RBED Revista Brasileira de Estudos de Defesa

Vol. 7, n. 2, jul./dez., 2020
DOI: 10.26792/RBED.v7n2.2020

ABED

ISSN: 2358-3932

Associação Brasileira de Estudos de Defesa
CNPJ 08.743.954/0001-04

REVISTA BRASILEIRA DE ESTUDOS DE DEFESA

Niterói, v. 7, nº 2, Jul./Dez. 2020

SOBRE A REVISTA

A *Revista Brasileira de Estudos de Defesa (RBED)* é um periódico acadêmico semestral editado pela Associação Brasileira de Estudos da Defesa (ABED), segundo normas internacionais de editoração científica.

A *RBED* foi criada em 2014 com o objetivo de promover o desenvolvimento das áreas de defesa e segurança, incentivando o intercâmbio de ideias, o debate de problemas pertinentes a esses temas e o diálogo acadêmico multidisciplinar que aborde, a partir de diferentes áreas do conhecimento, os campos de interesse da publicação.

A Revista publica artigos, ensaios e resenhas inéditas, aprovados pelo sistema de avaliação pelos pares. É voltada a trabalhos que tratem de temas relacionados à defesa nacional, segurança internacional, e seus temas afins, tais como: segurança nacional, guerra e paz, relações entre forças armadas e sociedade, ciência e tecnologia no âmbito da defesa nacional, estudos militares, estudos estratégicos, políticas públicas de segurança e defesa, relações internacionais, ciência política, engenharia de produção, dentre outros.

R454 Revista Brasileira de Estudos de Defesa / Associação Brasileira de Estudos de Defesa. v. 1, n. 1 (2014–). Niterói : Associação Brasileira de Estudos de Defesa, 2014–.
ISSN 2358-3932 - versão online
1. Defesa nacional – Periódicos. I. Associação Brasileira de Estudos de Defesa.
CDU 355.45(81)

Catalogação na publicação: Mônica Ballejo Canto – CRB 10/1023

ASSOCIAÇÃO BRASILEIRA DE ESTUDOS DE DEFESA (ABED)

Sumário

Ensaio

Artigos

Resenha

EDITORIAL

É com grande satisfação que publicamos o novo número da *Revista Brasileira de Estudos de Defesa (RBED)*. A nova edição apresenta as publicações que compõem o dossiê "Tecnologia, cibernética e defesa no Brasil", organizado pelo Prof. Dr. Marco Aurélio Guedes (UFPE). O dossiê congrega trabalhos que lançam luzes acerca do ciberespaço e de suas implicações para políticas de defesa, estratégia militar e fenômenos tradicionais da segurança internacional, como o terrorismo.

Em "Guerra Híbrida", Guedes e Casalunga abordam essa modalidade de beligerância sob a perspectiva do emprego da tecnologia da informação, tendo como palco o conflito Rússia-Ucrânia. Em sintonia com a avaliação das implicações estratégicas do ciberespaço e de suas tecnologias, Devanny,

Goldoni e Medeiros analisam em "The 2019 Venezuelan Blackout and the consequences of cyber uncertainty" como as ferramentas cibernéticas ampliam o horizonte de opções da interação conflitiva entre Estados. Entretanto, a ótica interestatal não é a única que está presente neste número. Tendo o Estado Islâmico como estudo de caso, o artigo "Cyberterrorism 2.0 or terrorist use of social media" de Vilar-Lopes e Medeiros, proporciona uma rica análise sobre como fenômenos clássicos da segurança internacional — como o terrorismo — se aproveitam do espaço cibernético para a produção de efeitos estratégicos. Diante das severas implicações para a defesa do desenvolvimento do domínio, estratégias e meios cibernéticos, o artigo de Loose e Pagliari — "Israel e defesa cibernética" — se debruça sobre como Israel articula os setores governamental, privado e acadêmico em busca de respostas aos seus desafios de segurança. De forma complementar, em "Guerra cibernética, ameaças às infraestruturas críticas", Pinto e Grassi lançam luzes sobre o caso brasileiro.

Conforme se observa, o presente número aborda, sob distintas perspectivas, as implicações do desenvolvimento do domínio cibernético, seus meios (cinéticos e não-cinéticos) e seus desdobramentos estratégicos. Nesse sentido, "Armas Inteligentes no Ciberespaço" de Assis, Bittencourt e Tavares analisa as oportunidades e desafios desses instrumentos na contemporaneidade. Encerrando o dossiê, o ensaio "Por que o Brasil deveria adotar uma distro Linux própria?" demonstra que os trabalhos desta edição refletem uma necessária e robusta agenda de pesquisa com importantes desdobramentos potenciais para a política de defesa no Brasil.

Somando-se aos artigos e ao ensaio que compõem o dossiê "Tecnologia, cibernética e defesa no Brasil", esta edição nos apresenta dois artigos de

peso acerca de um tema de fundamental relevância para os estudos de defesa no Brasil contemporâneo: as relações civil-militares. Com destacada profundidade analítica, Cortinhas e Vitelli abordam as limitações das reformas para o controle civil sobre as forças armadas. Com recorte temporal limitado aos governos do Partido dos Trabalhadores (PT), o artigo proporciona um rico panorama histórico e explicações que contribuem para iluminar desafios recentes. Também abordando o tema das relações civil-militares, Succi Junior e Saint-Pierre analisam comparativamente a relação entre Forças Armadas e Segurança Pública na Argentina e no Brasil. Em sintonia com a temática supracitada, Souza encerra esta edição com uma resenha do "Dicionário de Segurança e Defesa" (Unesp 2018).

Conforme o leitor pode perceber, o presente número apresenta uma mistura entre o novo (Tecnologia e Cibernética) e o tradicional (relações civil-militares) nos estudos de defesa. Certos de que a presente edição ilustra com primor a vitalidade de nossa comunidade epistêmica, a editoria da *Revista Brasileira de Estudos de Defesa* deseja a todos uma excelente leitura.

Augusto W. M. Teixeira Júnior
Editor-Chefe

Dossiê Ciber

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

Hybrid War: the use of information technology in Russia-Ukraine conflict (2014-2015).

Rev. Bras. Est. Def. v. 7, nº 2, jul./dez. 2020, p. 9-36
DOI: 10.26792/RBED.v7n2.2020.75208
ISSN 2358-3932

MARCOS AURÉLIO GUEDES DE OLIVEIRA
FERNANDO HENRIQUE CASALUNGA

INTRODUÇÃO

Nossa análise da guerra híbrida desencadeada entre Rússia e Ucrânia (2014-2015) objetiva responder ao seguinte questionamento: como a tecnologia da informação amplia a assimetria de poder entre os Estados contemporâneos?

Sem embargo, partimos do pressuposto de que, com o avanço das tecnologias de informação, o ciberespaço se tornou fulcral para projeção de poder do Estado russo. O argumento está ancorado na descrição temporal das operações que ratificam a relevância deste novo engenho de força para consecução de objetivos estratégicos da Federação Russa em seu entorno regional.

Destarte, sustentamos que, ao utilizar o ciberespaço para auxiliar as operações militares, a simbiose inovadora entre setores especiais das Forças Armadas russas e *hackers* civis produziu efeito sinérgico que resultou em vantagem considerável à Rússia durante o conflito com a anexação do território da península da Crimeia e apoio aos movimentos separatistas que ocuparam a região leste da Ucrânia.

A fim de sustentar a validade da inferência descritiva construída, o ponto chave do artigo é marcado pela identificação do funcionamento desta

Marcos Aurélio Guedes de Oliveira — Doutor em Government pela University of Essex, Professor Titular do Departamento de Ciência Política na Universidade Federal de Pernambuco. Coordenador Geral do projeto CAPES/MD Pro-Defesa IV "Ciência, Tecnologia e Inovação em Defesa: Cibernética e Defesa Nacional".
Fernando Henrique Casalunga — Doutorando do Programa de Pós-Graduação em Ciência Política pela Universidade Federal do Rio Grande do Sul/UFRGS. Bacharel e Mestre em Ciência Política pela Universidade Federal de Pernambuco (UFPE); Bacharel e Licenciatura em História pela Universidade Estadual Paulista (UNESP). Bolsista Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES).

simbiose, compreendida em sua condição de mecanismo capaz de conectar a estratégia russa ao nível operacional e tático de ação militar — razão pela qual aplicamos o método qualitativo da dependência da trajetória em conjunto com a técnica de rastreamento de processos para analisar relatórios de empresas especializadas em segurança cibernética e instituições governamentais à procura de evidências que permitam desvelar o funcionamento deste mecanismo.

De modo que este artigo se divide em duas seções: a primeira discute a relevância da segurança frente aos riscos e ameaças do espaço cibernético para delimitar o conceito de guerra híbrida utilizado neste estudo; a segunda identifica o mecanismo responsável por conectar os níveis estratégico, tático e operacional militar ao verificar as ações conjuntas de atores estatais e *hackers* não-estatais envolvidos no conflito.

