterman. A Timeline of All Russia-Related Sanctions: A Detailed Look at All The Sanctions Levied Against Russia, and its countersanctions, since 2014. **Radio Free Europe Radio Liberty**, 2018. Disponível em: https://www.rferl.org/a/russia-sanctions-timeline/29477179.html. Acesso em: 08 mai. 2020.

JENKINS, Ryan. Is Stuxnet Physical? Does It Matter?. **Journal of Military Ethics**, v. 12, n. 1, 2013. Disponível em: https://www.tandfonline.com/doi/abs/10.1080/15027570.2013.782640. Acesso em: 11 dez. 2023.

JIJUN, Li. Military Strategic Thinking and Scientific Decision-Making. **China Military Science**, v. 1, p. 28-38, 2006.

JOLLEY, Jason. Article 2(4) and Cyber Warfare: How do Old Rules Control the Brave New World?. **International Law Research**, v. 2, n.1, 2013. Disponível em: http://dx.doi.org/10.5539/ilr.v2n1p1. Acesso em: 07 jan. 2024.

JOHNSON, Derek B. Chinese Hacker Group Targets Tech Supply Chain, Report Says. **FCW NEWS**, set, 2018. Disponível em: https://www.nextgov.com/cybersecurity/2018/09/chinese-hacker-group-targets-tech-supply-chain-report-says/246801/. Acesso em: 10 mar. 2021.

JOSAN, Andrei Cristina. Hybrid Wars in The Age of Asymmetric Conflicts. **Review of the Air Force Academy**, n. 1, v. 28, 2015. Disponível em: https://ns.afahc.ro/ro/revista/2015_1/49.pdf. Acesso em: 03 jan. 2024.

KALHA, Ranjit Singh. **India-China Boundary Issues: Quest for Settlement**. New Delhi: Pentagon Press. 2014. 324 p. E-book.

KAMINSKI, Mariusz Antoni. Operation 'Olympic Games.' Cyber-Sabotage as A Tool of American Intelligence Aimed at Counteracting the Development of Iran's Nuclear Programme. **Security & Defense Quarterly**, v.29, n. 2, 2020. Disponível em: https://securityanddefence.pl/Operation-Olympic-Games-nCyber-sabotage-as-a-tool-of-American-nintelligence-aimed,121974,0,2.html. Acesso em: 28 dez. 2023.

KAPUSÑAK, Jan. Covert Operations Attributed to Israel's Intelligence Services Against Iran's Nuclear Program. *In:* MAJER, Marian; ONDREJCSÁK, Róbert. **Panorama of Global Security Environment 2013**. Bratislava: Centre for European and North Atlantic Affairs, 2013. p. 375-386.

KATZ, M. Russian-Iranian Relations in the Ahmadinejad Era. **The Middle East Journal**, v.62, n.2, p. 202–216, 2008. Disponível em: https://www.researchgate.net/publication/233627770_Russian-Iranian_Relations_in_the_Ahmadinejad_Era. Acesso em: 29 abr. 2020.

KELLO, Lucas. The Meaning of the Cyber Revolution Perils to Theory and Statecraft. **International Security**, v. 38, n. 2, p. 7-40, 2013. Disponível em: https://www.jstor.org/stable/24480929. Acesso em: 12 mai. 2020.

KELLO, Lucas. **The Virtual Weapon and International Order**. New Haven: Yale University Press, 2017. 336 p. E-book.

KELSEY, Davenport. UN Security Council Resolution on Iran. **Arms Control Association**. 2022. Disponível em: <https://www.armscontrol.org/factsheets/Security-Council-Resolutions-on-Iran. Acesso em: 29 fev. 2022.

KREKEL, Bryan.; PATTON, Adams.; BAKOS, George. Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage. **Northrop Grumman Corp**, mar. 2012. Disponível em: Corporation, 2012. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-066.pdf. Acesso em: 18 abr. 2022.

KJENNERUD, Erik Reichborn.; CULLEN, Patrick J. What is Hybrid Warfare? Norwegian Institute of International Affaris, n. 1, p. 1-4, 2016. Disponível em: https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/2380867/NUPI_Policy_Brief_1_Reichborn_Kjennerud_Cullen.pdf. Acesso em: 22 abr. 2020.

KOVAL, Nikolay. Revolution Hacking. Cys Centrum LLc, *In:* GEERS, Kenneth. **Cyber War in Perspective: Russian Aggression against Ukraine.** . NATO Cooperative Cyber Defense Centre of Excellence. EST: Tallinn, 2015, p. 55-58.

