idn nação e defesa

TECNOLOGIA, CIBERNÉTICA E DEFESA

idn Instituto da Defesa Nacional

P.V.P. 8,50 €
Quadrimestral

Dezembro 2022
n.º 163

NAÇÃO E DEFESA

Diretora
Isabel Ferreira Nunes
Editor
Luís Cunha
Assistente Editorial
António Baranita

Conselho de Redação
Isabel Ferreira Nunes, Luís Cunha, Rui Garrido, Patrícia Daehnhardt, Pedro Seabra

Conselho Editorial Nacional
André Barrinha (Universidade de Bath), Ana Paula Brandão (Universidade do Minho), Ana Santos Pinto (FCSH, Universidade Nova de Lisboa), António Horta Fernandes (FCSH, Universidade Nova de Lisboa), António Paulo Duarte (Instituto da Defesa Nacional), Armando Marques Guedes (Faculdade de Direito, Universidade Nova de Lisboa), Bruno Cardoso Reis (ISCTE-IUL), Carlos Branco (IPRI), Daniel Pinéu (Universidade de Amesterdão), Francisco Proença Garcia (Universidade Católica Portuguesa), João Vieira Borges (Comissão Portuguesa de História Militar), José Luís Pinto Ramalho (Exército Português), José Manuel Freire Nogueira (Universidade Autónoma de Lisboa), Luís Leitão Tomé (Universidade Autónoma de Lisboa), Manuel Ennes Ferreira (ISEG), Maria do Céu Pinto (Universidade do Minho), Maria Francisca Saraiva (Instituto da Defesa Nacional e Instituto Superior de Ciências Sociais e Políticas, Universidade de Lisboa), Mendo Castro Henriques (Universidade Católica Portuguesa), Miguel Monjardino (Universidade Católica Portuguesa), Paulo Jorge Canelas de Castro (Universidade de Macau), Paulo Viegas Nunes (Academia Militar), Raquel Freire (Universidade de Coimbra), Sandra Balão (Instituto Superior de Ciências Sociais e Políticas, Universidade de Lisboa), Teresa Ferreira Rodrigues (FCSH, Universidade Nova de Lisboa), Vasco Rato (Universidade Lusíada), Vítor Rodrigues Viana (Exército Português).

Conselho Consultivo Nacional
Abel Cabral Couto (Exército Português), António Martins da Cruz (Universidade Lusíada), António Vitorino (Organização Internacional das Migrações), António Silva Ribeiro (Armada Portuguesa), Carlos Gaspar (IPRI), Celso Castro (Fundação Getúlio Vargas), João Salgueiro (Eurodefense), José Manuel Durão Barroso (Goldman Sachs International), Luís Valença Pinto (Universidade Autónoma de Lisboa), Luís Moita (Universidade Autónoma de Lisboa), Manuel Braga da Cruz (Universidade Católica Portuguesa), Maria Carrilho (ISCTE-IUL), Nuno Severiano Teixeira (FCSH, Universidade Nova de Lisboa).

Conselho Consultivo Internacional
Bertrand Badie (Sciences Po, Paris), Christopher Dandeker (King's College, London), Christopher Hill (University of Cambridge), George Modelski (University of Washington), Josef Joffé (Hoover Institution), Ken Booth (University of Aberystwyth), Lawrence Freedman (King's College, London), Robert Kennedy (US Army War College), Todd Sandler (University of Texas).

Editorial Board
André Barrinha (University of Bath), Ana Paula Brandão (University of Minho), Ana Santos Pinto (Faculty of Social and Human Sciences, Nova University of Lisbon), António Horta Fernandes (Faculty of Social and Human Sciences, Nova University of Lisbon), António Paulo Duarte (National Defence Institute), Armando Marques Guedes (Law Faculty, Nova University of Lisbon), Bruno Cardoso Reis (ISCTE-University Institute of Lisbon), Carlos Branco (Portuguese Institute of International Relations), Daniel Pinéu (University of Amsterdam), Francisco Proença Garcia (Portuguese Catholic University), João Vieira Borges (Portuguese Commission of Military History), José Luís Pinto Ramalho (Portuguese Army), José Manuel Freire Nogueira (Autónoma University), Luís Leitão Tomé (Autónoma University), Manuel Ennes Ferreira (Lisbon School of Economics and Management), Maria do Céu Pinto (University of Minho), Maria Francisca Saraiva (National Defence Institute and Institute of Social and Political Sciences), Mendo Castro Henriques (Portuguese Catholic University), Miguel Monjardino (Portuguese Catholic University), Paulo Jorge Canelas de Castro (University of Macau), Paulo Viegas Nunes (Military Academy), Raquel Freire (University of Coimbra), Sandra Balão (Institute of Social and Political Sciences), Teresa Ferreira Rodrigues (Faculty of Social Sciences, Nova University of Lisbon), Vasco Rato (Lusíada University), Vítor Rodrigues Viana (Portuguese Army).

National Advisory Board
Abel Cabral Couto (Portuguese Army), António Martins da Cruz (Lusíada University), António Vitorino (International Organization for Migration), António Silva Ribeiro (Portuguese Navy), Carlos Gaspar (Portuguese Institute of International Relations), Celso Castro (Foundation Getúlio Vargas), João Salgueiro (Eurodefense Portugal), José Manuel Durão Barroso (Goldman Sachs International), Luís Valença Pinto (Autónoma University), Luís Moita (Autónoma University), Manuel Braga da Cruz (Portuguese Catholic University), Maria Carrilho (ISCTE-University Institute of Lisbon), Nuno Severiano Teixeira (Faculty of Social and Human Sciences, Nova University of Lisbon).

International Advisory Board
Bertrand Badie (Sciences Po, France), Christopher Dandeker (King's College, UK), Christopher Hill (University of Cambridge, UK), George Modelski (University of Washington, USA), Josef Joffé (Hoover Institution, USA), Ken Booth (University of Aberystwyth, UK), Lawrence Freedman (King's College, UK), Robert Kennedy (US Army War College, USA), Todd Sandler (University of Texas, USA).

Capa
Nuno Fonseca/nfdesign

Normas de Colaboração
Consultar final da revista

Propriedade, Edição e Sede da Redação
Instituto da Defesa Nacional
Calçada das Necessidades, 5, 1399-017 Lisboa
NIPC: 600014002
Tel.: 21 392 46 00 Fax.: 21 392 46 58 E-mail: idn.publicacoes@defesa.pt www.idn.gov.pt

Pré-Impressão, Impressão e Acabamento
EUROPRESS – Indústria Gráfica
Rua João Saraiva, 10-A – 1700-249 Lisboa – Portugal
Tel.: 218 444 340 Fax.: 218 492 061 E-mail: geral@europress.pt www.europress.pt

Direitos de Autor (c) 2022 Nação e Defesa | Copyright (c) 2022 Nação e Defesa

Esta publicação está licenciada sob a Licença Creative Commons Atribuição 4.0 Internacional. Para ver uma cópia desta licença, visite http://creativecommons.org/licenses/by/4.0/
This publication is licensed under the Creative Commons Attribution 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by/4.0/

ISSN 0870-757X Publicação Eletrónica ISSN 2183-9662
Depósito Legal 54 801/92
Tiragem 400 exemplares
Anotado na ERC Registada na Latindex – Sistema Regional de Informação em Linha para Revistas Científicas da América Latina, Caraíbas, Espanha e Portugal; MIAR, RedAlyC e JSTOR.
Disponível no RCAAP – Repositório Científico de Acesso Aberto de Portugal

As opiniões livremente expressas nas publicações do Instituto da Defesa Nacional vinculam apenas os seus autores, não podendo ser vistas como refletindo uma posição oficial do Instituto da Defesa Nacional ou do Ministério da Defesa Nacional de Portugal.

Este número temático da *Nação e Defesa* analisa os novos desafios tecnológicos trazidos pela exploração do espaço sideral e cibernético no campo da defesa.

Trata-se de um projeto realizado em cooperação com académicos brasileiros das áreas de segurança e defesa de instituições de ensino superior, civis e militares, selecionados pelo Programa de Apoio ao Ensino e à Pesquisa Científica em Defesa Nacional do Ministério da Defesa do Brasil com o apoio de várias universidades daquele país.

O primeiro artigo, da autoria de Ciro Telles e Gills Villar-Lopes analisa o espaço exterior como domínio de condução da guerra e proteção dos ativos espaciais, numa perspetiva multiplicadora do poder militar. Os autores consideram que algumas forças armadas incorporam já os ativos espaciais nas suas estratégias e doutrinas, analisando o seu impacto.

O uso do ciberespaço como ativo estratégico no conflito sino-indiano de 2020-2021, na perspetiva da China, é o tema do artigo assinado por Fernando Henrique Casalunga, Marcos Aurélio Guedes de Oliveira e Eduardo Munhoz Svartman. Os autores consideram que o domínio do ciberespaço amplia a assimetria de poder entre adversários regionais.

Por sua vez, Gabriel Olegário e Graciela de Conti Pagliari analisam as implicações político-estratégicas da guerra híbrida na Chéquia, evidenciando a tendência para securitizar as ameaças híbridas, em virtude da guerra de (des)informação.

Ainda no campo da cibernética, Jéssica Grassi e Danielle Jacon Ayres Pinto analisam o sistema de defesa cibernética do Brasil a partir da análise da dinâmica civil-militar existente neste setor. A este propósito consideram existir uma baixa participação e controle civil das Forças Armadas e dificuldades em estabelecer um diálogo efetivo entre civis e militares.

No âmbito da mesma temática, Marcelo Malagutti reflete sobre os obstáculos para um consenso sobre normas internacionais que regulem as ciberofensas patrocinadas por Estados. Em causa está a regulação do comportamento cibernético dos Estados. A análise engloba a aplicabilidade das regras atuais de conflitos armados ao contexto cibernético.

Na seção "Extra Dossiê", destaque para o artigo assinado por Bruno Garcês e Sónia Morgado sobre a ação da Polícia de Segurança Pública (PSP) em ambiente de pandemia. Os autores analisam a ação diferenciada da PSP em situação de estado de exceção e as dinâmicas geradas entre aquela força e a ação participativa e cívica dos cidadãos.

Uma última nota para referir que a direção editorial da revista *Nação e Defesa* decidiu, por uma questão de coerência e em respeito pela redação original, manter a grafia em vigor no Brasil para os artigos assinados pelos autores brasileiros.

Isabel Ferreira Nunes

Tecnologia, Cibernética e Defesa

Espaço Exterior como Domínio da Guerra e a Proteção dos Ativos Espaciais

Ciro Telles

Bacharel em Ciências Aeronáuticas e em Administração pela Academia da Força Aérea Brasileira (AFA). Especialista em Relações Internacionais pela Universidade Federal do Rio Grande do Sul (UFRGS) e Mestrando em Ciências Aeroespaciais pelo Programa de Pós-Graduação em Ciências Aeroespaciais (PPGCA) da Universidade da Força Aérea (UNIFA).

Gills Villar-Lopes

Doutor em Ciência Política pela Universidade Federal de Pernambuco (UFPE). Atualmente, é professor de Relações Internacionais e Coordenador do PPGCA-UNIFA e e Pesquisador da RedeCTIDC (Pró-Defesa IV/CAPES).

Resumo

Os sistemas e serviços baseados no espaço exterior têm ganhado destaque ao revolucionarem diferentes áreas e representarem fator multiplicador do poder militar. Não à toa, algumas forças armadas não só incorporaram ativos espaciais em suas estratégias, como também criaram organizações e doutrinas militares voltadas exclusivamente para esse domínio. Nesse sentido, o objetivo do presente artigo consiste em debater a importância do espaço para o poder militar em específico para o Brasil, e a consequente necessidade de proteção dos ativos espaciais. O recorte temporal se delimita de 1991 até 2022, compreendendo a chamada Segunda Era Espacial. O marco teórico parte dos conceitos de Paradigmas Estruturais, de Colin Gray, e Comando do Espaço, de Everett Dolman e John Klein, e na teoria dos Cinco Anéis, de John Warden. São trazidos exemplos que ilustram como grandes potências têm utilizado seu poder espacial para atingir objetivos políticos, em que pese a atuação de Estados Unidos e China nessa seara. Ao final, sugerem-se, à luz das análises conceituais e da casuística, algumas iniciativas para a defesa espacial brasileira, visando à garantia do Comando do Espaço.

Palavras-chave: Brasil; Comando do Espaço; Poder Aeroespacial.

Abstract
Outer Space as a Domain of War and the Protection of Space Assets

Outer space-based systems and services have gained prominence by revolutionizing different areas and representing a multiplier factor for military power. No wonder, some armed forces not only incorporated space assets into their strategies, but also created military organizations and doctrines focused exclusively on this domain. In this sense, the objective of this article is to discuss the importance of space for military power, specifically for Brazil, and the consequent need to protect space assets. The time frame is delimited from 1991 to 2022, comprising the so-called Second Space Age. The theoretical framework is based on the concepts of Structural Paradigms, by Colin Gray, and Space Command, by Everett Dolman and John Klein, and on the theory of the Five Rings, by John Warden. Examples are presented that illustrate how great powers have used their space power to achieve political goals, despite the performance of the United States and China in this area. At the end, we suggest, in the light of the conceptual analysis and the casuistry, some initiatives for the Brazilian space defense, aiming to guarantee the Space Command.

Keywords*: Brazil; Space Command; Aerospace Power.*

Artigo recebido: 25.07.2022
Aprovado: 11.11.2022
https://doi.org/10.47906/ND2022.163.01

Introdução

Durante as últimas décadas, sistemas baseados ou auxiliados por tecnologia espacial têm revolucionado diversas áreas, como ciência e tecnologia (C&T), economia e telecomunicações, além de representarem verdadeiros fatores multiplicadores de força para o poder militar. É nesse contexto que o chamado Comando do Espaço, a ser tratado aqui, passa a representar um paradigma estratégico na forma de planejar e conduzir operações militares voltadas ou baseadas em ativos espaciais, constituindo-se, assim, como condicionante para o desenvolvimento e a soberania dos Estados no século XXI, a exemplo do que se vê na guerra russo-ucraniana ou em testes isolados conduzidos pelas grandes potências da atualidade.

Dada tal importância dos ativos espaciais, bem como a consequente revolução informacional, é quase certo que os serviços baseados na órbita terrestre venham a impactar o equilíbrio de poder nas relações internacionais nos anos seguintes e que tal infraestrutura passe a constituir alvo estratégico nas guerras do futuro. A partir dessas considerações, o presente trabalho gira em torno da assimilação do espaço como um novo domínio da guerra e seus impactos estratégicos para o Brasil.

Para tanto, estabelece-se como objetivo geral contextualizar o papel do setor espacial para o poder militar, tendo em vista que a compreensão da importância do espaço e da necessidade de projetar sua exploração auxilia os Estados na busca por soberania em meio à multidimensionalidade como tendências das guerras do futuro. Entendemos que, devido à acensão do espaço como um dos três setores estratégicos para o Brasil em 2008, esta é uma preocupação que norteia estrategistas – civis e militares – deste país.

Como marco teórico para iluminar as análises aqui desenroladas, utilizam-se os conceitos de Paradigmas Estruturais, de Gray (1996), que aborda a evolução da guerra em virtude dos avanços tecnológicos, e de Comando do Espaço, desenvolvido pelos pensadores do poder espacial Dolman (2002) e Klein (2006). Paralelamente, alicerça-se também na ideia de Paralisia Estratégica e na teoria dos Cinco Anéis, de Warden (1988), que auxiliam na compreensão da relevância estratégica dos ativos espaciais em um cenário de beligerância.

Em termos metodológicos, o trabalho tem caráter exploratório e documental e utiliza como fontes documentos oficiais e literatura especializada em Estudos Estratégicos e Poder Aeroespacial. O recorte temporal se inicia em 1991, que compreende o início da chamada Segunda Era Espacial[1] (CEPIK, 2011) com a Guerra do Golfo, e vai até o ano da escritura deste artigo, ou seja, 2022, que marca o uso, sem prece-

1 Período marcado pela ampliação da exploração do espaço por outros atores que não apenas Estados Unidos e Rússia e maior protagonismo dos ativos espaciais para os setores civis e militares.

dentes de ativos espaciais e baseados no espaço no contexto da Guerra Russo-ucraniana e a consolidação do chamado *New Space*, por empresas privadas como a Space-X.

De modo a compreender, especificamente, como o Brasil pode melhor garantir a proteção de seus ativos espaciais, compara-se o caso brasileiro com o da China, país escolhido em virtude do enfoque paradigmático dado à garantia de seu Comando do Espaço. Entende-se que esta é, pois, uma alternativa para o Brasil e para países com características semelhantes.

O texto está dividido em quatro seções principais. Inicialmente, expõe-se a influência dos meios espaciais para o poder militar, como abordado por Gray (1996) e atestado nos conflitos do Kosovo em 1999 e Iraque em 2003. Na segunda seção, destaca-se a importância estratégica dos ativos espaciais à luz da ideia de Paralisia Estratégica e na teoria dos Cinco Anéis, de Warden (1988), para, na seção seguinte, abordar o conceito de Comando do Espaço e as potenciais ameaças aos ativos espaciais na atualidade. A quarta seção aborda os *cases* chinês, como exemplo de esforço no sentido de assegurar o Comando do Espaço, e brasileiro, para, por fim tecermos as considerações finais.

1. O Uso do Espaço e sua Importância para o Poder Militar

De acordo com Klein (2006), as atividades espaciais de um país podem ser divididas em quatro categorias: civil, comercial, Inteligência e militar. Dentre os mais de três mil satélites colocados em órbita, existem equipamentos destinados às mais diferentes finalidades, com o intento comum de prover suporte à vida na Terra. Desde as telecomunicações, passando pelas transações financeiras, previsão do tempo e de catástrofes naturais, além da exploração científica, a humanidade se encontra, na atualidade, dependente dos meios satelitais para as mais diversas atividades ordinárias e extraordinárias.

Em relação ao uso comercial do espaço, por exemplo, ressalta-se que a natureza dual das distintas tarefas desempenhadas pelos satélites – tais como telecomunicações, geolocalização, sensoriamento remoto, agricultura e defesa nacional – propiciou o desenvolvimento do chamado *New Space*, *i.e.*, maior protagonismo do setor privado nas atividades espaciais, a exemplo da SpaceX e da Virgin Galactic. Esse novo modelo de exploração espacial proporciona oportunidades tanto para a cadeia produtiva diretamente ligada ao ramo quanto para outras áreas, como economia, saúde, mineração e meio ambiente. Todavia, devido a seu amplo leque de possibilidades, também serve para fins militares – e, portanto, políticos –, tal como ocorreu com a utilização da constelação Starlink, da SpaceX, no atual conflito do leste europeu (DUFFY, 2022).

A facilidade e economicidade com que cargas úteis[2] podem, atualmente, ser lançadas ao espaço fizeram da exploração espacial um negócio consideravelmente rentável, desde a concepção de satélites passando pelo lançamento em si. De acordo com a Satellite Industry Association (SIA), em seu último "Relatório Anual sobre a Indústria de Satélites", o faturamento do setor em 2021 foi de mais de US$ 386 bilhões, sendo que a projeção é ultrapassar US$ 1 trilhão em 2040 (SIA, 2022).

Assim, o uso comercial do espaço, em transbordamento, possui potencial de impulsionar a indústria tecnológica e promover pesquisa e desenvolvimento (P&D) nessa área sensível, vindo a impactar positivamente diversos outros setores civis e militares. Nesse sentido, o caso norte-americano se revela um exemplo emblemático de como a corrida espacial desempenhou papel preponderante para seu avançado parque industrial, em que os investimentos em infraestrutura e capacitação realizados pela National Aeronautics and Space Administration (NASA), nas décadas de 1950 e 1960, contribuíram, sobremaneira, para consolidar o setor aeroespacial.

No que tange ao poder militar, cabe destacar que as mudanças proporcionadas pelos ativos espaciais não representam a única transformação na forma de conduzir as guerras atuais, mas a última e mais significativa de uma série de verdadeiros paradigmas estruturais (GRAY, 1996) que envolvem o fenômeno político da guerra. Tal marco, trazido pelo estrategista britânico Colin Gray, se revestiu de maior relevância durante a participação norte-americana na Guerra do Golfo de 1991. Já a partir das campanhas no Kosovo em 1999 e no Iraque em 2003, constata-se a consolidação do papel da interface espacial no combate moderno: enquanto os EUA utilizaram 52 satélites durante o primeiro conflito do Golfo, na segunda guerra do Iraque em 2003 foi empregado pelo menos o dobro desse número no apoio às forças da coalizão. Nesse sentido, estima-se que os norte-americanos tenham obtido 95% de suas informações de Inteligência, vigilância e reconhecimento (IVR) provenientes de satélites e, da mesma forma, 90% das comunicações militares e 100% da navegação (CHENG, 2011). Assim, similarmente à importância que o poder aéreo passou a representar para o combate ao longo do século XX, o poder espacial também parece constituir, atualmente, fator essencial para o emprego dos demais componentes do poder militar.

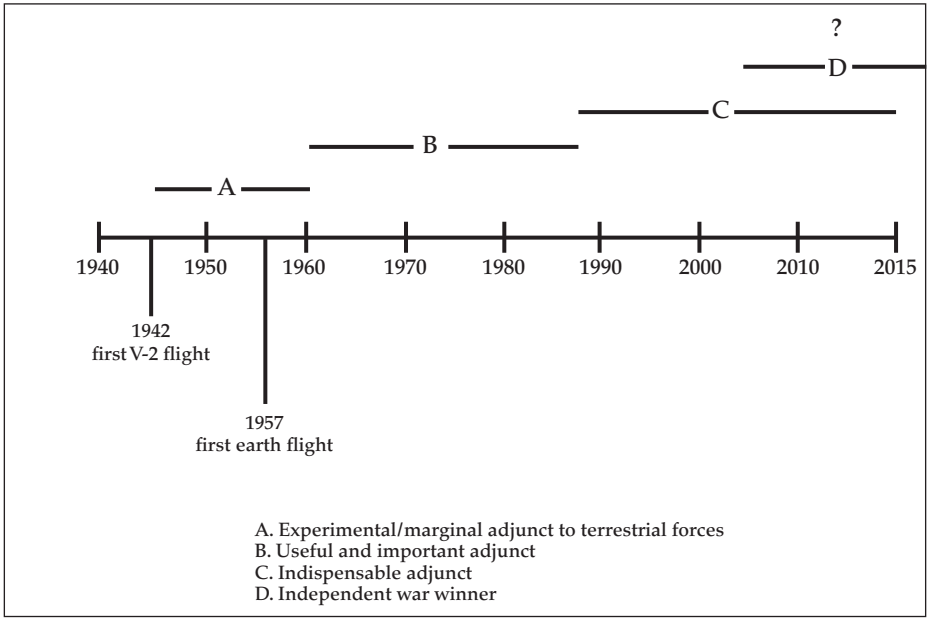
Neste ponto, faz-se necessário diferenciar dois conceitos que têm ganhado força e adeptos na literatura revisada: militarização e armamentização do espaço. Por um lado, a primeira resulta da colocação, em órbita, de satélites de IVR (HENRY, 2008), cuja tecnologia de coleta de informações contribui estrategicamente para o atingimento dos interesses dos Estados que a detêm e, da mesma maneira, proporcionam apoio logístico às tropas no teatro de operações (TO). Por outro lado, a armamentização caracteriza o domínio espacial como um ambiente de combate, seja por meio

2 Carga útil é a parte de um veículo espacial que se destina a cumprir os objetivos da missão.

do lançamento, à órbita terrestre, de armas – ou dispositivos que possam vir a se tornar uma –, seja por sua utilização para infringir danos a oponentes, com uso de armas não cinéticas, sabotagem de satélites via *malware*, dentre outras possibilidades.

Nesse contexto, observa-se que, de acordo com a taxonomia dos Paradigmas Estruturais proposta por Gray (1996), o poder espacial deixa de possuir o caráter de Componente Marginal, no período de 1942 a 1957 – época de seu surgimento, com o primeiro voo do V-2 nazista e o lançamento do Sputnik soviético –, e passa a representar um Componente Indispensável, a partir da Guerra do Golfo de 1991, constituindo-se atualmente em um verdadeiro *War Winner*, conforme se mostra na Figura 1.

Figura 1
Utilidade Estratégica do Poder Espacial



Fonte: GRAY (1996).

Conforme exposto, e tendo em vista a imprescindibilidade dos meios espaciais para o efetivo emprego das Forças Armadas, de acordo com Gray (1996), é lícito inferir que o espaço exterior poderá se consolidar como mais um domínio da guerra em um futuro próximo, algo que, por exemplo, o também clausewitziano Lonsdale (1999) já toma como realidade.

2. A Importância Estratégica do Domínio Espacial

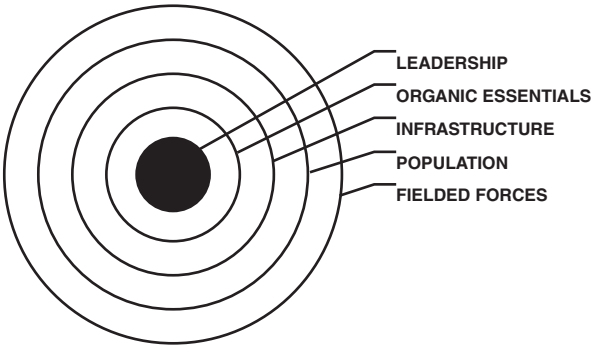
Ainda no sentido de elucidar a importância dos meios espaciais para o emprego do poder militar, é válida a análise de tal fato à luz da ideia de Paralisia Estratégica e da teoria dos Cinco Anéis, de John Warden (1988), as quais estão intimamente relacionadas entre si.

Para a devida compreensão, remete-se a Sun Tzu, que prega em "A Arte da Guerra" que os verdadeiros vencedores das batalhas são aqueles exércitos capazes de superar o oponente sem a necessidade de lutar. Com isso, Sun Tzu afirma que uma rápida incapacitação do inimigo é essencial. Hoje, como se vê nos conflitos na Ucrânia e na Síria, por exemplo, o uso de *drones* remotamente pilotados – em alguns casos, via satélite – tem sido uma estratégia que materializa o pensamento milenar do general chinês.

Após a Primeira Guerra Mundial, John Frederick Charles Fuller (1878-1966) e Basil H. Liddell Hart (1895-1970) foram os primeiros estrategistas modernos a se dedicar ao conceito de Paralisia Estratégica. Em 1919, Fuller desenvolveu o que talvez tenha sido o primeiro plano operacional moderno com o propósito de paralisar o inimigo. Além disso, o estudioso defendia que a maneira mais eficiente de se destruir a força militar oponente era por meio da guerra psicológica. Similarmente, Liddell Hart assumia que a maneira mais potente e econômica de se combater era paralisar o oponente por meio da incapacitação em vez de aniquilá-lo (FADOK, 1995). Nesse mesmo sentido, o Coronel John Warden, um dos estrategistas responsáveis pelo planejamento das campanhas norte-americanas na Guerra do Golfo em 1991, concebeu o modelo dos cinco anéis, o qual foi utilizado contra as forças iraquianas durante o mencionado conflito.

De acordo com Warden (2005), a guerra moderna não deve mais visar à destruição total do oponente, mas, sim, fazer com que o oponente ceda aos objetivos da força atacante, de modo a atingir seus objetivos políticos com os menores custos e esforços possíveis. Para tanto, os planejamentos devem buscar o ataque aos chamados Centros de Gravidade (CG) do inimigo, que são seus pontos mais vulneráveis e que, quando destruídos, podem levar à sua paralisia. A Figura 2 ilustra a teoria de Warden, com os cinco anéis concêntricos, organizados de dentro para fora da seguinte maneira: liderança, sistemas orgânicos essenciais, infraestrutura, população e forças militares no terreno (WARDEN, 1995).

Figura 2
Os Cinco Anéis, de Warden



Fonte: FADOK (1995).

Ainda em consonância com o autor, os anéis que compõem o sistema são interdependentes entre si, ou seja, cada um possui uma função e mantém certo grau de relacionamento com os demais (WARDEN, 1995). Em sua teoria, Warden realiza uma analogia com o corpo humano, comparando o anel mais interno com nosso cérebro, capaz de controlar as demais partes do corpo, sendo assim a parte mais crítica do sistema. Tal anel consiste na "Liderança", as pessoas responsáveis pelas tomadas de decisões, capazes de definir os rumos de uma guerra. Dessa forma, o domínio das informações e das comunicações, fatores fundamentais para os decisores, representa condição *sine qua non* para o sucesso em combate. É especialmente neste ponto em que o setor espacial pode se transformar de uma variável interveniente para uma independente – nossa hipótese aqui levantada – que possa explicar ou conduzir a vitória nas guerras hodiernas e do futuro.

Como já exposto, a exploração do espaço tem jogado um papel cada vez maior para a humanidade, ao longo do século XXI, e, assim, governos, empresas e até mesmo indivíduos se tornaram dependentes de satélites e das tecnologias de informação e comunicação (TIC) para as mais diversas atividades, incluindo, do ponto de vista estratégico, o suporte a infraestruturas críticas nacionais e binacionais – a exemplo do que ocorre com Brasil-Paraguai e EUA-Canadá – e, em especial, ao emprego do poder militar, o que, de acordo com a teoria dos Cinco Anéis, acaba por transformar as estruturas aeroespaciais – sejam elas em solo, sejam em órbita – em um complexo Centro de Gravidade para qualquer Estado.

Em face de tamanha importância da infraestrutura espacial, as principais potências mundiais têm buscado assegurar sua proteção por meio do chamado Comando do Espaço, uma extrapolação oriunda da estratégia naval e que é abordada na próxima seção.

3. Do Comando do Espaço e suas Ameaças

Costumeiramente interpretado de maneiras distintas na literatura revisada, o Comando do Espaço já foi abordado por Dolman (2002) como uma condição associada à ideia de controle militar do meio espacial e de negação de seu uso por outros atores. Contudo, tal conceito, a nosso ver, pode ser definido de forma mais completa, a exemplo do seguinte:

> [...] capacidade de um país garantir por meios próprios o seu acesso e uso do espaço em tempos de paz e de guerra, bem como a habilidade de impedir um adversário de lhe negar tal proveito. Isto é, a capacidade que um país tem de assegurar o acesso às suas próprias linhas de comunicação espaciais para propósitos civis, comerciais, militares e de inteligência (CEPIK, 2011, p. 2).

De modo semelhante, Klein (2006) argumenta que o Comando do Espaço pode ser exercido de três formas distintas, simultâneas e complementares entre si, a saber: *presença, coerção* e *força*, as quais contariam com a participação direta ou indireta de outros setores, como econômico e científico-tecnológico. Primeiro, o Comando do Espaço que é garantido pela *presença* mantém ativos espaciais na órbita terrestre em número suficiente para que determinado Estado seja minimamente reconhecido no cenário internacional como uma potência espacial. Podendo ser alcançado em tempos de paz e pelo desenvolvimento tecnológico, tal Comando garantiria, a seus detentores, a influência necessária em tratados e fóruns internacionais – como o Committee on the Peaceful Uses of Outer Space (COPUOS) das Nações Unidas –, influindo, portanto, na agenda da política internacional. Por sua vez, o Comando do Espaço via *coerção* envolve o uso direto ou indireto da força, visando impedir que outros atores tenham acesso ao espaço ou influenciando mudanças de posicionamento no tocante a contendas ou tratados nessa área. Finalmente, o exercício do Comando pela *força* implica a constituição de verdadeiras capacidades militares e o emprego de ações hostis contra a infraestrutura espacial, meios, ativos, rotas, posições, usos e aplicações derivadas da presença no espaço por outros Estados.

Para países cujos programas espaciais ainda são incipientes, como o Brasil, Klein (2006) afirma que, apesar de uma vitória em ambiente espacial ser pouco provável, a contestação do Comando do Espaço ainda seria possível por meio de ações não militares e, até mesmo, militares, via diplomacia, economia e Inteligência.

Considerando-se a teoria dos Cinco Anéis, de Warden, e a busca do Comando do Espaço pelos atuais *players* espaciais, por meio da coerção ou da força, pode-se inferir que a infraestrutura aeroespacial dos países passa a representar alvo prioritário de ameaças das mais distintas naturezas. Consoante Nguyen (2015, p. 60, tradução nossa), "indivíduos, grupos e atores patrocinados pelo Estado – assim

como estes mesmos – encontraram maneiras de manipular ou invadir esses sistemas para promover seus próprios objetivos", fato este que já se mostra como uma tendência nos últimos exercícios simulados por grandes potências espaciais como a China (VALDUGA, 2022).