Ao elucidar como a tecnologia de informação amplia, sobremaneira, as capacidades de projeção de poder regional de uma grande potência como a Rússia, o artigo contribui para o avanço dos estudos sobre a relevância deste novo engenho de força para os Estados contemporâneos.

GUERRA HÍBRIDA: CIBERESPAÇO, SEGURANÇA CIBERNÉTICA E AMEAÇAS PERSISTENTES AVANÇADAS

Em vista da crescente relevância estratégica concedida ao ambiente cibernético, comunidades acadêmicas, civis e militares têm se debruçado sobre o problema fundamental da Defesa e Segurança no ciberespaço, a fim de compreender os movimentos de atores estatais e não-estatais no que concerne às estratégias, táticas e operações utilizadas para atuarem no ciberespaço. À medida que a pesquisa científica avança, novos enigmas teóricos emergem, refletindo a complexidade analítica e a dinamicidade do desafio cibernético (Gartzke 2013; Kello 2013; Lindsay 2013; 2015; Geers 2015; Kjennerud and Cullen 2016; Vaczi 2016; Olszewski 2018; Weiss and Jankauskas 2019).

Neste ambiente, as ameaças se multiplicam e modificam dia a dia, e quase todas as hostilidades envolvem o uso de *softwares* maliciosos que são de difícil detecção e rastreamento. Razão pela qual Kello (2013) define o ciberespaço como um ambiente anárquico, que oferece ameaças à humanidade em três áreas: físicas, psicológicas e de infraestrutura crítica.

Com o advento do século XXI, a emergência de uma sociedade amplamente conectada fez com que a importância deste domínio para os Estados se tornasse indiscutível. Por conseguinte, o fracasso na proteção do fluxo de dados via ciberespaço gera problemas que perpassam diferentes segmentos, desde o funcionamento do comércio e do sistema financeiro, a tro-

ca de informações entre órgãos públicos e até a estabilidade de infraestruturas críticas, acarretando riscos à desestabilização de sociedades inteiras (Geers 2015).

Frente a este cenário, o conceito de segurança cibernética consiste, *grosso modo*, em adotar medidas para proteger as operações de um sistema de computador ou a integridade de seus dados frente a uma ação hostil (Weiss and Jankauskas 2019). Com pretensão de classificar os dilemas associados à segurança no espaço de informação, mais especificamente os riscos e as ameaças que circulam nesse ambiente, Weiss e Jankauskas (2019) constroem uma tipologia que se propõe a identificar a realidade fenomenológica da natureza desses problemas.

Os riscos estariam, então, associados à vulnerabilidade das infraestruturas críticas, instalações físicas, redes, serviços e bens responsáveis por proverem recursos essenciais à vida humana — energia elétrica, gás e água potável —, sistemas altamente integrados interconectados via ciberespaço que podem ter seu funcionamento comprometido por ameaças virtuais. De forma complementar, as ameaças são caracterizadas como os atores e as armas que "têm a capacidade de prejudicar a segurança de outros e que são percebidos por seus alvos potenciais como tendo intenção de fazê-lo" (Wallander and Keohane 1999, *apud* Weiss and Jankauskas 2019, 5).

Nomeadas como Ameaças Persistentes Avançadas (APA) estes grupos possuem alto grau de especialização, armas cibernéticas de difícil detecção, capacidade de adaptação e recursos para atuarem por longos períodos de tempo (Weedon 2015). Contudo, embora "originalmente usada para descrever invasões cibernéticas contra organizações militares, as APA evoluíram e não estão mais confinadas às forças armadas" (Olszewski 2018, 5). Pertencem, pois, a uma nova geração de ameaças que utilizam o ciberespaço para subtrair informações sigilosas que possam ser repassadas a terceiros ou mesmo utilizadas pelos setores de inteligência dos Estados (Gartzke 2013, 70).

Trata-se, portanto, de atores como espiões, *hackers*, criminosos e terroristas cibernéticos que atuam em esquemas altamente organizados, capazes de orquestrarem ataques sofisticados sem que sua presença seja notada até que a ação tenha ocorrido e os danos causados (Cavelty 2013, *apud* Weiss and Jankauskas 2019, 5). Todavia, além de representarem ameaças à segurança cibernética de estruturas físicas, as APA ganharam importância estratégica para os Estados contemporâneos como ferramentas úteis em operações ofensivas "eficazes para a infiltração de sistemas de defesa estrangeiros ou roubo de segredos militares, principalmente devido à relativa facilidade de execução, bem como um baixo risco de revelar a fonte real e o beneficiário de tal ataque" (Gajewski 2013, *apud* Olszewski 2018, 5).

No que concerne à análise dos riscos e ameaças à segurança cibernética, a literatura apresenta evidências que sustentam o pressuposto de que as capacidades convencionais de emprego da força pelos Estados fortes impõem restrições às ações ofensivas de entes mais fracos. Por essa lógica, os riscos de que ocorram ataques cibernéticos capazes de causar danos graves às infraestruturas físicas de países militarmente mais fortes é menor (Gartzke 2013; Lindsay 2013). Desse modo, ameaças de menor potencial de impacto, como aquelas especializadas em espionagem cibernética, despontam como estrategicamente mais atrativas aos Estados que pretendem utilizar o ciberespaço para atingirem seus objetivos estratégicos (Lindsay 2015).

Frente a esse cenário, soldados dividem espaço com engenheiros de combate cibernético, ao mesmo tempo em que a infantaria se converte em invasores de rede, cujas armas principais são computadores munidos por *malwares*[1] (Geers 2015). Em meio aos avanços tecnológicos que resultaram na produção destes novos engenhos de força, diversos conceitos foram propostos para explicar a realidade dos conflitos contemporâneos.

Inicialmente, termos como guerra convencional, irrestrita, composta e de quarta geração, fundiram-se em um grande guarda-chuva teórico conceitual denominado guerra híbrida, que se constitui com base nos postulados de diversas escolas de pensamento (Hoffman 2007, 30). O conceito formulado por Hoffman (2007) tornou-se chave para orientar o entendimento da literatura e de organismos internacionais dedicados ao estudo da interconexão entre as ações de agentes estatais e/ou não-estatais em conflitos contemporâneos, desde o nível estratégico até o operacional.

Neste ensejo, após a eclosão do conflito entre russos e ucranianos em 2014, documentos oficiais publicados pela Assembleia Parlamentar da Organização do Tratado do Atlântico Norte (OTAN) (2015) apresentavam um entendimento oficial do conceito semelhante ao proposto por Hoffman (2007), compreendido como "uma cadeia de táticas assimétricas que estão sendo realizadas apenas por meios não-militares e nas quais os meios militares têm apenas um papel de apoio" (Vaczi 2016, 23–24).

No entanto, embora capazes de descrever parte da composição da guerra contemporânea ao abordar a crescente sofisticação e complexificação da atuação dos atores não-estatais, tais entendimentos eram muito estreitos e desconsideravam o papel estratégico do Estado como ator fundamental das guerras híbridas (Kjennerud and Cullen 2016).

> A guerra híbrida do Estado envolve a plena integração dos meios militares e não-militares com o poder do Estado para alcançar obje-

> tivos políticos, nos quais o uso da força desempenha um papel central. Estados com habilidades altamente centralizadas para coordenar e sincronizar seus instrumentos de poder (governo, economia, mídia, etc.) podem criar efeitos multiplicadores de força sinérgica (Kjennerud and Cullen 2016, 1).

Kjennerud e Cullen (2016) ampliaram essa concepção e dividiram os instrumentos de poder nas categorias militar, política, econômica, civil e informacional, para identificar a relevância de sua utilização sincronizada e coordenada pelos Estados, com fins de atingir sistemas de informação e/ou infraestrutura crítica do oponente e produzir "mudanças no estado comportamental ou físico de um sistema ou elementos do sistema, de acordo com objetivos políticos" (Kjennerud and Cullen 2016, 1).

Por conseguinte, o International Institute for Strategic Studies (IISS) (2016), passou a descrever as guerras híbridas de modo mais preciso, na qualidade de "campanhas sofisticadas que combinam operações convencionais e especiais de baixo nível; ações cibernéticas e espaciais ofensivas; e operações psicológicas que usam a mídia social e tradicional para influenciar a percepção popular e a opinião internacional" (IISS, *apud* Vaczi 2016, 38). Por essa perspectiva, a guerra híbrida é entendida como o uso de todos os instrumentos de poder disponíveis ao Estado para atingir as vulnerabilidades do oponente.