KUMAR, Rajesh et al. APT Attacks on Industrial Control Systems: A Tale of Three Incidents. **International Journal of Critical Infrastructure Protection**, n. 37, p. 1-11, 2022. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S1874548222000129. Acesso em: 16 dez. 2023.

LANGNER, Ralph. Stuxnet: Dissecting a Cyberwarfare Weapon, **IEEE Security & Privacy**. v. 9, n. 3, p. 49–51, 2011. Disponível em: https://ieeexplore.ieee.org/document/5772960. Acesso em: 19 jun. 2023.

LAU, Stuart. How a Road on China and India's Border Led to the Two Powers Worst Stand-off in Decades. **South China Morning Post**, 2017. Disponível em: https://www.scmp.com/news/china/diplomacy-defence/article/2101578/how-road-china-and-indias-border-led-two-powers-worst. Acesso em: 11 abr. 2022.

LAVENDER, Darryl J. **China's Special Operations Forces Modernization, Professionalization and Regional Implications**. 2013. U.S. Army War College, Dissertação (Mestrado em Estudos Estratégicos), Department of Military Strategy, Planning, and Operations, United States Army War College, Philadelphia, 2013.

LIBICKI, Martin C. **Cyberdeterrence and Cyberwar**. 1.º ed. Santa Monica: RAND Corporation, 2009. 244 p. E-book.

LIBICKI, Martin C. The Cyber War That Wasn't. *In:* GEERS, Kenneth. **Cyber War in Perspective: Russian Aggression against Ukraine.** . NATO Cooperative Cyber Defense Centre of Excellence. EST: Tallinn, 2015. p. 49-55.

LIFF, Adam. Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War. **Journal of Strategic Studies**, v. 35, n. 3, p. 401–428, 2012. Disponível em: https://www.tandfonline.com/doi/abs/10.1080/01402390.2012.663252. Acesso em: 27 mar. 2023.

LILIENTHAL, Gary; AHMAD, Nehaluddin. Cyber-attack as Inevitable Kinetic War. **Computer Law & Security Review**, v. 31, n. 3, p. 390-400, 2015. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0267364915000564?via%3Dihub. Acesso em: 9 jun. 2023.

LIMNNÉL, Jarno. The Exploitation of Cyber Domain as Part of Warfare: Russo-Ukrainian War. **International Journal of Cyber-Security and Digital Forensics**, v. 4, n. 4, p. 521-532. 2015. Disponível em: https://sdiwc.net/digital-library/the-exploitation-of-cyber-domain-as-part-of-warfare-russoukrainian-war. Acesso em: 19 abr. 2020.

LINDSAY, Jon. Stuxnet and the Limits of Cyber Warfare. **Security Studies**, v. 22, n. 3, p. 365-404, 2013. Disponível em: https://www.tandfonline.com/doi/abs/10.1080/09636412.2013.816122. Acesso em: 28 mar. 2020.

LINDSAY, Jon. The impact of China on Cybersecurity: Fiction and Friction. **International Security**, v. 39, n. 3, p. 7-47, 2015. Disponível em: https://direct.mit.edu/isec/article/39/3/7/30310/The-Impact-of-China-on-Cybersecurity-Fiction-and. Acesso em: 28 mar. 2020.

LINDSAY, Jon.; CHEUNG, Tai Ming.; REVERON, Derek S. **China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain**. 1.º ed. New York: Oxford University Press, 2015. 406 p. E-book.

LIPOVSKY, R. Back in BlackEnergy: 2014 Targeted Attacks in Ukraine and Poland. Welivesecurity ESET, 2014. [Online] <Disponível em: https://www.welivesecurity.com/2014/09/22/back-in-blackenergy-2014>. Acesso em: 07.04.2020.

LI, Qi. Campaign Stratagem Application Under High-Tech Conditions. *In*: ZHANG, Xing.; ZHANG, Zhan Li. **Campaign Stratagems**. Beijing: National Defense Univeristy, 2002. p. 9-28.

LOOKINGLASS. Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare. **Lookingglass Cyber Threat Intelligence Group**, p. 3–51, 2015. Disponível em: https://www.ecirtam.net/autoblogs/autoblogs/lamaredugoffrblog_6aa4265372739b936776738439d4ddb430f5fa2e/media/88e3da25.Operation_Armageddon_FINAL.pdf. Acesso em: 12 abr. 2020.