Desde que conectados à rede mundial de computadores – ou a ela se conectem a partir de redes locais (LAN) –, satélites também são passíveis de ataques cibernéticos, bem como as próprias estruturas na Terra, as quais têm sido alvos recorrentes de ações hostis, em detrimento de objetivos essencialmente políticos, tendo em vista os efeitos estratégicos que uma eventual paralisia causa a qualquer país (DUTRA, 2007) interconectado e altamente globalizado, como é o caso do Brasil.

Dessa forma, é muito provável que, no curto e médio prazos, o espaço exterior se transforme em um campo de batalhas (STEINBERG, 2012) em que não apenas armas de efeito cinético – como as antissatelitais (ASAT) –, mas também ameaças cibernéticas sejam a nova tônica pelo Controle do Espaço.

Dentre as ameaças antissatélite de que se tem conhecimento, estão mísseis balísticos que podem ser lançados desde a Terra, cuja tecnologia já está à disposição de países como EUA há, pelo menos, seis décadas. Em 1962, durante um teste nuclear conduzido no Pacífico Sul, uma ogiva foi detonada (VALDUGA, 2022) a aproximadamente 400 km de altura, resultando em pulsos eletromagnéticos que destruíram três satélites norte-americanos fora de operação.

As capacidades ASAT não se limitam apenas à destruição de satélites por meios cinéticos e cibernéticos, como mencionado. A prática de "jameamento", por meio de uma sobrecarga de sinais enviados aos satélites alvos também está sendo desenvolvida pelas grandes potências espaciais, assim como canhões *laser,* que também podem ser disparados desde a superfície terrestre (STEINBERG, 2012).

Nesse contexto, o número crescente de atentados contra infraestruturas críticas e o estágio avançado de desenvolvimento de tecnologias ASAT têm preocupado diversos países, no que promovem o aperfeiçoamento de planos de proteção e de contingência relacionados ao setor espacial. A exemplo disso, recentemente, Reino Unido, França e Alemanha criaram Comandos Militares com o objetivo específico de proteger seus ativos espaciais. De acordo com a ministra da defesa alemã, à época da criação do Comando Espacial daquele país em julho de 2021, Annegret Kramp-Karrenbauer, "o espaço se tornou uma infraestrutura crítica que precisamos proteger" (SPUTNIK, 2021).

Já a maior potência espacial da atualidade deu um passo ainda maior, com a criação de uma força singular dedicada à defesa espacial: a US Space Force, cujas missões oficiais são: fornecer liberdade de operação para os Estados Unidos no espaço; proporcionar operações espaciais rápidas e sustentadas; e, por fim, proteger os interesses americanos no espaço, dissuadindo a agressão no espaço e conduzindo operações naquele ambiente.

Por sua vez, a China, que também dispõe de um robusto programa espacial, adotou alternativa distinta visando à defesa de sua infraestrutura espacial, com a criação de uma nova força singular, a exemplo dos EUA, porém com um enfoque mixto no domínio espacial e cibernético. Ademais, tal país consiste em um *case* em que a manutenção do Comando do Espaço pode ser exercida por meio das três formas – presença, coerção e força – e um exemplo de como tal conceito pode ser utilizado para o atingimento de objetivos nacionais, conforme debatido adiante.

4. Os Casos Chinês e Brasileiro

O programa espacial chinês, desde seu início em 1956, se guia pela influência e ameaça de fatores externos (CEPIK, 2011), como a possibilidade do uso de armas nucleares norte-americanas em meio à dissuasão mútua assegurada (MAD), a análise da campanha na Guerra do Golfo, com seus impactos sobre o poder militar e toda a revolução tecnológica proporcionada pelo advento dos meios satelitais. Desta feita, após identificar a importância do Comando do Espaço, a China tem promovido o franco desenvolvimento de seu programa espacial, que, após décadas de vultosos investimentos em P&D, se aproxima dos dois países mais avançados na área: EUA e Rússia.

Da maneira que é atualmente conduzido, o programa espacial chinês, no âmbito de sua Grande Estratégia, poderia ser resumido em três palavras: geografia, legitimidade e economia (CARLSON, 2020). Geograficamente, o espaço consiste, para os chineses, em uma área que pode ser conquistada e controlada. Em segundo lugar, a China encara o espaço como um fórum por meio do qual poderia consolidar sua liderança e o protagonismo internacional de seu atual regime. Por fim, o setor espacial é visto como um componente fundamental para o desenvolvimento de toda a economia doméstica. Em suma, os planos chineses poderiam ser definidos como a chave para alcançar sua ambição de longo prazo em se tornar uma potência primária no sistema internacional (CARLSON, 2020, p. 34).

Com relação à organização institucional, o programa espacial chinês foi constituído, originalmente, sob a liderança do Corpo da Segunda Artilharia responsável pelo controle das capacidades missilísticas chinesas. Contudo, após mudanças políticas internas e com a escassez de recursos da década de 1980, algumas áreas do programa passaram para o controle civil.

Desde 1999, a cadeia de comando do programa vem aumentando seu grau de institucionalização. Sua coordenação nacional passou a ser feita pela Administração Espacial Nacional da China (CNSA), órgão subordinado diretamente ao Conselho de Estado. Já a pesquisa militar, desenvolvimento, aquisição e uso de capacidades espaciais para as Forças Armadas passaram a ser de responsabilidade do Departa-

mento Geral de Armamento (GAD), um dos três departamentos da Comissão Militar Central (CMC) do Conselho de Estado.

A principal agência executora do programa espacial chinês é a Corporação de Ciência e Tecnologia Aeroespacial da China (CASC). Tal órgão está sob controle da CNSA e é voltado para o desenvolvimento de sistemas civis e militares, além de ser responsável pela condução do setor comercial, contando com mais de 130 organizações adicionais que possuem a mesma finalidade (CEPIK, 2011).

Assim, o programa espacial chinês desponta, atualmente, como um dos mais avançados do mundo, além de possuir, como já mencionado, papel de destaque na Grande Estratégia chinesa, fato atestado pela menção à busca pela autossuficiência tecnológica do país no campo espacial, feita no 14º Plano Quinquenal. Tal documento, elaborado de acordo com as recomendações aprovadas na quinta sessão plenária do 19º Comitê Central do Partido Comunista da China, em outubro de 2020, tem como objetivo guiar o país como potência industrial e tecnológica e classifica o domínio espacial como uma das "tecnologias de fronteira" que serão responsáveis por 17% do PIB chinês em 2025 (UNGARETTI, 2021).

Ao longo das últimas décadas, o país tem logrado feitos notáveis, como o início da construção de sua própria estação espacial, a presença constante na Lua, com o programa *Chang'e* e o lançamento de veículos e satélites lunares, além de haver se tornado o terceiro país do mundo a levar à órbita terrestre seus próprios astronautas.

Já no campo militar, tendo em vista a simbiose entre o ambiente espacial e cibernético, a qual representa a essência da revolução na condução dos combates modernos, o Exército de Libertação Popular (ELP), como são conhecidas as Forças Armadas chinesas, criou, em 2015, sua quinta e mais recente força singular: a Força de Suporte Estratégico (FSE), visando preparar o país para eventuais cenários de guerra do futuro, em que pese a atuação estratégico-militar no e a aprtir do espaço.

Os principais objetivos do novo braço armado chinês consistem em, primeiramente, prover o ELP de suporte informacional, o que inclui navegação, Inteligência, monitoramento e reconhecimento, bem como a proteção de toda a infraestrutura militar de comunicações. Em segundo lugar, a FSE objetiva conduzir operações nos ambientes espacial, cibernético e eletromagnético, além de também ser especializada em operações psicológicas. Por fim e, como uma das finalidades mais importantes, a criação da nova força visa a facilitar as operações multidomínio entre as demais forças singulares, ao centralizar as capacidades de guerra informacional do ELP em apenas uma organização militar.

Tendo em vista o esforço envidado pela China e demais potências, no sentido de proteger seus ativos e assegurar o Comando do Espaço, percebe-se o papel fundamental que a exploração espacial e o desenvolvimento de novas tecnologias jogam para os demais setores, em especial o militar, assim como a necessidade de desenvolvimento da defesa de ditas infraestruturas (CEPIK, 2011).

Desta forma, considerando-se as aspirações brasileiras em alçar o país à condição de potência espacial, faz-se mister identificar eventuais necessidades de adequação – organizacional, doutrinário e prospectiva – da sua realidade ao atual cenário, notadamente marcado pelo contínuo uso do espaço para fins pacíficos ou não.

No ano de 2018, visando adequar o contexto nacional à nova tônica trazida pelas possibilidades militares no espaço, o Ministério da Defesa brasileiro inseriu, na Política Nacional de Defesa (PND) e na Estratégia Nacional de Defesa (END), o uso e a proteção do espaço exterior e do espaço cibernético como "essenciais para resguardar a soberania e os interesses nacionais" (BRASIL, 2018, p. 8). A END, por sua vez, cita, no âmbito das Capacidades Nacionais de Defesa, a Capacidade de Proteção, que, para ser reforçada, deve adequar e estruturar "os sistemas de vigilância nas áreas de interesse e de controle sobre o território nacional, as Águas Jurisdicionais Brasileiras, o espaço aéreo sobrejacente, o *espaço exterior,* o espaço cibernético e outras *áreas de interesse*" (BRASIL, 2018, p. 19, grifo nosso).

Tendo como norte as diretrizes da END de 2018, que estabeleceram o Setor Espacial como estratégico para a defesa e para o desenvolvimento nacionais, a Força Aérea Brasileira (FAB) concebeu o Programa Estratégico de Sistemas Espaciais (PESE). Tal programa possui como meta lançar seis constelações de satélites de órbita baixa[3] e três satélites geoestacionários[4], com o objetivo de atender às principais necessidades militares e consolidar o protagonismo do Brasil no atual cenário, por meio de soluções nacionais e de tecnologia dual.

À luz da Teoria dos Cinco Anéis de Warden, observa-se que a abordagem dos documentos de Defesa brasileiros acerca do domínio espacial se mostra incompleta, uma vez que tais publicações não abordam a estrutura espacial brasileira como um Centro de Gravidade, assim como não consideram o espaço exterior como um dos domínios da guerra. Ademais, o estabelecimento do Comando do Espaço também não é citado, nem mesmo elencado como prioridade estratégica.

Assim sendo, tendo em vista sua importância para o emprego do poder militar (GRAY, 1996), observa-se a necessidade de adequação das defesas alocadas aos ativos espaciais brasileiros já em órbita e aos que serão lançados no curto e médio prazos, sob pena de ser gerada uma vulnerabilidade não apenas para as Forças Armadas, mas para o Estado brasileiro como um todo. O reforço de tais defesas deveria levar em consideração tanto o protagonismo do meio cibernético como as armas ASAT convencionais já desenvolvidas por diversos países na atualidade, o

3 De acordo com a Agência Espacial Europeia (ESA), as órbitas baixas consistem no espaço orbital situado entre a Linha Kárman e 1.000 km da superfície terrestre.

4 Ainda de acordo com a ESA, os objetos colocados em órbitas geoestacionárias circulam a Terra de oeste para leste, sobre a linha do equador, com mesma taxa de rotação do planeta, fazendo com que permaneçam fixos sobre um mesmo ponto na superfície terrestre.

que poderia ser exequível por meio da criação de uma nova força singular ou de um comando operacional conjunto com foco na interoperabilidade entre meios cibernéticos e espaciais, a exemplo da FSE chinesa.
Ademais, destaca-se que, ainda que também não tenha sido citado nos documentos de Defesa brasileiros, o fomento do *New Space* seria benéfico não apenas para o setor de Defesa mas para o país de uma maneira geral. Tal favorecimento se daria por meio de parcerias entre governo e empresas privadas, visando à contratação de produtos e serviços estratégicos, mormente relacionados à Inteligência e comunicações e também por meio da indução a um maior protagonismo brasileiro na seara espacial, o que, por sua vez, acarretaria uma maior participação em organismos internacionais.
Ambos os casos contribuiriam para a garantia do Comando do Espaço por meio da presença, confome sugerido por Klein (2006) como uma das medidas a serem buscadas por países cujos programas espaciais ainda se encontram em estágios prematuros de desenvolvimento.

Considerações Finais

Quando considerado o papel desempenhado pelos ativos espaciais para o poder militar, como ilustrado pelos Paradigmas Estruturais, de Gray (1996), chega-se, por meio da teoria dos Cinco Anéis de Warden (1995), à conclusão de que o espaço consiste em um novo do domínio da guerra (LONSDALE, 1999) e que as infraestruturas lançadas às órbitas terrestre certamente constituir-se-ão em alvos estratégicos em conflitos do futuro – temor este já publicizado pela China (VALDUGA, 2022).
Tendo em vista, ainda, a natureza das ameaças inseridas nesse novo contexto, como as armas ASAT e as ações hostis oriundas do ambiente cibernético, perpetradas por meio de negação de serviços, com o emprego de *malware* e outros recursos hostis (ESTADOS UNIDOS DA AMÉRICA, 2018), conclui-se pela necessidade de se pensar na multidimensionalidade do TO, representada pela simbiose entre os domínios espacial e cibernético como uma das principais características da guerra do futuro a ser levada em conta por estrategistas.
Após ser apresentado o conceito de Comando do Espaço, que, de acordo com Klein (2006), pode ser exercido por meio de presença, coerção e força, identificou-se, via estudo do caso chinês, como tal país busca assegurar, atualmente, este Comando pelos três exercícios mencionados: pela *presença*, com recorrentes missões à Lua e com lançamentos de inúmeros ativos à órbita terrestre; e pela *força*, com a criação de sua mais nova força singular – a FSE, que, aliada aos demais fatores, também assegura condições de exercer a *coerção* sobre os demais *players* e, dessa forma,

"garantir por meios próprios o seu acesso e uso do espaço em tempos de paz e de guerra, bem como a habilidade de impedir um adversário de lhe negar tal proveito" (CEPIK, 2011, p. 2).

Com relação ao caso brasileiro e, considerando-se a importância do setor espacial para o atingimento de objetivos políticos e econômicos nacionais, em contraste com algumas lacunas observadas nos documentos de Defesa nacionais, sugere-se para o nosso país, *a priori*, a criação de um grupo de trabalho (GT) multidisciplinar, com o intuito de deliberar acerca do fomento ao programa espacial brasileiro e de reforçar, para as mais altas esferas governamentais, a importância do setor para a defesa nacional e para o atingimento dos interesses brasileiros, os quais transcendem a esfera de defesa e transbordam também para o desenvolvimento nacional. Tal GT poderia contar com a Agência Espacial Brasileira (AEB), os Ministérios da Defesa e Ciência, Tecnologia e Inovação (MCTI), que são os entes governamentais já à frente do Programa Nacional de Atividades Espaciais (PNAE) e do PESE, além das demais hélices que rotacionam o desenvolvimento tecnológico e estratégico do País: a academia e a indústria.

Ademais, conclui-se pela necessidade de revisão da PND e da END, com a sugestão de uma ênfase ainda maior na necessidade de proteção dos ativos espacias brasileiros, na busca pelo Comando do Espaço e na formação de doutrina acerca de operações espaciais.

Tendo em vista a interdependência entre os setores espacial e cibernético, recomenda-se, também a exemplo da experiência chinesa, a criação de um comando estratégico conjunto que reúna assuntos afetos a ambos os domínios. Tal medida não acarretaria óbices inerentes à criação de uma nova força singular, como a FSE chinesa ou a U.S. Space Force (USSF), mas poderia apresentar ganhos estratégicos e operacionais equivalentes, ao proporcionar melhores condições de interoperabilidade àqueles que podem ser considerados como os domínios prevalentes da guerra no futuro, além de facilitar a alocação de recursos para tal finalidade.

Quanto à busca pelo Comando do Espaço, tendo em vista o estágio prematuro do programa espacial brasileiro e nossa incipiente capacidade de sustentar uma presença física significativa – pelo menos, a curto prazo – nas órbitas terrestres, é recomendável, como posto por Klein (2006), que reforcemos esforços diplomáticos no sentido de garantir nossos interesses no âmbito de organismos e tratados internacionais, fato que já vem ocorrendo por meio da representação diplomática brasileira junto ao COPUOS, o que, aliás, pode ser fortalecido junto a adidâncias aeronáuticas com assessores exclusivos para tal setor.

Dessa maneira, o Brasil poderá ser capaz de assegurar melhores condições para eventuais empreitadas futuras, sem que seu acesso ao espaço seja prejudicador pela política das grandes potências espaciais.

Referências

BEAUFRE, A. (1998), *Introdução à estratégia*, Biblioteca do Exército, Rio de Janeiro, RJ.

BRASIL (2018), 'Decreto nº 179, de 14 de dezembro de 2018. Aprova a Estratégia Nacional de Defesa.', *Diário Oficial da União.*

BRASIL Ministério da Defesa (2020), 'Doutrina de operações conjuntas'.

CARLSON, J. (2020), Space power ascendant, Los Angeles, CA.

CEPIK, M. (2011), 'O comando do espaço na grande estratégia chinesa: implicações para a ordem internacional contemporânea', *Carta Internacional*, 6, pp. 112-131.

CHENG, D. (2011), 'Spacepower in China', *Toward a Theory of Spacepower: Selected Essays*.

CLAUSEWITZ, C. V. (2007), *On war*, Oxford University Press, Oxford.

DOLMAN, E. (2002), *Astropolitik*, Frank Cass Publishers, London.

DUFFY, K. (2022), 'Elon Musk says SpaceX has sent 15,000 Starlink internet kits to Ukraine over the past 3 months'. *Business Insider*. URL: https://www.businessinsider.com/elon-musk-spacex-sent-starlink-satellite-internet-terminals-ukraine-2022-6

DUTRA, A. M. (2007), Introdução à Guerra Cibernética: a necessidade de um despertar brasileiro para o assunto, in ITA, 'Simpósio de Guerra Eletrônica', São José dos Campos, SP.

FADOK, D. (1995), *John Boyd and John Warden Air Power's Quest for Strategic Paralysis*, USAF School of Advanced Airpower Studies, Air University Press Maxwell Air Force Base, Alabama.

GUERRA, E. S. (2019), *Fundamentos do Poder Nacional*, ESG, Rio de Janeiro, RJ.

ESTADOS UNIDOS DA AMÉRICA. U.S. Air Force (2018), 'Competing in Space'. URL: https://media.defense.gov/2019/Jan/16/2002080386/-1/-1/1/190115-F-NV711-0002.PDF

ESTADOS UNIDOS DA AMÉRICA. Department of Defense (2015), 'The DoD Cyber Strategy'.

FERREIRA, C. W. & TEIXEIRA JÚNIOR, A. W. M. (2021), 'Estratégia militar aplicada: metodologia de emprego', FGV, Rio de Janeiro.

FLORIDI, L. (1999), *Philosophy and computing*: an introduction. Nova York, NY: Routledge.

GRAY, C. S. (1996), 'The influence of space power upon history', *Comparative Strategy*, 15(4), pp. 293-308.

HENRY, P. (2008), 'The militarization and weaponization of space: towards a European space deterrent', *Space Policy*, 24(2), pp. 61-66.

KLEIN, J. (2012), *Space warfare*, Routledge, Nova York, NY.

LONSDALE, D. J. (1999), 'Information Power: strategy, geopolitics, and the fifth dimension', *Journal of Strategic Studies*, 22(2-3), pp. 137-157.

LONSDALE, D. J. (2004), *The nature of war in the Information Age*, Routledge, Londres.

NGUYEN, N. (2015), 'Evolution of the battlefield: strategic and legal challenges to developing an effective cyber warfare policy', *Australian Defence Force Journal*, 196, pp. 60-69.

PROENÇA JR, D, DINIZ, E. & RAZA, S. (1999), *Guia de estudos de estratégia*, Jorge Zahar Editor, Rio de Janeiro, RJ.

Proteger infraestrutura crítica: Alemanha vira 4.º país da OTAN a criar comando espacial militar (2022), *Sputnik Brasil*. URL: https://br.sputniknews.com/20210714/proteger-infraestrutura-critica-alemanha-vira-4-pais-da-otan-acriar-comando-espacial-militar-17777324.html

Reino Unido, HM Government (2016), 'National Cyber Security Strategy 2016-2021'. URL: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

SHELDON, J. B. (2013), 'The rise of cyberpower', *Strategy in the contemporary world*, pp. 303--319.

SIA (2022), 'Satellite Industry Agency Releases 25th Annual State of the Satellite Industry Report'. URL: https://sia.org/commercial-satellite-industry-growing-as-it-continues-to-dominate-expanding-globalspace-business-sia-releases-25th-annual-state-of-the-satellite-industry-report

STEINBERG, A. (2012) 'Weapons in Space: The Need to Protect Space Assets', *Astropolitics: The International Journal of Space Politics & Policy*, pp. 248-267.

UNGARETTI, C. R. (2021), 'O 14.º Plano Quinquenal (2021-2025) da China em Perspectiva Doméstica e Internacional', *Economia, inovação e meio-ambiente*.

VALDUGA, F. (2022), 'Cientistas militares chineses simularam explosão nuclear no espaço para derrubar redes de satélites', *Cavok*. URL: https://www.cavok.com.br/cientistas-militares-chineses-simularam-explosao-nuclear-no-espaco-para-derrubar-redes-de-satelites

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

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

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

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

Resumo

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

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

Abstract

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

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

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

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

Introdução

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Considerações Finais

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

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

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

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

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

Referências

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Political-Strategic Perspectives of Hybrid Warfare in the Czech Republic

Gabriel Olegário
Graduado em Relações Internacionais na Universidade Federal de Santa Catarina e graduando em Ciência Política na Universidade de Hradec Králové, na República Tcheca. Participou do Grupo de Pesquisa e Extensão em Segurança Internacional e Defesa (GESED). Pesquisador voluntário do Grupo de Pesquisa em Estudos Estratégicos e Política Internacional Contemporânea (GEPPIC-UFSC).

Graciela de Conti Pagliari
Professora Associada da Universidade Federal de Santa Catarina. Doutora em Relações Internacionais pela Universidade de Brasília (2009). Mestre em Relações Internacionais pela Universidade Federal do Rio Grande do Sul (2004), Graduada em Direito pela Universidade do Vale do Rio dos Sinos. É autora do livro O Brasil e a Segurança na América do Sul e co-autora do Guia de Defesa Cibernética na América do Sul.

Abstract

Since the first conceptualization of Hybrid Warfare by Hoffman in 2007, the term has been used by politicians and academics to refer to a new concept of war strategy. Therefore, the use and definition of the term are important, considering the growing literature in the academic field after 2014, with the annexation of Crimea by Russia. This paper aims to demonstrate the political-strategic perspectives of the Czech Republic on the issue of Hybrid Warfare, demonstrating the tendency to securitize hybrid threats. Later, a detailed analysis of information warfare is done due to the relevance of the cyber dimension and the importance of disinformation as a hybrid threat in the security environment of the Czech Republic. It is concluded that strategic responses centered only on the State may be insufficient, and a joint effort with society is necessary to pursue the objective of the "Resilient Czech Society 4.0".

Keywords: Hybrid Warfare; Czech Republic; Hybrid Threat; National Strategy Defense.

Resumo
Perspectivas Político-Estratégicas da Guerra Híbrida na República Tcheca

Desde a primeira conceituação de Guerra Híbrida em 2007, o termo tem sido usado por políticos e acadêmicos para se referir a um novo conceito de estratégia de guerra. Portanto, o uso e definição do termo é importante, considerando a crescente literatura no campo acadêmico após 2014, com a anexação da Crimeia pela Rússia. Este artigo tem como objetivo demonstrar as perspectivas político-estratégicas da República Tcheca sobre a questão da Guerra Híbrida, demonstrando a tendência de securitizar ameaças híbridas. Uma análise mais longa sobre a guerra de informação é feita devido à relevância da dimensão cibernética e à importância da desinformação como ameaça híbrida no ambiente de segurança da República Tcheca. Conclui-se que as respostas estratégicas centradas apenas no Estado podem ser insuficientes, sendo necessário um esforço conjunto com a sociedade para atingir o objetivo da "Sociedade Checa Resiliente 4.0".

Palavras-chave: *Guerra Híbrida; República Tcheca; Ameaça Híbrida; Estratégia Nacional de Defesa.*

Artigo recebido: 25.07.2022
Aprovado: 18.10.2022
https://doi.org/10.47906/ND2022.163.03

Introduction

The security issues of the 21st century have been under a rapid socio-technical transformation and increasing fragmentation of political power and authority, establishing hybrid warfare as one of the main State concerns. Therefore, Cavelty and Wenger (2022) maintain that hybrid threats will enlarge in complexity and political significance due to the technological developments that have been shaping the relationship between politics and technology.

The drawback of this article deals with hybrid threats that States are facing under these rapid transformations in society and the recognition of cyberspace as an operational domain in 2016 by NATO (Czech Republic, 2021b). Therefore, the main aim of this article is to identify the developments of hybrid warfare in the current Czech Republic's political-strategic perspective and to select and analyze one hybrid threat relevant in the Czech Republic's context. With that being said, the next chapter delves into the definition of Hybrid Warfare and Hybrid Threat to set the ground for this article.

Definition of Hybrid Warfare

The concept of Hybrid Warfare is wide and subjective to interpret how technological development influences the relationship between the State and Warfare. Thus, formulating a precise definition of Hybrid Warfare is important for both civil society and government national security bodies, especially in the formulation of policies and legislation that encompasses a concept that is still under construction and constantly changing (Clarke and Knake, 2010). One of the first strategists to write about the topic, Hoffman (2009) maintains that seeking a proper definition for the concept of Hybrid Warfare is essential because it facilitates the improvement of policies and defense strategies centered on hybrid threats to better prepare for different internal and external vulnerabilities.

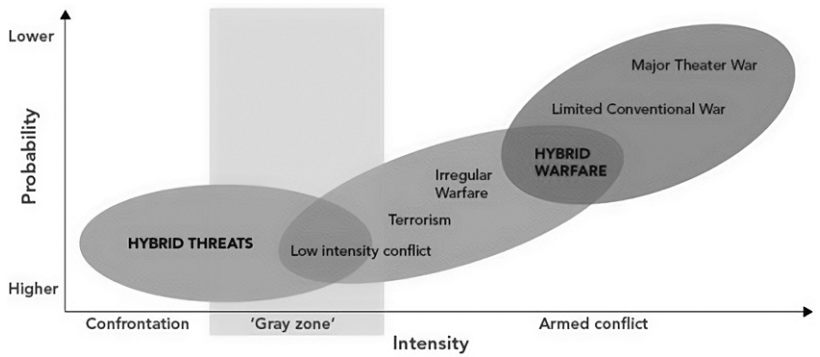
The concept of Hybrid Warfare and Hybrid Threats can be conflicting due to the diversity of possible overlapping definitions, mainly because it is a concept that is still being constructed and modified. The situation is complicated also by the fact that the concept of hybrid warfare or hybrid threats has no legal definition (Łubiński, 2022; Berzins, 2022). As Hoffman referred to in his pivotal work: "Hybrid Warfare incorporates a range of different models of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder" (Hoffman, 2007, p. 14). Thus, hybrid warfare presumes a combination of civilian and military activity, which reaches significant intensity and could result in some level of violence. Interestingly, it has

to be noted that many non-western international relations scholars oppose the existence of such a concept, for example, when Russian scholars talk about the same topic they use terms known as new generation warfare and non-linear warfare (Wither, 2016).

Additionally, an important differentiation is the concept of hybrid threat, as the European Centre of Excellence for Countering Hybrid Threats refers to: as "an action conducted by state or non-state actors, whose goal is to undermine or harm a target by combining overt and covert military and non-military means" (Hybrid CoE, 2022). In other words, the threats could be any phenomenon that could undermine or harm the interests and values protected by the State. Furthermore, due to the hybrid aspect diminishing boundaries between civilian tools and military weapons, hybrid threats have a lower intensity and take place in the "gray zone" compared to hybrid warfare (Filipec, 2022, p. 5).

The image below differentiates both concepts visually, conceptualizing the probability and intensity of a conflict in those terms. Therefore, there is a difference between managing a hybrid threat and hybrid warfare, the same way terrorism and irregular warfare are in the same continuum of conflict, however, they require different tactics to tackle it.

Image 1
Hybrid Warfare and Hybrid Threats



Source: Hoffman (2009).

To understand how Hybrid Warfare and Hybrid Threats are intertwined with the Czech Republic's security environment, we shall proceed to the next subsection.

Czech Republic's strategic environment

The Czech Republic (as well as Central European countries) redirected its geopolitical values after the Cold War, starting a process of *westernization* (Cadier, 2019). According to Cadier (2019), this process of *westernization* is best known as the *return to Europe*, a transition embracing liberal democracy, capitalism, and Euro-Atlantic political structures that were seen as contemporary solutions to 90's geopolitical issues. Thus, there is a historical background to explain Czech Republic's pathway to westernization. To summarize, since 1993, the Czech Republic's security environment has been developing three main pillars in the form of challenges. The first concerns the adequacy of Western European patterns of change in the Czech security environment and changes in domestic, economic, and social transformation policies. The second is related to the implementation of the defense policy, which most of the time encounters difficulties because it is not being adequately financed, resulting in a defense sector that has insufficient resources and the lag of defense capabilities. The third pillar is associated with the evolution of the concept of the Armed Forces of the Czech Republic, more specifically, the role of the Armed Forces was primarily the defense of the national territory which contemporaneously becomes (after the 1990s) Expeditionary Forces that has in its core the principle of collective defense and provider of know-how for international crisis management (Czech Republic, 2015).

Three main tendencies can be retrieved from the Security Strategy of the Czech Republic (2015), the first trend concerns that the risks of invasions or direct military conflicts against the Czech Republic are low, however, the possibility of using force in conjunction with NATO allies or EU members cannot be ruled out. This point is underpinned by the general decline in security and stability on the flanks of Europe and in the EU's neighboring countries which can take the form of threats of a classical military nature or the form of Hybrid Warfare. Furthermore, the increasing dependence of the Czech state and society on technology generates vulnerabilities (Czech Republic, 2015).

The second trend is in line with the first since the Czech Armed Forces are increasingly preparing to transform themselves into Expeditionary Forces due to the lack of internal use of military force. Thus, the second trend is that the security environment of the Czech Republic is defined beyond national and the EU borders, recognizing that any global conflict could affect the Czech Republic. The Security Strategy of the Czech Republic (2015) states that "one of the characteristic aspects of the current environment is that our security can be directly affected by the instability and conflicts existing far beyond the borders of Europe" (Czech Republic, 2015, p. 10). Moreover, the Czech Republic encompasses a much wider spectrum of crisis management with a combination of military and civilian tools, in addition to diplomatic, legal, and economic means (Czech Republic, 2015).

The third trend is associated with the growing ambition of some actors around the Czech security environment ready to use military force in pursuit of their interests at the expense of stability in other countries. Therefore, according to the Security Strategy of the Czech Republic,

> The aspirations of these actors are associated with a substantial increase in their military capabilities, including offensive cyber capabilities, weapons of mass destruction, and their means of delivery, and with their growing demand for essential raw materials, activity in financial markets, struggle for influence in strategic areas and increasingly aggressive promotion of its political ambitions in international forums [...] In addition, another consequence of the aspiration of these actors is the destabilization of the strategic environment of NATO, the EU, and the Czech Republic, resulting in conflicts that violate human rights, including political, social and environmental rights. Such actors (state or otherwise) normally violate the international order and basic principles of international law in the pursuit of power (Czech Republic, 2015, p. 10).

After the elucidation of the Czech Republic's security environment, we shall continue with how the official Czech documents strategically perceive Hybrid Warfare and Hybrid Threats.

The Czech Republic's political-strategic perspectives

As detailed above, the Czech Republic relies on the *westernization process* and this leads the Czech Republic to affirm explicitly or implicitly in the documents that membership in NATO and the EU is the best guarantee for the National Security of the Czech Republic. According to the 2017 Defense Strategy, we observe that

> The Defence Strategy is based on the applicable national law regulating defense, particularly the Czech Constitution, international treaties, and relevant Acts. It stems from the Security Strategy of the Czech Republic and reflects NATO's Strategic Concept, the EU's Global Strategy, and other relevant national, international and allied documents (Czech Republic, 2017, p. 6).