Frente ao exposto, adotamos o modelo analítico proposto por Kjennerud e Cullen (2016) em consonância com o Balanço Militar (2015) do IISS (2016) para operacionalizar o conceito de guerra híbrida tomando o uso do ciberespaço como ferramenta chave para consecução das diretrizes estratégicas, operacionais e táticas da Rússia no conflito com a Ucrânia (2014-2015).

Destarte, nossa análise do emprego da tecnologia da informação neste conflito destaca os movimentos conjuntos de atores estatais e/ou não-estatais no ambiente cibernético e cinético para compreensão da guerra híbrida conforme empregada pela Rússia, marcada pela coordenação de atividades adaptáveis e flexíveis para produzir força sinérgica capaz de auxiliar na consecução de seus objetivos estratégicos regionais.

A seção seguinte apresenta inferência descritiva sobre a ação conjunta de grupos *hackers* e forças especiais russas em ataques cibernéticos e ações físicas, e revela algumas das principais ameaças e armas cibernéticas utilizadas no conflito. Assim, fomentamos o debate sobre como novos engenhos de força podem ser utilizados para ampliar a assimetria de poder entre Estados contemporâneos.

A SIMBIOSE *HACKER*-EXÉRCITO: O EMPREGO DA TECNOLOGIA DA INFORMAÇÃO NO CONFLITO RÚSSIA-UCRÂNIA (2014-2015)

Nesta seção apresentamos evidências que comprovam a congruência dos ataques cibernéticos com as ações físicas durante o conflito Rússia-Ucrânia (2014-2015). A metodologia adotada contribui para que possamos oferecer uma explicação robusta sobre as conjunturas históricas e as consequências da guerra híbrida para o aumento da assimetria de poder regional entre estes Estados.

Ao aplicarmos a técnica da dependência da trajetória,[2] procuramos pontuar momentos críticos do conflito que sinalizem o modo inovador como o Estado russo utilizou o ciberespaço para consecução de objetivos estratégicos durante o conflito. Nesse ensejo, utilizamos o rastreamento de processos[3] para conferir se a incorporação da dimensão cibernética ao modo de operação das Forças Armadas russas (simbiose) foi suficiente para produzir força sinérgica neste conflito.

Deste modo, o componente descritivo da série de momentos específicos que marcaram as principais etapas do processo causal observável (PCO) torna-se o ponto fulcral da análise (Mahoney 2012, 586). Por essa lógica, a condição em que ocorrem os movimentos dos atores é identificada mediante a coleta de evidências que permitam verificar o funcionamento do mecanismo. Por essa razão destacamos como o ciberespaço foi utilizado para ampliar a capacidade de projeção de poder da Federação Russa em seu entorno regional.

Os relatórios de agências especializadas em segurança cibernética e de instituições governamentais analisados contêm uma série de evidências que indicam a ligação entre as atividades de atores não-estatais (APA) em conjunto com as forças especiais russas (Spetsnaz),[4] simbiose que compõe o mecanismo causal ora identificado enquanto condição suficiente para promoção de nosso fenômeno de interesse, a guerra híbrida.

Sem embargo, as atividades russas estiveram vinculadas a uma série de ataques de infiltração via ciberespaço, que fizeram uso de *spear phishing*[5] para instalar armas cibernéticas capazes de subtrair informações sigilosas e/ou causar danos cinéticos, paralisando sistemas de computador, setores de comunicação, bancários, eleitorais e de infraestruturas críticas (Crowdstrike 2014; 2015; 2016; FireEye 2014; 2016; F-Secure Labs 2016; LookingGlass 2015; ICS-CERT 2016; E-ISAC 2016).[6]

A partir da correlação observada entre os ataques cibernéticos e o conflito cinético, o relatório do Grupo de Inteligência sobre Ameaças Cibernéticas (CTIG) apresenta evidências que revelam como a Rússia utilizou o ciberespaço para consecução de seus interesses estratégicos regionais em território ucraniano, destacando "uma mistura alarmante entre espionagem cibernética, guerra física e as forças políticas por trás delas" (LookingGlass 2015, 3).

Conforme aponta o relatório, a ligação entre a campanha de espionagem cibernética e atores estatais das agências do Serviço Federal de Segurança (FSB) e de Comunicações e Informações Governamentais (FAGCI) da Federação Russa é ponto chave para compreensão da vantagem militar russa sobre as forças ucranianas, "além das motivações políticas e militares, a análise da linha do tempo dos ataques, juntamente com o mundo real e o contexto digital, sugere o envolvimento da Rússia" (LookingGlass 2015, 6).

Cientes da dificuldade de atribuição das ações cibernéticas ofensivas, o Serviço de Segurança da Ucrânia (SBU) e a LookingGlass chamaram a atenção para o modo como as agências estatais russas envolvidas no conflito fizeram uso estratégico, tático e operacional do ciberespaço, destacando os movimentos da 16ª divisão da FAGCI e do 18º Centro do FSB. Não obstante, o SBU frisou que a subtração de informações do governo, polícia e militares pelos *hackers* forneceu detalhes dos planos de curto prazo delimitados pelo governo central de Kiev para conter o avanço das tropas do Kremlin (LookingGlass 2015).

Os ciberataques utilizaram *spear phishing* com informações úteis para os alvos ucranianos, os *e-mails* continham arquivos de extração automática (SFX) que colhiam documentos com informações legítimas relativas ao conflito russo-ucraniano para depois serem usados como iscas na próxima onda de ataques. A análise da infraestrutura de rede e das ameaças utilizadas pelos *hackers* identificou nomes de arquivos similares e períodos de maior volume de ataques cibernéticos coincidentes com o horário de trabalho em Kiev, fatores que facilitaram o rastreamento das atividades dessas ameaças (LookingGlass 2015, 18).

O quadro 1 sumariza as informações do relatório, que apresenta em detalhes a ligação entre os ataques cibernéticos e os principais eventos políticos e militares que ocorreram durante o conflito entre russos e ucranianos.

Quadro 1
Cronograma da campanha de espionagem cibernética
operação "Armadegon"

2014	Ação física	2014	Ação cibernética
15 Abril	Após separatistas tomarem o controle das cidades de Luhansk e Donetsk, o governo ucraniano anuncia uma "operação antiterrorista" para retomada dos territórios	16 abril	"install_flashplayer_aih.exe" dropper SFX instalado em arquivo formato Microsoft Word disparado via *spear phising* para alvos militares, mídia e org. governamentais
14 Junho	Separatistas derrubam avião militar ucraniano com 49 oficiais	14 Junho	Novos ciberataques são detectados utilizando o mesmo *malware* e portas de entrada TTPs para buscar informações sobre como a Ucrânia iria responder ao ocorrido
20 Junho	**Primeiro cessar-fogo** (1 semana)	20 Junho	Os ataques cibernéticos cessam (1 semana)
17 Julho	Queda do voo MH17 Malaysian Airlines (298 civis mortos), as forças armadas russas auxiliam a retomada das cidades ucranianas do leste que haviam sido tomadas pelas tropas do governo central	17 julho	"install.flashplayer_aih.exe" nova versão, o 123.cmd não inclui mais uma senha necessária para abrir o arquivo SFX de "sex.exe". Direcionado para alvos militares, mídia e org. governamentais. Arquivo contém relatório legítimo para notificação diária da Administração do Presidente da Ucrânia sobre as operações antiterroristas na Ucrânia, dados sobre ataques terroristas contra o exército ucraniano e suas perdas
24 Agosto	Após invasões das forças armadas russas nos territórios do leste, as forças ucranianas são forçadas a se retirar	26 agosto	Os ataques cibernéticos cessam na região leste, início da retomada da operação de espionagem

2014	Ação física	2014	Ação cibernética
12 Setembro	SBU anuncia que identificaram movimento de forças especiais russas programando novos ataques cibernéticos contra a Ucrânia	30 outubro 26 novembro	*Spear phising* com dois arquivos datados de 21 de agosto endereçados via email para contas pessoais e do Tribunal Internacional de Arbitragem Comercial da Câmara de Comércio e Indústria da Ucrânia são encontrados com *links* para páginas falsas de acesso ao Google Chrome
15 janeiro 29 janeiro	Após um longo combate as tropas ucranianas perdem o controle do aeroporto de Donetsk para os separatistas	25 janeiro	Execução de arquivo SFX contendo *malware* indexado a documento oficial escrito em ucraniano com dados sobre equipamentos e batalhões de reconhecimento envolvidos no conflito em julho de 2014
8 fevereiro	**Segundo cessar-fogo** Chefe do centro antiterrorista da SBU divulga informações sobre os ataques das forças especiais russas	15 fevereiro 16 fevereiro	Os ataques cibernéticos não param até a retirada das tropas ucranianas do Debaltaseve, só então os ataques cibernéticos cessaram. As ameaças foram movidas para servidores de uma transportadora internacional de logística de carne e uma loja de eletrônicos
			Dropper com relatório do centro antiterrorista da SBU sobre os territórios do leste é utilizado em novos ataques *spear phising* contra alvos militares
13 março	SBU divulga comunicado oficial sobre atividade cibernética russa atribuída à 16ª antiga agência do governo federal de comunicação e informação (FAGCI) e 18º centro de segurança federal (FSB) da Rússia	25 março	Após a publicação do relatório oficial da SBU novos ataques *spear phising* são identificados, dessa vez com as entradas de servidor TTPs monitoradas pela SBU modificadas. Dois arquivos SFX com novos códigos "tron.cmd" contendo malwares identificados

Fonte: Elaborado pelos autores com base em LookingGlass (2015)

Durante o conflito, distintas APA pró-rússia utilizaram táticas de intrusão sofisticadas para comprometer sistemas de informação do governo, mídia e infraestrutura crítica da Ucrânia, com ataques cibernéticos de negação

de serviço e espionagem. Destacamos as APA28: CyberBerkut; FancyBear/Sofacy/Pawn Storm e Sandworm (Crowdstrike 2014; 2015; 2016).