MAHONEY, James. The Logic of Process Tracing Tests in the Social Sciences. **Sociological Methods & Research**, v. 41, n. 4, p. 570-597, 2012. Disponível em: https://journals.sagepub.com/doi/abs/10.1177/0049124112437709. Acesso em: 3 mar. 2020.

MALIARCHUK, Tamara; DANYK, Yuriy.; BRIGGS, Chad. Hybrid Warfare and Cyber Effects in Energy Infrastructure. **Connections QJ**, n. 1-2, p. 93-110, 2019. Disponível em: https://connections-qj.org/system/files/18.1.06_hybrid_cip.pdf. Acesso em: 07 jan. 2024.

MALIK, Mohan. **China and Indian: Great Power Rivals**. 1.º ed. Colorado: Lynne Rienner Publishers, 2011. 385 p. E-book.

MANDIANT. APT1 Exposing One of China's Cyber Espionage Units. Virginie, **Mandiant**, p. 1-76, 2013. Disponível em: https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf. Acesso em: 20 abr. 2022.

MANSOOR, Peter R. Hybrid Warfare in History. *In:* MURRAY, Williamson; MANSOOR, Peter R. **Hybrid Warfare: Fighting Complex Opponents From The Ancient World**. New York: Cambridge University Press, 2014. p. 1-10.

MATUSZAK, Slawomir. The Oligarqhic Democracy. The Influence of Business Groups on Ukrainian Politics. **Centre for Eastern Studies**, n. 42, 2012. E-book. Disponível em: https://www.osw.waw.pl/sites/default/files/prace_42_en_0.pdf. Acesso em: 12.08.2022.

MAURER, Tim. The Case for Cyberwarfare. **Foreign Policy**, 2011. Disponível em: https://foreignpolicy.com/2011/10/19/the-case-for-cyberwarfare/. Acesso em: 05 mai. 2020.

MAURER, Tim; JANZ, Scott. The Russia-Ukraine Conflict and Information Warfare in a Regional Context. **Swiss Federal Institute of Technology Zurich**, p. 1–4, out. 2014. Disponível em: https://www.files.ethz.ch/isn/187945/ISN_184345_en.pdf. Acesso em 18. abr. 2020.

MAURER, Tim. Cyber Proxies and the Crisis in Ukraine. New America. *In:* GEERS, Kenneth. **Cyber War in Perspective: Russian Aggression against Ukraine.** . NATO Cooperative Cyber Defense Centre of Excellence. EST: Tallinn, 2015, p. 79-86.

MAXWELL, Neville. **India's China War**. UK. ed. India: Natraj Publishers, 2013. 475 p. E-book.

MCCONNEL, M. Cyberwar is the New Atomic Age. New Perspectives Quarterly, vol. 26, n. 3, p. 72-77, 2009.

MCKUNE, Sarah. Foreign Hostile Forces: The Human Rights Dimension of China's Cyber Campaigns. *In:* LINDSAY, Jon.; CHEUNG, Tai Ming.; REVERON, Derek S. **China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain**. 1.º ed. New York: Oxford University Press, 2015. p. 260-293.

MEARSHEIMER, John J. Why the Ukraine Crisis is the West Fault. **Foreign Affairs**, v. 93, n. 5, p. 77-89, 2014. Disponível em: https://www.jstor.org/stable/24483306. Acesso em: 10 abr. 2020.

MEHRA, Parshotam. **Essays in Frontier History: India, China and the Disputed Border**. 1.º ed. New Delhi: Oxford University Press, 2007. 320 p. E-book.

MEYERS, Adam. Danger Close: FancyBear Tracking of Ukrainian Field Artillery Units. **Crowdstrike blog**, p. 1–6, 2016. Disponível em: https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/. Acesso em: 20 abr. 2020.

MIELNICZU, Fabiano. A Crise Ucraniana e Suas Implicações Para as Relações Internacionais. **Conjuntura Austral**, v. 5. n. 23, 2014. Disponível em: https://seer.ufrgs.br/index.php/ConjunturaAustral/article/view/46849. Acesso em: 13 mai. 2020.