This strategy strongly emphasized security threats that did not pose greater risks to the Czech Republic itself but were associated with a degree of risk to NATO members. In practice, this means that international terrorism has become the number one security threat, with the proliferation of weapons of mass destruction in second place, which was not the primary agenda for the national defense of the Czech Republic in 2017 (Kriz, 2021). However, as NATO and the EU have been

preparing to increase the resilience against hybrid warfare in their official documents, the instability created by the 2022 Ukrainian-Russian war will likely increase the significance of hybrid warfare and threats to the NATO/EU members as well as the Czech Republic (The economist, 2022). The concept of Hybrid Warfare not only gained some popularity in public opinion, but hybrid campaigns or hybrid threats gained relevance after 2012 in the main security documents of the Czech Republic such as Security Strategy of the Czech Republic (2015), Defence Strategy of the Czech Republic (2017), National Cyber Security Strategy of the Czech Republic for the period from 2021 to 2025, the National Strategy to Combat Interference Hybrid as well as official reports from the Czech Republic's intelligence agency. To find a satisfactory answer regarding The Czech Republic's political-strategic perspectives, the next subsections go further into the document's details.

Security Strategy of the Czech Republic (2015)

The introduction to the Security Strategy of the Czech Republic (2015) document cites that "In today's crisis-ridden world, the Czech Republic naturally has to face a huge number of challenges. Economic and social development is our main and immediate concern" (Czech Republic, 2015, p. 3). Therefore, the Czech Republic understands that immediate concerns (economic and social development) will only progress if strategic interests are promoted as such,

> security and stability, especially in the Euro-Atlantic area; preventing and managing local and regional conflicts and mitigating their impacts; maintaining the UN's global stabilising role and increasing its efficiency; strengthening the cohesion and efficiency of NATO and the EU and retaining a functional and credible transatlantic link; reinforcing the NATO-EU strategic partnership, including the strengthening of cooperation in the complementary development of defence and security capabilities; developing the OSCE's role in the prevention of armed conflicts, in democratisation and in building mutual confidence and security; a functioning and transparent conventional arms control regime in Europe; supporting and developing regional cooperation; supporting international stability through cooperation with partner countries; supporting democracy, fundamental freedoms, and the principles of the rule of law; safeguarding internal security and protecting the population; safeguarding the Czech Republic's economic security and strengthening the competitiveness of the economy; safeguarding the Czech Republic's energy, raw-material and food security and an appropriate level of strategic reserves; safeguarding the Czech Republic's cyber security and defence; preventing and suppressing security threats affecting the security of the Czech Republic and its allies (Czech Republic, 2015, p. 8).

The Security Strategy of the Czech Republic (2015) that is currently in force was adopted in the context of various hybrid threats such as the annexation of Ukraine by Russia as well as the cyberattacks on the Baltic countries (Czech Republic, 2015). Learning the lessons from a lack of a joint response against both events, the Security Strategy of the Czech Republic (2015) brings a perspective that focuses on international cooperation, as the "weakening of the cooperative security mechanism and of political and international legal commitments in the area of security" (Czech Republic, 2015, p. 13).

Although Russia is not explicitly mentioned in this document, the idea is developed from the recent strategies used by Russia, the document states that revisionist States might use hybrid instruments to achieve their goals such as

> conventional and non-conventional military means with non-military tools (propaganda using traditional and new media, disinformation intelligence operations, cyber attacks, political and economic pressures, and deployment of unmarked military personnel) (Czech Republic, 2015, p. 13).

Yet, a very important remark is the affirmation of the volatile nature of the present security threats and the requirement to have a broad-based approach to security, combining military and non-military tools to defeat hybrid threats. Therefore, the document affirms that "The Czech Republic develops tools for promoting its security interests at the national level as well as through active engagement in multilateral and bilateral relations". The purpose of having such a broad-based approach is due to the abstract nature of threats that might occur, taking into account the development of new technologies and consequently new threats.

The Defence Strategy of the Czech Republic (2017)

In the Defence Strategy of the Czech Republic (2017), the Czech Republic seeks to achieve a comprehensive security approach that goes beyond the framework of pure military security, following the same tendency in the Security Strategy of the Czech Republic (2015). Moreover, the comprehensive security approach is a core principle of NATO and the EU that is also affirmed in the Defence Strategy of the Czech Republic (2017) with the aim of ensuring

> the defence of its sovereignty and territorial integrity, primarily within the framework of NATO's collective defence as set out in Article 5 of the Washington Treaty. Nevertheless, the Czech Republic's membership of international organisations does not free it from its primary responsibility of defending its own national territory. Autonomously, and in cooperation with other states, the Czech Republic maintains and develops,

> in line with Article 3 of the North Atlantic Treaty, its individual and collective capacity to resist an armed attack. The defence policy of the Czech Republic is based on the country's membership of NATO and the EU, and benefits from the provision of home defence and security while, in turn, committing the Czech Republic to adequately contribute to the development of the collective defence of other member countries (Czech Republic, 2017, p. 15).

In the 2017 Defense Strategy, the threat of the Russian Federation and its imperialist ambitions against the Czech Republic and the West is explicit, and the document continuously develops the foreign and security policy orientation that the Czech Republic has followed since 1993, namely pro-Western and anti-Russia orientation, ties to the transatlantic security partnership and building the security dimension of the European integration.

> Since 2012, the security situation in Europe has significantly deteriorated. In Eastern Europe, the Russian Federation blatantly carries out its power ambitions, including through use of military force. In doing so, the Russian Federation violates the norms of international law, including the territorial integrity of its neighbouring states. It has executed hybrid operations against NATO nations and EU Member States, including targeted disinformation activities and cyber-attacks (Czech Republic, 2017, p. 7).

As stated in the Defense Strategy document, the Czech Republic is responding by increasing the defense budget at the expense of the instability of its strategic environment. Still, it is claimed that the

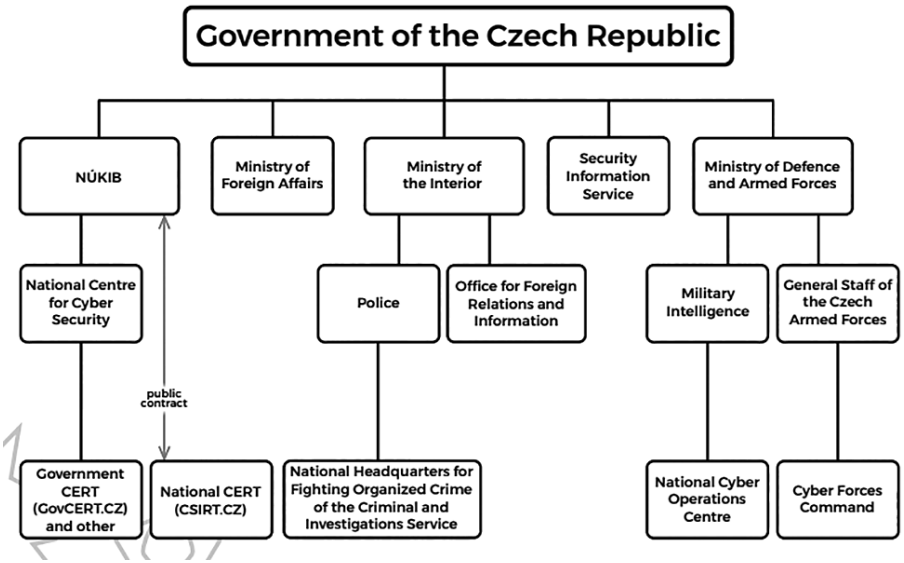
> response to the deteriorating security environment, the Czech government has begun to increase defence funding. The most pressing task is to redress the consequences of the slump in the level of defence capabilities, and the personnel, technology and material negligence that had built up over the previous years, and to develop the Czech Armed Forces so that they are able to fulfil their tasks (Czech Republic, 2017, p. 7).

Another feature described is the national defence system interlinked with the allied structures. The primary function of the national defence system is "to prepare, manage, coordinate and support activities of the relevant authorities, forces, and assets in order to ensure the defense of the Czech Republic. This includes early detection, prediction, and evaluation of potential threats, including hybrid threats" (Czech Republic, 2017, p. 16). Importantly, the operational activities are provided for and controlled by the President of the Czech Republic, Parliament and the Government of the Czech Republic, working and advisory bodies, ministries and other central government authorities.

Czech Republic National Cyber Security Strategy 2021-2015

According to the Czech Republic National Cyber Security Strategy 2021-2015 document, the Czech government has been funding and renewing its cybersecurity strategy against the variety of threats that the cyber dimension has been producing. Therefore, the scheme below demonstrates how Cyber Security is ensured by the Czech Republic, demonstrating that cyberspace is one of the most recent and vulnerable dimensions due to the lack of preparation States have to securitize technology.

Image 2
Ensuring Cyber Security in the Czech Republic



Source: Czech Republic (2021b, p. 8).

According to the document, each unit shown in the figure above has a specific function, mainly specified in the document that complements the National Cybersecurity Strategy of the Czech Republic 2021-2015 called the Action Plan for the National Cybersecurity Strategy of the Czech Republic 2021-2015. For didactic purposes, the Action Plan will not be analyzed, as the most important result is to understand the complexity of cyber protection networks and the primary role of the government of the Czech Republic in ensuring cyber security.

The Czech Republic Cyber Strategy (2021b) can be structured and summarized in three main points: a) confidence in cyberspace, b) strong and reliable alliances and c) Resilient Society 4.0. The three points correspond with the future of the strategic

direction of the coming years. The overview of "The Czech Republic will have a resilient society and infrastructure, will act confidently in cyberspace and will actively confront the entire spectrum of threats while strengthening reliable alliances" (Czech Republic, 2021, p. 21).
Thus, considering the three points mentioned in the document, the summary of the strategic objectives can be found in the table below,

Table 1
Strategic objectives according to the National Cyber Security Strategy of the Czech Republic for the period from 2021 to 2025

Confidence in Cyberspace	Strong and Reliable Alliances	Resilient Society 4.0
Strategic Goals		
• A national approach emphasizing information sharing, coordination, and cooperation • Developing state cyber security capabilities and capacities • Strengthening the security and resiliency of infrastructure • Developing prediction, detection, and agile reactions to cyberattacks • An effective communication strategy • Preventing and fighting cybercrime	• Effective international cooperation • Creating alliances • Promoting Czech interests abroad • Creating dialogues in the international environment • Supporting open and safe behaviour in cyberspace • Exporting knowledge	• Ensuring the security of state administration / eGovernment digitalization • A high-quality education system • Raising awareness • Cooperation between the state, the private sector, and citizens • Creating a broad base of experts

Source: Czech Republic (2021, p. 21).

Therefore, the strategic objectives are focused on the resilience of the State against cyber vulnerability, both in terms of hardware and social issues (Czech Republic, 2021). Following the broad-based approach to counter hybrid threats, society (ordinary internet users) needs to get used to protecting itself, recognizing possible threats, and understanding the dynamics of cyberspace. This is precisely why the document states that it will invest in primary and secondary education to modernize the country's educational system and also invite sectors of society to participate in courses on digital hygiene to improve digital resilience, especially positions that demand knowledge and use of the internet with sensitive data (Czech Republic, 2021).

National Strategy to Combat Hybrid Interference

Hybrid Interference has become a relevant security matter and the National Strategy to Combat Hybrid Interference defines the objectives and determines the essential defense capabilities for the protection of the national interests of the Czech Republic. Such a document has a strong appeal for the comprehensive security proposed by NATO and the EU, as it focuses on a wide variety of security threats, in addition to human security (Czech Republic, 2021a).

Thus, the document states that hybrid threats can include the overt or discreet influence of political structures and the decision-making process in politics, courts, police, military, media and public opinion. The opponents' objectives would be to destabilize or divide Czech society and diminish the trust that citizens have in the country's institutions (Czech Republic, 2021a).

Still, the hybrid threats that can affect the economic interests of the Czech Republic, and the strategic sectors that the Czech Republic cites are dependence on strategic resources from foreign countries, such as oil, natural gas, and nuclear fuel. Therefore, the Czech Republic states that it will guarantee the defense of the opening of the economy and its orientation towards exports, foreign investments, and loans that are in strategic sectors of the economy or that lead to strategic dependence on its suppliers (Czech Republic, 2021a). In addition to the dependence on strategic resources for the development of the Czech economy, it is also necessary to understand that hybrid threats can manifest through technologies such as 5G networks and artificial intelligence used by the private sector (Czech Republic, 2021a).

Other risks also concern corruption, links between diplomacy, the private sector, espionage, and the interest of foreign powers in the Czech Republic. Hybrid threats can include the mobilization of interest groups (defined by religion, ethnicity, nationality, or language) or criminal groups acting against the security interests of the Czech Republic and violating public order. Hybrid interference that seeks to delay or paralyze decision-making processes in the defense and security domain also poses a risk. This includes NATO collective defense and EU defense and political cooperation (Czech Republic, 2021a).

The hybrid threat of informational warfare and (dis)information in the Czech Society

Since the concept of warfare has existed in human societies, it has always been connected with information. Therefore, decisions and actions of any nature can be understood in informational terms. For example, controlling the flow of information and its characteristics can represent an important factor in influencing the

behavior of certain targets, and consequently can be weaponized to achieve political goals (Filipec, 2019).

The democratic system in the Czech Republic has alleged asymmetrical vulnerabilities and is characterized by uncertainty about the impact of disinformation, leading to an increase in the securitization of information. Furthermore, the empirical evidence is short related to foreign disinformation campaigns having a substantial long-term effect on public discourse and public policy, and the potential macro effects on policy-making and psychological influence are difficult to understand and prove (Štětka, Mazák and Vochocová, 2021).

According to the Czech intelligence service, the Czech Republic has become a laboratory for the Russian Hybrid War (Bezpecnostní Informacni Sluzba, 2020). It is important to remember that due to the geographical situation of the Czech Republic and its past, 'less Europe' automatically means 'more Russia'. To some extent, Rychnovska and Kohut (2018) affirm that Russia's policy of inflicting fear is in the national interest, and one of the goals that Russia has is to gain more support for its foreign policy through the use of the disinformation strategy (Rychnovska and Kohut, 2018).

One of the dangers of defining disinformation is to similarly conceptualize "fake news", "misinformation", "coordinated inauthentic behavior" and "propaganda" in the same category due to the amount of news misusing these terms. For the majority of news consumers, this difference might be not that relevant, however, Ó Fathaigh, R. & Helberger, N. and Appelman, N. (2021) maintain that this constellation of different concepts is the defining political communication topic of our time, which most likely will increase over time. A clear definition of those terms is essential to any State that fancies creating cyber strategies and defensive capabilities.

In fact, there are various definitions and overlapping concepts which may significantly vary in different contexts, and the Czech Republic is no different. A primary definition by the High-Level Expert Group of Fake News and Online Disinformation of the European Commission affirms that "Disinformation… includes all forms of false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for-profit" (De Cock Buning, 2018, p. 3). That is the reason why the definition above has some critical criteria as a) deception, b) potential for harm, and 3) an intent to harm. It thus excludes deceptive messages that may cause harm without the disseminators' knowledge (misinformation) and non-deceptive messages intended to harm others (e.g. hate speech).

To summarize those three critical criteria, disinformation is misleading information that has the purpose to be intentionally misleading, intentionally providing manipulated content, and therefore intentionally creating false beliefs. Disinformation is still informational nonetheless, taking into account the nature of the phenomenon (De Cock Buning, 2018).

Moreover, the Czech Ministry of Interior distinguishes between disinformation, understood as a "systematic and intentional spread of false information mainly by state actors or its affiliates against foreign states or media with the aim to influence decision-making or opinions of those, who adopt decisions" and misinformation which refers to "incorrect or misleading information, which is not spread systematically nor with the intention to influence decision-making or the opinions of those who adopt decisions" (Czech Republic, 2019).

Quoting one of the most influential Czech politicians, former President, and Philosopher Václav Havel: "It is a natural disadvantage of a democracy that it ties the hands of those who wish it well, and opens unlimited possibilities for those who do not take it seriously" (Havel, 1971, p. 12). Therefore, it is evident that democracies have a shortcoming in tackling disinformation, and Central and Eastern European countries might have specific factors that make it even more difficult. After those necessary definitions, the next subsection deals with countering information warfare and (dis)information in the Czech Society

Countering information warfare and (dis)information in the Czech Society

To a certain extent, democratic countries have more barriers to counter information warfare as they try to find a balance between freedom of expression and protection of one's basic rights, as censorship is not acceptable in the Czech constitution. To delve further into the Czech Republic's perspective, foreign disinformation campaigns were assessed as a serious threat to internal security and one of the recommendations to combat these forms of hybrid warfare was to "establish departments within relevant government institutions for the assessment of disinformation campaigns and other manifestations of foreign power influence" (Czech Republic, 2016, p. 61).

Thus, a response by the Czech government to this problem was the establishment of the Center against terrorism and hybrid threats (Centrum proti terorismu a hybridním hrozbám) in 2017. However, one of the points and difficulties that States have is to fight disinformation at the expense of basic rights, such as the right to expression, leading the current president of the Czech Republic, Milos Zeman, to suggest that the Center would infringe on freedom of expression (Reuters, 2021).

This is exactly why the Czech Republic finds barriers to penalizing disinformation, as such a term does not exist in the Czech legislative system. As there is no specific term for disinformation, the Czech Republic has different crimes that can be typified as disinformation, as in the Penal Code, Chapter II criminal offenses against liberty, privacy and personal rights and confidentiality only in the case of § 181 violation rights of others, § 184 defamation, § 345 false accusations, § 355 defama-

tion of the nation, race, ethnicities or other groups of people, § 356 instigation of hatred against groups of people or the suppression of rights and freedoms, § 357 spreading news §364 incitement to criminal offenses, § 365 approval of criminal offenses, § 404 expressing sympathies for movements that seek to suppress human rights and freedoms in accordance with act nº 40/2009 (Filipec, 2019).
The National Cyber and Information Security Agency maintains in the National Cyber Security Strategy of the Czech Republic for the period from 2021 to 2025 that

> the Strategy's main actors are the state's security services and other public administration bodies. However, the Strategy also supports and informs other parts of Czech society to enable them to better understand the state's actions when facing cyber threats and risks [...] leaving cyber security solely to the Czech state is not enough, however. Every institution, private company, and individual has their role and can positively contribute to cyber security. The Czech Republic must therefore set up and support a cyber security policy that will consistently incorporate all of society into cyber security processes and thus increase its resilience to cyber threats (Czech Republic, 2021, p. 3).

In other words, there is a glimpse into what the Czech Republic considered as proper cyberdefense capabilities: a tendency to decentralize the securitization of information through the increase of resilience of the civil society, the private and the public sectors. Furthermore, the key strategy against disinformation is resilience in the Czech society, more specifically, to increase the capacity to recover as fast as possible from difficulties or toughness (Czech Republic, 2021).
According to the National Cyber Security Strategy of the Czech Republic for the period from 2021 to 2025, "the central challenge for the Czech Republic in this area is to concentrate not only on current cyber security threats but also to acquire the ability to adapt to the new and constantly changing security environment" (Czech Republic, 2021, p. 6). Therefore, there is a flexible tendency for adopting defense policies along the way, proving that the Czech Republic maximizes its capacities and constantly seeks new strategies against future cyber threats.
With that being said, the securitization of information warfare or disinformation happens primarily with the emergence of a new network of professionals composed of think tanks and journalists who manage to reach the public and influence policy-makers. Thus, this network is formed by professionals from different fields connecting different institutions. One of the examples is European Values and the Ministry of Interior of the Czech Republic, which have working connections and develop policies together (Rychnovska and Kohut, 2018).
The European Values initiated a series of reports about the Kremlin, and consequently, the expert endorsement was published to legitimize the aggressive policies of the Russian government. Another point is to analyze how the Ministry of

the Interior was influenced, legitimizing the activities of European Values and bringing the whole problem of disinformation to the forefront of media attention (Rychnovska and Kohut, 2018).

Also, according to Rychnovska and Kohut (2018), there are different networks that have different audiences in information warfare debates. For example, while the Prague Security Studies Institute (PSSI) think tank mainly communicates with domestic and international civil society and private actors, European Values has a much closer relationship with the Czech Republic's security apparatus.

Still, the relationship between politicization and securitization of disinformation complicates the possibilities of responses by the Czech government, however, the addition of independent institutions creates new measures that can be adopted in different contexts counting on the potential social mobilization, in addition to just creating untrustworthy media blacklists, selecting individuals who share pro-Russian propaganda, fact-checking tools or digital education (Rychnovska and Kohut, 2018).

Therefore, comprehending the limitation of the Czech government in fighting disinformation, and how this limitation gave space for non-governmental organizations to enter as agents fighting disinformation is a must. Consequently, the decentralization of the fight against disinformation can be one of the solutions for the Czech Republic to continue with its democratic and transparent narrative, giving space for non-governmental organizations to filter information that matches reality.

Conclusion

To conclude, this article demonstrated the strategic responses and the capacity that the Czech Republic has against hybrid threats that are related to its strategic environment (which has been changing since 1993). In other words, the State's inability to securitize all technological advances creates different responses and strategies against hybrid threats, such as the strengthening of the concept of resilience among all parts of society, in addition to the use of independent organizations that can be used strategically against disinformation.

Furthermore, the concept of Hybrid Warfare and the underlying hybrid threats are still constantly changing, and the metamorphic nature of the results of this work is possible. Therefore, when we analyze disinformation in Czech society, we infer that democracies may have obstacles to censoring and filtering information that will pass through digital media. At last, it is analyzed that in order to tackle disinformation, the decentralization of the strategy against disinformation can be an efficient response, such as the joint work between independent organizations such as think tanks and the Czech government.

References

Berzins, V. (2022). 'Hybrid warfare: weaponized migration on the eastern border of the EU?' *The Interdisciplinary Journal of International Studies*, 12(1), 3-19. Available at: https://130.225.53.24/index.php/ijis/article/view/6992 (Accessed: 21 February 2022).

Cadier, D. (2019). 'The geopoliticisation of the EU's Eastern Partnership'. *Geopolitics*, 24(1), pp. 71-99. DOI: 10.1080/14650045.2018.1477754

Czech Republic. Bezpečnostní informační služby (2020). VÝROČNÍ ZPRÁVA 2020. Available at: https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2020-vz-cz-2.pdf (Accessed: 21 February 2022).

Czech Republic. Minister of Interior (2016). National Security Audit. Available at: http://www.mvcr.cz/cthh/soubor/national-security-audit.aspx (Accessed 9 February 2022).

Czech Republic. Ministry of Defence of the Czech Republic (2015). Security Strategy of the Czech Republic. Available at: https://www.army.cz/images/id_8001_9000/8503/Security_Strategy_2015.pdf (Accessed: 21 February 2022).

Czech Republic. Ministry of Defence of the Czech Republic (2017). THE DEFENCE STRATEGY OF THE CZECH REPUBLIC. Available at: https://www.army.cz/assets/en/ministry-of-defence/strategy-and-doctrine/defencestrategy2017.pdf (Accessed: 21 February 2022).

Czech Republic. Ministry of Defence of the Czech Republic (2021a). NATIONAL STRATEGY FOR COUNTERING HYBRID INTERFERENCE. Available at: https://www.army.cz/assets/en/ministry-of-defence/basic-documents/national-strategy---aj-final.pdf (Accessed: 21 February 2022).

Czech Republic. National Cyber and Information Security Agency (2021b). National Cyber Security Strategy of the Czech Republic for the period from 2021 to 2025. Available at: https://nukib.cz/download/publications_en/strategy_action_plan/NSCS_2021_2025_ENG.pdf (Accessed: 21 February 2022).

Czech Republic. Ministry of Interior (2019). 'Definice dezinformací a propagandy'. Available at: https://www.mvcr.cz/cthh/clanek/definice-dezinformaci-a-propagandy.aspx Accessed 6 February 2022

De Cock Buning, M. (2018). *A multi-dimensional approach to disinformation : report of the independent High level Group on fake news and online disinformation*. Luxembourg: Publications Office of the European Union. Available at: https://hdl.handle.net/1814/70297

Filipec, O. (2019). 'Towards a disinformation resilient society?: The experience of the Czech republic' *Cosmopolitan Civil Societies: an Interdisciplinary Journal*, 11(1), pp. 1-26. DOI: https://search.informit.org/doi/10.3316/informit.327461541708193

Filipec, O. (2022). 'Multilevel analysis of the 2021 Poland-Belarus Border Crisis in the Context of Hybrid Threats'. *Central European Journal of Politics*. DOI: 10.24132/cejop_2022_1

Havel, V. (1971). Spiklenci. *Václav Havel Library*. Available at: https://archive.vaclavhavel-library.org/Archive/HavelWork?eventType=Dramatick%C3%BD%20text&eventYear=1971# (Accessed 9 February 2022).

Hoffman, F. G. (2009). *Hybrid threats: Reconceptualizing the evolving character of modern conflict*, Vol. 240. Washington: Institute for National Strategic Studies, National Defense University.

Kříž, Z. (2021). 'The security perception and security policy of the Czech Republic, 1993-2018'. *Defense & Security Analysis*, 37(1), pp. 38-52. DOI: 10.1080/14751798.2020.1831231

Łubiński, P. (2022). 'Hybrid Warfare or Hybrid Threat–The Weaponization of Migration as an Example of the Use of Lawfare–Case Study of Poland'. *Polish Political Science Yearbook*, 51, pp. 1-13. Available at: https://rep.up.krakow.pl/xmlui/bitstream/handle/11716/11174/Lubinski_Hybrid_warfare_or_hybrid_threat_the_weaponization_of_migration.pdf?sequence=1&isAllowed=y (Accessed: 21 February 2022).

Ó Fathaigh, R., Helberger, N. and Appelman, N. (2021). The perils of legally defining disinformation. *Internet Policy Review*, 10(4). DOI: 10.14763/2021.4.1584. 2021

Reuters (2017). Czech "hybrid threats" centre under fire from country's own president. Available at: https://news.trust.org/item/20170104185631-56r53 (Accessed 9 February 2022).

Rychnovská, D. and Kohút, M. (2018). The battle for truth: mapping the network of information war experts in the czech republic. *New Perspectives*, 26(3), 57-87. DOI: 0.1177/2336825X1802600304

Štětka, V., Mazák, J., and Vochocová, L. (2021). "Nobody Tells us what to Write about": The Disinformation Media Ecosystem and its Consumers in the Czech Republic. *Javnost-The Public*, 28(1), pp. 90-109. DOI: 10.1080/13183222.2020.1841381

Hybrid CoE (2022). The European Centre of Excellence for Countering Hybrid Threats, 'Countering Hybrid Threats'. Available at: https://www.hybridcoe.fi/ (Accessed: 21 February 2022).

The Economist (2022). What is hybrid war, and is Russia waging it in Ukraine? Available at: https://www.economist.com/the-economist-explains/2022/02/22/what-is-hybrid-war-and-is-russia-waging-it-in-ukraine (Accessed: 21 February 2022).

Wither, J. K. (2016). Making sense of hybrid warfare. *Connections*, 15(2), pp. 73-87. Available at: https://www.jstor.org/stable/26326441?casa_token=taWB4vxTxu8AAAAA:yeXZdcrKrVlNv0K1eTq0Aie47OVcWgdl0bIHv_2bkiuU9oHV81IgNx8ZqK94Oyk309KNUuxsJaypGD7lfdxFiwiww2JOh2dD5-xE5vSUUE-GRqAuwaCl (Accessed: 21 February 2022).

O Sistema de Defesa Cibernética do Brasil: Dinâmica Civil-Militar e Maturidade Democrática

Jéssica Grassi
Doutoranda no Programa de Pós-Graduação em Relações Internacionais na Universidade Federal de Santa Catarina (UFSC), Brasil. Professora Substituta no Curso de Relações Internacionais da Universidade Federal do Rio Grande (FURG), Brasil. Pesquisadora do Grupo de Pesquisa em Estudos Estratégicos e Política Internacional Contemporânea (GEPPIC). Pesquisadora na REDE CTIDC, no projeto "Pró-Defesa IV: Ciência, Tecnologia e Inovação em Defesa Cibernética e Defesa Nacional".

Danielle Jacon Ayres Pinto
Coordenadora da Pós-Graduação em Relações Internacionais da Universidade Federal de Santa Catarina (UFSC), Brasil. Doutora (2016) em Ciência Política na linha de Política Internacional pela UNICAMP, Brasil. Possui Pós-Doutorado (2019) em Ciências Militares na Escola de Comando e Estado-Maior do Exército (ECEME), Brasil. Coordenadora do Grupo de Pesquisa em Estudos Estratégicos e Política Internacional Contemporânea (GEPPIC/UFSC). Pesquisadora Associada da Rede CTIDC, no projeto "Pró-Defesa IV: Ciência, Tecnologia e Inovação em Defesa Cibernética e Defesa Nacional".

Resumo

O objetivo do artigo é compreender o sistema de defesa cibernética do Brasil a partir da análise da dinâmica civil-militar existente neste setor. Portanto, a pergunta que norteia o desenvolvimento deste estudo é: como caracterizar a dinâmica civil-militar no sistema de defesa cibernética brasileiro? Acreditamos que, com um processo de securitização do ciberespaço em curso no Brasil, a dinâmica civil-militar permanece muito semelhante a tradicional, isto é, com baixa participação e controle civil das Forças Armadas e dificuldades em estabelecer um diálogo efetivo entre civis e militares. Isso traz implicações em termos democráticos para o país e para efetividade da defesa nacional. Ainda assim, os documentos oficiais destacam a necessidade de estabelecer relações mais eficientes e a preocupação com a formação e capacitação de especialistas civis e militares na área.

Palavras-chave: Defesa Cibernética; Forças Armadas; Relação civil-militar.

Abstract
Brazil's Cyber Defense System: Civil-Military Dynamics and Democratic Maturity

The purpose of the article is to understand the cyber defense system in Brazil, by analyzing the civil-military dynamics that exist in this sector. Therefore, the guiding question of the development of this research is: How are civil-military dynamics characterized in the Brazilian cyber defense system? We argue that, with an ongoing cyberspace securitization process in Brazil, the civil--military dynamic remains very similar to the traditional one. That is, there is low civilian participation and control of the Armed Forces and there are difficulties in establishing an effective dialogue between the civilians and the military. This brings implications in democratic terms for the country and for the effectiveness of national defense. Even so, there are officials documents highlighting the need to establish improved relationships and there are concerns about the formation and training of civilians and military experts in this area.

Keywords: *Cyber Defense; Armed Forces; Civil--Military Relations.*

Artigo recebido: 25.07.2022
Aprovado: 05.12.2022
https://doi.org/10.47906/ND2022.163.04

Introdução

As relações civis-militares no Brasil possuem uma história de desequilíbrio, principalmente se comparado com democracias ocidentais consolidadas. No entanto, com o desenvolvimento das novas tecnologias, novos desafios para a segurança e a defesa nacional e as particularidades do ciberespaço, que o tornam uma esfera diferenciada de atuação, torna-se basilar repensar as dinâmicas tradicionais de defesa dos Estados e avançar para uma atuação coordenada entre setor público, privado e academia na área.

Tendo em vista essa discussão, a pergunta que norteia o desenvolvimento deste artigo é: como caracterizar a dinâmica civil-militar no sistema de defesa cibernética brasileiro? Partimos da hipótese de que apesar do discurso acerca da necessidade em estabelecer um diálogo mais estreito entre civis e militares, isso não se evidencia significativamente na prática. Assim, com a securitização[1] do ciberespaço em curso no Brasil, a dinâmica civil-militar ainda se assemelha à tradicional no país, com o baixo controle civil das Forças Armadas. Isso tudo traz implicações em termos democráticos para o país e para efetividade da defesa nacional.

Isso posto, o objetivo geral do presente estudo é analisar as políticas e estratégias de defesa cibernética do Brasil e a dinâmica civil-militar implementada no setor. Para isso, empregamos o método hipotético-dedutivo e a técnica de pesquisa bibliográfica e documental. Desse modo, serão desenvolvidas três seções neste artigo. A primeira seção introduz sobre as relações civis-militares e essa interação historicamente no Brasil a partir de literatura especializada. A seguinte analisa o setor cibernético nos documentos de defesa do Brasil, identificando como estes abordam as relações civis-militares.