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

Uma das armas cibernéticas mais utilizadas na Ucrânia foi o BlackEnergy (BE), a evolução deste *malware* têm sido acompanhada por diversas empresas especializadas em segurança cibernética que apontam a convergência entre as atividades criminosas e a espionagem russa através do ciberespaço (FireEye 2014; F-Secure Labs 2016). No início do conflito variações como o BE.lite[7] e BlackEnergy2 (BB2)[8] atingiram alvos políticos na Ucrânia, ocasionando a queda de diversos sítios eletrônicos do governo, incluindo o do gabinete presidencial (Bergen and Maurer 2018); em sua versão recente, o *malware* comprometeu setores de infraestrutura crítica (ICS 2016; E-ISAC 2016).

Em fevereiro de 2014, uma onda de ataques cibernéticos utilizou essas variações para interferir nos serviços de telefonia celular dos membros do parlamento ucraniano, dificultando a comunicação e o processo decisório de resposta à invasão russa ao território da Crimeia. Apenas quatro dias após as operações via ciberespaço, instalações da empresa de comunicações Ukrtelecom foram invadidas e os cabos de fibra ótica adulterados, inviabilizando a conexão entre a península e o restante da Ucrânia (Maurer 2015, 81). A operação de sabotagem evitou que o poder público tomasse uma atitude com relação ao movimento das forças russas na Crimeia (Weedon 2015, 76).

No mês de março de 2014, o CyberBerkut assumiu a responsabilidade por atacar a página da rede do governo da Ucrânia, que ficou fechada por três dias, além dos *sites* oficiais, telefones celulares dos parlamentares ucranianos também foram invadidos (Weedon 2015, 76). Na ocasião, o grupo composto por antigos membros das forças policiais ucranianas vinculou notícias na Internet contendo informações que denunciavam a "ilegitimidade do governo que assumiu a Ucrânia após a expulsão do ex-presidente Viktor Yanukovych" (Crowdstrike 2014, 26–27).

Ao utilizar as variações do BlackEnergy (BE.lite e BB2), a ameaça foi capaz de subtrair informações sigilosas como códigos de execução e

senhas de acesso remoto de seus alvos, demonstrando alta capacidade para afetar políticos do alto escalão do governo ucraniano por intermédio de operações conduzidas no ciberespaço. O vazamento periódico de documentos sigilosos em sua página na Internet prosseguiu durante os primeiros meses do conflito "foram mais de 50 itens exclusivos, emails, relatórios, acordos, propostas, imagens aéreas e identificação pessoal" (Crowdstrike 2015, 29).

Os ataques cibernéticos ocorreram em perfeita sincronia com as ações das forças especiais russas, os "homens de verde" (*Spetsnaz*), grupos armados e agentes de inteligência sem identificação, responsáveis pelas operações militares que tomaram controle da península e apoiaram os movimentos separatistas do leste (Giles 2015, 20).

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

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

Em abril de 2014, quando o conflito eclodiu em Donbass, as operações cibernéticas aumentaram exponencialmente, acompanhando os eventos militares de coleta de informações vitais para os setores de inteligência, ações que ofereceram vantagem significativa às tropas russas no campo de batalha físico (LookingGlass 2015). Naquele mês, os alvos da CyberBerkut foram empresas militares privadas que operavam no conflito, novamente chama a atenção o grau de alinhamento das operações com as prioridades estratégicas do Estado russo que passou a oferecer apoio técnico e tático aos separatistas do leste (Crowdstrike 2014, 27).

Os ataques cibernéticos seguiam uma dinâmica paralela às ações diplomáticas e estratégicas tomadas pelos Estados da Rússia e Ucrânia. Foi assim que, em 21 maio de 2014, logo após a declaração de independência dos territórios de Donbass do governo central de Kiev, a CyberBerkut de-

clarava a autoria dos ataques que atingiram a rede da Comissão Central de Eleições (CEC) (Koval 2015).

Na ocasião, a ameaça assumiu o controle da página que exibia a apuração eleitoral em tempo real. Minutos antes do encerramento da contagem, os *hackers* postaram no *site* da CEC uma foto anunciando a vitória do conservador Dmitry Yarosh nas urnas, notícia falsa que imediatamente foi compartilhada pelos canais de TV russos (Koval 2015, 56).

A coordenação da propaganda distribuída e das informações da mídia revelou como os serviços de inteligência da Federação Russa procuravam atingir seus objetivos estratégicos utilizando meios cibernéticos (Crowdstrike 2014, 26). O relatório Crowdstrike (2014) frisa a coordenação das transmissões da mídia estatal russa, que passou a divulgar a informação falsa vinculada pelos *hackers* em tempo real, conduzindo a opinião pública a colocar em dúvida a legitimidade do pleito, como indício dessa ação conjunta. No dia seguinte, quando o sistema da CEC teve seu funcionamento reestabelecido pelo serviço de segurança ucraniano, a comissão precisou confirmar a invasão do sistema pelos *hackers* para só então declarar a vitória do social-democrata Petro Poroshenko que assumiu a presidência do país (Koval 2015, 56).

Embora o relatório não afirme que a ação foi patrocinada diretamente pela Rússia ou se a CyberBerkut atuou de modo independente, Koval (2015, 55) destaca que "a quantidade e a gravidade dos ataques cibernéticos contra a Ucrânia aumentaram paralelamente aos eventos políticos em andamento". Tais ações atingiram alvos do alto escalão do governo ucraniano (ministro de Relações Exteriores, o ministro da Defesa, a administração executiva e as embaixadas no exterior), demonstrando o alto potencial de interferência no conflito causado por ações dessa ameaça via ciberespaço (Crowdstrike 2015, 29).

Igualmente identificada nas operações cibernéticas que atingiram a Ucrânia durante o conflito, a APA FancyBear/Sofacy/PawnStorm é apontada como responsável por atingir diversas organizações políticas com armas cibernéticas multifuncionais, enviadas via *e-mail spear phishing*. Classificada como representante dos interesses da Federação Russa, vinculada ao Departamento de Inteligência Militar (GRU) (Crowdstrike 2016, 8), a campanha de espionagem cibernética orquestrada por essa ameaça usurpou credenciais de acesso corporativo a sistemas de informação de importantes organizações governamentais da Ucrânia, como Forças Armadas, Ministério da Defesa, indústria da Defesa, partidos políticos, mídia e governos (Hacquebord 2015).

Em agosto de 2014, *e-mails spear phishing* foram identificados contendo uma lista com os nomes de membros do parlamento ucraniano que esta-

riam oferecendo apoio aos separatistas do leste. Enviados em nome do primeiro ministro da Ucrânia Arzeniy Yatsenyuk aos órgãos de investigação como Ministério Público, Serviço de Segurança, Ministério de Assuntos Internos e o Ministério da Justiça, a isca continha diretrizes oficiais para que essas instituições verificassem a veracidade das informações contidas nos documentos. No entanto, o arquivo em anexo estava infectado com uma versão do BE.lite que, ao ser aberto, oferecia acesso às contas dos servidores dessas instituições aos *hackers* (Lipovsky 2014, 2–3).

As amostras dos *malwares* presentes nos *e-mails* coletados pelo FireEye (2014), contêm códigos escritos em idioma russo e apresentam atividade em horário comercial de acordo com o fuso horário das principais cidades da Federação Russa, "evidências de operações focadas e de longa data que indicam um patrocinador do governo — especificamente, um governo com sede em Moscou" (FireEye 2014, 3).

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

O relatório indica que as amostras analisadas "utilizam a mesma sequência de descriptografia e algoritmos semelhantes para codificação e decodificação" (FireEye 2014, 21). Para verificar as semelhanças encontradas, os analistas identificaram um padrão nos códigos destes *e-mails*, "arquivos com nomes específicos, hashes MD5, carimbos de data e hora, funções personalizadas e algoritmos de criptografia, *backdoors* com endereços de IP e Comando e Controle similares e nomes de domínios incorporados" (FireEye 2014, 29).