MILEVSKI, Lukas. Stuxnet and Strategy: A Special Operation in Cyberspace?. **Joint Force Quarterly**, v. 63, n. 69, 2011. Disponível em: <https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-63/jfq-63_64-69_Milevski.pdf?ver=Jy0SW9E8UBbatlrmrw-egQ%3D%3D>. Acesso em: 20 jun. 2023.

MOREIRA, Bruna. The Sino-indian Border Dispute and Its Consequences for Security. **Mundorama**, p. 1-3, 2016. Disponível em: https://www.academia.edu/30973975/The_Sino_Indian_Border_Dispute_and_its_Consequences_for_Asian_Security. Acesso em: 19 mai. 2022.

MORGADE, Alba. EUA X Irã: O Que Originou a Rivalidade de Décadas Entre os Dois Países. **BBC NEWS Brasil**, 2020. Disponível em: https://www.bbc.com/portuguese/internacional-50983943. Acesso em: 21 jul. 2023.

MOROZOV, Evgeny. Cyber-Scare: The Exaggerated Fears Over Digital Warfare. **Boston Review**, jul/ago, 2009. Disponível em: https://www.bostonreview.net/articles/cyber-scare-evgeny-morozov/. Acesso em: 26 mar. 2020.

MORTON, Chris. Stuxnet, Flame e Duqu – the Olympic Games. *In*: HEALEY, Jason - **A Fierce Domain: Conflict in Cyberspace, 1986 to 2012**. USA: Cyber Conflicts Studies Association, 2013. p. 212-231.

NAKASHIMA, Ellen; WARRICK, Joby. Stuxnet Was the Work of US and Israel Specialists. **The Washington Post**, 2012. Disponível em: https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html. Acesso em: 29 jun. 2023.

NATIONAL CYBER POWER INDEX. Cyber Project. **Belfer Center For Science and International Affairs**, p. 1-66, 2022. Disponível em:

https://www.belfercenter.org/publication/national-cyber-power-index-2022. Acesso em: 07 jan. 2024.

NIU, Li.; JIANGZHOU, Li.; DEHUI, Xu. Planning and Application of Strategies of Information Operations in High-Tech Local War. **China Military Science**, n. 4, p. 115-122, 2000.

NOURIAN, Arash; MADNICK, Stuart. A Systems Theoretic Approach to The Security Threats in Cyber Physical Systems Applied to Stuxnet. **IEEE Transactions on Dependable and Secure Computing**, v. 15, n. 1, p.2-13, 2018. Disponível em: https://ieeexplore.ieee.org/document/7360168. Acesso em: 15 jun. 2023.

MURATBEKOVA, Albina. The Sino-Indian Border Issue as a Factor for The Development of Bilateral Relations. **Asian Journal of Comparative Politics**, v. 3. n.1, p. 3-12, 2018. Disponível em: https://journals.sagepub.com/doi/10.1177/2057891117690453. Acesso em: 24 abr. 2022.

NUNES, Daniela Pereira. Mikhail Gorbachev, The Human Factor, and The Implosion of The Soviet Union. **Universidade Autônoma de Lisboa**, v. 12, n.1, p. 265-271, 2021.
Disponível em: https://repositorio.ual.pt/bitstream/11144/5041/1/0%20EN-vol12-n1-note1.pdf. Acesso em: 22 jan. 2022.

NURKULOV, Nurshod. New Cyber Strategy of China and The Alterations in the Field. **Journal of Political Science & Public Affairs**, v. 5, n. 4, p.1-6, 2017. Disponível em: https://www.longdom.org/open-access-pdfs/new-cyber-strategy-of-china-and-the-alterations-in-the-field-2332-0761-1000310.pdf. Acesso em: 11 mai. 2022.

OLSZEWSKI, Boguslaw. Advanced Persistent Threats as a Manifestations of State Military Activity in Cyber Space. **Scientific Journal of the Military University of Land Forces**, v. 50, n. 3, p. 57-71, 2018. Disponível em: https://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-2d9af743-971c-43e1-9d7d-92e893a6a1a5. Acesso em: 28 abr. 2020.

PAVLIKOVA, Miroslava. Cybernet Network Between Russia and Ukraine in the Framework of Ukraine Conflict. **Defense and Strategy**, 2016. Disponível em: https://www.obranaastrategie.cz/filemanager/files/256890.pdf. Acesso em: 18 mai. 2020.

PIERSON, Paul. Increasing Returns, Path Dependence, and the Study of Politics. **American Political Science Review**, v. 94, n. 2, p. 251-267, 2000. Disponível em: https://www.jstor.org/stable/2586011. Acesso em: 28 mar. 2020.