A última seção explora os principais mecanismos, ferramentas e/ou programas que estão sendo desenvolvidos para a ciberdefesa de modo a compreender como têm

1 O processo de definição das ameaças à segurança nacional é considerado socialmente e discursivamente construído. A partir disso, pode-se definir três categorias para demarcar uma ameaça: i) não-politizado – o assunto não tem atenção do Estado; ii) politizado – é parte da agenda política do governo, demandando decisões governamentais sobre as atribuições; iii) securitizado – a ameaça é vista como existencial e demanda medidas emergenciais (Buzan; Waever; De Wilde, 1998). No caso do setor cibernético, Hansen e Nissenbaum (2009) propõem: i) hipersecuritização – extensão dos níveis de securitização, devido a capacidade de atingir outros setores; ii) práticas diárias de segurança – discursos englobam constantemente aspectos que atingem o cidadão, assegurando a parceria dos indivíduos para protegerem as redes, deixando a hipersecuritização mais aceitável; iii) tecnificações – despolitização da questão, restringindo-a a opinião dos especialistas em Segurança da Informação e usando-a no discurso político. Desse modo, segundo Lobato e Kenkel (2014), a securitização cibernética envolve um movimento duplo: do político ao securitizado; e do político ao técnico.

ocorrido a interação entres civis e militares e analisar implicações democráticas de uma possível deficiência na dinâmica civil-militar no setor especificamente.

As relações civis-militares: perspectivas teóricas e essa interação no Brasil

Em termos conceituais, algumas definições precisam ser esclarecidas. Militares, ou as Forças Armadas, são definidos por Croissant e Kuehn (2017, p. 3) como "todas as organizações estatais permanentes e seus membros cuja função principal, autorizada por lei, é aplicar poder coercitivo para defender o território do Estado contra ameaças externas"[2]. Civis, por outro lado, são definidos como "todas as organizações e membros não militares do governo e do legislativo com a autoridade para formular, implementar e supervisionar decisões políticas"[3] (Croissant e Kuehn, 2017, p. 3).

As relações civis-militares se caracterizam, segundo os mesmos autores, como "todas as interações entre a liderança das Forças Armadas, por um lado, e as elites políticas não-militares que têm o poder de tomar decisões políticas, por outro"[4]. Portanto, controle civil está relacionado à autoridade dos civis eleitos para decidir sobre as políticas nacionais e implementá-las, assim como delegar determinado poder de decisão e implementação aos militares (Croissant e Kuehn, 2017).

Ao analisar a dinâmica civil-militar de um país deve-se considerar que esta é moldada pela ação e interação entre os agentes civis e militares. Contudo, essas relações não ocorrem em um vácuo histórico, social ou cultural, ou seja, ocorrem dentro de um determinado ambiente estrutural, institucional e ideacional, o qual influencia, restringe ou afeta os interesses, objetivos, ações e interações entre estes agentes. Essas abordagens, que integram argumentos agenciais e estruturais, são chamadas de integrativas (Hunter, 2001; Kuehn e Lorenz, 2011; Pion-Berlin, 2011; Croissant e Kuehn, 2017).

Outro fator relevante diz respeito às influências internacionais, as quais podem afetar a capacidade do controle civil. Sobre isso, Croissant e Kuehn (2017) apontam cinco fatores importantes: os efeitos das ameaças externas; a participação em fóruns

2 Tradução nossa do original: "all permanent state organizations and their members whose primary function, authorized by law, is to apply coercive power in order to defend the territory of the state against external threats."

3 Tradução nossa do original: "are all organizations and non-military members of the government and the legislature with the authority to formulate, implement, and oversee political decisions."

4 Tradução nossa do original: "all interactions between the leadership of the armed forces on the one hand, and non-military political elites who have the power to make political decisions on the other."

ou organizações internacionais; cooperação bilateral entre militares; participação em operações multilaterais de manutenção de paz; e a mudança de pensamento de segurança no pós-Guerra Fria com o surgimento de novas ameaças.

Sobre a relação entre controle civil e efetividade, os estudiosos destacam o efeito positivo do controle mais rígido dos civis sobre assuntos militares, bem como da delimitação precisa do papel e das tarefas das Forças Armadas (Bruneau e Tollefson, 2014; Croissant e Kuehn, 2017). Huntington (1957), por sua vez, ressalta a importância do controle civil objetivo das Forças Armadas, o qual se caracterizaria pela redução do poder dos militares, tornando-os instrumentos do Estado, de forma a garantir a proteção da sociedade e a segurança contra as ameaças externas. Esse controle exigiria, segundo o autor, o reconhecimento da autonomia do profissionalismo militar. Para isso seria necessário o controle social interno, uma ética que definisse os valores e normas do grupo e um sentimento de lealdade e obediência ao poder civil (Huntington, 1957; Oliveira e Soares, 2000).

As relações civis-militares se convertem ao longo dos anos em questão prioritária no que se refere a consolidação política e democrática dos Estados (Martinez e Filgueira, 1993; Bruneau e Matei, 2008; Kuehn e Lorenz, 2011). Nesse sentido, por um lado, cabe determinar o papel desempenhado pelos militares e suas interferências nas instituições políticas e, por outro, pensar as instituições militares como dependentes das estruturas políticas e assegurar o controle civil da corporação militar (Martinez e Filgueira, 1993). Bruneau e Matei (2008) ponderam sobre a necessidade de fortalecer outras instituições de segurança, de modo que haja um trabalho colaborativo com as Forças Armadas nos aspectos relativos à defesa e à manutenção da base essencial para uma consolidação democrática.

Principalmente a partir das mudanças nos campos da segurança e defesa no pós-Guerra Fria, as Forças Armadas não podem mais lidar sozinhas com as novas ameaças à segurança uma vez que garantir a segurança requer a abordagem colaborativa entre vários atores da sociedade, em especial as instituições militares e aos analistas civis (Kümmel e Bredow, 2000; Bruneau e Matei, 2008). Nessa perspectiva, torna-se necessário civis com amplo conhecimento e treinamento em assuntos militares, defesa e estratégia, para a efetiva tomada de decisão sobre as políticas nacionais, sendo essas a força motriz para que o tema não se restrinja ao ator militar que é o braço mais prático dessa relação. Nessa dinâmica mostra-se relevante o papel das universidades (Oliveira e Soares, 2000; Bruneau e Tollefson, 2014). São elas as promotoras do quadro civil na área, mas também, e principalmente, disseminadoras de um conteúdo analítico-crítico que vai dar tanto ao especialista civil como ao militar recursos cognitvos e teóricos para melhor pensar a defesa e com isso fortalecer a democracia.

Todavia, essa relação cooperativa não foi uma constante na região. Com relação às Forças Armadas na América Latina, e no Brasil particularmente, observa-se uma

permanente intervenção destas nos assuntos políticos dos Estados desde seus processos de independência. No entanto, essa situação se acentuou com os golpes e as instaurações das ditaduras militares nos países no século XX (Martinez e Filgueira, 1993). Desde então, o papel das Forças Armadas latino-americana também esteve consideravelmente associado à influência da Doutrina de Segurança Nacional norte-americana e a agenda militar deste país na região (Martinez e Filgueira, 1993; Santos, 2004).

Além disso, com as mudanças do pós-Guerra Fria e o Pós-11 de Setembro de 2001, e o redirecionamento da agenda de segurança hemisférica, as Forças Armadas ficaram sem uma missão clara ou um papel bem definido, nem são identificados objetivamente os inimigos do país. Desse modo, tem sido atribuído às Forças Armadas, muitas vezes, o "papel de polícia", havendo, nessa perspectiva, uma crise de identidade ou crise de missão (Oliveira e Soares, 2000; Santos, 2004). Esse cenário cria no binômio da relação civil-militar na maioria das vezes uma clivagem, que se assenta não na incompatibilidade entre os dois atores, mas sim, na percepção distinta da função precípua que as forças militares tem, criando assim um distanciamento conceitual entre eles que prejudica o fortalecimento da defesa nacional em parâmetros cada vez mais colaborativos entre eles.

Sendo assim, as Forças Armadas acabam sendo demandadas na luta contra o narcotráfico e o crime organizado, para controlar a violência e os distúrbios urbanos e, quando solicitadas, juntam-se às forças de paz das Nações Unidas (Oliveira e Soares, 2000; Santos, 2004). Além disso, não há na Constituição Federal Brasileira uma definição precisa sobre o papel das Forças Armadas, apenas estabelece que estão encarregadas da defesa nacional, de garantir os poderes constitucionais e, se solicitadas, garantir a lei e a ordem (Oliveira e Soares, 2000; Santos, 2004).

Sobre isso, cabe ressaltar que os militares negociaram os termos na transição democrática, mantendo uma ampla gama de prerrogativas institucionais (Martinez e Filgueira, 1993; Hunter, 2001), sendo esta, portanto, uma "transição pactuada" (Oliveira e Soares, 2000, p. 100). Observa-se que os militares desenvolveram um *lobby* eficiente, podendo pressionar os congressistas em questões de seu interesse (Oliveira e Soares, 2000; Santos, 2004). Percebe-se que, no Brasil, as Forças Armadas possuem grande capacidade para "preservar seus interesses institucionais mesmo que numa posição frontalmente contrária aos movimentos e ações internacionais" e, por outro lado, "a incapacidade do poder civil em contrariar os interesses da corporação" (D'Araújo, 2016, p. 50).

Ao longo dos anos, as Forças Armadas continuaram a exercer influência sobre políticas que vão muito além de questões de segurança e defesa – intercalando períodos de maior ou menor ingerência –, principalmente se comparado com outras democracias ocidentais avançadas. Além disso, apesar dos incentivos para diminuírem a influência militar, os líderes políticos evitam antagonizar as Forças Arma-

das (Hunter, 2001) e essa instituição ainda possui enorme autonomia e capacidade de intimidação (Pion-Berlin, 2011).

Somando-se a isso, devido à competição eleitoral, o interesse dos partidos e políticos se direciona a sua sobrevivência, mantendo sua popularidade entre os cidadãos. Por isso, sua posição é apelar aos anseios populares e às demandas principais, sendo pouco discutidas questões relativas à defesa e à segurança internacional (Hunter, 2001). Nesse sentido, o tema da Defesa Nacional também não é discutido pelos candidatos em períodos eleitorais, apenas a segurança interna é objeto de debate público (Santos, 2004).

> Em democracias consolidadas, a sociedade tem um papel ativo na formulação e na implementação da política de defesa. O Congresso Nacional desempenha um papel bastante importante ao supervisionar o processo de tomada de decisão dessa política, enquanto ONGs e grupos de interesse pressionam para que haja transparência ao longo desse processo, participam de debates públicos e encaminham seus interesses por diversos canais aos tomadores de decisão. No Brasil, entretanto, a sociedade como um todo não está interessada na questão da defesa nacional (Santos, 2004, p. 121).

Nessa mesma direção, Oliveira e Soares (2000) defendem que o Congresso Nacional desempenha um papel limitado, ineficiente e mesmo irresponsável no que diz respeito às decisões sobre questões militares e, de modo semelhante, é a atuação da sociedade civil. Para Carvalho (2006), os políticos têm se omitido em relação aos problemas de natureza das Forças Armadas, havendo poucos capacitados para discutir temas militares, de inteligência nacional, de defesa e estratégia. Partindo disso, o autor ressalta que a omissão civil é fator fundamental para a volta de militares ao governo e pondera ser indispensável estimular os estudos de assuntos militares por acadêmicos civis. Todavia, vale ressaltar aqui que a ideia não é promover entre esses atores uma competição na qual disputam a hegemonia pelo tema da defesa na burocracia do Estado. Isso seria altamente prejudicial para o interesse nacional. A proposta é uma simbiose entre esses dois atores, de forma que os civis passem a exercer o seu fulcral papel no estado democrático que é o controle do Estado, onde as forças militares, de suma importância, exerçam um papel de especialistas efetivos, tirando de suas costas o peso das decisões políticas que não cabem a esse ator institucional e, principalmente, não é sua função constitucional no Brasil.

Nessa perspectiva, torna-se essencial o estímulo à "renovação do pensamento militar, a cooperação com as universidades e a relação com a sociedade", a superação da herança da Guerra Fria de "defesa interna", a qual militariza a segurança pública, e o desenvolvimento de "um modelo teórico operacional de defesa do Estado democrático de direito" (Oliveira e Soares, 2000, p. 114).

Importa mencionar que a criação do Ministério da Defesa (MD) no Brasil, em 1999, foi um marco na efetivação de uma estrutura e de instituições que dão uma direção política sobre o poder militar. Isso significou, no plano político, uma "adequação necessária e oportuna para a sedimentação da direção política sobre o poder armado" e, no plano estrutural-organizativo, uma "resposta pertinente à racionalização de recursos e meios de defesa" (Oliveira e Soares, 2000, p. 113).

Apesar disso, para que haja orientação civil neste ministério e, nesse sentido, controle efetivo sobre as Forças Armadas, é necessário que a estrutura organizacional deste não seja predominantemente militar. Portanto, é primordial haver presença decisiva de civis para a formulação e implantação de políticas públicas na área militar, enquanto os militares permanecem com a autonomia institucional para as decisões de nível tático e técnico. Essa divisão é o fundamento para o amadurecimento das relações civil-militares (Oliveira e Soares, 2000) e, portanto, da democracia.

No entanto, como bem menciona Pion-Berlin (2019, p. 1), "às vezes os líderes políticos confiam demais nas forças armadas, cedendo-lhes autoridade excessiva, atribuindo-lhes tarefas e cargos que deveriam ter sido de civis"[5]. O autor defende que nos "países cujos civis têm déficits de longa data no conhecimento de defesa muitas vezes se submetem a oficiais com maiores entendimentos"[6] (Pion-Berlin, 2019, p. 2). Assim, ao longo do tempo, reverter a situação, e retomar o controle pelos civis, torna-se tarefa sensível. Isso porque os civis tornam-se mais dependentes dos militares, os quais podem passar a reivindicar mais atribuições, cargos adicionais, maiores recursos orçamentários pra si, podendo perceber, com o tempo, a delegação civil como uma admissão de incompetência, como se os civis não estivessem à altura da atribuição (Pion-Berlin, 2019).

No caso do Brasil, apesar de algumas afirmações contrárias, tem se observado aumento considerável de civis especialistas em temas de defesa. Ocorre o amadurecimento do campo de pesquisa nas universidades e a academia tem se engajado com as temáticas que antes eram predominantemente dos militares. Existem cursos acadêmicos voltados à área, com participação de civis e militares, as escolas militares têm passado contar com maior participação de civis. Ademais, em 2005, foi criada a Associação Brasileira de Estudos de Defesa (ABED), como também, revistas acadêmicas e diversos projetos e grupos de pesquisas dedicados à àrea.

Adicionalmente, há um alargamento da atuação conjunta entre civis e militares, inclusive devido a própria ampliação das tarefas militares que perpassa as áreas

5 Tradução nossa do original: "sometimes political leaders rely too much on the armed forces by ceding to them excessive authority, assigning them tasks and positions that should have gone to civilians."

6 Tradução nossa do original: "[...] countries whose civilians have longstanding deficits in defense knowledge often defer to officers with greater understandings."

industrial e tecnológica e cria espaços de interação, os quais tem resultado na maior capacitação para ambos os setores (Carvalho, 2006). Além disso, o Ministério da Defesa tem investido na realização de estudos, pesquisas e reflexões com um diálogo entre civis e militares impulsionados, por exemplo, pela Escola Superior de Guerra (ESG) e pelo Instituto Pandiá Calógeras (IPC), organizações diretamente ligadas ao ministério. Fazem parte deste esforço também o Centro de Estudo Político-Estratégico da Escola de Guerra Naval (CEPE-EGN), o Centro de Estudos Estratégicos da Escola de Comando e Estado-Maior do Exército (CEEEx-ECEME) e o Centro de Estudos Estratégicos da Universidade da Força Aérea (CEA-UNIFA) (Brasil, 2020).

Apesar disso, mais do que a simples participação conjunta, deve-se possibilitar a participação harmoniosa. Isso porque há uma complicada interação entre civis e militares em determinados ambientes de discussão conjunta e a necessidade do desenvolvimento de uma cultura da cooperação entre os profissionais militares e civis.

Por fim, diante do desenvolvimento e da difusão de novas tecnologias, há alterações nas dinâmicas de segurança e defesa, assim como deve haver nas relações civis-militares. Conforme apontado por Zekulić, Godwin e Cole (2017, pp. 32, 33 e 35):

> O ambiente de segurança dentro do qual a cooperação civil-militar deve ser construída para aumentar a resiliência nacional representa uma mudança distinta do ambiente dos anos da Guerra Fria. [...] Renovar a resiliência nacional contra ameaças contemporâneas requer uma abordagem intergovernamental e abrangente, revigorando a cooperação civil-militar e criando sistemas de apoio que compreendam as profundas interdependências entre os setores militar, civil e privado. [...] Embora os setores militar, civil e privado possam abordar a resiliência de diferentes ângulos, no ambiente de segurança contemporâneo eles estão se tornando mais interdependentes.[7]

Exigem-se, com isso, modificações na concepção do serviço militar, maior controle civil e maior abertura por parte das Forças Armadas para essa interação cooperativa, uma vez que também são demandados recursos humanos com novas qualifi-

7 Tradução nossa do original: "The security environment within which civil–military cooperation must be built to enhance national resilience represents a distinct shift from the environment of the Cold War years. [...] Renewing national resilience against contemporary threats requires a cross-governmental and comprehensive approach, reinvigorating civil–military cooperation, and creating the support systems that understand the deep interdependencies between the military, civil and private sectors. [...] Although the military, civil and private sectors may approach resilience from different angles, in the contemporary security environment they are becoming more interdependent."

cações. Desse modo, após essas perspectivas teóricas acerca das relações civis e militares e a dinâmica tradicional desenvolvida no Brasil, a seção seguinte apresentará brevemente algumas considerações sobre as dinâmicas de defesa no ciberespaço e analisará os documentos de defesa do Brasil.

O ciberespaço e os documentos de defesa do Brasil

Os avanços tecnológicos, os novos meios e ameaças advindos do espaço cibernético, fazem deste um elemento fundamental ao pensar políticas e estratégias de defesa nacionais. O ciberespaço tem particularidades que o tornam uma esfera diferenciada de atuação e trazem a necessidade de atenção especial dos políticos, estrategistas, estudiosos e profissionais da área da segurança e defesa.

As informações obtidas pelo meio cibernético resultam na possibilidade de ultrapassar esse domínio, podendo trazer ameaças à soberania nacional, uma vez que ataques imprevisíveis, invisíveis e anônimos podem vir a ser direcionados às infraestruturas críticas nacionais (Olson, 2012; Ventre, 2012; Lobato e Kenkel, 2014). Nesse sentido, alerta-se sobre os altos prejuízos e o potencial destrutivo nos campos político, econômico e social, digital e físico, da utilização e aperfeiçoamento dos recursos cibernéticos (Olson, 2012).

O Brasil é o país da América Latina que mais sofreu ataques cibernéticos nos últimos anos, estando entre os que mais sofrem no mundo (Oliveira *et al*., 2017). Nessa perspectiva, com o aumento do número de ataques ao Brasil renova-se constantemente a preocupação acerca das medidas a serem tomadas no âmbito da ciberdefesa e da cibersegurança. Diante da discussão proposta neste artigo, esta seção analisará os principais documentos de defesa do Brasil e como estes preveem a dinâmica civil-militar no que diz respeito às medidas pensadas e adotadas pelo país para a defesa cibernética.

O Livro Branco de Defesa Nacional (LBDN), de 2012[8], salienta que "a ameaça cibernética se tornou uma grande preocupação por colocar em risco a integridade de infraestruturas sensíveis, essenciais à operação e ao controle de diversos sistemas e órgãos diretamente relacionados à segurança nacional" (Brasil, 2012b, p. 69). Desse modo, o setor cibernético passou a ser enquadrado como setor estratégico para a Defesa Nacional, juntamente com o setor aeroespacial e nuclear, ficando sob coordenação do Exército (Brasil, 2012a).

A Estratégia Nacional de Defesa do Brasil (END) salienta que um projeto de defesa forte favorece um projeto consistente de desenvolvimento. Assim, entre outros

8 Atualmente em vigor, uma vez que o documento de 2020 ainda não foi aprovado pelo Congresso Nacional.

fatores, aponta ser indispensável: 1) a independência nacional por meio da capacitação tecnológica autônoma, com o domínio de tecnologias sensíveis; 2) a mobilização de recursos físicos, econômicos e humanos para investir no potencial produtivo do país; e 3) a democratização das oportunidades educativas e econômicas, assegurando a participação popular nos processos decisórios (Brasil 2012a). Ressalta, especificamente:

> [...] a importância de se desenvolver uma política de formação de cientistas, em ciência aplicada e básica, já abordada no tratamento dos setores espacial, cibernético e nuclear, privilegiando a aproximação da produção científica com as atividades relativas ao desenvolvimento tecnológico da BID [Base Industrial de Defesa] (Brasil, 2012a, p. 101).

Assim, estão entre prioridades apontadas no documento: 1) fomentar a pesquisa científica e estruturar a produção de conhecimento na área; 2) incrementar medidas de apoio tecnológico por meio de laboratórios específicos; 3) desenvolver a capacitação para a proteção das infraestruturas estratégicas; e 4) criar a Escola Nacional de Defesa Cibernética (ENaDCiber). O documento ainda incentiva ações no setor cibernético que contemplem a multidisciplinariedade e a dualidade das aplicações, visando a promoção de empregos, aquisição de conhecimentos e o desenvolvimento de soluções nacionais inovadoras (Brasil, 2012a).

A END reitera o comprometimento do país para o fortalecimento de pesquisas científica, por meio da ENaDCiber, de instituições acadêmicas no âmbito do Ministério da Defesa e demais instituições de ensino superior nacionais e internacionais. Ademais, há, no documento, a previsão da criação de uma carreira civil específica para atuar na formulação e na gestão de políticas públicas de defesa nacional. Este estudo deveria ser realizado pelo MD, juntamente com a Casa Civil e o Ministério do Planejamento, Orçamento e Gestão (Brasil, 2012a), todavia, poucos avanços se viram nesse sentido no Brasil nos últimos dez anos.

A Política Cibernética de Defesa (PCD), aprovada no final de 2012, visa coordenar e integrar as ações de defesa cibernética no âmbito do MD no nível estratégico, operacional e tático. Dentre seus objetivos, destacamos: 1) assegurar o uso efetivo do espaço cibernético pelas Forças Armadas e impedir ou dificultar sua utilização contra os interesses da defesa nacional; 2) capacitar e gerir os recursos humanos necessários à condução das atividades do setor cibernético no âmbito do MD; 3) colaborar com a produção do conhecimento de Inteligência; 4) adequar as estruturas de ciência, tecnologia e inovação (CT&I) das três Forças; e 5) implementar atividades de pesquisa e desenvolvimento para atender às necessidades do setor (Brasil, 2012c, p. 13).

O documento também prevê: 1) fomentar o desenvolvimento e o intercâmbio de teses, dissertações e outros trabalhos em instituições de ensino superior civis e mili-

tares de interesse para as atividades cibernéticas; 2) promover o intercâmbio doutrinário, normativo e técnico, com instituições civis e militares; 3) criar um comitê permanente constituído por representantes do MD, de outros ministérios e de agências de fomento, para intensificar e explorar novas oportunidades de cooperação em CT&I; e 4) criar parcerias e cooperação entre os centros de pesquisa e desenvolvimento militares e civis (públicos e privados) (Brasil, 2012c, pp. 15-17).

Para cumprir estes objetivos, dispõe de uma série de diretrizes, entre as quais mencionamos a criação e implantação do Sistema Militar de Defesa Cibernética (SMDC), no qual participariam civis e militares da Marinha, do Exército e da Aeronáutica. O Ministério da Defesa estaria responsável por definir os perfis do pessoal necessário para atuar nas atividades setor cibernético, criar cargos e funções, selecionar o pessoal, civis e militares, com as competências e habilidades necessárias e capacitá-los (Brasil, 2012c).

A partir disso, foi criada a Doutrina Militar de Defesa Cibernética (DMDC), em 2014, a qual aborda aspectos técnicos e operacionais de modo a coordenar as ações militares no âmbito da defesa cibernética (Oliveira *et al.*, 2017). A DMDC frisa que a defesa cibernética é missão das Forças Armadas por ser um componente da defesa nacional. Contudo, diante das peculiaridades do ciberespaço, admite que o cumprimento da missão só será exitoso com "o comprometimento da sociedade como um todo, imbuída do sentimento de responsabilidade individual e coletiva pela proteção das infraestruturas críticas nacionais no Espaço Cibernético". Desse modo, além do MD, deveriam ser inclusos a comunidade acadêmica, os setores público e privado e a base industrial de defesa (Brasil, 2014, p. 25).

Cabe destacar que tais documentos ressaltados costumam ser vagos do ponto de vista de possíveis medidas práticas para implementação dos elementos propostos. Outra situação que vale ser mencionada é que ainda não foi elaborada uma Estratégia Nacional de Defesa Cibernética, o que consiste em uma lacuna no direcionamento estratégico para a área, bem como na articulação entre os diferentes setores civis e militares que, conjuntamente, poderiam avaliar a melhor orientação para o âmbito da defesa cibernética brasileira.

Além desses documentos de defesa, no âmbito da segurança cibernética ressalta-se a formulação do Livro Verde de Segurança Cibernética (LVSC), em 2010, o Marco Civil da Internet, de 2014, e a Estratégia Nacional de Segurança Cibernética (E-Ciber), aprovada em 2020. Esta última se insere no contexto da Política Nacional de Segurança da Informação (PNSI) e da Estratégia Nacional de Segurança da Informação (ENSI)[9] e vinha sendo elaborada desde 2018 pelo Gabinete de Segu-

9 Devido à abrangência da Segurança da Informação, a PNSI indicou que a ENSI "seja construída em módulos, a fim de contemplar a segurança cibernética, a defesa cibernética, a segurança das infraestruturas críticas, a segurança da informação sigilosa e a proteção contra vaza-

rança da Informação (GSI) com a colaboração de diversos órgãos da Administração Pública Federal (APF). Em 2020, também entrou em vigor a Lei Geral de Proteção de Dados Pessoais (LGPD). Porém, esses documentos buscaram no seu escopo uma tecnicidade regulatória que corrobora os pontos vista anteriormente observados nos instrumentos legais primeiramente relatados e negligenciam, novamente, a questão da materialização do papel dos civis – academia e sociedade civil em geral – na formulação e na prática da política de defesa voltada para área cibernética. O preço a se pagar por esse descompasso pode ser alto para o Brasil, pois pode prejudicar a defesa cibernética em si, mas principalmente, relegar o país a um atraso conceitual e prático nessa área que pode ser difícil de recuperar no futuro.

Entretanto, diante da delimitação deste estudo, não cabe aqui aprofundar os aspectos mais específicos relativos à segurança cibernética do país. A partir do apresentado nesta seção, a seguir busca-se compreender o Sistema Militar de Defesa Cibernética e organismos que o constituem. Estes mecanismos, ferramentas e programas são desenvolvidos pelo Ministério da Defesa e pelas Forças Armadas para enfrentar as novas ameaças advindas do ciberespaço e ampliariam, conforme os documentos, a interação civil-militar se comparado com as dinâmicas tradicionais de defesa nacional.

Organismos da defesa cibernética brasileira e a dinâmica civil-militar no setor

A partir das novas dinâmicas impostas pelo espaço cibernético e a necessidade de desenvolvimento de novas abordagens e novas capacidades, tem-se proposto como indispensável a mudança da estrutura das Forças Armadas, maior parceria entre profissionais civis e militares e maior abertura ao diálogo conjunto. Nos documentos analisados na seção anterior, o intercâmbio entre instituições civis e militares, os incentivos à pesquisa e capacitação e novas parcerias foram postos como fundamentais.

A partir do exposto nos documentos de defesa, alguns avanços foram observados na área cibernética e alguns mecanismos e organismos foram sendo implementados, como o Centro de Defesa Cibernética (CDCiber), o Comando de Defesa Cibernética das Forças Armadas (ComDCiber) e a Escola Nacional de Defesa Cibernética (ENaDCiber). Nessa perspectiva, essa seção avança para o entendimento desse

mento de dados." Considerando a segurança cibernética "como a área mais crítica e atual a ser abordada, o Gabinete de Segurança Institucional da Presidência da República elegeu, em janeiro de 2019, a Estratégia Nacional de Segurança Cibernética – E-Ciber como primeiro módulo da Estratégia Nacional de Segurança da Informação, a seu cargo, a ser elaborada" (Brasil, 2020).

sistema de defesa cibernética nacional, ao passo que se busca compreender as dinâmicas civis-militares no setor.

O Sistema Militar de Defesa Cibernética (SMDC) pode ser definido como "um conjunto de instalações, equipamentos, doutrina, procedimentos, tecnologias, serviços e pessoal essenciais para realizar as atividades de defesa no Espaço Cibernético" (Brasil, 2014, p. 25). Cabe a ele assegurar a proteção cibernética do Sistema Militar de Comando e Controle (SMCC[2]), assim como das infraestruturas críticas nacionais (Brasil, 2014).

O SMDC possui quatro níveis de decisão, são eles: 1) o nível político, que abrange a Segurança da Informação e Comunicação (SIC) e a Segurança Cibernética, cujos atores principais são o Gabinete de Segurança Institucional da Presidência da República (GSI-PR) e o Comitê Gestor da Internet no Brasil; 2) o nível estratégico, que abrange a defesa cibernética, a cargo do Estado-Maior Conjunto das Forças Armadas (EMCFA), por intermédio do ComDCiber e demais órgãos de defesa cibernética, dos Centros de Tratamento de Incidentes de Redes (CTIR) e outras instituições parceiras; 3) nível operacional, que abrange ações de guerra cibernética, sob responsabilidade dos Comandos Operacionais e seus Estados-Maiores; e 4) nível tático, abrange as ações de Guerra Cibernética, a cargo das Forças Componentes e o Destacamento Conjunto de Guerra Cibernética (Brasil, 2014).

O órgão central do SMDC é o ComDCiber, o qual foi criado em 2015, vinculado à estrutura regimental do Exército Brasileiro. O ComDCiber é um Comando Conjunto que tem como braço operacional o CDCiber (Lobato e Kenkel, 2015; Amin, 2019; Costa, 2019). O CDCiber foi criado anteriormente ao ComDCiber, ainda em 2010 e "mantém canal técnico para coordenação e integração com os órgãos de interesse envolvidos nas atividades de Defesa Cibernética (CERT.br, CTIR Gov, órgãos de Defesa/Guerra Cibernética das FA, Ministérios, Agências Governamentais, APF e outros)" (Brasil, 2014, p. 26). Segundo Costa (2019), o exercício do CDCiber reúne órgãos civis de diversas áreas estratégicas, experiência importante para a resolução de diversos problemas no espaço cibernético e, inclusive, sendo considerado referência e atuando cooperativa com outros países.

O Centro de Defesa Cibernética do Exército tem como objetivo: a melhoria da capacitação dos recursos humanos; a atualização doutrinária; o fortalecimento da segurança; respostas a incidentes de redes; a incorporação de lições aprendidas; e a proteção contra ataques cibernéticos (Brasil, 2012b, p. 69). Sua implantação visa contribuir "para elevar a segurança e a capacidade de atuar em rede tanto na área militar quanto em diferentes setores do governo e da sociedade" (Brasil, 2012b, p. 209).

Já ENaDCiber foi ativada oficialmente em fevereiro de 2019 – embora desde 2015 funcionada como um núcleo na Estrutura Regimental do Comando do Exército (Sena, 2016) – e tornou-se o braço acadêmico do ComDCiber. A Escola tem estrutura

de ensino dual, civil e militar, e tem como missão "fomentar e disseminar as capacitações necessárias à Defesa Cibernética [...] bem como contribuir com as áreas de pesquisa, desenvolvimento, operação e gestão do assunto e para a melhoria da qualificação da mão de obra nacional para o setor" (Brasil, 2019, s.p.).

No momento, ela oferece cursos na modalidade Ensino a Distância (EaD), tendo oferecidos mais de mil cursos, predominantemente para oficiais militares – o que é apontado como uma situação temporária (Defesa TV, 2019). Nessa perspectiva, sua atuação ainda é consideravelmente limitada, no entanto, se avançar com o proposto na sua criação, pode vir a cumprir um papel importante na aproximação de especialistas civis e militares no setor cibernético.