Não obstante, as ações cibernéticas do grupo Pawn Storm parecem se conectar com às da CyberBerkut ao facilitarem o intercâmbio de informações roubadas e o vazamento de documentos confidenciais. Embora a relação entre ambas as ameaças tenha sido pouco explorada, analistas revelam que a "CyberBerkut publicou informações roubadas durante as campanhas do Pawn Storm" (Hacquebord 2017, 8).

O X-Agent[9] é outra arma cibernética associada ao grupo. O relatório Crowdstrike (2014) apresenta indicadores técnicos, como localidades dos recursos e informações de registro em domínio de comando e controle (C2) que apontam para a relação da APA com a Federação Russa em operações conduzidas via ciberespaço contra entidades militares e instituições políticas contra a Ucrânia. Devido à sua característica modular, a forma de

infecção dos sistemas alvo pode mudar desde protocolos de transferência de hipertextos (HTTP), até *e-mails* e/ou mídias removíveis. Ataques mais recentes envolveram ofuscação de fluxo de código para impedir o rastreamento dos invasores (Crowdstrike 2014, 58-59).

Uma variante do X-Agent — desenvolvida em formato de aplicativo pelo oficial ucraniano Yaroslav Shertuk com a promessa de oferecer maior eficiência aos sistemas de artilharia do Exército, reduzindo o tempo de disparo de minutos para segundos — foi apresentada em fóruns militares ocorridos na Ucrânia, e chegou a ser utilizada por quase nove mil usuários (Meyers 2016). No entanto, ao ser instalada, a ferramenta implantava de modo sigiloso o *malware* nos sistemas operacionais dos celulares destes usuários que, em grande parte, integravam a artilharia ucraniana (Meyers 2016).

Uma vez infectados, os aparelhos forneciam aos *hackers* a localização exata, e em tempo real, das tropas inimigas. Este dados eram repassados aos setores de inteligência russos permitindo que as Forças Armadas do país antecipassem os movimentos do adversário no campo de batalha. A análise do *malware* apresentou uma série de artefatos em língua russa de natureza militar que indicam uma correlação entre o FancyBear e o setor de inteligência militar russa que operava em apoio aos separatistas no leste da Ucrânia (Meyers 2016).

A última APA identificada no conflito é o Sandworm, grupo apontado como responsável por atacar setores de infraestrutura crítica da Ucrânia em meados de 2015 (Lipovsky 2014). Os principais *malwares* utilizados nos ataques foram o BlackEnergy 3 (BB3)[10] e o KillDisk (KD).[11]

Instituições governamentais norte-americanas do Departamento de Segurança Interna (DHS), por intermédio da Equipe de Resposta a Emergências Cibernéticas de Sistema de Controle Industrial (ICS-CERT), atuando em parceria com o setor privado através do instituto SysAdmin, Auditoria, Rede, Segurança (SANS) e do Centro de Análise e Compartilhamento de Informações de Eletricidade (E-ISAC), produziram relatórios confirmando que a interrupção no fornecimento de energia foi causada por uma série de ataques cibernéticos, que indicaram a presença de *hackers* especializados em táticas de espionagem cibernética (E-ISAC, 2016; ICS-CERT, 2016).

O incidente na região de Ivano-Frankvisk, reportado em 24 de dezembro pela Kyivoblenergo (companhia regional de distribuição de energia elétrica), revelou que terceiros obtiveram acesso ilegal ao sistema de tecnologia de informação da rede elétrica, desconectando sete subestações 110kV e 23 35kV, por três horas (ICS 2016, 1). Os resultados do relatório confirmaram o envolvimento de uma rede de planejamento e coordenação

de difícil detecção, capaz de ocultar os rastros contidos nos dispositivos atingidos (ICS-CERT 2016, 1-2).

Não obstante, o relatório (E-ISAC 2016) revelou em detalhes o alto grau de complexidade técnica empregado nos ataques. Tratou-se de uma operação de longo prazo, estimada em aproximadamente seis meses, entre o reconhecimento do sistema e o ataque propriamente dito, que só poderia ser levada a cabo por atores especializados em táticas de intrusão, com acesso a recursos externos e treinamento profissional, para subtrair credenciais e informações privadas e obter acesso aos controles da rede de energia sem que sua presença tivesse sido notada pelos sistemas de segurança (E-ISAC 2016, 4).

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

O relatório ressalta que as etapas de planejamento e execução dos ataques seguiram o modelo apresentado por Assante e Lee (2015). De acordo com o documento que descreve a operação, o primeiro estágio da invasão foi composto pelas fases de preparação e execução da intrusão cibernética, envolvendo a espionagem ou operação de inteligência para reconhecimento do sistema e armazenamento da ameaça (E-ISAC 2016, 8).

Durante a fase de planejamento, os computadores da companhia regional de distribuição de energia elétrica foram infectados com o uso de *spear phising* enviados a usuários com acesso à rede administrativa das empresas. Os *e-mails* continham arquivos em formato Microsoft Office Excel e Word infectados com o BB3, que permitiram aos *hackers* extrair códigos de informação e senhas de acesso aos sistemas operacionais das instalações. Após a infiltração, os invasores atuaram no ambiente infectado como usuários autorizados; o acesso irrestrito e indetectável permitiu que descobrissem as vulnerabilidades do sistema e extraíssem os dados necessários para um ataque efetivo (E-ISAC 2016, 6-8).

Uma vez conectados ao sistema de Comando e Controle (C2), os *hackers* utilizaram a própria rede privada virtual (VPN) das estações para obter acesso aos dados administrativos das empresas e lançar comandos destrutivos à distância. Desse modo a APA conseguiu atingir os alvos físicos sem que fossem detectados pelo sistema de segurança (E-ISAC 2016, 9–10).

A fase seguinte resultou no desenvolvimento e execução do ataque cibernético que danificou os sistemas operacionais das estações e subestações elétricas de modo simultâneo, impactando mais de 225 mil clientes. Após o feito, para evitar o rastreamento, os *hackers* utilizaram o KD para destruir os arquivos corrompidos do sistema e apagar o rastro dos invasores (E-ISAC 2016, 5). Em arremate, utilizaram um ataque do tipo de negação de serviço (D-DoS) no sistema de comunicação telefônica, congestionando o serviço de central de atendimento da empresa de energia para garantir que os usuários atingidos não conseguissem relatar as interrupções (E-ISAC 2016, 12).

A ação imperceptível ofereceu tempo suficiente para que os *hackers* pudessem desenvolver um *firmware* malicioso para dispositivos *serial-to-ethernet*, que foi capaz não apenas de danificar os disjuntores das subestações elétricas dos sistemas SCADA, como também evitar que as estações fossem recuperadas com uso de comandos remotos (E-ISAC 2016, 10-12). O relatório confirma que os *softwares* maliciosos BB3 e KD não foram os causadores da interrupção do funcionamento dos sistemas SCADA de energia elétrica, mas serviram como ferramentas sofisticadas para obtenção de informações de acesso privilegiado da administração dos sistemas operacionais dessas infraestruturas (E-ISAC 2016, 13).

Em suma, a execução do ataque utilizou o controle do próprio sistema para afetar o funcionamento de uma infraestrutura crítica. Todavia, desde o ano anterior à operação, as atividades do Sandworm já estavam sendo monitoradas pelo FireEye (2014), que alertou sobre uma invasão em curso aos sistemas de energia de empresas polonesas e agências do governo ucraniano: "[...] o grupo parecia estar desenvolvendo métodos para atingir as arquiteturas especializadas de computadores usadas para gerenciar remotamente os equipamentos industriais físicos" (Greenberg 2017, 11).

Ao utilizar ataques para atingir alvos dessa natureza, a ameaça inaugurou uma nova fase no conflito, que explicitou a alta capacidade dos atores envolvidos para causar danos cinéticos via ciberespaço, aumentando os ricos à segurança das infraestruturas críticas. De acordo com o relatório do FireEye (2016),

> O sucesso desses incidentes ao comprometer sistemas-chave para atingir um objetivo político ou demonstrar as capacidades de um adversário nos faz esperar que os adversários de um Estado-nação explorem cada vez mais vulnerabilidades específicas da ICS (FireEye 2016, 10).

Mediante a verificação do alto grau de sofisticação dos ataques cibernéticos e a capacidade de atualização das ameaças, é difícil refutar a suspeita

de que a ação dos *hackers* tenha sido impulsionada por um ente capaz de financiar esse tipo de campanha de longo prazo. Tamanha complexidade aponta para o envolvimento de um ente estatal robusto capaz de alavancar consideravelmente as ações no ciberespaço, uma vez que, para ser efetiva, a ação cibernética requer largo investimento em tecnologia da informação e infraestrutura, bem como uma organização operacional profissional (Weedon 2015, 70–1).