POLLPETER, Kevin. Chinese Writing on Cyberwarfare and Coercion. *In:* LINDSAY, Jon.; CHEUNG, Tai Ming.; REVERON, Derek S. **China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain**. 1.º ed. New York: Oxford University Press, 2015. p. 138-162.

PONS, Silvio. **A Revolução Global: História do Comunismo Internacional 1917-1991**. 1.º ed. Rio de Janeiro: Contraponto editora, 2014.

QINGMIN, Dai. **On Integrating Network Warfare and Electronic Warfare**. **China Military Science**, v. 15, n. 2. 2002.

RECORDED FUTURE. Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3. **Recorded Future**, p. 1-13, 2017. Disponível em: https://www.recordedfuture.com/blog/chinese-mss-behind-apt. Acesso em: 27 mai 2022.

RECORDED FUTURE. 2021. China-lined Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions. **Recorded Future**. p. 1-20, 2021. Disponível em https://www.recordedfuture.com/blog/redecho-targeting-indian-power-sector>. Acesso em: 28 mai. 2022.

RECORDED FUTURE. Continued Targeting of Indian Power Grid Assets by Chinese State-Sponsored Activity Group. **Recorded Future**, p. 1-11, 2022. Disponível em: https://www.recordedfuture.com/blog/continued-targeting-of-indian-power-grid-assets. Acesso em: 29 mai. 2022.

REMPEL, Gerhard. Gorbachev and Perestroika. **Internet Archive WayBackMachine**, 2008. Disponível em: https://web.archive.org/web/20080828102933/http://mars.wnec.edu/~grempel/courses/wc2/lectures/gorrev.html. Acesso em: 19 abr. 2020.

REPÚBLICA POPULAR DA CHINA. **China's National Defense in 2008. Information Office of the State Council of PRC**. Beijing: Information Office of the State Council The Central People's Government of the People's Republic of China, 2009. Disponível em: https://programs.fas.org/ssp/nukes/2008DefenseWhitePaper_Jan2009.pdf. Acesso em: 22 mai. 2022.

REPÚBLICA POPULAR DA CHINA. **China's National Defense in 2010. Information Office of the State Council of PRC**. Beijing: Information Office of the State Council, 2011. Disponível em: https://www.gov.cn/jrzg/2011-03/31/content_1835289.htm. Acesso em: 23 mai. 2022.

REPÚBLICA POPULAR DA CHINA. **The Diversified Employment of China's Armed Forces** Beijing: Information Office of the State Council, 2013. Disponível: em: http://english.www.gov.cn/archive/white_paper/2014/08/23/content_281474982986506.htm. Acesso em: 27 mai. 2022.

REPÚBLICA POPULAR DA CHINA. **China's Military Strategy**. Beijing: Information Office of the State Council, 2015. Disponível em: http://eng.mod.gov.cn/xb/Publications/WhitePapers/4887928.html. Acesso em: 29 mai. 2022.

REPÚBLICA POPULAR DA CHINA. **China's National Defense in the New Era**. Beijing: Information Office of the State Council of PRC, 2019. Disponível em: https://english.www.gov.cn/archive/whitepaper/201907/24/content_WS5d3941ddc6d08408f502283d.html. Acesso em: 28 mai. 2022.

REUTERS. Chinese Hackers Target Indian Vaccine Makers SII, Bharat Biotech, Says Security Firm. **REUTERS**, 2021. Disponível em https://www.reuters.com/article/health-coronavirus-india-china-idINKCN2AT21O. Acesso em: 02 fev. 2022.

RID, Thomas. Cyber War Will Not Take Blace. **Journal of Strategic Studies**, v. 35, n. 1, p. 5-32, 2012. Disponível em: https://www.tandfonline.com/doi/abs/10.1080/01402390.2011.608939. Acesso em: 06 abr. 2020.

ROSENBAUM, Ron. Richard Clarke on Who Was Behind the Stuxnet Attack. **Smithsonian Magazine**, 2012. Disponível em: https://www.smithsonianmag.com/history/richard-clarke-on-who-was-behind-the-stuxnet-attack-160630516/. Acesso em: 22 jun. 2023.

ROWE, Neil. The Ethics of Cyberweapons in Warfare. **International Journal of Technoethics**, v. 1, n. 1, p. 20-31, 2010. Disponível em: https://www.igi-global.com/gateway/issue/38885. Acesso em: 27 jul. 2023.