Vale mencionar também a implantação, em 2013, do Simulador Nacional de Operações Cibernéticas (Simoc), voltado especificamente ao treinamento de militares para combate cibernético. Este é posto como uma ferramenta de ensino, que poderia ser utilizado para capacitar pessoal de qualquer área, podendo oferecer simulações para a academia, por exemplo – porém ainda se percebem restrições nesse sentido (EBC, 2013; Lobato e Kenkel, 2015).

De acordo com Amin (2019), são 5 os pilares da atividade cibernética: 1) inteligência; 2) ciência e tecnologia; 3) operações; 4) doutrina; e 5) as pessoas. Para o General Amin, do ComDCiber, "o ser humano é o maior recurso que nós temos para nos contrapor a essas ameaças", no entanto, o Comando ainda possui um quantitativo muito restrito de pessoal (Amin, 2019, p. 37).

Contudo, percebe-se que a aplicação das diretrizes das políticas e estratégias de defesa cibernética são bastante limitadas, bem como o nível de especialização na comunidade de inteligência, uma das bases para mecanismos de defesa cibernética, está longe de atingir o nível necessário para enfrentar as ameaças atuais (Lobato e Kenkel, 2014). Ademais, há dificuldades no alinhamento entre os organismos e setores civis e militares para o aprimoramento de uma atuação no modelo de tríplice hélice (atuação cooperativa entre setor público, privado e academia) (Pagliari, Ayres Pinto e Viggiano, 2020).

Diante disso, retoma-se o posicionamento de Zekulić, Godwin e Cole (2017, p. 33), os quais defendem que "aumentar a resiliência nacional requer uma abordagem de toda a nação para mesclar recursos, conhecimentos e mecanismos de organizações e órgãos governamentais, comunidades e indivíduos dentro deles"[10].

Tentativas de implementar essa atuação conjunta tem sido observadas em países desenvolvidos. Esse é o caso da França que anunciou o recrutamento de mais 770 especialistas em defesa cibernética, além dos 1100 já planejados, o que resultará em

10 Tradução nossa do original: "Enhancing national resilience requires a whole-of-nation approach to merge resources, knowledge and mechanisms of government organisations and bodies, communities and the individuals within them"

5000 'combatentes cibernéticos' até 2025. O país decidiu aumentar e diversificar seu pessoal recrutando especialistas em tecnologia da informação e redes, mas também linguistas, psicólogos, especialistas em relações internacionais e outras possíveis áreas (Chapleau, 2021; Ministère Des Armées, 2021).

Entre as justificativas estão a crescente multiplicação e a gravidade dos ataques cibernéticos, a necessidade de fortalecer sua defesa cibernética e adquirir conhecimentos aprofundados nas variadas áreas que perpassam os desafios cibernéticos do país. Essa diversificação pode possibilitar uma melhor compreensão em relação às ameaças que o país enfrenta e, consequentemente, desenvolver melhores estratégias de atuação. Como aponta a Ministra das Forças Armadas Francesas, é "essencial [também] ter um conhecimento detalhado dos diferentes ambientes culturais e políticos em que nossos exércitos estão engajados" (Chapleau, 2021; Samama, 2021).

Enquanto isso, no Brasil, ainda não foi estabelecida uma carreira civil no âmbito da defesa nacional, o profissional civil segue sendo a exceção na defesa nacional. Além disso, constata-se um papel protagonista e centralizador dos militares em relação ao setor cibernético em geral, os quais acabam por assumir funções que extrapolam o campo da defesa e adentram o âmbito da segurança cibernética (Solar, 2020; Hurel, 2021), o que demonstra a debilidade das instituições civis em coordenar os processos na área.

Cabe também mencionar que no governo de Jair Bolsonaro – Capitão reformado do Exército – conta-se com uma participação massiva de militares da ativa no executivo, principalmente do Exército. Em 2019 houve um acréscimo de mais de 13% de integrantes das Forças Armadas em comparação com o ano anterior. Os militares se concentram principalmente no Gabinete de Segurança Institucional (GSI) – organismo que gerencia o nível político do setor cibernético do país, e é, particularmente, responsável pelas medidas no âmbito da Segurança Cibernética –, na Advocacia Geral da União (AGU) e Ministério de Minas e Energia (MME). (Shinohara, 2019).

Já os militares da reserva são os que ocupam cargos no alto escalão. O número de ministros militares supera três dos cinco presidentes da ditadura militar (Emílio Garrastazu Médici, Ernesto Geisel e João Figueiredo) (Barrucho, 2020). Ademais, desde 2016 o Ministério da Defesa é chefiado por militares da reserva e, conforme mencionado anteriormente, são necessárias uma orientação civil e uma estrutura organizacional predominante civil neste ministério para que se observe um efetivo controle civil sobre as Forças Armadas. O aumento de militares em cargos do Executivo, em esferas que deveriam ser resguardadas a civis, resulta em maior poder de ação e decisão destes e o transbordamento de seu papel, inclusive no setor cibernético.

Isso é visto com grande preocupação, uma vez que as evidências históricas indicam que o efetivo controle civil das Forças Armadas é considerado importante para a

manutenção das democracias e amadurecimento das relações civis-militares, como foi ressaltado na primeira seção deste artigo. Para Harig (*apud* Barrucho, 2020, s. p.), "já é problemático ter vários militares da reserva no governo, mas convidar os da ativa afeta diretamente as Forças Armadas como instituição e evidentemente ridiculariza seu suposto papel 'não partidário' na democracia brasileira".

Como pondera Pion-Berlin (2019, p. 5), para que os ministérios façam seu trabalho, eles devem ter uma forte preponderância de diretores, gerentes e funcionários civis", caso contrário, pode representar "riscos para o governo democrático", uma vez que "o objetivo dos ministérios da defesa é preparar as Forças Armadas para servir aos objetivos políticos do governo, e não o contrário". Segundo o autor,

> [...] a superdelegação de postos a soldados também traz problemas de dependência, à medida que os civis se acostumam com o manejo militar da política de defesa. Uma dependência excessiva dos militares para preencher postos pode persuadir os civis de que as forças armadas fornecem a única solução viável e o farão no futuro, normalizando completamente seu domínio.[11] (Pion-Berlin, 2019, p. 1).

Observa-se também, a partir dos documentos, mecanismos e programas analisados, um processo de securitização do ciberespaço em curso no Brasil. Porém Lobato e Kenkel (2014) defendem que este ainda necessita de maior reconhecimento e atenção para se concretizar. Segundo os autores, diante dos discursos acentuados sobre as ameaças à segurança nacional que surgem no ciberespaço e as previsões catastróficas de ataques às infraestruturas críticas, há uma ampliação do processo de securitização deste ambiente.

Assim, com o objeto securitizado, haveria a possibilidade de legitimar meios extraordinários de resolução, podendo fazer uso de legislação de emergência, mobilizando as Forças Armadas ou outros meios. Isso poderia gerar consequências na política pública e nos gastos, bem como uma resposta militar exagerada poderia afetar os direitos básicos dos cidadãos (Muggah, Glenn e Diniz, 2014; Solar, 2020).

Solar (2020) defende que "militarizar o ciberespaço em ambientes políticos e políticos frágeis pode se tornar um tanto arriscado para o governo democrático", assim como, "casar a proteção do espaço digital com forças armadas altamente politizadas pode se tornar um desafio ao tentar configurar uma Internet segura e igualitária".

De acordo com Muggah, Glenn e Diniz (2014) a abordagem securitizada do tema, o papel de liderança dado às Forças Armadas na proteção do ciberespaço, com

11 Tradução nossa do original: "[...] the overdelegation of posts to soldiers also invites problems of dependency, as civilians grow accustomed to the military handling defense policy. An overreliance on the military to fill posts can persuade civilians that the armed forces provide the only viable solution and will do so well into the future, thus completely normalizing their dominance."

grande parte dos investimentos e capacitação cibernética direcionados aos militares, demonstra a busca pela atribuição de um novo papel as Forças Armadas, de modo a ampliar seu protagonismo no novo cenário de defesa e segurança internacional. Esses investimentos, ainda assim, são ínfimos comparados ao que o setor, no geral, necessita, além de muito pouco realmente destinado ao desenvolvimento de tecnologia e capacitação de pessoal.

Considerações finais

O presente artigo teve por objetivo caracterizar as relações civis-militares no sistema de defesa cibernética do Brasil, analisando as políticas e as estratégias propostas pelo país e discutindo a importância de relações civis-militares equilibradas para a maturidade da democracia brasileira. Partiu-se da percepção de que há um acentuado discurso nos documentos oficiais em relação à busca pelo estabelecimento de um avançado diálogo e uma efetiva cooperação entre instituições e atores civis e militares no setor cibernético, a partir da acertada compreensão de que o setor cibernético exige novas abordagens e profissionais com novas características e capacidades diversas. No entanto, defendeu-se que a dinâmica civil-militar no setor permanece muito semelhante à tradicional, ou seja, com baixo controle civil das Forças Armadas e relações civis-militares que precisam ser aprimoradas.

Desde que o setor cibernético foi considerado prioritário para a defesa do país, este vem se destacando nas preocupações da defesa nacional, buscando-se identificar os principais desafios, potencialidades e meios para a redução das deficiências nos sistemas de segurança e defesa. Desde então, alguns projetos e organismos tomaram forma, como o SMDC, o CDCiber e o ComDCiber, a ENaDCiber e o Simoc.

No entanto, ao explorar a atuação brasileira no campo da defesa cibernética, ressaltam-se as vulnerabilidades e desafios presentes, a necessidade de maior atenção e aporte financeiro, um controle civil objetivo para o setor, bem como maiores incentivos a pesquisadores e especialistas civis, de modo a contribuir ativamente nos projetos que vêm sendo desenvolvidos pelo MD e pelas Forças Armadas. Exige-se o fortalecimento de um modelo de atuação em rede de modo a criar uma proteção interconectada e que torne possível uma mobilização nacional mais eficiente no setor, ampliando a atuação em tríplice hélice (Pagliari, Ayres Pinto e Viggiano, 2020). Isso poderia garantir mais efetividade a esse domínio, desenvolvimento de pesquisas, tecnologias e ferramentas avançadas para a área.

Sobre isso, cabe mencionar que tem se observado o amadurecimento do campo de pesquisa nas universidades, a academia tem se engajado com as temáticas que antes eram predominantemente dos militares e há um aumento de pesquisas de qualidade sobre cibernética sendo feitas nessas instituições. Esse é um fator funda-

mental visto que são necessários civis com amplo conhecimento e treinamento em assuntos militares, defesa e estratégia, para uma efetiva tomada de decisão sobre as políticas nacionais de defesa

A preocupação na capacitação de recursos humanos e o incentivo à parceria e colaboração de civis são observados nos documentos de defesa nacional, no entanto, ainda carecem de maior desenvolvimento na prática. A dinâmica civil-militar no quesito defesa cibernética permanece como a desenvolvida tradicionalmente, baixo controle civil,pouca discussão entre os políticos, além da falta de materialização da atuação da academia, e da sociedade civil em geral, na formulação e na prática da política de defesa voltada para área cibernética. Permanece a dificuldade de se estabelecer uma interação harmoniosa e efetiva entre civis e militares em determinados ambientes de discussão conjunta e há a necessidade de melhor desenvolvimento de uma cultura de cooperação entre os profissionais de ambos os setores.

Ademais, como ainda não foi estabelecida uma carreira civil no âmbito da defesa nacional, o profissional civil segue sendo a exceção na esfera, apesar do crescente interesse por parte de acadêmicos, pesquisadores e outros profissionais na área. Com isso, acredita-se que o país está perdendo oportunidades de intercâmbio importantes para o desenvolvimento do setor cibernético e utilizando de forma precária o material humano e analítico que, principalmente, as universidades disponibilizam para pensar e atuar na defesa nacional.

A esse cenário soma-se o aumento considerável de militares em cargos executivos do governo, sendo o Ministério de Defesa chefiado desde 2016, após o impeachment da Presidente Dilma Roussef, por militares da reserva, o que não ocorria desde a redemocratização pós-ditadura militar e posterior criação do ministério da defesa no governo de Fernando Henrique Cardoso. Tudo isso leva ao desequilíbrio nas relações civil-militares do país e, especificamente, no setor cibernético. As relações civis-militares de um país são diretamente relacionadas com a estabilização democrática e a efetividade da sua defesa nacional, conforme ressaltados pelos autores da primeira seção do artigo.

Nesse sentido, a área da defesa cibernética exige novas abordagens estratégicas, com profissionais capazes de atuar e compreender a multidimensionalidade dos desafios do ciberespaço – como já vem sendo observado em países mais desenvolvidos. A falta dessa pluralidade – além dos demais fatores mencionados anteriormente – indica que o setor da defesa cibernética brasileira ainda não está totalmente preparado para lidar com os novos desafios provenientes do ciberespaço, permanecendo amarrado às estratégicas tradicionais de defesa. Nesta perspectiva, a ENaDCiber também poderá cumprir um papel central na dinâmica civil-militar no setor cibernético, desde que cumpra com o proposto na sua criação e supere as barreiras identificadas ao longo do artigo nas relações entre civis e militares.

Referências

AMIN, Guido. Setor Estratégico Cibernético. In: RAMOS, Carlos Eduardo Franciscis, *et al.* (Org.), *XXI Ciclo de Estudos Estratégicos – Ciberespaço: a nova dimensão do campo de batalha*, pp. 30-44, jul., 2019.

BARRUCHO, Luís. Brasil de Bolsonaro tem maior proporção de militares como ministros do que Venezuela; especialistas veem riscos. *BBC News Brasil*, 26 de fevereiro de 2020. Disponível em: https://www.bbc.com/portuguese/brasil-51646346. Acesso em: 01 mar. 2020.

BRASIL, Ministério da Defesa do. *Escola Nacional de Defesa Cibernética é inaugurada em Brasília.* Notícia. Brasília, 11 de fevereiro de 2019. Disponível em: https://www.defesa.gov.br/noticias/52690-escola-nacional-de-defesa-cibernetica-e-inaugurada-em-brasilia. Acesso em: 28 fev. 2020.

BRASIL, Ministério da Defesa do. *Estratégia Nacional de Defesa*. Brasília, 2012a. Disponível em: https://www.defesa.gov.br/arquivos/2012/mes07/end.pdf. Acesso em: 21 fev. 2020.

BRASIL, Ministério da Defesa do. *Estudos estratégicos.* Disponível em: https://www.defesa.gov.br/ensino-e-pesquisa/estudos-estrategicos. Acesso em: 21 fev. 2020.

BRASIL, Ministério da Defesa do. *Doutrina Militar de Defesa Cibernética.* Brasília, 2014. Disponível em: https://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_2014.pdf. Acesso em: 28 fev. 2020.

BRASIL, Ministério da Defesa do. *Livro Branco de Defesa Nacional.* Brasília, 2012b. Disponível em: https://www.defesa.gov.br/arquivos/2012/mes07/end.pdf. Acesso em: 28 fev. 2020.

BRASIL, Ministério da Defesa do. *Política Cibernética de Defesa.* Brasília, 2012c. Disponível em: https://www.defesa.gov.br/arquivos/File/legislacao/emcfa/publicacoes/md31_p_02_politica_cibernetica_de_defesa.pdf. Acesso em: 28 fev. 2020.

BRUNEAU, Thomas C.; MATEI, Florina Cristiana. Towards a new conceptualization of democratization and civil-military relations. *Democratization*, vol. 15, n.º 5, pp. 909-929, 2008.

BRUNEAU, Thomas C.; TOLLEFSON, Scott D. Conclusion. In: BRUNEAU, Thomas C.; TOLLEFSON, Scott D. (Org.), *Who Guards the Guardians and How: Democratic Civil-Military Relations.* Austin: University of Texas Press, 2006.

BUZAN, Barry; WAEVER, Ole; DE WILDE, Jaap. *Security: A New Framework for Analysis.* Boulder: Lynne Rienne, 1998.

CARVALHO, José Murilo de. *Forças Armadas e Política no Brasil*, 2.ª edição. São Paulo: Editora Todavia, 2006.

CHAPLEAU, Philippe. 770 nouveaux cyber-combattants vont être recrutés par les armées. *Journal Ouest-France*, setembro de 2021. Disponível em: https://www.ouest-france.fr/

politique/defense/770-nouveaux-cyber-combattants-vont-etre-recrutes-par-les-armees-bfdb59dc-109e-11ec-9056-0987937f47bd. Acesso em: 21 nov. 2021.

COSTA, Alan Denilson Lima. Centro de Defesa Cibernética. In: RAMOS, Carlos Eduardo Franciscis, *et al.* (Org.), *XXI Ciclo de Estudos Estratégicos – Ciberespaço: a nova dimensão do campo de batalha,* pp. 88-98, jul., 2019.

CROISSANT, Aurel; KUEHN, David. Introduction, pp. 1-21. In: CROISSANT, Aurel; KUEHN, David (Ed.), *Reforming civil-military relations in new democracies: Democratic control and military effectiveness in comparative perspectives*. Cham: Springer, 2017.

D'ARAÚJO, Maria Celina Soares. A persistente primazia política da corporação militar. *Revista Brasileira de Estudos de Defesa*, vol. 3, n.º 2, pp. 41-54, jul./dez. 2016.

DEFESA TV. *Escola Nacional de Defesa Cibernética será base de formação para militares na área de segurança de dados.* 22 de maio de 2019. Disponível em: https://www.defesa.tv.br/escola-nacional-de-defesa-cibernetica-sera-base-de-formacao-para-militares-na-area-de-seguranca-de-dados/. Acesso em: 02 mar. 2020.

EBC. Exército apresenta Simulador Nacional de Operações Cibernéticas. Empresa Brasil de Comunicação (EBC), 22 de janeiro de 2013. Disponível em: http://www.ebc.com.br/noticias/brasil/2013/01/exercito-apresenta-simulador-nacional-de-operacoes-ciberneticas. Acesso em: 28 fev. 2020.

FERREIRA, Juliana Aguiar de Barros. *A questão cibernética nas relações entre os Estados: uma nova forma de projeção de poder na atualidade*, pp. 121. Dissertação de Mestrado em Estudos Estratégicos da Defesa e da Segurança, Instituto de Estudos Estratégicos, Universidade Federal Fluminense, Niterói, 2017.

GONZALES, Selma Lúcia de Moura; PORTELA, Lucas Soares. A geopolítica do espaço cibernético sul-americano: (in) conformação de políticas de segurança e defesa cibernética? *Austral: Revista Brasileira de Estratégia e Relações Internacionais*, Porto Alegre, vol. 7, n.º 14, pp. 217-241, jul./dez., 2018.

HANSEN, Lene; NISSENBAUM, Helen. Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly,* vol. 53, pp. 1155-1175, 2009.

HUNTER, Wendy. Reason, Culture, or Structure? Assessing Civil-Military Dynamics in Brazil. In: PION-BERLIN, David (Ed.), *Civil-military relations in Latin America: New analytical perspectives.* Chapel Hill: University of North Carolina Press, 2001.

HUNTINGTON, Samuel P. *The Soldier and the State: The Theory and Politics of Civil-Military Relations.* Cambridge, MA: Harvard University Press, 1957.

HUREL, Louise Marie. *Cibersegurança no Brasil: uma análise da estratégia nacional.* Instituto Igarapé, AE 54, abr., 2021.

KUEHN, David; LORENZ, Philip. Explaining civil–military relations in new democracies: Structure, agency and theory development. *Asian Journal of Political Science*, vol. 19, n.º 3, pp. 231-249, 2011.

KÜMMEL, Gerhard; BREDOW, Wilfried von. *Civil-Military Relations in an Age of Turbulence: Armed Forces and the Problem of Democratic Control.* Sozialwissenschaftliches Institut der Bundeswehr, 2000.

LOBATO, Luísa Cruz; KENKEL, Kai Michael. Discourses of cyberspace securitization in Brazil and in the United States. *Revista Brasileira de Política Internacional*, vol. 58, n.º 2, pp. 23-43, 2015.

MARTINEZ, Ismael Crespo; FILGUEIRA, Fernando. La intervención de las Fuerzas Armadas en la política latinoamerica. *Revista de Estudios Políticos*, n.º 80, abr./jun., 1993.

MINISTÈRE DES ARMÉES. FIC 2021: Florence Parly annonce le recrutement de 770 cyber-combattants supplémentaires d'ici à 2025. *Délégation à l'information et à la communication de la Défense (DICoD)*, setembro de 2021. Disponível em: https://www.defense.gouv.fr/actualites/articles/fic-2021-florence-parly-annonce-le-recrutement-de-770-cyber-combattants-supplementaires-d-ici-a-2025. Acesso em: 21 nov. 2021.

MUGGAH, Robert; GLENN, Misha; DINIZ, Gustavo. Securitização da cibersegurança no Brasil. *Cadernos Adenauer* XV, n.º 4, pp. 69-109, 2014.

OLIVEIRA, Eliézer Rizzo de; SOARES, Samuel Alves. Brasil: Forças Armadas, direção política e formato institucional, pp. 98-125. In: D'ARAUJO, Maria Celina; CASTRO, Celso. *Democracia e Forças Armadas no Cone Sul.* Rio de Janeiro: Editora FGV, 2000.

OLIVEIRA, Marcos Aurelio Guedes; PAGLIARI, Graciela de Conti; MARQUES, Adriana A.; PORTELA, Lucas Soares; FERREIRA NETO, Walfredo Bento. *Guia de defesa cibernética da América do Sul.* Recife: Ed. UFPE, 2017.

OLSON, Soren. "Treino de Sombra": A Guerra Cibernética e o Ataque Econômico Estratégico. *Military Review*, pp. 73-83, set./out., 2012.

PION-BERLIN, David. Delegation or Dereliction? When Governments Assign Too Many Defense Posts to Military Officials. *Democracy and Security*, vol. 16, n.º 1, pp. 81-96, 2019.

PION-BERLIN, David. The Study of Civil-Military Relations in New Democracies. *Asian Journal of Political Science*, vol. 19, n.º 3, pp. 222-230, 2011.

SAMAMA, Pascal. Recherche Cyber-Combattants: L'armée Annonce 770 Recrutements Supplémentaires. *BFM Business*, setembro de 2021. Disponível em: https://www.bfmtv.com/economie/recherche-cyber-combattants-l-armee-annonce-770-recrutements-supplementaires_AN-202109080375.html. Acesso em 21 nov. 2021.

SANTOS, Maria Helena de Castro. A Nova Missão das Forças Armadas Latino-Americanas no Mundo Pós-Guerra Fria: o caso do Brasil. *Revista Brasileira de Ciências Sociais*, vol. 19, n.º 54, 2004.

SENA, Danielly Alcina Freitas de. *Ciberdefesa: estrutura de defesa cibernética brasileira*, pp. 58. Monografia, Graduação em Relações Internacionais. Centro Universitário Tabosa de Almeida, Caruaru, 2016.

SILVA, Júlio Cezar Barreto Leite da. Guerra cibernética: a guerra no quinto domínio, conceituação e princípios. *Revista da Escola de Guerra Naval,* Rio de Janeiro, vol. 20, n.º 1, pp. 193-211, jan./jun., 2014.

SINGER, Peter Warren; FRIEDMAN, Allan. *Cybersecurity and Cyberwar: What Everyone Needs to Know.* Oxford University Press. 1.ª ed., jan., 2014.

SHINOHARA, Gabriel. Número de militares da ativa no governo federal cresce 13% com Bolsonaro. *O Globo,* 5 de agosto de 2019. Disponível em: https://oglobo.globo.com/brasil/numero-de-militares-da-ativa-no-governo-federal-cresce-13-com-bolsonaro-23854701. Acesso em: 01 mar. 2020.

SOLAR, Carlos. Cybersecurity and cyber defence in the emerging democracies. *Journal Of Cyber Policy*, vol. 3, n.º 1, 2020.

VENTRE, Daniel. Ciberguerra. In: MINISTERIO DE DEFENSA. *Seguridad global y potências emergentes em um mundo multipolar.* XIX Curso Internacional de Defensa. Espanha: Academia General Militar; Universidad Zaragoza, 2012.

ZEKULIĆ, Vlasta; GODWIN, Christopher; COLE, Jennifer. Reinvigorating Civil–Military Relationships in Building National Resilience. *The RUSI Journal*, vol. 162, n.º 4, pp. 30-38, 2017.

Regulating States Cyber-Behaviour: Obstacles for a Consensus

Marcelo Malagutti
Doutor em Ciências Militares pela Escola de Comando e Estado-Maior do Exército (ECEME). Mestre em Estudos de Guerra pelo King's College London. Pesquisador Sênior do Instituto Vegetius.

Abstract

What are the leading obstacles to reaching a consensus on international norms that regulate state-sponsored cyber-offences? This type of operation increases swiftly, whilst issues related to international law go unnoticed, are poorly understood, or are manipulated, clouding the debate on norms of international conduct in cyberspace. This article analyses the main obstacles to regulating such cyber--offences. It argues that the main difficulties concern statecraft and state power promotion, not novelty or innovation speed, ideological or technological issues, as usually claimed. The analysis encompasses the applicability of the current rules of armed conflicts to the cyberspace context, the perspectives and positions regarding multilateral conventions, the option for bilateral or regional agreements and the *normalisation* of some cyber-activities as means of influencing consuetudinary law. It is shown that some nations advocate for maintaining the *status quo* that favours them, whilst others insist on the need for specific regulations.

Keywords: International Norms; Cyber--Behaviour; Interstate Conflicts.

Resumo
Regulação do Comportamento Cibernético dos Estados: Obstáculos para um Consenso

Quais os principais obstáculos para um consenso sobre normas internacionais que regulem as ciberofensas patrocinadas por Estados? Esse tipo de operação cresce rapidamente, enquanto questões relacionadas ao direito internacional passam despercebidas, são mal compreendidas ou manipuladas, ofuscando o debate sobre normas internacionais de conduta no ciberespaço. Este artigo analisa os principais óbices para essa regulação. Argumenta que as principais dificuldades dizem respeito ao estadismo e incremento do poder estatal, e não à novidade ou à velocidade da inovação, questões ideológicas ou tecnológicas, como comumente se afirma. A análise engloba a aplicabilidade das regras atuais de conflitos armados ao contexto cibernético, as perspectivas e posições relativas às convenções multilaterais, a opção por acordos bilaterais ou regionais e a normalização de algumas ciberatividades como meio de influenciar o direito consuetudinário. Mostra-se que algumas nações defendem a manutenção do status quo que as favorece, enquanto outras insistem na necessidade de regulamentações específicas.

Palavras-chave: *Normas Internacionais; Comportamento Cibernético; Conflitos Inter*estatais.

Artigo recebido: 25.07.2022
Aprovado: 12.12.2022
https://doi.org/10.47906/ND2022.163.05

Introduction

In February 2018, the UN Secretary-General expressed twice his concern about the absence of specific international norms to regulate cyber conflicts. He repeatedly used the words *cyberwar* and *cyberattacks* and stated that 'episodes of cyber warfare between states already exist', that 'there is no regulatory scheme for that type of warfare' and that 'we have not yet been able to discuss whether or not the Geneva Conventions apply to cyberwar or whether or not international humanitarian law [IHL] applies to cyberwar' (Guterres, 2018; Khalip, 2018).

What are the obstacles to reaching a consensus on international norms regulating state-sponsored cyber-offences? For this article, these offences consist of more 'peacetime' (or even 'grey zone') operations, such as intelligence gathering (either surveillance or espionage), coercion and influence cyber operations, and more traditional military objectives, such as power projection, area denial, disruption and force multiplier (Malagutti, 2016). Accusations of these operations increase swiftly (Hollis et al., 2020; Nathan and Scobell, 2020). The article analyses recent initiatives on the international regulation of interstate activities in cyberspace and the difficulties in reaching a consensus on common rules. Arguments used in various initiatives are analysed, based on official documents, and academic and international news articles, in an attempt to identify different perspectives. The research deconstructs the arguments, usually found in official speeches and academia, that the problem stems from ideological, technological, novelty or speed of innovation issues. It concludes that the difficulty in regulating cyberspace is exclusively geopolitics, as usual, in its sense of the study of spaces in international politics and the production of knowledge to subsidise statecraft and promote the power of states (Tuathail and Agnew, 1992). Subjacent to the arguments repeatedly used by different countries in multilateral forums, there is a geopolitical struggle; while western powers try to maintain the *status quo* of the technology gap that favours them, there is firm resistance on the part of their opponents to buy time to organise their internal environments and to limit the disadvantages and risks posed to them by this gap.

On the Foundations of International Laws Development

Article 38 of the statute of the International Court of Justice (ICJ) lists the sources of international law. International conventions are the first, establishing rules expressly recognised by signatory States. Then, there is international custom, as evidence of a general practice, accepted as law, and 'general legal principles recognised by civilised nations'. In another group, as subsidiary means, are judicial decisions and

the doctrine 'of the most qualified lawyers from different nations' (UN, 1945). Nevertheless, the 'advent, over the last decades, of new actors at the international level, has contributed to expanding how international law has come to manifest itself', and Article 38 'never intended to constitute a peremptory and exhaustive formula from the sources of international law, but only as a guide to the activity of the International Court' (Cançado Trindade, 2017).

Although not expressly written, customary law (international customs) is binding similarly to treaties. It is consolidated under the influence of two elements: one objective, which consists of practice (the *usus*); and another subjective, which consists of the belief that the action was taken in the form of an obligation (the *opinio juris*) (Schmitt and Vihul, 2014). Despite the large number of international treaties signed in recent decades, customary law remains relevant because even nations that are not signatories to certain treaties generally follow them. For example, even though the USA and Israel are not part of the 1977 Additional Protocols to IHL, they generally respect its rules (Schmitt and Vihul, 2014). In the absence of international conventions, States that manage to establish (or demonstrate) the existence of customs, an international practice, or even create specific doctrines, may influence international regulation in the future. As will be seen, such a future is not necessarily a distant one, and some States are endeavouring to seek to meet conditions for this.

On the (False) Novelty of 'Cyber-Things'

A justification frequently used for the absence of a legal *corpus* suitable for cyberspace refers to the novelty of technologies and their use. The adequacy of the International, political, and legal systems to new technologies often comes after a long time of assimilation; thus, considering the novelty of cyber-activities, few treaties deal specifically and directly with the topic (Toffler, 1991; Schmitt and Vihul, 2014). Similarly, Joseph Nye (Nye, 2018) argues that the first international cooperative agreements of the nuclear era took more than two decades to be signed, and that if cyberspace is considered 'not since its creation in the early 1970s', but from 'its dissemination since the late 1990s', then it would be taking a similar term. Note the proposed 'adjustment', cutting almost three decades (from the early 1970s to the late 1990s) to corroborate his comparison with nuclear agreements.

Despite, typical examples of international 'cyber-treaties' are the 1992 Convention and Constitution of the International Telecommunications Union (ITU) and the 1992 International Telecommunications Regulations, the 2001 Convention on Cybercrime (the Budapest Convention), its 2006 Additional Protocol, and the 2008 Shanghai International Cooperation Organization Information Security Agreement

(Schmitt and Vihul, 2014). It shall be noted that, among the examples cited, the 1992 Conventions are almost three decades old, while the Budapest Convention on Cybercrime dates from nearly two decades. Besides, the first known case of military technology cyber-theft from American universities by foreign agents occurred already in 1989 (Stoll, 1990). Thus, iconic cases started in the early 1990s, as well as the negotiation of international norms. Hence, 'neither cyber-conflict nor legal arguments about it can be remotely described as new concepts' (Giles and Monaghan, 2014). Therefore, the argument of novelty does not prosper.

Moreover, historically, international consensus is achieved quickly in other regulatory contexts, such as that of contagious diseases; in the severe acute respiratory syndrome (SARS) epidemic, the World Health Organization issued norms, both binding and non-binding, to allow the control of the spreading virus (Finnemore and Hollis, 2016; Fidler, 2003). In 2005 these norms were consolidated under the new International Health Regulations (IHR) (Nunes, 2017). The example of the 'immediate customary law' also weighs against the novelty argument. In 1963, the UN General Assembly approved the Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space, without any previous regulation, or even tradition, based only on the tacit agreement between the two only relevant space actors of the time, the USA and the USSR (Cançado Trindade, 2017). That debate reflected divergent positions between the two superpowers as to the best regulatory alternative (as it happens in the case of the cyber-norms, indeed), but a 'pragmatic' agreement was achieved:

> [...] while the then USSR preferred a treaty, the USA insisted on a General Assembly resolution, a formula that the USSR was finally persuaded to accept given the complicated and politically uncertain procedure of concluding treaties under USA constitutional law (Cançado Trindade, 2017).