Não obstante, o relatório da Crowdstrike (2015) anuncia que o alto potencial dessa APA para empregar combinações de *softwares* maliciosos visando obter acesso ao sistema operacional de setores da infraestrutura crítica, sinaliza o envolvimento russo nessa operação (Crowdstrike 2015, 26). A ação representou uma resposta às ações do governo central de Kiev, que, no final de novembro de 2015, destruiu alvos físicos da região leste. Na ocasião, os ataques às linhas de energia que forneciam o serviço para a península anexada da Crimea deixaram mais de dois milhões de pessoas que residem na região sem energia elétrica (Crowdstrike 2015, 27–8).

Apesar de a Rússia negar agir em consonância com os grupos *hackers*, as evidências descritas pela análise dos relatórios apresentados nesta seção são fortes indícios do funcionamento do mecanismo de simbiose entre *hackers* e as Forças Armadas da Federação Russa. Destacamos as seguintes evidências: a coincidência cronológica entre os ataques cibernéticos e as invasões por terra; os horários de funcionamento das APA; a engenharia da informação por detrás dos códigos das armas identificadas; e, o alto grau de sofisticação e complexidade das operações realizadas.

CONCLUSÃO

Frente ao exposto, apresentamos uma breve discussão dos resultados de nossa análise sobre o funcionamento do mecanismo e o emprego da tecnologia da informação no conflito com intuito de oferecer uma resposta ao questionamento central deste artigo.

Ao aplicarmos as técnicas de análise qualitativa, identificamos como as operações cibernéticas realizadas pelas APA28 ofereceram vantagens estratégicas para as operações militares no mundo físico.

As principais agências estatais russas envolvidas com as operações cibernéticas identificadas foram: o Serviço Federal de Segurança (FSB); o Serviço de Comunicações e Informações Governamentais (FAGCI); e o Departamento de Inteligência (GRU), órgão ao qual estão subordinadas as forças especiais russas (*Spetsnaz*). Já as ameaças identificadas nos ataques cibernéticos foram: CyberBerkut, FancyBear/PawnStorm/Sofacy e Sandoworm; as armas cibernéticas: BlackEnergy; X-Agent e o KillDisk.

Os relatórios publicados por empresas especializadas em cibersegurança e instituições governamentais apresentam evidências de como se deu o uso destas armas e o modo de operação das ameaças cibernéticas. A análise destes relatórios verificou um aumento das capacidades qualitativas de ação da Federação Russa, manifestada por meio da sinergia produzida pela simbiose entre os atores estatais e não-estatais, compreendida como condição suficiente para comprometer o funcionamento de setores vitais da Ucrânia, como organizações políticas, militares e infraestruturas críticas.

Neste ensejo, a guerra híbrida conforme empregada pela Rússia contra a Ucrânia, em geral, envolveu ataques cibernéticos que ofereceram suporte à ação das forças especiais russas que, ao avançarem sobre as fronteiras ucranianas, foram capazes de comprometer setores estratégicos mediante uso de informações privilegiadas coletadas por campanhas sofisticadas de intrusão e coleta e/ou destruição de dados. De tal modo que as operações cibernéticas desvelam como o domínio da tecnologia da informação contribuiu para ampliar a assimetria de poder entre estes Estados, conectando os níveis estratégico, tático e operacional, de modo a facilitar a anexação do território da península da Crimeia e apoiar os movimentos separatistas que ocuparam a região leste da Ucrânia.

Note-se, portanto, que a condição em que ocorre a guerra híbrida entre russos e ucranianos reflete o potencial das ameaças cibernéticas na qualidade de novos engenhos de força para exploração de complexos sistemas de informação, capazes de causar danos cinéticos significativos aos adversários. Por essa lógica, a inferência descritiva do processo sustenta o pressuposto da centralidade que assume o ciberespaço na projeção regional do poder nacional russo. Ressaltamos, pois, a importância da segurança cibernética como fator chave para os Estados contemporâneos.

REFERÊNCIAS

Assant, Michael and Lee Robert. 2018. "The Industrial Control System Cyber Kill Chain." *SANS Institute Information Security Reading Room*: 1–21.

https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297.

Bergen, Peter and Tim Maurer. 2018. "Cyberwar hist Ukraine." *CNN*: 1–3. https://edition.cnn.com/2014/03/07/opinion/bergen-ukraine-cyber-attacks/.

Chuka, Neil. 2014. *Hybrid warfare implications for CAF force development.* Ottawa: Defence Research and Development Canada.

Collier, David. 2011. "Understanding Process Tracing." *Political Science and Politics* 44, no. 4 (Outubro): 823–30.

Crowdstrike. 2014. "Global Threat Intel Report." *Crowdstrike*: 4–76.

https://www.crowdstrike.com/2014-global-threat-report.

Crowdstrike. 2015. "Global Threat Intel Report." *Crowdstrike*: 3–89. https://go.crowdstrike.com/rs/281-OBQ-266/images/15GlobalThreatReport.pdf.

Crowdstrike. 2016. "Cyber Intrusion Services Casebook." *Crowdstrike*: 2–25.

https://www.crowdstrike.com/resources/reports/crowdstrike-cyber-intrusion-services-casebook-2016/.

E-ISAC. Electricity Information Sharing and Analysis Center. 2016. "Analysis of the Cyber Attack on the Ukranian Power Grid." *SANS ICS TLP:White*: 1–29.

https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

FireEye. 2014. "APA28: A Window Into Russia's Cyber Espionage Operations?" *FireEye*: 3–44. https://www.fireeye.com/current-threats/APA-groups/rpt-APA28.html.

_____. 2016. "Overload Critical Lessons From 15 Years of ICS Vulnerabilities." *Industrial Control Systems (ICS) Vulnerability Trend Report*: 3–11. https://www.fireeye.com/solutions/industrial-systems-and-critical-infrastructure-security/rpt-industrial-control-systems-vulnerability-trend-report-2016.html.

F-Secure Labs. 2014. "BlackEnergy Rootkit, Sort Of. News From The Lab Archive." *News From The Lab Archive*, 1-2. https://www.f-secure.com/weblog/archives/00002715.html.

F-Secure Labs. 2016. "Blackenergy & Quedagh: The convergence of crimeware and APA attacks." *F-Secure Labs Security Response Malware Analysis Whitepaper*: 1–16. https://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf.

Gartzke, Erik. 2013. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." *International Security* 38, no. 2: 41–73.

Geers, Kenneth. 2015. "Introduction: Cyber war in Perspective." *NATO CCD COE / Atlantic Council / Taras Shevchenko National University of Kyiv*: 13–8. In: _____. "Cyber War in Perspective: Russian Aggression Against Ukraine". Tallinn: NATO CCD COE.

Greenberg, Andy. 2017. "Your Guide to Russia's Infrastructure Hacking Teams. Wired Security." *Wired Security*: 1–11. https://www.wired.com/story/russian--hacking-teams-infrastructure/.

Hacquebord, Feike. 2015. "Pawn Storm's Domestic Spying Campaign Revealed: Ukraine and US Top Global Targets." *Trendmicro Security Intelligence*: 1–7. http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storms-domestic-spying-campaign-revealed-ukraine-and-us-top-global-targets/.

_____. 2017. "Two Years of Pawn Storm Examing and Incresingly Relevant Threat." *A TrendLabs Research Paper*: 4–42. https://documents.trendmicro.com/assets/wp/wp-two-years-of-pawn-storm.pdf.

Hoffman, Frank. 2007. *Conflict in the 21 Century The Rise of Hybrid Wars*. Arlington, Virginia: Potomac Institute for Policy Studies.

ICS-CERT, Industrial Control Systems. 2016. "Cyber-Attack Against Ukrainian Critical Infrastructure". *Department of Homeland Security (IR-ALERT-H-16-056-01)*: 1–5. https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

Janz, Scott and Maurer, Tim. 2014. "The Russia-Ukraine Conflict and Information Warfare in a Regional Context." *Swiss Federal Institute of Technology Zurich*: 1–4. https://www.files.ethz.ch/isn/187945/ISN_184345_en.pdf.

Kello, Lucas. 2013. "The meaning of the Cyber Revolution Perils to Theory and Statecraft." *International Security* 38, no. 2: 7–40.

Kjennerud, Erik and Cullen, Patrick. 2016. "What is Hybrid Warfare?" *Norwegian Institute of International* Affaris 1 (Jan): 1–4.

Koval, Nikolay. 2015. "Revolution Hacking." *Cys Centrum LLc*, 55-58. In: _____. "Cyber War in Perspective: Russian Aggression Against Ukraine". Tallinn: NATO CCD COE.