SANGER, David. Obama Order Sped Up Wave of Cyberattacks Against Iran. **New York Times**, 2012. Disponível em: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html. Acesso em: 21 jun. 2023.

SCOTT, David. Sino-Indian Territorial Issues: The 'Razor's Edge'? *In*: PANT, Harash V. **The Rise of China: Implications for India**. India: Cambridge University Press, 2011. p. 197-220.

SCOTT, David. India's China Challenge: Foreign Policy Dilemmas Post-Galwan and Post-Covid. **The Journal of Indian and Asian Studies**, v. 2, n. 2, jul, 2021. Disponível em: https://www.worldscientific.com/doi/abs/10.1142/S2717541321400039. Acesso em 14 abr. 2022.

SEBESTYEN, Victor. The K.G.B.'s Bathhouse Plot. **The New York Times Opinion**, 2011. Disponível em: https://www.nytimes.com/2011/08/21/opinion/sunday/the-soviet-coup-that-failed.html. Acesso em: 20 mai 2020.

SHAKARIAN, Paulo. Stuxnet: Cyberwar Revolution in Military Affairs. **Small Wars Journal**, abr, 2011. Disponível em: https://apps.dtic.mil/sti/pdfs/ADA546439.pdf. Acesso em: 19 mai. 2020.

SHELDON, Robert.; MCREYNOLDS, Joe. Civil-Military Integration and Cybersecurity: A Study of China Information Warfare Militias. *In:* LINDSAY, Jon.; CHEUNG, Tai Ming.; REVERON, Derek S. **China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain**. 1.º ed. New York: Oxford University Press, 2015. p, 188-220.

SIMONS, Greg; DANYK, Yuriy; MALIARCHUK, Tamara. Hybrid War and Cyber-Attacks: Creating Legal and Operational Dilemmas. **Global Change, Peace & Security**, v. 32, n. 3, p. 1-6, 2020. Disponível em: https://www.tandfonline.com/doi/full/10.1080/14781158.2020.1732899. Acesso em: 05 jan. 2024.

SINGER, Peter W; ALLAN, Friedman. **Cybersecurity and Cyberwar: What Everyone Needs To Know**. 1.º ed. UK: Oxford University Press, 2014. 306 p. E-book.

STOKES, Mark A. The Chinese People's Liberation Army Computer Network Operations Infrastructure. *In:* LINDSAY, Jon.; CHEUNG, Tai Ming.; REVERON, Derek S. **China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain**. 1.º ed. New York: Oxford University Press, 2015. p. 163-187.

STOKES, Mark A.; LIN, Jenny.; HSIAO, Russel. The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure. **The Project 2049 Institute**, 2011. Disponível em: https://project2049.net/2011/11/11/the-chinese-peoples-liberation-army-signals-intelligence-and-cyber-reconnaissance-infrastructure/. Acesso em: 12 abr. 2022.

THE MILITARY BALANCE. The Annual Assessment of Global Military Capabilities and Defence Economics. **The International Institute For Strategic Studies**, 2022. Disponível em: https://www.iiss.org/publications/the-military-balance/the-military-balance-2022 . Acesso em: 07 jan. 2024.

THE NEW YORK TIMES. China Appears to Warn India: Push Too Hard and the Lights Could Go Out. **NYT News**, fev, 2021. Disponível em: https://www.nytimes.com/2021/02/28/us/politics/china-india-hacking-electricity.html. Acesso em: 04 mar. 2022.

THE PRINT. 4, 9 or 14? Even China 'Isn't Sure' How Many PLA Soldiers Died in Galwan Valley. **PRINT News**, mar, 2021. Disponível em: https://theprint.in/defence/4-9-or-14-even-china-isnt-sure-how-many-pla-soldiers-died-in-galwan-valley/613372/. Acesso em: 12 mar. 2022.

THE WASHINGTON FREE BEACON. Pentagon Links Chinese Cyber Security Firm to Beijin Spy Service. **WFB News**, nov, 2016. Disponível em: https://freebeacon.com/national-security/pentagon-links-chinese-cyber-security-firm-beijing-spy-service/. Acesso em 08.04.2021.

THOMAS, Timothy L. **China Military Strategy: Basic Concepts and Examples of Its Use**. USA: Foreign Military Studies Office, 2014. 350 p. E-book.