The International Committee of the Red Cross (ICRC) stated in a position paper that the ICJ's Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons recalled that the established principles and rules of IHL applicable in armed conflict apply 'to all forms of warfare and to all kinds of weapons', including 'those of the future' (ICRC, 2019). Therefore, for the ICRC, any new law must comply with those principles.

Whilst the novelty argument does not subsist, a genuine obstacle to the consensus regards the terminology adopted. In international law, it can qualify or disqualify the application of a particular norm. The term cyberwar could have a different receptivity if replaced by *cyber-armed conflict*, or even *conflict with cyber weapons*. In the UN Charter, the word *war* appears only in the preamble, whether the Geneva Conventions adopted the generic expression *international armed conflicts*, due to 'the large number of wars that were not considered as such' (Pereira, 2010).

Another conflicting term among the legal community is attack. *Armed attack* is a legal term established in *jus ad bellum* and IHL. The term is defined in Article 49 of the Additional Protocol to the Geneva Conventions, as consisting of acts of violence against an opponent, both offensive and defensive. The definition of *attack* lies at the heart of IHL; many of the bans are defined in terms of the ban on attacks, the paradigmatic example being that of attacks on civilians or civilian objects (Schmitt and Vihul, 2014). However, there is no widely accepted definition of what a cyberattack is. Definitions vary from 'unwelcome attempts to steal, expose, alter, disable or destroy information through unauthorized access to computer systems' to 'a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization' or actions that 'aim to damage or gain control or access to important documents and systems within a business or personal computer network' (IBM, n.d.; CISCO, n.d.; Microsoft, n.d.)

On the Distinctive Perspectives Regarding Cyberspace and Its Regulation

Two opposing views concentrate the clash over the regulation of States' behaviour in cyberspace. 'Western democracies', mainly the USA and its closest allies, push for a more open Internet concerning individual freedom of expression, while others, such as Russia and China, insist on the importance of sovereign control of cyberspace (Nye, 2018). Nonetheless, there is controversy even on the very nature of cyber-conflicts. The USA understands cybersecurity as the protection of hardware, software and information. Conversely, China and Russia favour the concept of 'information security', which allows the State to control online content to preserve the stability of their regimes (Grigsby, 2017). Such differences, in practice, have been the 'apple of discord' that hampers the consolidation of international law on state-sponsored cyber-offences.

A superficial analysis of the official arguments would indicate that the western powers defend individual rights and free business in cyberspace, the very foundations of the creation of the Internet itself, whilst Russians and Chinese aim at surveilling their citizens and protecting their regimes. This antagonism is impregned with the view of the 'Western' liberal world order implemented after WWII under the leadership of the United States (Barrinha and Renard, 2020). Such a simplification hides other relevant aspects and makes other countries' positions somewhat ambiguous. Brazil, for instance, has internal laws that largely reinforce net neutrality and the protection of individual privacy, but resists the USA diplomatic line regarding international regulation. In what starts to be called 'post-liberal order', the 'liberal-order' is challenged not only by the China-Russia-led group, but also by

the then U.S. President Trump's view of multilateralism and his commercial war on China; it is also confronted by opinions expressed by the Hungarian, Polish and Brazilian governments (Barrinha and Renard, 2020).

The Huawei case exemplifies illiberal actions promoted by a post-liberal West. The USA accuses Huawei, the world leader in 5G telephony, of having obscure connections with Chinese intelligence. The USA argues that it prefers the use of equipment from the Swedish Ericsson and Finnish Nokia, although more expensive, and personalities of the Trump Administration have even suggested the acquisition of the control of these companies (Kharpal, 2020). The USA also pressure its allies to veto the use of Chinese technology. In May 2020, the UK reformed a previous authorization of limited Huawei participation in British networks, and announced a complete ban on the company. The German Deutsche Telekom (32% state-owned) posed that excluding Huawei from its networks would be 'Armageddon'. Despite, although not restricting its participation, it recently announced that Ericsson was chosen as its 5G supplier (Petzinger, 2020; Alleven, 2020; Ericsson, 2020). Similarly, France decided not to ban Huawei from its networks, but 'encourage' their telecom companies to avoid it (Rose and Harvey, 2020). Under enormous pressure from the USA regarding the participation of Huawei in Brazilian networks, with the U.S. ambassador threatening 'consequences', in a very pragmatic position, the Brazilian military reportedly told their government that 'the same eventual exposure that Brazil may suffer from Chinese technology with Huawei will also occur with any other company' (Amado et al., 2020; Rosa and Antunes, 2020).

In a similar take, in the early stages of the COVID-19 pandemic, when the German company CureVac announced promising results in its research for the development of a vaccine, the U.S. government offered advantages to the company if it moved its research to the U.S., provoking immediate reaction of the German government (Morris, 2020; Carrel and Rinke, 2020). Albeit elucidative of current inter-State competition, this last example does not relate to cyberspace. Nonetheless, the pandemic also provides examples of fierce competition in the cyber realm. The COVID-19 'vaccine nationalism' increased the scale of cyberespionage actions targeting vaccine R&D promoted by intelligence agencies from many countries (Fidler, 2020). Specialists argued for the applicability of international law to cyberattacks targeting the healthcare sector and vaccine research and even argued that vaccine installations configure critical infrastructure, although not explicitly addressing cyber espionage (Fidler, 2020).

The aforementioned cases constitute clear and fresh evidence of increasing competition not only among rivals, but also among traditional western allies. Therefore, it is not the case of considering the different views regarding international norms for cyberspace a simple question of different ideological positions of the 'west and the rest', becoming necessary to analyse the context with other lenses. One could

argue that the 'west' is only reacting in the same way it has suffered in recent years. To tackle this argument, it is necessary to go back in time.

Despite Russian agents' apparent (or even likely) use of Twitter and Facebook for disinformation campaigns, using social networks for political purposes was not a Russian invention. In June 2009, the U.S. Secretary of State Hillary Clinton asked Twitter to postpone a programmed update of the app, which would leave it unavailable for a few hours during the final phase of Iran's election campaign. She claimed that the app was enabling a revolution in that country. On the same day, President Obama said that 'people's voices should be heard and not suppressed in Iran'. The company postponed that planned maintenance, but the Iranian government-supported candidate won the elections easily (Plening, 2009; Nuttall and Dombey, 2009).

Albeit the Iranian case, the Russians claim that other western interference cases succeeded. They argue that the Gaddafi government failed to control social media in Libya, leaving great freedom of action to its opponents, which led to military support from the USA and NATO, ultimately allowing the fall of the regime and culminating in the civil war in Libya (Giles and Monaghan, 2014). The 'Arab Spring', which led to the fall of regimes in Tunisia (2010) and Egypt (2011), would also have been greatly influenced by social network actions promoted by western intelligence agencies. Similarly, in Syria, protests promoted in these networks in January 2011 evolved into a violent civil war that persists until today, with the direct engagement of the USA and Russia on opposite sides. Sergei Smirnov, Deputy Director of the FSB (Federal'naya Sluzhba Bezopasnosti, or Federal Security Service of the Russian Federation), the successor of the famous KGB (Komitet Gosudarstvennoy Bezopasnosti, or Committee for State Security), declared in 2012: 'new technologies are used by Western secret services to create and maintain a level of continuous tension in society with serious intentions, even reaching a regime change' (Giles and Monaghan, 2014). Therefore, Russian concerns regarding the misuse of social media must be analysed in the context of this perception of existential threat, not merely ideological paranoia (Giles and Monaghan, 2014).

During the Cold War, when the world was ideologically divided into two blocs, a leading American strategist defined the USA as a *status quo* nation, 'determined to keep what it has, including existence in a world of which half or more is friendly or at least not sharply and perennially hostile' (Brodie, 1959). With the fall of the USSR, the USA became an unchallenged superpower, no longer interested only in half of the world.

> [...] American leaders from both the Democratic and Republican parties have made it clear that they believe that the United States, to quote Madeleine Albright, is the 'indispensable nation' and thus has both the right and the responsibility to police the entire planet (Mearsheimer, 2010).

The U.S. software industry is the largest in the world, being a net exporter and concentrating many of the best programmers in the world; computer courses at their universities are ranked at the top; the Pentagon has been working on public-private partnerships to build superior military capabilities in cyberspace (Libicki, 2009; Lynn, 2010; Morgan, 2010; Rid and McBurney, 2012; Libicki, 2019). Even though there is considerable secrecy about USA cyber offensive capabilities, it is widely believed that they are probably the best in the world.

Albeit demonstrating some advanced capabilities, and often being accused of cyberattacks against the West, Russians and Chinese are deeply uncomfortable with American cyber policy, seeing it as 'evidence of muscle flexion and dominant behaviour', compounded by the perception of a massive gap comparing USA cyber capabilities with theirs (Austin, 2016). Such a gap, favourable to the 'threatening west', broadens their perception of existential risk, with the consequent need for technologically asymmetric responses, and results from the perception that the gap is too big to be overcome (Giles and Monaghan, 2014).

This technological gap can also be associated with the problem of attribution of cyberattacks. It is well known that attributing cyberattacks is harsh (Buchanan and Rid, 2014; Lupovici, 2014). It is also a fundamental step for the application of international laws of conflict. Nevertheless, it is presumably easier for countries with advanced cyber capabilities, and harder for those with limited ones. Thus, the acceptance of current international law to cyberspace operations would favour those with advanced capabilities, maintaining their *status quo*. And this would also limit their interest in sharing technical information on cyberattacks with the less skilled group, re-feeding the process.

Faced with the perception of a growing threat, the Russian parliament passed a law prohibiting its Internet traffic from being redirected to servers in other countries, creating what the Western press has called the 'Internet Iron Curtain' (Deutsche Welle, 2019; BBC, 2019). For their part, the Chinese implemented *The Great Firewall of China* (Raud, 2016).

On the other hand, the Western feeling of Russia as a constant threat to the stability of the West is reinforced by the view that cybercrime is rampant in Russian cyberspace, leading many to conclude that the government of that country is in collusion, a perception aggravated by the country's non-accession to the Convention of Budapest on Cybercrime. This feeling partly stems from the little publicity (in the western media) of the efforts against cybercrime in Russia. Even these efforts are perceived in the West as attempts to control the freedom of expression and censorship of the Internet, even if they are in accordance with corresponding international norms (Giles and Monaghan, 2014).

The Russian perception of vulnerability increases their usual emphasis on international norms as the essential framework underpinning all interstate activity, and

partly explains the Russian persistence in the search for international normative instruments to govern cyberspace (Giles and Monaghan, 2014). Russia's primary objective concerning cyberspace norms has been the promotion of a treaty that could limit the development of cyber-weapons or the use of cyber means to interfere in the internal affairs of other states. Fundamentally, they argue that new technologies demand new laws that guide States to use them peacefully (Grigsby, 2017). The Chinese argue the same (Huang and Mačák, 2017). The USA opposes; initially, arguing that the 'information security' view could legitimise censorship by authoritarian governments, what 'would be unacceptable for democratic governments'; subsequently, claiming that such a treaty would be unverifiable (Nye, 2015, 2018).

Treaties require the express consent of States. Gary Corn, a former USCyberCom legal adviser, notes that the basic principle of any negotiation is that 'no one negotiates against himself' (Daskal et al., 2019). Insofar having strategically or operationally useful capabilities, some States have no incentive to limit the option of using them (Mačák, 2016). These same countries, however, are also vulnerable to hostile operations by other states with similar or even lower capabilities. Therefore, different bodies in the same country see national interests from different perspectives and may differ in how that country should characterise a particular practice (Schmitt and Vihul, 2014). Despite, while the rationale points to a net advantage of the pros facing the cons, the case in favour of the maintenance of strategic advantage prevails.

It turns out that these different perspectives are not limited to the mentioned countries, extending to their respective allies and even to countries not naturally aligned with one or the other group, but who feel threatened by the positions of both groups. This *split*, essentially guided by the different pragmatic views of the use of the Internet as a weapon of power, a tool for statecraft, or an instrument for free dissemination of information and expression, can better explain the difficulty of obtaining consensus, or even of implementing what has already been agreed.

On the Applicability of The Current Armed Conflicts Law

A key issue in the debate is the applicability of the current *jus ad bellum* and *jus in bello* to cyberspace activities. On the one hand, it is argued that, in the absence of specific rules, states should work by analogy, either by equating cyberattacks to traditional armed attacks and treating them under the laws of war or by equating them to criminal activities and dealing with them in the manner of internal criminal laws (Sklerov, 2010). The USA and its allies, particularly in NATO, favour this argument, even though some fundamental principles remain unresolved, such as

what would be a cyberattack or characterise the use of force in cyberspace. On the other hand, Russia, China and Brazil, among others, express considerable reluctance to agree with the applicability of non-specific rules, considering the need for specific agreements as an imperative (Schmitt and Vihul, 2014; Giles and Monaghan, 2014).

It was in the context of the applicability of the current rule that, under the auspices of NATO, an international group of academics produced the *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Schmitt, 2013). The work was expanded with the 'Tallinn 2.0' Project, published four years later, full of examples that illustrate an interpretation of the application of current rules to cyber operations (Schmitt, 2017). The Chinese often argue that the initiative is a clear example of an attempt to legalise military use of cyberspace by western powers (Henriksen, 2019; Huang and Mačák, 2017).

Although the doctrine is a secondary source of international law, it constitutes a 'highly persuasive' element in the interpretation of the provision of treaties and the identification of international custom. A doctrine common to several states can evolve into a 'general legal principle recognised by civilised nations', and later develop into a custom. Therefore, in the absence of conventions or customs related to cyber-conflicts, academic works such as the Tallinn Manual can be a relevant tool for identifying and formatting legal norms for cyberspace (Schmitt and Vihul, 2014). And this may be contrary to the interests of those who oppose the primacy of the USA.

Since 2010, the USA has been relatively successful in getting some top cyber powers to agree to an increasingly prescriptive set of rules on what they could and could not apply in cyberspace. The process failed, however, in obtaining explicit consent to the applicability of laws of war to cyber-conflicts. Russia, China and Cuba, among others, have refused to do so, ruled by the suspicion that this would constitute a 'green light' for hostile actions in cyberspace (Grigsby, 2017).

Not only traditional USA opposers disagree, however. Even NATO members have worked to shape customary law, expressing different views on fundamental aspects. While the United Kingdom disregards the nature of sovereignty in cyberspace, France defined it clearly (Wright, 2018; France-MdA, 2019). France also disagrees with relevant parts of the Tallinn Manual, for instance, regarding the due diligence principle and actions initiated by non-state actors inside a State against another State (France-MdA, 2019).

Current 'laws of war' establish that a State's recurrent inability to curtail illegal actions in its territory against other States may result in its qualification as a *sanctuary*. Besides, States victimised by armed attacks promoted by non-state actors located in another state can respond by force, when host states violate their duty to prevent such attacks (Pereira, 2010).

If such rules apply to cyberspace, the imputation of responsibility for cyberattacks originating in a State would provide a legal path for others to use active defences (and other offensive capabilities) without the need for conclusively attributing the attack to that State or its agents (Sklerov, 2010). This configures a good reason for countries where cybercrime is rampant, like Russia and Brazil, to privilege the elaboration and application of internal laws before recognising the applicability of international armed conflict laws to cyberspace.

Moreover, both the USA and the Netherlands recently adopted an understanding that the use of force defensively in the cyber realm is permitted under the auspices of Article 51 of the UN Charter, even if a cyberattack by a non-state actor cannot be formally attributed to another state. It is unclear when a cyberattack will be severe enough to be considered an armed attack in the sense provided for that article. According to the Tallinn Manual, cyber operations that cause 'significant' damage, destruction, injury or death qualify as such (Schmitt and Vihul, 2014). Significant, however, remains a subjective concept.

Finally, despite the American insistence that current international regulations apply to cyberspace, for which States should not knowingly attack critical infrastructures in other States, in 2010, the USA and Israel allegedly used Stuxnet to compromise uranium enrichment facilities in Iran. Different experts considered such action to be an illegal act of violence under international law (Zetter, 2013).

On the Perspectives of a 'Digital' Multilateral Convention

In November 2019, the UN Assembly approved two separate proposals to debate the regulation of cyberspace activities: one from the USA, creating a Group of Government Experts (GGE); and another from Russia, creating an Open-Ended Working Group (OEWG) (Achten, 2019; Grigsby, 2018; Colatin, 2018).

GGEs are common in the UN routine, constituted *ad hoc* when any subject deserves UN attention, with experts from 15 to 25 countries, but they are rarely successful (Achten, 2019; Nye, 2018). GGEs related to cyber regulation are nothing new. Those of 2004-5 and 2009-10 did not obtain significant results; however, the 2012-13 one had considerable success. For the first time, 15 countries, including Russia, China, the USA, India, the United Kingdom, France and Germany, understood that the *jus ad bellum* (the UN Charter) would apply to cyberspace. However, there was no agreement on *jus in bello* (IHL). The 2014-15 GGE developed new rules to guide the activity of States in cyberspace in times of peace but did not achieve the same success as its predecessor, as intended by the USA (Fidler, 2018; Grigsby, 2017).

Differently, OEWGs are forums open to all nations. The USA opposed this one, arguing that two separate discussion groups would divide efforts and that Russia's

intention was to delay the discussion in a broader forum (Achten, 2019; Grigsby, 2018; Colatin, 2018). However, already in 1998, Russia was the first nation to propose an international UN treaty to ban electronic and informational weapons (including for propaganda purposes), which could be used to 'adversely affect the security of states', with a resolution passed by the Assembly General (Grigsby, 2017; Nye, 2018). In 2011, Russia, China, Tajikistan and Uzbekistan proposed rules at the UN to regulate 'the dissemination of information incompatible with the domestic policy and the social and economic stability of countries, as well as their cultural and social environment' (Stevens, 2012).

In any analysis, however, the approval of these two groups by the General Assembly shows that international concern with the issue is general and that the arguments of both sides are being heard. This concern is also evident in other initiatives.

In 2011, in London, the Global Conference on Cyberspace (GCCS), also called London Process, was held to establish principles of behaviour on the Internet. The GCCS continued with conferences in Budapest (2012), Seoul (2013), The Hague (2015) and New Delhi (2017). In 2017, the Dutch think tank The Hague Centre for Security Studies (HCSS) announced the creation of The Global Commission on the Stability of Cyberspace (GCSC) with the aim of 'helping to develop norms and policies that promote international security and the stability of cyberspace' (Nederlands-HCSS, 2017). In 2018 GCSC published the Singapore Standard Pack (GCSC, 2018), and in November 2019, issued its final report (GCSC, 2019).

Private companies also promote initiatives. In September 2018, Microsoft launched its Digital Peace campaign, with a set of proposals aimed at protecting the privacy and security of customers in the computer industry. The following month, the German group Siemens, whose software for controlling Iranian centrifuges was targeted by Stuxnet, published its Charter of Trust, seeking adherence to a 'global standard' of cybersecurity (Laudrain, 2018).

In November 2018, France announced the Paris Call, based on the UN Charter and recognising the applicability of IHL to cyber conflicts, as well as international human rights law and customary law in general (Laudrain, 2018). In 2018, the initiative counted 75 countries, 341 civil society organisations and 624 private companies, recognising the relevance of companies and other non-governmental organisations to the stability of cyberspace (France-Diplomatie, 2018; Laudrain, 2018). The absence of the USA, China and Russia as signatories is not surprising, while the absence of Brazil and India may cause the initiative to lose traction (Laudrain, 2018). Although legally non-binding, the initiative tries to establish some basic principles of consensus, which could, in the future, be consolidated in international law (Shackelford, 2019).

Despite the attention paid in the last decade to the international debate on norms, the conclusion of new cyber treaties is unlikely in the short term, given the strong

opposition of Western nations (Schmitt and Vihul, 2014). Some argue that any international treaty on the subject would probably be riddled with reservations, thus degrading its practical effect (Elliott, 2011). This argument can also be factually contested. For example, the Budapest Convention on Cybercrime reached 64 ratifications, with 32 reservations and 29 declarations. Excluding Russia, Ireland and Sweden, all other 44 members of the Council of Europe (EC) joined it, plus non-EC member countries such as the USA, Canada, Japan, Australia and Argentina (Council of Europe, 2019).

Until 2019, none of the BRICS had yet joined the Budapest Convention (South Africa signed it but did not ratify). In December 2019, Brazil announced it started its accession to it (Brasil-MRE and Brasil-MJSP, 2019). This accession was concluded only in November 2022. Historically, Brazil used two arguments to justify not joining the Convention. First, 'Brazilian foreign policy privileges the agreements whose drafting Brazil participated in, to place our brand, our interest' (Vital, 2008). It reflects a legitimate concern with the dominance of the great powers in the debate, which is explicit in the statement by the then-Secretary for Combating Transnational Offenses of the Brazilian Ministry of Foreign Affairs:

> In a way, there is a democracy of vulnerability. Both developed and developing countries are in the same pattern. In this sense, Brazil intends not only to react but also to make its own proposals, so that more technologically developed countries do not dominate the debate (BOL, 2011).

This argument is consistent with the notion that treaties are *one*, and not *the*, product of international negotiations; another product is the negotiation process itself; 'The journey matters as much as the destination' (Finnemore and Hollis, 2016). In this process, several components take part: incentives, such as favourable trade agreements; *coercion*, in the form of bribes or threats; *persuasion*, in the search for changing attitudes; and *socialisation*, when countries with asymmetric capacities are considered as equals whose opinion has value (Finnemore and Hollis, 2016). In other words, some countries try to become 'norm-makers' instead of only 'norm-takers' (Reilly, 2012). Not being part of the Council of Europe, sponsor of the Budapest Convention, and thus excluded from the negotiation, Brazil urged for the European text to be discussed under the auspices of the UN (Vital, 2008).

The second argument was that 'what matters primarily is our internal legal system' (Vital, 2008). It reflects a concern with the internal stabilisation of cybercrime before acceding international conventions or recognising their validity, probably related to formal accountability or designation as a *sanctuary*. The official note itself nods in this direction when declaring that 'Brazil's accession initiative to the Budapest Convention comes in addition to Law 12,965/2014, named Marco Civil da Internet, for the criminal prosecution of cybercrimes' (Brasil-MRE and Brasil-MJSP, 2019).

If multilateral agreements cannot be quickly reached, bilateral ones become an option. In 2014, China and the USA agreed that their governments would not conduct or knowingly endure economic cyber-espionage, fulfilling an old objective of the USA in containing Chinese thefts from American companies. Subsequently, bilateral agreements were signed between many G20 members (Grigsby, 2017). In 2015, Russia and China signed a bilateral cooperation agreement in cyberspace, which in addition to reflecting their previous diplomatic positions, innovated with a mutual commitment to non-aggression (Korzak, 2015b, 2015a; Roth, 2015). All of these bilateral agreements lay the foundations for customary law.

On the Difficulties of Customary Law in Cyberspace

A significant impediment to the emergence of customary law is the lack of visibility of what happens in cyberspace. Generally, only the effects of cyberattacks are publicly observed; in many cases, not even these are perceived by the general public. Some victim states avoid revealing cyber incidents since doing so might reveal capabilities considered essential for their security (Schmitt and Vihul, 2014). In the 2014 Sony case, the USA quickly attributed the attack to North Korea, facing widespread scepticism, until the press revealed that the Americans had access to North Korean computer networks (Nye, 2015). The revelation almost certainly 'burned' some USA intelligence sources. Even so, then-President Obama classified the incident as an act of 'cyber-vandalism', a statement with no legal implications under international law (Sander, 2019).

The 'silence' regarding cyber-offences has additional motivations: the desire to maintain some ambiguity that allows them a desired (or necessary?) 'operational flexibility' in cyberspace; the existence of geopolitical interests, possibly not directly related to cyberspace; difficulties of attribution or regarding measures taken in response to cyber-offences; or the desire of not linking such offences to a particular international standard, or to legitimise certain practices of other states (Sander, 2019). States may also wish not to indicate to their opponents when they could resort to the argument of self-defence, or prefer not to make clear their threshold to resort to 'use of force'; remaining silent, they reserve space for some 'strategic ambiguity' (Schmitt and Vihul, 2014). The general nations' silence regarding the Stuxnet case does not mean they considered the operation legal. They may have concluded it was illegal, since it did not occur in response to an armed attack, but that it was more acceptable than a preventive kinetic attack (Schmitt and Vihul, 2014).

Despite, acts not made public do not constitute a customary practice. International custom emerges from the 'interaction of rival claims by States'; 'the State that can cite more precedents will have an advantage over its opponent, regardless of the

mode of peaceful settlement of the dispute, for the consolidation of customary international law' (Cançado Trindade, 2017).

Other requirements for the formation of customs are consistency and density, reflecting the support of other nations. In 2013, in the wake of the Snowden case, Brazil argued within the UN General Assembly that interception of communications represents a case of disrespect for national sovereignty. It is unlikely that a sufficient number of other States will support such a claim to the extent that a customary standard will be established (Schmitt and Vihul, 2014).

Another problem lies in the 'normalisation' of some practices in the cyber context that are contrary to international custom regarding armed conflicts (Libicki, 2019). Literature is full of different threat names: viruses, worms, botnets, Trojan Horses, malware, 'rogue code', logic bombs, and so on. Nevertheless, they all have two things in common: they consist of software, and they must be 'implanted' (installed) in advance on the target networks. Generally, malware implantation takes weeks, even months, in advance for a relevant cyberattack to be successful.

In June 2019, an international crisis unfolded when Iran seized a British oil tanker in the Persian Gulf. The Royal Navy immediately sent a war vessel to prevent subsequent seizures of British ships, in an attitude easily characterised as self-defence under current international norms. Subsequently, it was revealed that the USA carried out cyberattacks that damaged the database used by the Iranians to carry out the arrests, even though no USA vessel had been affected. (Barnes, 2019). The database hack itself configures a preventive action. Furthermore, it probably demanded the use of implants deployed long before.

While the principle of self-defence has a legal provision of customary nature, there is no legal support for preventive actions (Pereira, 2010). The Bush Doctrine, published a year after the 9/11 terrorist attacks, reiterated that the USA has long insisted on the possibility of pre-emptive attacks, and went further advocating for the legitimacy of preventive strikes (Bush, 2002). A pre-emptive attack is carried out when an attack is imminent; a preventive attack is carried out to prevent the enemy from being able to attack in the non-imminent future. Notwithstanding such a differentiation, both are carried out before an enemy attack occurs, and thus cannot be considered self-defence in line with the legally accepted framework (Pereira, 2010).

The threat of retaliation against cyber-offences through kinetic attacks is another practice that became somehow 'normalised', notably by nations such as the USA, the United Kingdom and France. It should be noted, however, that only Israel has used kinetic forces (an air attack) in retaliation against cyberattacks by Hamas hackers, and yet within an existing state of 'war on terror' (Newman, 2019).

All in all, the consolidation of customary law on cyber-conflicts seems more likely from the interpretation of already established customs, in which case interpretive

dilemmas will certainly arise (Schmitt and Vihul, 2014). NATO member nations appear to rely on this scenario, which is why the Tallinn Manual reflects several examples of the application of current international norms to cyberspace situations.

Conclusion

Great Powers achieved some alignment regarding specific basic rules on the applicability of international law to cyberspace. However, attempts to go further, as in obtaining an explicit endorsement for *jus in bello*, still seem distant.

Contrary to common belief, this is not a problem related to the novelty of the topic, nor even ideological issues such as authoritarianism versus the right to privacy. Part of the problem lies in the fact that cyber-conflicts, as they do not directly result in physical effects (destruction or death), are considered 'grey zone conflicts', below the threshold of armed conflict. Therefore, outside the original context of the existing norms. Besides, cyber operations are largely associated with espionage, a practice not regulated in international law on armed conflicts.

Different interest groups stand on opposing sides in the debate, making consolidating comprehensive international law rules challenging. On one side, there is the USA and a large part of NATO member states, interested in maintaining the *status quo*, and taking advantage of their technological edge. On the other side, there are mainly Russia and China, whose cyber technical capabilities (and investments in them) are considerably lower than those of the previous group, despite significant recent advances. The current gap is perceived as limiting their capabilities and leaving them vulnerable if certain interpretations of the current regulatory framework are applied.

In this arm wrestling, the application and interpretative evolution of the existing international regulation, or at least the creation of doctrine and custom, is more likely in the short term, as the Western powers intend, instead of specific new treaties, as desired by Russia, China and Brazil.

Negotiations continue, with nations of the second group gradually making concessions while accelerating their efforts to evolve their internal legal frameworks to make them compatible with the standards of the Western powers, attempting to prevent legal pretexts for actions against them.

References

Achten, N. (2019) New U.N. Debate on Cybersecurity in the Context of International Security. *Lawfare*.

Alleven, M. (2020) Deutsche Telekom selects Ericsson for 5G RAN in Germany. *FierceWireless* [online]. Available from: https://www.fiercewireless.com/operators/deutsche-telekom-selects-ericsson-for-5g-ran-germany.

Amado, G. *et al*. (2020) O recado das Forças Armadas ao Ministério da Defesa sobre o 5G – Época. *Época*. [online]. Available from: https://epoca.globo.com/guilherme-amado/o-recado-das-forcas-armadas-ao-ministerio-da-defesa-sobre-5g-24571588.

Austin, G. (2016) 'Middle Powers and Cyber-Enabled Warfare: The Imperative of Collective Security', in *Asian Security Conference 2016*. 2016 p.

Barnes, J. (2019) U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say. *The New York Times*. [online]. Available from: https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html

Barrinha, A. & Renard, T. (2020) Power and diplomacy in the post-liberal cyberspace. *International Affairs*. [online] 96 (3), 749-766.

BBC (2019) Russia internet: Law introducing new controls comes into force. *BBC News* [online]. Available from: https://www.bbc.co.uk/news/world-europe-50259597

BOL (2011) Itamaraty pede política global no combate a crimes cibernéticos. *BOL Notícias*. [online]. Available from: https://noticias.bol.uol.com.br/internacional/2011/09/09/itamaraty-pede-politica-global-no-combate-a-crimes-ciberneticos.htm

Brasil-MRE & Brasil-MJSP (2019) *Processo de adesão à Convenção de Budapeste – Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública* [online]. Available from: http://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/21146-processo-de-adesao-a-convencao-de-budapeste-nota-conjunta-do-ministerio-das-relacoes-exteriores-e-do-ministerio-da-justica-e-seguranca-publica

Brodie, B. (1959) The Anatomy of Deterrence. *World Politics* [online], 11(02), 173-191.

Buchanan, B. & Rid, T. (2014) Attributing Cyber attacks. *Journal of Strategic Studies* [online], 38(1-2), 4-37.

Bush, G. W. (2002) *The National Security Strategy United States of America*. (September), 1-31. [online]. Available from: http://www.state.gov/documents/organization/63562.pdf

Cançado Trindade, A. A. (2017) *Princípios do Direito Internacional Contemporâneo*. 2nd edition. Vol. 1. Brasília: FUNAG.

Carrel, P. & Rinke, A. (2020) Germany tries to halt U.S. interest in firm working on coronavirus vaccine | Reuters. *Reuters*. [online]. Available from: https://www.reuters.com/article/us-health-coronavirus-germany-usa-idUSKBN2120IV

CISCO (n.d.) *What Is a Cyberattack?* [online]. Available from: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html (Accessed 11 December 2022).

Colatin, S. (2018) *A surprising turn of events: UN creates two working groups on cyberspace* [online]. Available from: https://ccdcoe.org/incyder-articles/a-surprising-turn-of-events-un-creates-two-working-groups-on-cyberspace/

Council of Europe (2019) Chart of signatures and ratifications of Treaty 185 (Convention on Cyber Crime). Council of Europe [online]. Available from: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures

Daskal, J. *et al*. (2019) Data and Sovereignty. CyCon US.

Deutsche Welle (2019) Russos protestam contra 'cortina de ferro' na internet. *Deutsche Welle*. [online]. Available from: https://www.dw.com/pt-br/russos-protestam-contra-cortina-de-ferro-na-internet/a-47844381

Elliott, D. (2011) Deterring Strategic Cyberattack. *IEEE Security & Privacy Magazine* [online], 9(5), 36-40.