Lindsay, Jon. 2013. Stuxnet and the Limits of Cyber Warfare. *Security Studies* 22, no. 3: 365-404.

Lindsay, Jon. 2015. The impact of China on Cybersecurity. *Journal of Strategic Security* 39, no. 3: 7-47.

Lipovsky, Robert. 2014. "Back in BlackEnergy: 2014 Targeted Attacks in Ukraine and Poland." *Welivesecurity ESET*: 1–12. https://www.welivesecurity.com/2014/09/22/back-in-blackenergy-2014.

LookingGlass. 2015. "Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare." *Lookingglass Cyber Threat Intelligence Group*: 3–51. https://www.lookingglasscyber.com/wpcontent/uploads/2015/08/Operation_Armageddon_Final.pdf.

Mahoney, James. 2012. "The logic of Process Tracing Tests in the Social Sciences." *Sociological Methods & Research* 41, no. 4: 570–97.

Maurer, Tim. "Cyber Proxies and the Crisis in Ukraine." *New America*, 79–86. In: _____. "Cyber War in Perspective: Russian Aggression Against Ukraine". Tallinn: NATO CCD COE.

Meyers, Adam. 2016. "Danger close: FancyBear Tracking of Ukrainian Field Artillery Units." *Crowdstrike blog*: 1–6. https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/.

Olszewski, Boguslaw. 2018. "Advanced Persistent Threats as a Manifestations of State Military Activity in Cyber Space." *Institute of International Studies* 189, no. 3: 57–71.

Pierson, Paul. 2000. "Increasing Returns, Path Dependence, and the Study of Politics." *American Political Science Review* 94, no. 2: 251–67.

USAOC. The United States Army Special Operations Command. 2015. "Little Green Men: a prime on Modern Russian Unconventional Warfare Ukraine 2013-2014." *Johns Hopkins University Apllied Physics laboratory*: 1–65.

Vaczi, Norbert. 2016. "Hybrid Wafare: How to Shape Special Operations Forces" *U.S Army Command and General Staff College*: 3–88.

Weedon, Jen. 2015. "Beyond Cyber War: Russia's use of Strategic Cyber Espionage and Information Operations in Ukraine." *FireEye*: 67–78. In: _____. "Cyber War in Perspective: Russian Aggression Against Ukraine". Tallinn: NATO CCD COE.

Weiss, Moritz and Jankauskas, Vytautas. 2019. "Securing Cyberspace How States Design Governance Arrangements." *International Journal of Policy, Administration, and* Institutions 32, no. 2: 259–75.

NOTAS

1. *Malware*: termo utilizado para designar um *software* projetado para interferir na funcionalidade do computador ou para degradar a integridade dos dados. Engloba uma gama de códigos de computador maliciosos —vírus, worms, trojan, spyware, adware, etc-. Pode ser projetado para fornecer acesso a um sistema de computador adversário, e/ou para atacá-lo (Kello 2013, 18).
2. Técnica que analisa um determinado período de tempo para indicar como mudanças institucionais dificultam a reversão ao ponto inicial de movimentos iniciados por um Estado (Pierson 2000, 252).
3. Técnica que sistematiza uma análise qualitativa a partir de uma perspectiva capaz de explicar relações causais mediante a observação de como determinadas condições produzem um fenômeno observável. Trata-se de uma ferramenta útil para extrair inferências descritivas e causais a partir de evidências compreendidas como parte de uma sequência temporal de eventos ou fenômenos (Collier 2011, 824).
4. Spetsnaz (Спецназ): grupos especiais de intervenção da polícia, dos ministérios de justiça e assuntos internos russos, Serviço Federal de Segurança (FSB), Serviço de Inteligência Estrangeira (SVR), Agência Federal de Comunicações e Informações Governamentais (FAGCI), bem como do exército russo.
5. *Spear phishing*: comunicação eletrônica direcionada a indivíduos, organização ou negócios específicos com intenção de instalar *malwares* espiões nos computadores dos alvos.
6. Os relatórios analisados representam fontes secundárias que contêm informações produzidas por especialistas em segurança cibernética reconhecidos mundialmente. Tratam-se, pois, de um recurso central para coleta de evidências sobre as operações envolvendo atores estatais e ameaças cibernéticas.
7. Arma cibernética que utiliza diretórios temporários para executar arquivos iscas infectados com o *malware* que são carregados por comandos "rundll32.exe", a variante não utiliza *rootkit* para ocultar objetos no sistema ou *driver kernel* para descarregar os arquivos (Lipovsky 2014, 3).
8. Arma cibernética capaz de esconder os processamentos de rotina utilizados nos ataques, mantém uma lista codificada de *offsets* em estruturas de *driver kernel* que oferece acesso total às informações dos sistemas contaminados (F-Secure Labs 2014, 1).
9. Arma cibernética de acesso remoto capaz de infectar sistemas operacionais como Windowns, iOS e plataformas móveis. Possui arquitetura modular que combina a funcionalidade de implante necessária de acordo com o equipamento utilizado pelo alvo escolhido (Crowdstrike 2014, 59).
10. Arma cibernética utilizada para infiltração e roubo de informações que não utiliza componente de *driver kernel*, invade diretamente a pasta de dados do

aplicativo local e instala um arquivo LNK para executar o malware usando o "*rundll32.exe*" (F-Secure Labs 2016, 11).

11. Arma cibernética desenvolvida para apagar o rastro dos processos de infiltração conectados via *serial-to-ethernet* e substituir o arquivo executável por dados aleatórios (E-ISAC 2016, 6).

GUERRA HÍBRIDA: O EMPREGO DA TECNOLOGIA DA INFORMAÇÃO NO CONFLITO RÚSSIA-UCRÂNIA (2014-2015).

RESUMO

Como a tecnologia da informação amplia a assimetria de poder entre os Estados contemporâneos? Com o objetivo de responder ao questionamento, o artigo descreve o processo de utilização do ciberespaço para consecução dos objetivos estratégicos da Federação Russa em seu entorno regional, durante o conflito desencadeado com a Ucrânia (2014-2015). A partir da análise de relatórios de empresas especializadas em segurança cibernética e instituições governamentais, aplicamos as técnicas qualitativas da dependência da trajetória e rastreamento de processos para explicitar a complexidade das operações conjuntas entre as forças especiais russas e *hackers* civis, bem como a sofisticação das principais ameaças e armas utilizadas nos ataques cibernéticos. Desse modo, identificamos o mecanismo responsável por conectar os níveis estratégico, tático e operacional militar ao verificarmos o processo de ação simbiótica entre os atores envolvidos no conflito. As evidências coletadas indicam como a guerra híbrida empregada pela Federação Russa incorporou a dimensão cibernética como peça chave para a desestabilização de territórios e consecução de interesses em seu entorno estratégico.

Palavras-chave: Guerra Cibernética. Estratégia. *Hacker*. Rússia.

ABSTRACT

How does information technology expand power asymmetry between contemporary states? In order to answer this question, the article describes a process of using cyberspace to achieve strategic objectives of the Russian Federation in its regional environment, during the conflict unleashed with Ukraine (2014-2015). Based on analysis of reports from companies specialized in cybersecurity and government institutions, we apply qualitative techniques of path dependence and process tracing to explain the complexity of joint operations between Russian special forces and civilian *hackers*, as well as the sophistication of main threats used in cyber attacks. In this way, we identified a mechanism responsible for connecting strategic, tactical and military operational levels when verifying the process of symbiotic action between the actors involved in this conflict. The evidence collected indicates how hybrid warfare employed by the Russian Federation incorporated cyber dimension as a key point to destabilizing territories and achieving interests in its strategic environment

Keywords: Cyber War. Strategy. Hacker. Russia.

Recebido em 01/07/2020. Aceito para publicação em 19/04/2021.