TSYGANKOV, Andrei P. **Russia's Foreign Police: Changes and Continuity in National Identity.** UK: Rowman & Littlefield Publishers, 2010. 308 p.

USAOC. The United States Army Special Operations Command. Little Green Men: A Prime on Modern Russian Unconventional Warfare Ukraine 2013-2014. **Johns Hopkins University Apllied Physics Laboratory**, p. 1–65. 2015. Disponível em: https://nsarchive.gwu.edu/document/16170-us-army-special-operations-command-little-green. Acesso em: 29 mai. 2020.

VISSENTINI, Paulo. O Golpe de Moscou de 19 de Agosto de 1991 e o Fim da URSS. **NERINT**, ago, 2021. Disponível em: https://www.ufrgs.br/nerint/o-golpe-de-moscou-de-19-de-agosto-de-1991-e-o-fim-da-urss/. Acesso em: 26 set 2021.

XUE GUOAN. Characteristics of China's Traditional Strategic Thought. **China Military Science,** n.3, p. 116-122, 2010.

ZETTER, Kim. How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History. **WIRED Security**, 2011. Disponível em: https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/. Acesso em: 13 mai. 2023.

ZEDONG, Mao. Problems of Strategy in China's Revolutionary War. **Marxists Org**, 1936. Disponível em: http://www.marxists.org/reference/archive/mao/selected-works/volume-1/mswv1_12.htm. Acesso em: 09 mar. 2022.

ZHANG, Hongzhou; LI, Mingjang. Sino-Indian Border Disputes. **Analysis ISPI**, n.181, 2013. Disponível em: https://www.ispionline.it/sites/default/files/pubblicazioni/analysis_181_2013.pdf. Acesso em: 19 abr. 2022.

ZHANG, Yu; SIHAI, Liu; CHENGXIAO, Xia. On Art of Controlling a War Situation in Informatized Warfare. **China Military Science**, n. 2, p. 24-31, 2010.

ZHENG, Fan; BAO, Ma. **The Theory of Military Strategy**. Beijing: National Defense University Publishing House, 2007. E-book.

ZHENG, Ye, From Cyberwarfare to Cybersecurity in the Asia-Pacific and Beyond. *In:* LINDSAY, Jon.; CHEUNG, Tai Ming.; REVERON, Derek S. **China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain**. 1.º ed. New York: Oxford University Press, 2015. p. 123-136.

WANQUAN, Chang; GUOHUA, Yu. PRC PLA Analysis of 20th Century Combat Theory. **Peoples Liberation Army Daily**, v. 5, 2000.

WALT, Stephen. M. Is the Cyber Threat Overblown? **Foreign Policy**, mar. 2010. Disponível em: https://foreignpolicy.com/2010/03/30/is-the-cyber-threat-overblown/. Acesso em: 29 abr. 2020.

WEBER, Valentin. Linking cyber strategy with grand strategy: the case of the United States. **Journal of Cyber Policy**, v. 3, n. 2, 2018. Disponível em: https://www.tandfonline.com/doi/full/10.1080/23738871.2018.1511741. Acesso em: 29 jun. 2023.

WEEDON, Jen. Beyond Cyber War: Russia´s Use of Strategic Cyber Espionage and Information Operations in Ukraine. *In:* GEERS, Kenneth. **Cyber War in Perspective: Russian Aggression against Ukraine.** . NATO Cooperative Cyber Defense Centre of Excellence. EST: Tallinn, 2015. p. 67-78.

WEISS, Moritz; JANKAUSKAS, Vytautas. Securing Cyberspace How States Design Governance Arrangements. **International Journal of Policy, Administration, and Institutions**, v. 32, n. 2, p. 259-275, 2019. Disponível em: https://onlinelibrary.wiley.com/doi/10.1111/gove.12368. Acesso em 25 abr. 2020.

WESTCOTT, Stephen. **The Intractable Sino-Indian Border Dispute: a theoretical and Historical Account**. 2007. 374 f. Tese (Doutorado em Filosofia) Philosophy Department, Murdoch University, Perth, 2017.

WITHER, James K. Hybrid Warfare Revisited: A Battle of ‘Buzzwords’. **Connections QJ**, n. 1, p. 7-27, 2023. Disponível em: https://connections-qj.org/article/hybrid-warfare-revisited-battle-buzzwords. Acesso em: 13 jan. 2024.