Ericsson (2020) *Deutsche Telekom and Ericsson strengthen partnership with 5G deal – Ericsson* [online]. Available from: https://www.ericsson.com/en/press-releases/2020/7/deutsche-telekom-and-ericsson-strengthen-partnership-with-5g-deal

Fidler, D. (2003) Developments involving SARS, International Law, and Infectious Disease Control at the Fifty-Sixth Meeting of the World Health Assembly | ASIL. *Insights*. 8(14), [online]. Available from: https://asil.org/insights/volume/8/issue/14/developments-involving-sars-international-law-and-infectious-disease

Fidler, D. (2020) *The Cyber Side of Vaccine Nationalism | Council on Foreign Relations* [online]. Available from: https://www.cfr.org/blog/cyber-side-vaccine-nationalism

Fidler, D. (2018) The UN Secretary-General's Call for Regulating Cyberwar Raises More Questions Than Answers. *Council on Foreign Relations Blog*, 2-5.

Finnemore, M. & Hollis, D. B. (2016) Constructing Norms for Global Cybersecurity. *American Journal of International Law* [online], 110(3), 425-479.

France-Diplomatie (2018) *Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace* [online]. Available from: https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in

France-MdA (2019) *International Law Applied to Operations in Cyberspace* [online]. Available from: https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf

GCSC (2019) Advancing Cyberstability. GCSC Final Report.

GCSC (2018) *Norm Package Singapore* (November).

Giles, K. & Monaghan, A. (2014) Legality in Cyberspace: An Adversary View. *The Letort Papers* (March) [online]. Available from: http://www.carlisle.army.mil/ssi

Grigsby, A. (2017) The end of cyber norms. *Survival* [online], 59(6), 109-122.

Grigsby, A. (2018) The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased. Council on Foreign Relations, 1-4.

Guterres, A. (2018) *Secretary-General's address at the Opening Ceremony of the Munich Security Conference*. p. 1-6. [online]. Available from: https://www.un.org/sg/en/content/sg/statement/2018-02-16/secretary-general's-address-opening-ceremony-munich-security

Henriksen, A. (2019) The end of the road for the UN GGE process: The future regulation of cyberspace. *Journal of Cybersecurity* [online], 5(1), 1-9.

Hollis, D. *et al*. (2020) *Elaborating International Law for Cyberspace » directions blog* [online]. Available from: https://directionsblog.eu/elaborating-international-law-for-cyberspace/

Huang, Z. & Mačák, K. (2017) Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches. *Chinese Journal of International Law* [online], 16(2), 271-310.

IBM (n.d.) *What is a cyberattack?* [online]. Available from: https://www.ibm.com/topics/cyber-attack (Accessed 11 December 2022).

ICRC (2019) IHL and cyber operations during armed conflicts. UN OEWG/GGE Cyber [online]. Available from: https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts

Khalip, A. (2018) U.N. chief urges global rules for cyber warfare. *Reuters*, 1-6.

Kharpal, A. (2020) US should take stake in Nokia, Ericsson to counter Huawei in 5G: Barr. *CNBC*.

Korzak, E. (2015a) Have Russia and China signed a Cyber Nonaggression pact? *The Diplomat*, [online]. Available from: http://thediplomat.com/2015/08/have-russia-and-china-signed-a-cyber-nonaggression-pact/

Korzak, E. (2015b) *The Next Level For Russia- China Cyberspace Cooperation ?* [online]. Available from: https://www.cfr.org/blog/next-level-russia-china-cyberspace-cooperation

Laudrain, A. (2018) Avoiding A World War Web: The Paris Call for Trust and Security in Cyberspace. *Lawfare* [online], 1-2. Available from: https://www.lawfareblog.com/avoiding-world-war-web-paris-call-trust-and-security-cyberspace

Libicki, M. (2009) *Cyberdeterrence and Cyberwar*.

Libicki, M. (2019) 'Norms and Normalization', in *CyCon US*. 2019 Washington: Army Cyber Institute. p.

Lupovici, A. (2014) The 'Attribution Problem' and the social construction of 'Violence': Taking Cyber deterrence literature a step forward. *International Studies Perspectives* [online], n/a-n/a.

Lynn, W. (2010) Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs*, 89(5).

Mačák, K. (2016) 'Is the international law of cyber security in crisis?', in *8th International Conference on Cyber Conflict* [online]. 2016 Tallinn: NATO/CCDCOE, 127-139.

Malagutti, M. (2016) State-sponsored cyber-offences. *Revista da Escola de Guerra Naval* [online], 22(2), 261-290.

Mearsheimer, J. (2010) The gathering storm: China's challenge to US power in Asia. *The Chinese Journal of International Politics* [online], 3(4), 381-396.

Microsoft (n.d.) *What is a cyberattack?* [online]. Available from: https://www.microsoft.com/en-us/security/business/security-101/what-is-a-cyberattack (Accessed 11 December 2022).

Morgan, P. (2010) 'Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm', in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy (2010)*. 2010 National Academies Press, 55-76.

Morris, L. (2020) Germans to discuss reported U.S. attempt to buy CureVac coronavirus vaccine rights – The Washington Post. *The Washington Post* [online]. Available from: https://www.washingtonpost.com/world/europe/germany-coronavirus-curevac-vaccine-trump-rights/2020/03/15/8d684c68-6702-11ea-b199-3a9799c54512_story.html

Nathan, A. & Scobell, A. (2020) *2020 Data Breach Investigations Report* [online]. Available from: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf%0Ahttp://bfy.tw/HJvH

Nederlands-HCSS (2017) *The Global Commission on the Stability of Cyberspace* [online]. Available from: https://www.hcss.nl/news/global-commission-stability-cyberspace

Newman, L. H. (2019) *What Israel's Strike on Hamas Hackers Means For Cyberwar* [online]. Available from: https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/

Nunes, J. (2017) Disease Diplomacy: International Norms and Global Health Security by Sara E. Davies, Adam Kamradt-Scott, and Simon Rushton – Ethics & International Affairs : Ethics & International Affairs. *Ethics & International Affairs* [online], 31(3). Available from: https://www.ethicsandinternationalaffairs.org/2017/disease-diplomacy-international-norms/

Nuttall, C. & Dombey, D. (2009) US urges Twitter to delay service break. *Financial Times* [online]. Available from: https://www.ft.com/content/f317a12e-5acc-11de-8c14-00144feabdc0.

Nye, J. (2018) How Will New Cybersecurity Norms Develop? *Project Syndicate*, 3-5.

Nye, J. (2015) International Norms in Cyberspace. *Project Syndicate*.

Pereira, A. C. A. (2010) A legítima defesa no Direito Internacional contemporâneo. *Revista Interdisciplinar de Direito*, 7(1), 21-36.

Petzinger, J. (2020) Deutsche Telekom describes potential Huawei ban as 'Armageddon' scenario. *MSN* [online]. Available from: https://www.msn.com/en-gb/money/technology/deutsche-telekom-describes-potential-huawei-ban-as-armageddon-scenario/ar-BB15BxQM

Plening, S. (2009) U.S. State Department speaks to Twitter over Iran. *Reuters* [online]. Available from: https://www.reuters.com/article/us-iran-election-twitter-usa-idUSWBT01137420090616.

Raud, M. (2016) *China and Cyber: Attitudes, Strategies, Organisation*. NATO CCDCOE.

Reilly, J. (2012) A norm-taker or a norm-maker? Chinese aid in Southeast Asia. *Journal of Contemporary China* [online], 21(73), 71-91.

Rid, T. & McBurney, P. (2012) Cyber-Weapons. *The RUSI Journal* [online], 157(1), 6-13.

Rosa, B. & Antunes, C. (2020) Embaixador dos EUA alerta que se Brasil permitir chinesa Huawei no 5G enfrentará 'consequências'. Jornal O Globo. *O Globo*.

Rose, M. & Harvey, J. (2020) France won't ban Huawei, but encouraging 5G telcos to avoid it: report | Reuters. *Reuters* [online]. Available from: https://www.reuters.com/article/us-france-huawei-5g-idUSKBN2460TT.

Roth, A. (2015) Russia and China Sign Cooperation Pacts. *The New York Times* [online], 1-5. Available from: https://www.nytimes.com/2015/05/09/world/europe/russia-and-china-sign-cooperation-pacts.html.

Sander, B. (2019) 'The Sound of Silence: International Law and the Governance of Peacetime Cyber Operations', in T Minárik *et al*. (eds.) *CYCON*. 2019 Tallinn: NATO/CCDCOE, 361-381.

Schmitt, M. (2017) *Tallinn Manual 2.0 on the International Law Applicable To Cyber Operations*. NATO/CCDCOE (ed.). Cambridge: Cambridge University Press.

Schmitt, M. (2013) *Tallinn Manual on the International Law Applicable to Cyber Warfare* [online]. NATO/CCDCOE (ed.), Cambridge University Press.

Schmitt, M. & Vihul, L. (2014) The Nature of International Law Cyber Norms. *CCDCOE Tallinn Papers* [online], 5.

Shackelford, S. (2019) Meet the Coalition Pushing for 'Cyber Peace' Rules. *Defense One*, September.

Sklerov, M. (2010) 'Responding to international cyber attacks', in Jeffrey Carr (ed.) *Inside Cyber Warfare: Mapping the Cyber Underworld*. Sebastopol, CA: O'Reilly, 46-62.

Stevens, T. (2012) A Cyberwar of ideas? Deterrence and norms in Cyberspace. *Contemporary Security Policy* [online], 33(1), 148-170.

Stoll, C. (1990) *The cuckoo's egg: Tracking a spy through a maze of computer espionage*. The Bodley Head, London.

Toffler, A. (1991) *Powershift: Knowledge, wealth, and violence at the edge of the 21st century*. Bantam Books (Transworld Publishers a division of the Random House Group).

Tuathail, G. Ó. & Agnew, J. (1992) Geopolitics and discourse. Practical geopolitical reasoning in American foreign policy. *Political Geography* [online], 11(2), 190-204.

UN (1945) *Estatuto da Corte Internacional de Justiça* [online]. Available from: http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/cdhm/comite-brasileiro-de-direitos-humanos-e-politica-externa/EstCortIntJust.html

Vital, A. (2008) Tratado sobre crimes digitais sob desconfiança. *Congresso em Foco*.

Wright, J. (2018) Cyber and International Law in the 21st Century. Chatham House.

Zetter, K. (2013) Legal Experts: Stuxnet Attack on Iran Was Illegal "Act of Force". Wired.

Extra Dossiê

Estado de Direito *versus* Pandemia: a Ação da Polícia de Segurança Pública

Bruno Garcês
Oficial de Polícia (Subcomissário) da Polícia de Segurança Pública. Doutorando em Relações Internacionais: Geopolítica e Geoeconomia, Universidade Autónoma Lisboa. Mestre em Ciências Policiais pelo Instituto Superior Ciências Policiais e Segurança Interna – PSP.

Sónia Morgado
Investigadora do Centro de Investigação (ICPOL) do Instituto Superior de Ciências Policiais e Segurança Interna. Professora Auxiliar Convidada do ISCPSI. Gestora da equipa portuguesa do Consórcio associado ao projeto europeu IMPROVE.

Resumo

O SARS Cov 2 determinou uma nova forma de actuação no âmbito da saúde pública. O ano de 2020 ficou marcado pela declaração da pandemia de COVID-19, e com a rutura dos serviços de saúde. Os Estados viram-se obrigados a recorrer à sua autoridade, com a implementação de estados de exceção constitucional, para procurar mitigar os efeitos desta pandemia que se revelou implacável. Com o estado de exceção a ação policial reverteu-se em operacionalizar as limitações impostas pelos Estados, que se consubstanciavam em limitação de limitações de direitos com repressão sobre os infratores. Neste sentido pretende-se aflorar a forma como a ação policial da Polícia de Segurança Pública foi exercida neste contexto. O estudo teórico leva-nos a aduzir que a sua ação foi diferenciada, por estar subordinada à axiologia do estado excecional, congregando nesta dinâmica a abordagem participativa e cívica dos cidadãos.

Palavras-chave: COVID-19; Estado Democrático e de Direito; Ação; Polícia; Estados excecionais

Abstract
Rule of Law* versus *Pandemic: The Action of the National Public Security Police

SARS Cov 2 determined a new way of doing public health. The year 2020 was marked by the declaration of the COVID-19 pandemic and the breakdown of health services. States were forced to resort to their authority, with the implementation of constitutional states of exception, to try to mitigate the effects of this pandemic, which proved to be relentless. With the state of exception, police action reverted to operationalizing the limitations imposed by the states. It embodied restrictions in liberty and human rights with repression of the infractors. In this sense, we intend to outline how the police action of the Public Security Police was exercised in this context. The theoretical study leads us to deduce that its action was differentiated, for being subordinated to the axiology of the exceptional state, congregating in this dynamic the participative and civic approach of the citizens.

***Keywords**: COVID-19; Democratic and Rule of Law State; Action; Police; Exceptional State*s

Recebido: 15.05.2022
Aprovado: 07.06.2022
https://doi.org/10.47906/ND2022.163.06

1. Introdução

A metamorfose da sociedade é um processo inevitável, porquanto, esta transmutou-se para uma sociedade mais turbulenta e esmaecida de princípios, naquilo a que muitos designam de uma mudança de Era (Levisky, 2007). De facto, existe uma "força destruidora em toda a natureza, esta força que nada cria senão para destruir-se e destruir o que cerca ao mesmo tempo" (Goethe, 1771). A irreversibilidade do processo de globalização económica, social, cultural, de saúde (Morgado, 2013) permitida pelas tecnologias, congrega em si mesmos elementos de profusão de acontecimentos e externalidades positivas e negativas.

Na sociedade contemporânea, as ameaças e riscos à sociedade (terrorismo, aquecimento global, pandemias) são, na sua maioria, de cariz não-governamental, não se encontram associados a uma nação, apresentam diversas formas, e tornam-se inclusive imprevisíveis acabando muitas das vezes por atingir os pilares dos Estados de direito democráticos (Elias, 2013). Tanto os riscos, como a incerteza e a insegurança sempre caminharam lado-a-lado com o ser humano, todavia, atualmente a sociedade enfrenta "nova categoria de riscos que se não forem prevenidos podem originar consequências irreversíveis" (Ribeiro, 2011, p. 129).

O risco de pandemia tem sido equacionado ao longo dos anos. No *The Global Risk Report 2020* essa possibilidade tem sido referida, todavia só nos relatórios de 2017 e 2018 é que a mesma assumiu relevância, pelo posicionamento 4.º e 5.º lugar, respetivamente, no *Top 5 Global Risks in Terms of Impact* (World Economic Forum, 2020). Em 2020, essa hipótese confirmou-se de uma forma sem precedentes na sociedade atual. De facto a dimensão sanitária nem sempre foi objeto de análise, sendo que a maior parte dos riscos eram identificados Para Portugal cingiam-se a: i) país e território (por exemplo, envelhecimento da população, emigração, ensino), ii) problemas económico-financeiros (corrosão e corrupção do tecido social e dos serviços públicos), iii) de problemas de integração europeia (fragilidade da economia); iv) sectores estratégicos da economia (controlo por multinacionais); e, v) dependência energética (pouca diversificação de energias) (Morgado e Mendes, 2013, 2014 e 2015).

O dilema sanitário tornou-se um desafio que alterou o *status quo*, o modo de vida, e o equilíbrio estrutural da economia, da segurança e da sociedade. Neste contexto, os Estados confrontaram-se com a dinâmica de Kant quanto à liberdade, de saber como são possíveis a liberdade e a necessidade (Kant, 2013).

Aliado a este surto pandémico surgem medidas restritivas associadas em alguns casos a estados de emergência e similares, causando um terrível impacto na vida de milhões de pessoas, mudando em grande escala a maioria das democracias ocidentais.

A implementação das medidas, acompanhando o crescente número de infeções, compreendera diligências de distanciamento social, uso de máscaras em público, quarentenas voluntárias e *lockdown's* (Bradford *et al.*, 2020; Canestrini, 2020; Jones, 2020; Kooistra *et al.*, 2020; Perry e Jonathan-Zamir, 2020; Reicher e Stott, 2020a; Reicher e Stott, 2020b; Van Rooij *et al.*, 2020).

Neste contexto, o outrora defendido por (Zucca, 2009) de que os direitos individuais e a liberdade devem ser garantidos pelos Estados de direito aquando da regulação da vida privada e pública, foram suspensas em prol da saúde pública. Apesar da valia destes princípios em momentos de crise económica, mudanças tecnológicas, ambiente de paz instável representativas da sociedade de incerteza (Mendes e Morgado, 2017), essa valia não se coadunou face a uma emergência sanitária. Perante esta, o indivíduo foi obrigado a excluir-se do seu sistema de relações humanas, pelo que lhe foi subtraído a personalidade, a autonomia e autodeterminação, semelhante ao universo kafkaniano de *A Metamorfose* (Kafka, 2021).

A nova realidade, especialmente durante a vigência dos estados de emergência (mas não só), leva a que haja um reforço dos poderes das forças de segurança (FS), para o cumprimento e fiscalização das medidas. Este entorno leva a que autores como Albuquerque (2020), refiram que em alguns casos as medidas tomadas no Reino Unido, são tão limitadoras que se corria o risco de se transformar num "Estado policial". No seu entender, as democracias europeias "aprovaram restrições manifestamente excessivas aos direitos fundamentais" (Albuquerque, 2020, p. 47).

Decorrente deste cenário, importa perceber qual o impacto que este reforço de poderes da Polícia criou no seio da sociedade, especialmente no que diz respeito à sua ação policial. A forma como a comunidade se posiciona face à Polícia, e a forma como reconhece a sua autoridade como legítima, são fundamentais na sustentabilidade de qualquer instituição, bem como o Estado que representa, especialmente quando esta detém o monopólio do uso legítimo da força (Crowl, 2017; Herbert, 2006; Kääriäinen, 2007; Worden e McLean, 2017).

No seu conjunto, as forças e serviços de segurança portugueses (FSS) procuraram durante todo o estado de emergência uma abordagem progressiva. Esta tinha como propósito atingir a proporcionalidade e o equilíbrio entre a proteção da saúde pública e a contenção da pandemia, procurando o cumprimento da lei sem descurar o respeito pelos direitos, liberdades e garantias dos cidadãos (EMEE, 2020a, 2020b e 2020c). O mesmo aconteceu durante as situações de exceção administrativa, baseadas na Lei de Bases da Proteção Civil (LBPC) que vigoraram ao longo do ano de 2020, que apesar de não apresentarem medidas tão restritivas quanto as que vigoraram durante o estado de emergência, as mantidas reverteram-se num empenho constante das FS, na sua fiscalização e cumprimento.

É importante procurar estudar a ação policial face a determinadas situações de crise, como por exemplo ataques terroristas (Jonathan-Zamir e Weisburd, 2013).

A pandemia de COVID-19 levou a que essa necessidade emergisse, havendo uma real preocupação com a forma como esta afetou a relação entre a sociedade e a autoridade dos Estados, bem como das suas polícias, devido à resposta a esta crise sanitária (Jones, 2020; Kooistra *et al.*, 2020; Perry e Jonathan-Zamir, 2020; Reicher e Stott, 2020a; Van Rooij *et al.*, 2020). Como refere Jones (2020, p. 3) "a forma como a polícia reagirá nesta crise atual terá impactos duradouros na legitimidade e nas relações polícia-comunidade muito para além do alcance da pandemia".
Pelo exposto, pretende-se neste estudo teórico avaliar e verificar a ação policial e os seus contornos no Estado de direito em regime de estados excecionais no combate à epidemia.
Para este desígnio, o artigo segue a estrutura formal dos estudos teóricos, com a introdução, estado de arte; Perspectivas/directrizes, Discussão/Conclusão.

2. Estado de Arte

A garantia da legalidade democrática, da segurança interna e dos direitos do cidadão são apanágio da atuação policial. As existências de mecanismos previstos na Constituição da República Portuguesa (CRP), para a garantia da liberdades e direitos humanos, convergem para a necessidade de segurança pública, a defesa da ordem jurídica, a garantia da segurança interna. Estes elementos ratificam a relevância da atuação policial num Estado de Direito Democrático. O respaldo desses mecanismos consubstancia-se na legislação nacional e internacional, não obstante os mesmos serem estruturantes e aplicáveis a quase todas as situações de crise que se convertam em tendências securativistas da intervenção da polícia, ou seja da intervenção estatal.
Não obstante o seu primacial fundamento, um estado excecional pode subverter estes elementos, causando disrupção na ação policial, enquanto garante do disposto na CRP. As diretrizes dos estados de exceção decorrentes da pandemia provocada por SARS-COV" é disso exemplo.

2.1. O Direito *versus* Pandemia Covid-19

A 11 de março de 2020, a OMS declara oficialmente a pandemia de COVID-19 (Ghebreyesus, 2020; Murphy, et al., 2020). Por todo o mundo os Estados redobraram esforços para combater esta calamidade de saúde pública, sendo que para além de medidas de reforço sanitário, muitos Estados avançaram com restrições em certos direitos e liberdades (nomeadamente o direito de circulação e liberdades económicas, entre outros). Surgiram por todo o mundo diversos países a imple-

mentar estados de exceção (entre eles Espanha, Itália, França, Alemanha, etc), semelhantes aos que a Constituição Portuguesa consagra. ´

Estes estados de exceção são as modalidades mais intensas do estado de necessidade no Direito constitucional português (Miranda, 2018). No âmbito securitário, tem surgido recentemente um aumento de situações que faz com que se equacione este tipo de regimes de exceção, pondo à prova as unidades estruturais do Estado, especialmente do prisma orgânico-administrativo. Vejamos como exemplo o do terrorismo internacional, que materializa sérias dificuldades às FS, e que obrigou a França a instaurar um estado de emergência devido aos ataques terroristas que assolaram aquele território (Silva, 2016).

Num Estado de Direito Democrático, e mais concretamente no Estado Português, só pode haver lugar à restrição dos direitos, liberdades e garantias nos casos expressamente previstos na lei constitucional (art.º 18 da CRP) enquadrando-se como o princípio da autorização constitucional expressa. As situações onde as regras gerais do Estado podem ser suspensas enquadram-se nos estados de exceção referidos no art.º 19 da CRP (Elias, 2020; Gouveia, 2011, 2020; Miranda, 1986, 2018; Silva, 2016), nomeadamente o Estado de Sítio e Estado de Emergência.

Importa ainda referir, que no caso português para além dos estados de exceção constitucional, encontramos os estados de exceção administrativa, sendo que os utilizados em 2020, tiveram por base a Lei de Bases da Proteção Civil (LPBC), nomeadamente a situação de alerta, contingência e calamidade.

Com a declaração de pandemia por parte da OMS a 30 de janeiro de 2020, o primeiro recurso legal a ser utilizado por parte do Governo foi a declaração da situação de alerta em todo o território nacional, a 13 de março de 2020 segundo o Despacho conjunto do MAI e MS, n.º 3298-B/2020. Este estado teve como intuito de conter e controlar as possíveis linhas de contágio de COVID-19, cuja previsão seria vigorar até dia 9 abril de 2020 (Leite, 2020).

Conforme refere Freitas (2020, p. 46) "entre a declaração do estado de emergência e a da situação de calamidade, deverão ser ponderados, designadamente, a extensão, a intensidade e a gravidade dos danos antecipados ou causados pela calamidade em causa". A estes acresce a necessidade de ter em conta a adequação de meios e a sua capacidade para a resolução do problema, sendo que há diversas medidas que não podem ser implementadas numa situação de calamidade, mas apenas numa situação de exceção constitucional.

2.2. A Ação Policial

Incumbe ao Estado garantir a segurança de todos os cidadãos, bem como a dos seus bens e outros direitos consagrados no ordenamento jurídico português. Sendo que

a Polícia tem como função a prossecução e garantia da segurança interna constituindo o "braço prossecutor e rosto visível da prossecução de uma das tarefas fundamentais do Estado", deverá sempre considerar o princípio do respeito pela dignidade da pessoa humana como pilar fundamental (Valente, 2019, p. 137).

Um estado liberal deverá ser proporcional na sua intervenção, deixando a sociedade funcionar com o mínimo de perturbação, potenciando assim a expressão dos seus cidadãos. Compete-lhe ainda assegurar a manutenção geral da ordem, fundamentadas nas constituições que fornecem o pilar no que é permitido e proibido ao Estado, criando um conjunto de regras que vinculam o comportamento do mesmo (Herbert, 2006).

Outrora, as formas de policiamento tinham por base a reação ao crime, numa ótica de ocupação do terreno, e o combate e controlo da criminalidade baseava-se na promessa da punição e prisão dos delinquentes (Sunshine & Tyler, 2003). Todavia, mesmo que a Polícia executasse a sua missão de forma eficaz, o seu método poderia não ter o apoio da comunidade (O'Brien & Tyler, 2019; Sunshine & Tyler, 2003; Tyler, 2002). Há que considerar que a Polícia não se cinge ao combate ao crime e fiscalização de trânsito. São-lhe atribuídas diversas tarefas: i) prevenção do terrorismo; ii) ordem pública em grandes eventos, e, iii) investigação criminal (Huq, et al., 2016). Porém, o primado da ação policial é garantir o direito à segurança aos cidadãos (Clemente, 2010).

A interação polícia-cidadão pode dar-se de diversas formas: desde pequenas abordagens relacionadas com ilícitos de qualquer tipo, à comunicação de um crime ou prestação de informações, são inúmeras as situações e podem levar a diferentes dinâmicas (Jackson e Pósch, 2019). Os polícias não são apenas responsáveis por este tipo de tarefas, todos representam a ordem na sua sociedade, pelo que são o exemplo na sua comunidade (Hough, et al., 2010; Wolfe & Piquero, 2011), porque o seu comportamento em relação aos cidadãos induz a sentimentos de pertença e identidade social perante os quais se identifica uma cooperação ativa (Bradford, 2014).

É também o cidadão, na sua individualidade, que deve procurar cooperar com a Polícia e com o Estado, na defesa de um objetivo que deve ser comum a todos: a segurança e tudo o que dela deriva (Clemente, 2000). "As pessoas concedem poder à polícia em troca de ordem social; cedem poder e autoridade à polícia em troca de regulação social e justiça (...)" (Bradford *et al.*, 2014, p. 567). A Polícia detém o uso legítimo do recurso à força para impor a sua autoridade, sendo que esta deriva do Estado e da confiança que a sociedade lhe confere (Kääriäinen, 2007; Jackson *et al.*, 2013). De facto, a sociedade "não abdica da liberdade e anseia pela segurança" (Clemente, 2010, p. 144).

Os polícias encontram-se legitimados a recorrer à força e à coerção para a aplicação da lei. Este recurso encontra-se balizado por normas legais, internas e até pelas

expectativas da sociedade. Podemos referir dois tipos de uso da força por parte da Polícia, por um lado o uso razoável, ou seja, aquele que é proporcional à gravidade da ameaça e que é suficiente para a cessar, por outro, o uso excessivo da força quando o recurso à força é superior à gravidade da ameaça, mostrando-se, portanto um recurso desproporcional (Gerber e Jackson, 2016).

Ao longo da sua existência as forças policiais sempre foram escrutinadas e contestadas pela sociedade. Como refere (Haberfeld, 2016, p. 296) a "sociedade democrática muda de um extremo para outro, de acusações de racismo e uso excessivo da força, um modelo "guardião" verdadeiramente falhado, para as exigências de um conceito de "guerreiro"(…)". Devemos ter presente que sempre que os polícias falham aos olhos dos cidadãos, violando a lei ou até mesmo as expectativas da sociedade, surgem várias consequências, muitas vezes diferentes, irregulares e inconsistentes face a cada situação (Harkin, 2015). Hoje, os cidadãos esperam demais da Polícia, graças a uma ideia romantizada sobre a ação policial (Haberfeld, 2002).

Ao interagir com as pessoas, um polícia transmite a forma como se posiciona dentro da sociedade, ou dentro de determinado grupo. Se apresentar um tratamento baseado na dignidade e respeito para com o cidadão, reforça o seu estatuto como um membro importante daquele grupo social, caso não o faça, e opte por um tratamento oposto, depreciativo ou humilhante, transmite à sociedade que a Polícia não valoriza os cidadãos do grupo (Gau *et al.*, 2012). "Quando as pessoas confiam na polícia por ser justa, decente e respeitosa, é mais provável que a polícia seja considerada legítima" (Bradford *et al.*, 2014, p. 248). No entanto, é de referir que o público espera sempre que os polícias exibam uma boa postura e autocontrolo, mesmo face a provocações, por muito insultuosas que estas sejam (Haberfeld, 2016).

Tradicionalmente, a sociedade considera mais legítimas as polícias que efetivamente combatem o crime, prendendo criminosos em que a consequência imediata é o desencorajar a prática de ilícitos criminais (Hinds e Murphy, 2007), bem como as instituições policiais que apostam na visibilidade policial de determinada comunidade, porquanto transmite ao cidadão que a Polícia se encontra a exercer a sua função de combater o crime (Hawdon *et al.*, 2003).

A sociedade reconhece a autoridade e o poder da Polícia, não só quando esta atua de forma justa, ou quando previne e combate eficazmente o crime na sua zona, mas também quando a ordem social da comunidade é mantida, revelando aqui a importância de uma vertente mais ampla da ação policial no seio comunidade (Bradford *et al.*, 2014; Tyler, 2004). Podemos, portanto, referir que a atividade policial é de extrema importância no seio da sociedade. Segundo Clemente (2010), a vida social assenta em determinadas regras e encontra-se constantemente a sofrer certas agressões, devido a comportamentos desviantes do sujeito. Segundo o autor, o comportamento individual oscila entre a conformidade e a transgressão. Se existe uma norma, há de igual modo o seu desvio; é inevitável, portanto, um plano de norma-

lidade expectável e uma desviância associada. "Cada sociedade tem a sua marginalidade: o crime é um facto universal" (Clemente, 2010, p. 145).
O papel do público na interação com a polícia é importante para todo o sistema judicial. as denúncias, a cooperação com investigações, cooperação enquanto testemunhas, a simples desobediência a uma ordem etc. Tudo isto pode ter repercussões neste mesmo sistema. Por este facto tem existido um esforço por parte da Polícia em adaptar o policiamento moderno para que se promova uma melhoria da perceção pública acerca da instituição e da própria aplicação da lei, fomentando a cooperação e aumentando a autoridade da Polícia (Hamm *et al.*, 2017; Papp *et al.*, 2019; Tyler, 2003; Tyler e Jackson, 2013). A Polícia depende da legitimidade percecionada pelo cidadão para garantir o seu apoio, cooperação e a conformidade (Gau, 2014), por sua vez esta é crucial na legitimidade mais ampla dos Estados democráticos, a sua ligação ao cumprimento da lei e a forma como aplica a força. Todos estes fatores modelam a legitimidade policial. O conhecimento e o entendimento dos seus antecedentes são cruciais para o cidadão e consequentemente a sociedade considerar a sua Polícia legítima. Com base nesta agnição a consequência visível será a tendência para cooperar, ajudando no controlo e combate da criminalidade (Bradford *et al.*, 2014; Jackson *et al.*, 2012; Tyler, 2006).

3. Perspetivas e Diretrizes

Por todo o mundo, a resposta dos estados implicou recurso a situações de exceção, nova legislação e um reforço evidente dos poderes da Polícia e outras entidades (Canestrini, 2020; Fradella, 2020; Leite, 2020; Popelier, 2020). Nesta crise de saúde pública sem precedentes é expectável que a Polícia responda ativamente e coopere na resolução do problema, seguindo as orientações do Governo. Porém, a forma de atuação se for demasiado militarista, demonstrando falta de cuidado ao nível da justiça processual, poderá resultar em situações de agitação social e desordem pública, provocadas pela perda de confiança e legitimidade da Polícia (Jones, 2020; Reicher e Stott, 2020a; Reicher e Stott, 2020b).
De ressalvar que estando na linha da frente da pandemia, os polícias colocam as suas vidas em risco, por duas razões. A primeira é a essência da sua profissão, e a segunda, a carência de equipamentos de proteção e interação com pessoas (Fradella, 2020).
Com a pandemia assiste-se a um acréscimo de responsabilidades derivadas da resposta pandémica que são anexadas às que a Polícia tem em situações de normalidade (prevenção criminal, ordem pública, atividade administrativa). Este acréscimo poderá não resultar forçosamente num aumento de trabalho no seio da instituição, mas sim em menos recursos disponíveis para o serviço ordinário (Perry e Jonathan-Zamir, 2020).

Apesar de determinados países instaurarem estados de emergência que limitam direitos fundamentais, constitucionalmente consagrados, como aconteceu em Portugal, as Polícias devem ter o cuidado de procurar honrar esses direitos, apesar das suas limitações (Fradella, 2020). Se por um lado, há quem compreenda e apoie as medidas ditadas pelos Estados e operacionalizadas pelas FS, por outro, há quem ache que estas mesmas medidas são desnecessárias, desproporcionais e violam os direitos fundamentais (Bradford *et al.*, 2020). O receio de "estados policiais" emergiu (Albuquerque, 2020), devendo todos procurar "proteger o direito à saúde bem como o Estado de direito e impedir que o vírus infecte o Estado de direito" (Canestrini, 2020, p. 122).

É claro que haverá sempre quem viole o que é determinado, nomeadamente a distância social, as limitações de acesso a determinados locais, os confinamentos, entre outras situações. A Polícia, deverá então procurar, através do diálogo, em vez da abordagem punitiva (autuação), uma abordagem pedagógica, explicando a necessidade de determinadas medidas (Jones, 2020). Foi esta a abordagem usada por Portugal desde março de 2020, "o aconselhamento em vez da punição; a adesão em vez de repressão" (EMEE, 2020a, p. 47, 2020b, p. 55, 2020c, p. 66). Este tipo de abordagem, que passa de uma posição de autoridade e poder, para uma forma de postura mais justa e de respeito pelo cidadão, reforça a opinião pública acerca da Polícia e promove a cooperação e acatamento das normas e ordens legais (Sunshine e Tyler, 2003; Tyler, 2002)

O recurso a modelos de policiamento comunitário poderá ser útil para a resposta a esta crise pandémica (Fradella, 2020), sendo de igual forma crucial que todos os poderes que sejam confiados à Polícia sejam claros, consistentes e transparentes, para não quebrar a relação de confiança com o cidadão (Palmer, 2020). O ideal será informar e levar a que "as pessoas hajam com base nos seus sentimentos de obrigação e responsabilidade, envolvendo-se em comportamentos auto-reguladores" (Tyler, 2004, p. 91).

Os poderes das FS não se redefinem por fatores pandémicos. De facto, as FS detêm diversos poderes coercivos para aplicar aos incumpridores, porém o ideal será procurar deixar a sociedade promover a sua autorregulação, ou um controlo social informal, mais eficiente e menos dispendioso que qualquer tipo de policiamento ou controlo oficial exercido pelas autoridades (Kääriäinen, 2007; Jackson, 2018; Jackson e Bradford, 2009; Tyler, 2004 e 2011).

Todavia, como Perry e Jonathan-Zamir (2020) referem, há uma relutância tácita dos cidadãos em aceitar a regulamentação de emergência como uma lei, levando a que ao não cumprimento voluntário, e à não comunicação das infrações presenciadas em relação a outros crimes. Carece acrescentar que as leis e outras normas, em situações de normalidade constitucional, apresentam uma certa ambiguidade, podendo ser interpretadas de forma diferente até no seio de uma só instituição, o

que pode causar confusão alguma na sociedade (Haberfeld, 2016). Numa situação de exceção esse risco acaba por ser potenciado, havendo situações em que surgem sérias dúvidas na aplicação da lei (Leite, 2020; Palmer, 2020; Perry e Jonathan-Zamir, 2020).

As decisões que os polícias tomam são diferentes da maioria das outras profissões, uma vez que estas podem ter implicações sérias na vida dos cidadãos (podendo em certos casos ser situações de vida ou morte). Para além destas implicações, de cariz individual, podem também causar problemas no equilíbrio da sociedade, havendo consequentemente distúrbios na ordem social e até casos de desordem generalizada (Haberfeld, 2016). Numa situação de crise como esta, esse equilíbrio é ténue, culminando por vezes em situações de conflito social (Reicher e Stott, 2020a). Numa sociedade onde a desordem seja aparente e exista falta de coesão social no seu seio, há uma maior probabilidade do julgamento sobre a Polícia e responsabilização por isso, levando a que haja uma consequente falha no reconhecimento da sua autoridade e respeito (Bradford *et al.*, 2014).

Conforme refere Tyler (2004, p. 87) "quando as pessoas sentem que uma autoridade é legítima, autorizam essa autoridade a determinar qual será o seu comportamento dentro de um determinado conjunto de situações", sendo crucial em tempos de crise que se avalie e fomente os processos que levam a que a sociedade reconheça as suas FS como legítimas, e assim facilite a sua atuação (Jones, 2020). No entanto, quanto mais temerem pela sua segurança, mais facilmente o cidadão poderá aceitar o emprego de violência, desde que o objetivo seja a sua proteção (Jackson *et al.*, 2013).

Durante o ano de 2020, Portugal passou por dois períodos excecionais (sendo que o último transitou para 2021), e entre estes vivenciou diversas limitações impostas pelas situações de exceção administrativa da LBPC.

Apesar de ser a 13 de março de 2020 que o Governo Português avança com a tentativa de resposta à pandemia, é a 18 de março, com a declaração do estado de emergência que uma nova realidade surge: as medidas e limitações que colidiram com direitos fundamentais, impostas pelo estado de exceção. Nessa primeira declaração, é no art. º 32 º, sobre a epígrafe de "Fiscalização", que surgem as forças e serviços de segurança com o seu papel de fiscalização e cumprimento das diretivas emanadas pelo governo português durante o estado de exceção (Dec. n.º 2-A/2020, 2020).

Optou-se por diversas ações de fiscalização nas principais vias rodoviárias, tirando partido de cada força de segurança existente, com intuito de procurar que os cidadãos acatassem as medidas implementadas, nomeadamente o confinamento à sua residência e a ausência de deslocações desnecessárias. Importa ainda acrescentar a preocupação da fiscalização e controlo de parques públicos, praças, estações de transportes, bem como dos estabelecimentos que mantiveram a atividade (EMEE, 2020a).

Nos diferentes níveis de ação policial, micro (indivíduo – cidadão), meso (famílias – equipas de ação, por exemplo patrulhas) e macro (sociedade/país/países – Polícias), a ação policial passou a ser mais abrangente, porquanto lhe foi afeta tarefa de fiscalização no âmbito da pandemia e que envolve os três níveis de interação.

4. Discussão/Conclusão

Num momento de excecionalidade um dos maiores desafios da Polícia foi a procura de um equilíbrio no momento de conturbação sanitária, gerindo a sua ação policial, e que permitisse, num momento em que os direitos e liberdades fundamentais foram questionadas, manter o livre e legítimo exercício dos mesmos.
Neste entorno, enquanto rosto de uma democracia, impôs-se também à ação policial um novo caminho, que se transmutou, para além dos valores de liberdade e dos direitos humanos face a um inexorável fenómeno sanitário extraordinário e pandémico que reforçou a necessidade de se converter temporariamente alguns dos direitos adquiridos, por forma a condicionar e a suster a evolução do vírus.
O caminho da garantia e do exercício de um Estado democrático, em que prevalecem os direitos humanos, não é simples, nem fácil. É sempre um trajeto e um projeto temerário para a Polícia, que lhe exige "uma consciência jus constitucional de que a sua ação incide sobre seres humanos e não sobre entes abstratos invisíveis" (Valente, 2012, p. 260). Esta audácia é consubstanciada pela génese jurídico-constitucional e sociológica da ação policial. O inimaginável fenómeno pandémico transformou o olhar sobre o Estado democrático e de direito, tendo-se apropriado dos seus elementos constituintes, a liberdade e a garantia dos direitos fundamentais dos cidadãos.
O momento de crise securitário-sanitária revelou que a Polícia estava subordinada a axiologia do estado excecional, que temporariamente transfigurou o Estado constitucional de direito material social e democrático. Neste desiderato, enquanto voz e ação do Estado, prevaleceu o papel de ator de manutenção científica inteligente da segurança de cariz sanitária que estava imbuída de novas diretrizes governamentais díspares das constitucionais, à semelhança e transversais a uma miríade de países, cumpridas em função dos valores, princípios e axiomas constitucionais, contribuindo para uma abordagem participativa e cívica de todos os cidadãos.
O desafio com que a Polícia, a Constituição e o cidadão se deparou ante esta crise de saúde pública, que colocou restrições na liberdade e direitos humanos, impôs-lhe uma ação policial diferenciada, retirando o componente hermenêutico-constitucional de liberdades e direitos fundamentais, cumprindo a ordem jurídica imposta em regime de excecionalidade.

Referências

Albuquerque, P. P., 2020. Entrevista a Paulo Pinto de Albuquerque (Giustizia Insieme 15 de Abril 2020). Em: Estado de Emergência – COVID-19 Implicações na Justiça. Lisboa: Centro Estudos Judiciários.

Bradford, B., 2014. Policing and social identity: procedural justice, inclusion and cooperation between police and public. *Policing and Society,* Vol. 24, n.º 1, pp. 22-43.

Bradford, B., *et al.*, 2020. *Policing the lockdown: compliance, enforcement and procedural justice.* [Online] Available at: http://eprints.lse.ac.uk/104227/1/Jackson_Posch_policing_the_lockdown.pdf [Acedido em Janeiro 2021].

Bradford, B., Huq, A. e Jackson, J., 2014. What price fairness when security is at stake ?: police legitimacy in South Africa. *Regulation and Governance,* Vol. 8, n.º 4, pp. 246-268.

Bradford, B., Jackson, J. e Hough, M., 2014. Police Legitimacy in Action: Lessons for Theory and Practice. Em: M. D. Reisig e R. J. Kane, eds., *The Oxford Handbook of Police and Policing*. Oxford: Oxford University Press, pp. 551-570.

Canestrini, N., 2020. Covid-19 Italian emergency legislation and infection of the rule of law. *New Journal of European Criminal Law,* Vol. 11, n.º 2, pp. 116-122.

Clemente, P. J. L., 2000. *A Polícia em Portugal: da dimensão política contemporânea da seguridade pública.* Lisboa: Universidade Técnica de Lisboa.

Clemente, P. J. L., 2010. Polícia e Segurança : breves notas. *Lusíada:Política Internacional e Segurança,* Vol. n.º 4, pp. 139-169.

Crowl, J. N., 2017. The effect of community policing on fear and crime reduction, police legitimacy and job satisfaction: an empirical review of the evidence. *Police Practice and Research,* Vol. 18, n.º 5, pp. 449-462.

Decreto n.º 2-A/2020, de 20 de março. Regulamento aplicação do estado de emergência decretado pelo Presidente da República. *Diário da República* n.º 57/2020, 1.º *Suplemento, Série I de 2020-03-20. Presidência do Conselho de Ministros.*

Elias, L., 2013. A externalização da segurança Interna. *Relações Internacionais,* n.º 40, pp. 9-29.

Elias, L. A., 2020. Gestão de crises e a pandemia de COVID-19. *Nação e Defesa*, n.º 156, pp. 9-44.

EMEE, 2020a. *Relatório sobre a aplicação da 1.a declaração do Estado de Emergência: 19 de março de 2020 a 2 de abril de 2020.,* Lisboa: EMEE .

EMEE, 2020b. *Relatório sobre a aplicação da 2.a declaração do estado de emergência 3 de abril de 2020 a 17 de abril de 2020,* Lisboa: EMEE.

EMEE, 2020c. *Relatório sobre a aplicação da 3.a declaração do estado de emergência 18 de abril de 2020 a 2 de maio de 2020,* Lisboa: EMEE.

Fradella, H. F., 2020. Why the special needs doctrine is the most appropriate fourth amendment theory for justifying police stops to enforce COVID-19 Stay-at-Home Orders. *ConLawNOW,* Vol. 12, pp. 1-14.

Freitas, T. F. d., 2020. A execução do estado de emergência e da situação de calamidade nas regiões autónomas: o caso da pandemia COVID-19. *e-Pública: Revista Eletrónica de Direito Público,* Vol. 7, n.º 1, pp. 44-77.

Gau, J. M., 2014. Procedural Justice and Police Legitimacy: A Test of Measurement and Structure. *American Journal of Criminal Justice,* Vol. 39, n.º 2, pp. 187-205.

Gau, J. M., Corsaro, N., Stweart, E. A. e Brunson, R. K., 2012. Examining macro-level impacts on procedural justice and police legitimacy. *Journal of Criminal Justice,* Vol. 40, n.º 4, pp. 333-343.

Gerber, M. M. e Jackson, J., 2016. Justifying violence: legitimacy, ideology and public support for police use of force. *Psychology, Crime & Law,* Vol. 23, n.º 1, pp. 79-95.

Ghebreyesus, T. A., 2020. *WHO Director-General's opening remarks at the media briefing on COVID-19.* Genebre: WHO.

Goethe, J. W. v., 1771. *Os sofrimentos do jovem Werther.* São Paulo: Alvorada/Martin Claret.

Gouveia, J. B., 2011. Regulação e limites dos direitos fundamentais. Em: U. d. Lisboa, ed., *Dicionário Jurídico de Administração Pública.* Lisboa:Universidade de Lisboa, pp. 450-472.

Gouveia, J. B., 2020. *Estado de exceção no direito constitucional.* Coimbra: Almedina.

Haberfeld, M., 2002. *Critical Issues in Police Training*. 1.ª ed. Upper Saddle River, New Jersey: Prentice Hall.

Haberfeld, M., 2016. The triangle of recruitment, selection and training in 21st Century policing. *Sociology of Crime Law and Deviance,* pp. 295-313.

Hamm, J. A., Trinkner, R. e Carr, J. D., 2017. Fair Process, Trust, and Cooperation: Moving Toward an Integrated Framework of Police Legitimacy. *Criminal Justice and Behavior,* Vol. 44, n.º 9, pp. 1183-1212.

Harkin, D., 2015. Police legitimacy, ideology and qualitative methods: A critique of procedural justice theory. *Criminology and Criminal Justice,* Vol. 15, n.º 5, pp. 594-612.

Hawdon, J. E., Griffin, S. P. & Ryan, J., 2003. Policing Tactics and Perceptions of Police Legitimacy. *Police Quarterly,* Vol. 6, n.º 4, pp. 469-491.

Herbert, S., 2006. Tangled up in blue: Conflicting paths to police legitimacy. *Theoretical Criminology,* Vol. 10, n.º 4, pp. 481-504.

Hinds, L. e Murphy, K., 2007. Public satisfaction with police: Using procedural justice to improve police legitimacy. *Australian and New Zealand Journal of Criminology,* Vol. 40, n.º 1, pp. 27-42.

Hough, M., *et al.*, 2010. Procedural justice, trust, and institutional legitimacy. *Policing,* Vol. 4, n.º 3, pp. 203-210.

Huq, A. Z., Jackson, J. e Trinkner, R., 2016. Legitimating Practices: Revisiting the Predicates of Police Legitimacy. *British Journal of Criminology,* Vol. 57, n.º 5, pp. 1101-1122.

Jackson, J., 2018. Norms, normativity and the legitimacy of justice institutions: International perspectives. *Annual Review of Law and Social Science,* Vol. 14, pp. 145–165.

Jackson, J. e Bradford, B., 2009. Crime, policing and social order: On the expressive nature of public confidence in policing. *British Journal of Sociology,* Vol. 60, n.º 3, p. 493-521.

Jackson, J., *et al.*, 2012. Why do People Comply with the Law?: Legitimacy and the Influence of Legal Institutions. *British Journal of Criminology,* Vol. 52, n.º 6, pp. 1051-1071.

Jackson, J., Hug, A. Z., Bradford, B. & Tyler, T. R., 2013. Monopolizing force? Police legitimacy and public attitudes toward the acceptability of violence. *Psychology, Public Policy, and Law,* Vol. 19, n.º 4, pp. 479-497.

Jackson, J. e Pósch, K., 2019. New directions of research in fairness and legal authority. Em: E. A. Lind, ed. *Social Psychology and Justice.* New York: Routledge, pp. 181-212.

Jonathan-Zamir, T. & Weisburd, D., 2013. The effects of security threats on antecedents of police legitimacy: Findings from a quasi-experiment in Israel. *Journal of Research in Crime and Delinquency,* Vol. 50, n.º 1, pp. 3-32.

Jones, D. J., 2020. The potential impacts of pandemic policing on police legitimacy: Planning past the COVID-19 crisis. *Policing: A Journal of Policy and Practice,* Vol. 14, n.º 3, pp. 579--586.

Kääriäinen, J. T., 2007. Trust in the Police in 16 European Countries. *European Journal of Criminology,* Vol. 4, n.º 4, pp. 409-435.

Kafka, F., 2021. *A metamoforse.* Lisboa: Editorial Presença.

Kant, I., 2013. *Crítica da razão pura*, 9.ª ed. Lisboa: Fundação Calouste Gulbenkian.

Kooistra, E. B., *et al.*, 2020. Mitigating covid-19 in a nationally representative uk sample: Personal abilities and obligation to obey the law shape compliance with mitigation measures. *Amsterdam Law School Research Paper,* Vol. 2020-19, pp. 1-36.

Lei n.º 27/2006, de 3 de julho. Lei de Bases da Protecção Civil. *Diário da República*, n.º 126/2006, Série I de 2006-07-03. Assembleia da República.

Leite, A. L., 2020. "Desobediência em tempos de cólera": a configuração deste crime em estado de emergência e em situação de calamidade. *Revista do Ministério Público:* Número Especial COVID-19, pp. 165-191.

Levisky, D. L., 2007. Aspectos do processo de identificação do adolescente na sociedade contemporânea e suas relações com a violência. Em: *Adolescência e Violência: Consquências da realdiade brasileira.* São Paulo: Casa do Psicologo, pp. 1-34.

Mendes, S. & Morgado, S., 2017. Intelligence services intervention: Constraints in portuguese democratic state. Em: *International Conference on Risks, Security and Citizens: Proceedings.* Setúbal: Município de Setúbal .

Miranda, J., 1986. Os direitos fundamentais na Ordem Constitucional Portuguesa. *Revista Española de Derecho Constitucional,* Vol. 6, n.º 18, pp. 107-140.

Miranda, J., 2018. *Direitos fundamentais*, 2.ª ed. Coimbra: Almedina.

Morgado, S., 2013. *Going global: Health organizations and networking – information society and social media.* Slovak Republic, EDIS – Publishing Institution of the University of Zilina, pp. 47-51.

Morgado, S. e Mendes, S., 2013-2014-2015. O futuro numa década: Os desafios económicos e securitários de Portugal. *Politeia: Revista do Instituto de Ciências Policiais e Segurança Interna,* 1: Studio varia (Estudos Comemorativos dos 30 anos do Instituto Superior de Ciências Policiais), pp. 9-35.

Murphy, K., Williamson, H. e Sargeant, E., 2020. Why people comply with COVID-19 social distancing restrictions: Self-interest or duty?, pp. 477-496. doi: *Australian & New Zealand Journal of Criminology,* Vol. 53, n.º 4, p. 53(4).

O'Brien, T. C. e Tyler, T. R., 2019. Rebuilding trust between police & communities through procedural justice & reconciliation. *Behavioral Science & Policy,* Vol. 5, n.º 1, pp. 35-50.

Palmer, D., 2020. Pandemic policing needs to be done with the public's trust, not confusion. *The Conversation.* [Online] Available at: https://theconversation.com/pandemic-policing-needs-to-be-done-with-the-publics-trust-not-confusion-135716 [Acedido em 5 Janeiro 2021].

Papp, J., Smith, B., Wareham, J. e Wu, Y., 2019. Fear of retaliation and citizen willingness to cooperate with police. *Policing and Society,* Vol. 29, n.º 6, pp. 623-639.

Perry, G. & Jonathan-Zamir, T., 2020. Expectations, effectiveness, trust, and cooperation: Public attitudes towards the Israel Police during the COVID-19 pandemic. *Policing: A Journal of Policy and Practice*, pp. 1-19.

Popelier, P., 2020. COVID-19 legislation in Belgium at the crossroads of a political and a health crisis. *The Theory and Practice of Legislation,* Vol. 8, n.º 1-2, pp. 131-153.

Reicher, S. e Stott, C., 2020a. On order and disorder during the COVID-19 pandemic. *British Journal of Social Psychology,* Vol. 59, n.º 3, pp. 694-702.

Reicher, S. e Stott, C., 2020b. Policing the coronavirus outbreak: Processes and prospects for collective disorder. *Policing: A Journal of Policy and Practice,* Vol. 14, n.º 3, pp. 569-573.

Ribeiro, L. J. B. R., 2011. A relevância do princípio da precaução numa política integrada para o mar. *Nação e Defesa,* n.º 128, pp. 125-158.

Silva, S. T. d., 2016. *Direito Constitucional I.* Coimbra: Instituto Jurídico da Faculdade de Direito da Universidade de Coimbra.

Sunshine, J. e Tyler, T. R., 2003. The Role of Procedural Justice and Legitimacy in Shaping Public Support for Policing. *Law and Society Review,* Vol. 37(3), pp. 513-548.

Tyler, T. R., 2002. A National Survey for Monitoring Police Legitimacy. *Justice Research and Policy,* Vol. 4(1-2), pp. 71-86.

Tyler, T. R., 2003. Procedural Justice, Legitimacy, and the Effective Rule of Law. *Crime and Justice,* Vol. 30, pp. 283-357.

Tyler, T. R., 2004. Enhancing Police Legitimacy. *Annals of the American Academy of Political and Social Science,* Vol. 593(1), pp. 84-99.

Tyler, T. R., 2006. *Why people obey the law.* New Jersey: Princeton University Press.

Tyler, T. R., 2011. Trust and legitimacy: Policing in the USA and Europe. *European Journal of Criminology*, Vol. 8(4), pp. 254-266.

Tyler, T. R. e Jackson, J., 2013. Popular legitimacy and the exercise of legal authority: Motivating compliance, cooperation, and engagement. *Psychology, Public Policy, and Law,* Vol. 20(1), pp. 78-95.

Valente, M. M. G., 2012. Os desafios emergentes de uma polícia de um estado de direito e democrático. *Politeia,* Vol. 9, pp. 255-272.

Valente, M. M. G., 2019. *Teoria Geral do Direito Policial.* Coimbra: Almedina.

Van Rooij, B., *et al.*, 2020. Compliance with COVID-19 mitigation measures in the United States. *Amsterdam Law School Research Paper,* Vol. 2020-21, pp. 1-41.

Wolfe, S. E. e Piquero, A. R., 2011. Organizational justice and police misconduct. *Criminal Justice and Behavior,* Vol. 38(4), pp. 332-353.

Worden, R. E. e McLean, S. J., 2017. Research on police legitimacy: the state of the art. *Policing,* Vol. 40(3), pp. 480-513.

World Economic Forum, 2020. *The Global Risks Report 2020.* [Online] Available at: http://wef.ch/risks2019 [Acedido em 26 Janeiro 2022].

Zucca, L., 2009. A Transatlantic divide between fundamental rights and security. *Boston College International and Comparative Law Review,* Vol. 32, n.º 2, pp. 231-240.

REVISTA NAÇÃO E DEFESA
Números temáticos publicados

1998	84	Inverno	Uma Nova NATO numa Nova Europa
	85	Primavera	Portugal e o Desafio Europeu
	86	Verão	O Desafio das Águas: Segurança Internacional e Desenvolvimento Duradouro
	87	Outono	O Estado em Mudança
1999	88	Inverno	Mulheres nas Forças Armadas
	89	Primavera	Portugal na NATO: 1949-1999
	90	Verão	Economia & Defesa
	91	Outono	Operações de Paz
2000	92	Inverno	Portugal e as Operações de Paz na Bósnia
	93	Primavera	Novos Rumos da Educação para a Cidadania
	94	Verão	Democracia e Forças Armadas
	95/96	Outono-Inverno	Prevenção de Conflitos e Cultura da Paz
2001	97	Primavera	Nova Ordem Jurídica Internacional
	98	Verão	Forças Armadas em Mudança
	99	Outono	Segurança para o Século XXI
	100	Inverno	De Maastricht a Nova Iorque
2002	101	Primavera	Europa e o Mediterrâneo
	102	Verão	Repensar a NATO
	103	Outono-Inverno	Novos Desafios à Segurança Europeia
	Extra	Dezembro	Cooperação Regional e a Segurança no Mediterrâneo (C4)
2003	104	Primavera	Evolução das Nações Unidas
	Extra	Abril	A Revolução nos Assuntos Militares
	105	Verão	Soberania e Intervenções Militares
	106	Outono-Inverno	A Nova Carta do Poder Mundial
2004	107	Primavera	Forças Armadas e Sociedade. Continuidade e Mudança
	Extra	Julho	Educação da Juventude. Carácter, Liderança e Cidadania
	108	Verão	Portugal e o Mar
	109	Outono-Inverno	Segurança Internacional & Outros Ensaios
2005	110	Primavera	Teoria das Relações Internacionais
	111	Verão	Raymond Aron. Um Intelectual Comprometido
	112	Outono-Inverno	Número não Temático
2006	113	Primavera	Número não Temático
	114	Verão	Segurança na África Subsariana
	115	Outono-Inverno	Portugal na Europa Vinte Anos Depois

2007	116	Primavera	Número não Temático
	117	Verão	Número não Temático
	118	Outono-Inverno	Políticas de Segurança e Defesa dos Pequenos e Médios Estados Europeus
2008	119	Primavera	Transição Democrática no Mediterrâneo
	120	Verão	Número não Temático
	121	Outono-Inverno	Estudos sobre o Médio Oriente
2009	122	Primavera	O Mar no Pensamento Estratégico Nacional
	123	Verão	Portugal e a Aliança Atlântica
	124	Outono-Inverno	Que Visão para a Defesa? Portugal-Europa-NATO
2010	125	Primavera	Visões Globais para a Defesa
	126		O Conceito Estratégico da NATO
	127		Dinâmicas da Política Comum de Segurança e Defesa da União Europeia
2011	128		O Mar no Espaço da CPLP
	129		Gestão de Crises
	130		Afeganistão
2012	131		Segurança em África
	132		Segurança no Mediterrâneo
	133		Cibersegurança
2013	134		Ásia-Pacífico
	135		Conselho de Segurança da ONU
	136		Estratégia
2014	137		Reflexões sobre a Europa
	138		Brasil
	139		Portugal na Grande Guerra
2015	140		Nuclear Proliferation
	141		Arquipélago dos Açores
	142		India
2016	143		Terrorismo Transnacional
	144		The EU Comprehensive Approach: Concepts and Practices
	145		Leituras da Grande Guerra
2017	146		Drones
	147		Brexit
	148		Grupos Islamistas Radicais

2018	149		Europe and Refugees
	150		European Defence
	151		Geopolítica Aplicada
2019	152		Terrorismo e Violência Política
	153	Agosto	Segurança Energética e Economia do Gás
	154	Dezembro	Pontes Sobre o Atlântico
2020	155	Abril	Desafios Europeus
	156	Agosto	Segurança em Tempo de Crise
	157	Dezembro	Mulheres, Paz e Segurança
2021	158	Abril	Segurança Internacional
	159	Agosto	Desafios Geopolíticos
	160	Dezembro	Relações Europa-África
2022	161	Abril	Conflitos Armados
	162	Agosto	O Espaço Pós-Soviético

Política Editorial

A *Nação e Defesa* proporciona um espaço de reflexão que privilegia diferentes paradigmas e perspetivas relevantes para o conhecimento e análise de questões no quadro da segurança e defesa, no plano teórico e aplicado. A revista encontra-se vocacionada para a compreensão, exame crítico e debate de matérias no âmbito da segurança e defesa internacional e nacional.

Tem como prioridade promover o conhecimento e a reflexão pluridisciplinar, nomeadamente no campo dos Estudos de Segurança, Estudos Estratégicos, Ciência Política, História, Estudos Diplomáticos, Relações Internacionais, Sociologia, Direito Internacional Público e Economia.

Nação e Defesa é uma publicação periódica de natureza científica, que adota o sistema de arbitragem por pares na admissão e aprovação dos artigos submetidos.

Editorial Policy

Nation and Defense provides a space for reflection that privileges different paradigms and perspectives relevant to theoretical and applied analysis of security and defense matters. The journal is dedicated to the critical examination and scientific debate on international security and defense.

Its priority is to promote a multidisciplinary approach to Security Studies, Strategic Studies, Political Science, History, Diplomatic Studies, International Relations, Sociology, International Law and Economics.

Nation and Defense is a scientific publication, which adopts the peer review system in the admission and approval of submitted articles.

NORMAS DE COLABORAÇÃO

O artigo proposto para publicação, em português ou inglês, deve ser enviado via correio eletrónico para idn.publicacoes@defesa.pt devendo observar as seguintes normas:

- Ter entre 5.000 a 8.000 palavras (espaços incluídos) em Word;
- Ser acompanhado de um resumo em português e em inglês (até 150 palavras cada);
- Ter título e palavras-chave em português e inglês;
- Ser redigido de acordo com o sistema de referências de Harvard.

Os textos submetidos devem ser inéditos, não editados ou apresentados em quaisquer outras publicações.

O artigo, sem indicação do autor e acompanhado pela Ficha de Identificação (disponível em https://www.idn.gov.pt/conteudos/documentos/FichadeAutor.pdf devidamente preenchida, será apreciado em regime de anonimato (*blind peer review*).

A revista *Nação e Defesa* adota o sistema de referência bibliográfica de Harvard, disponível em https://library.aru.ac.uk/referencing/harvard.htm. Este sistema emprega a referência autor e data no corpo do texto e uma lista de referências bibliográficas no final do artigo escrito, organizada por ordem alfabética. A lista de referências contém uma relação detalhada dos livros, revistas e fontes eletrónicas citadas.

Os artigos publicados são da inteira responsabilidade do autor.

Cada autor receberá dois exemplares da revista na morada indicada.

Ao submeter um manuscrito à revista, o(s) autor(es) declara(m) que autoriza(m), a título gracioso, a digitalização, o carregamento e a divulgação do referido artigo nas plataformas de conteúdos digitais do IDN e em repositórios e bases de dados bibliográficos. Os casos não especificados nestas normas de colaboração deverão ser apresentados ao Editor.

COLLABORATION RULES

The article submitted for publication, in Portuguese or English, must be sent by email to idn. publicacoes@defesa.pt observing the following rules:

- Length between 5,000 and 8,000 words (spaces included) in a Word format;
- Abstract in Portuguese and English (up to 150 words each);
- Title and keywords in Portuguese and English;
- Adoption of the Harvard reference system.

Submitted texts must be unpublished, unedited or presented in any other publications.

The article, without the author name and accompanied by the Identification Form available in https://www.idn.gov.pt/conteudos/documentos/author_form.pdf duly completed, will be evaluated anonymously (blind peer review).

Nation and Defense adopts the Harvard bibliographic reference system - https://library.aru.ac.uk/referencing/harvard.htm. This system uses the author and date in the text body and a list of references at the end of the article, organized in alphabetical order. The reference list contains a detailed list of cited books, journals and electronic sources.

Published articles are the sole responsibility of the author.

Each author will receive two copies of the journal.

By submitting a manuscript to the journal, the author (s) declare that they gracefully allow the digitization, upload, and dissemination of the article on IDN digital content platforms, repositories and bibliographic databases. Cases not specified in these collaboration rules should be submitted to the Editor

NAÇÃO E DEFESA

Revista quadrimestral

Nome/Name _____

_____

Morada/Adress _____

_____

Localidade/City _____

Cód. Postal/Zip _____ - _____ _____

_____ NIF _____

Country _____

E-mail _____

Tel./Phone _____

☐ Renovação/Renewal – Assin. nº/Subscrip. nr. _____

☐ Nova assinatura/New subscription

Assinatura/Signature _____

Data/Date _____

Assinatura Anual/Annual Subscription (3 nºs /issues)

☐ Instituições/Institutions 40,00 €

☐ Individuais/Individuals 25,00 €

☐ Estudantes/Students 20,00 € (anexar comprovativo deste ano)

Números Anteriores/Previous Issues – 8,50 € cada/each + portes/ /postage charges

☐ ☐ ☐ ☐ ☐ ☐

Pré-Pagamento/Prepayment

☐ **Numerário**

☐ **Cheque** nº _____ Banco _____ à ordem do IDN

☐ **Transferência Bancária** NIB 0781 0112 0000 000 7777 20
(anexar comprovativo da Transferência)

☐ **Bank Transfer** (compulsory for foreign subscriptions)

IBAN – PT50 0781.0112 0000 000 7777 20
BIC (SWIFT) – IGCPPTPL

INSTITUTO DA DEFESA NACIONAL
Calçada das Necessidades, 5, 1399-017 Lisboa
PORTUGAL

www.idn.gov.pt
idn.publicacoes@defesa.pt
tel. + 351 21 392 46 00 Fax + 351 21 392 46 58