The 2019 Venezuelan Blackout and the consequences of cyber uncertainty

O blecaute venezuelano de 2019 e as consequências da incerteza cibernética

Rev. Bras. Est. Def. v. 7, nº 2, jul./dez. 2020, p. 37-57
DOI: 10.26792/RBED.v7n2.2020.75204
ISSN 2358-3932

JOE DEVANNY
LUIZ ROGÉRIO FRANCO GOLDONI
BRENO PAULI MEDEIROS

INTRODUCTION[1]

Geopolitics and digital technologies are inextricably interconnected. This manifests in different ways, aligning with broader strategic issues, including: debates about foreign ownership or involvement in domestic infrastructure, such as the U.S.-led campaign to restrict the Chinese company Huawei's role in 5G communications networks across the globe; and concern about the potential for digital media, including social media platforms, to be exploited to pursue disinformation and subversion, as occurred during the 2016 U.S. presidential election campaign. Digital technology and geopolitics also combine in contemporary debates about the practice and limits of digital espionage and offensive cyber operations, particularly following the 2011-12 discovery of the U.S.-Israeli Stuxnet/Op OLYMPIC GAMES cyber operation against Iranian nuclear infrastructure (Sanger 2012; Zetter 2014) and the 2013 revelations by Edward Snowden about the extent of U.S. and allied digital surveillance capabilities (Ball, Borger & Greenwald 2013; Harding 2014; Harris 2014). State threats to digital infrastructure — and the strategic implications of those threats — were visible more recently in the major incidents regarding SolarWinds and Microsoft Exchange (Alperovitch and Ward 2021;

Joe Devanny — Lecturer in the Department of War Studies at King's College London and deputy director of the Centre for Defence Studies at King's.
Luiz Rogério Franco Goldoni — Professor in the Postgraduate Program in Military Sciences of the Meira Mattos Institute (PPGCM-IMM) at the Army Command and General Staff School (ECEME).
Breno Pauli Medeiros — PhD student in Military Sciences at the Army Command and General Staff School (ECEME).

Devanny 2021). The contemporary strategic impact of cyber (as threat and opportunity) on defense and security policies highlights the social, economic and political ubiquity of digital technologies and the Internet.

As digital technologies such as social media platforms accelerate the volume and velocity of "speech acts" in public diplomacy, it has become more difficult to control narratives surrounding controversial events or crises, and for publics to establish "truth" in a world of "alternative facts" and "fake news". This polluted information environment exacerbates the problem of determining truth in areas of technical complexity, in a global public sphere suffering from a "knowledge asymmetry" that undermines the ability of citizens (and some governments) to determine which party to believe in a contested narrative.

In the case of alleged cyber operations, this knowledge asymmetry is magnified by the high level of technical knowledge and capability necessary to conduct an exercise in attribution analysis. All but the most sophisticated state actors and private sector analysts are unable to conduct or comprehend such an analysis, meaning that most people are reliant on secondary sources for information and assessment, with all the caveats about the contemporary media environment that were highlighted above. This information environment complicates the contemporary trend towards coordinated public attribution (Egloff and Smeets 2021), taking place in a broader geopolitical context that shapes reception of the *cui-bono* logic of attribution (Cavelty 2015).

To illuminate these issues, this article adopts the starting point of Venezuelan President Nicolás Maduro's allegation that March 2019 energy outages in Venezuela were caused by a U.S. cyber attack. It argues that global public opinion about the Trump administration's Venezuela policy and its emerging cyber strategy potentially contributed to an information environment in which false claims of attribution were treated more credibly than they should have been. The article concludes by reflecting on the consequences of cyber uncertainty for international relations. As Martin Libicki — another author to recognise the illustrative potential of the Venezuela case — observed: "facts of cyberwar are becoming secondary to misperceptions that governments either shape or influence" (Libicki 2020, 85).

The article uses the Venezuela case to highlight the geopolitical impact of uncertainty in cyberspace. It argues that the instrumental value — and cost — of cyber uncertainty should inform decisionmaking about cyber strategy. The article is structured in four parts followed by a conclusion. First, it presents the Venezuelan case, situating Maduro's cyber allegation in the context of fraught bilateral relations between Venezuela and the United States. Second, it introduces the concept of cyber uncertainty, iden-

tifying the impact of knowledge asymmetries on broader public perceptions of perceived and real cyber operations. Third, it analyses the conduct and consequences of U.S. cyber operations, assessing the relevance of the recent shift in U.S. strategy. Fourth, it discusses the Trump administration's discernible strategy for Venezuela and the second-order diplomatic effects of U.S. cyber strategy. The article concludes by appraising the Venezuelan case as an illumination of emerging trends in cyber operations, disinformation and contested strategic narratives, all in the wider social context of knowledge asymmetries and prevailing cyber uncertainty.

ENERGY OUTAGE AND CYBER ALLEGATIONS IN VENEZUELA

Between March 7 and 14, 2019, a major blackout left many homes, businesses and public buildings in Venezuela without electricity (Daniels 2019). The blackout prompted the interruption of services at airports and in hospitals (Sequera and Buitrago 2019). It led to local businesses being ransacked and clashes between owners and looters. This occurred against a nationwide backdrop of on-going protests in opposition to Maduro (Casey 2019).

Some experts have speculated that the blackout was caused by a technical issue, particularly following the deterioration of national infrastructure during Venezuela's continuing economic and political crisis (Leetaru 2019; Jones 2019). There were other reports that Russian military personnel (reportedly including cybersecurity experts) arrived in Venezuela later in March (Gunia 2019). The reported presence of Russian cyber experts indicated support to the Maduro regime, perhaps including digital surveillance of opponents, as well as infrastructure cyber security (Spetalnick 2019).

Reporting of technical analysis regarding the cause of the blackout occurred in a contested media environment. One striking feature was the diplomatic disagreement via social media between Venezuelan president Maduro and then U.S. Secretary of State Mike Pompeo. Maduro and Pompeo traded insults on the social media platform Twitter, after Maduro had alleged that the U.S. was responsible for a cyber attack against Venezuela's energy infrastructure, using this as the explanation for the blackouts (Maduro 2019). Pompeo responded quickly, rejecting the allegation and countering that regime-change would occur in Venezuela (Pompeo 2019). The Trump administration's special representative for Venezuela, Elliott Abrams, also said that the outages were: "a reminder that the country's once quite sophisticated infrastructure has been plundered and allowed to decay under Maduro's misrule" (Sheridan and Zuniga 2019).

This heated exchange via social media was part of a longer period of deterioration in U.S-Venezuela bilateral relations. In early 2019, the

Trump administration had recently officially recognised the head of the national assembly, Juan Guaidó, as the interim president of Venezuela. Guaidó's presidency would subsequently be recognised by 58 nations. The bilateral relationship had already been antagonistic: in November 2018 the then US national security adviser, John Bolton, had publicly grouped Venezuela with Cuba and Nicaragua as countries regarded as regional threats, denouncing:

> This Troika of Tyranny, this triangle of terror stretching from Havana to Caracas to Managua…[as] the cause of immense human suffering, the impetus of enormous regional instability, and the genesis of a sordid cradle of communism in the Western Hemisphere (Rogin 2018; Bolton 2020, 249).

Although the Trump administration had not publicly threatened Venezuela with cyber attacks prior to the March 2019 energy outages, it is clear from other evidence that it possessed both the capability and willingness to target infrastructure using this instrument to pursue national policy. For example, Trump would reportedly authorize a cyber operation against Iran just three months later (Nakashima 2019) and had previously streamlined the authorization process to make it easier for U.S. Cyber Command and the Central Intelligence Agency to conduct cyber operations than it had been under the Obama administration (Devanny 2021, 11).

According to John Bolton's memoir, the Trump administration wanted to remove Maduro from office, but suffered from an ineffective strategy, "bureacratic footdragging", disagreement amongst senior figures and President Donald Trump's tendency to change his mind, including after a persuasive conversation with Russian President Vladimir Putin (Bolton 2020, 271–4, 282–3). Similarly, efforts by the opposition to create splits in Maduro's regime, particularly with the military, were reportedly proceeding at the time of the energy outages, culminating in a failed attempt by Guaidó in late April 2019 to secure military support in his bid to replace Maduro (Faiola 2019a). The failure of this move led Maduro's intelligence chief, with whom the opposition had collaborated, to flee to Colombia, after which the U.S. government lifted sanctions against him (Faiola 2019b) in exchange for cooperation against Maduro. Throughout the rest of 2019, the opposition suffered from increasing weakness, harassed and divided by the government, with splits developing between opposition parties, and dissension and corruption allegations surfacing within Guaidó's own party (Faiola 2019c).

The opposition lost further momentum in January 2020 when the Maduro government arranged for a rival to Guaidó to be sworn in as

head of the national assembly — the position from which Guaidó derives legitimacy for his claim to be the interim president (Krygier and Faiola 2020). As the opposition experienced these setbacks, the US government pursued alternative approaches, tightening economic sanctions and deciding in March 2020 to indict Maduro and five others on criminal charges of narco-terrorism, offering US$15m in reward for Maduro's capture (Faiola, Zapotosky, and DeYoung 2020). In this context, in May 2020 two U.S. former Special Operations soldiers were arrested in Venezuela, reportedly following a failed *coup d'etat* (Tharoor 2020).

There is no evidence that the Trump administration was involved in this failed effort, or indeed in the March 2019 energy outages, but bilateral relations were then so poor that no trust existed between the two governments. Indeed, following the arrest of the two former U.S. soldiers after the failed coup in May 2020, the U.S. State Department said: "There is a major disinformation campaign underway by the Maduro regime, making it difficult to separate facts from propaganda" (DeYoung, Faiola, and Horton 2020).

The 2019 episode in Venezuela thus offers an interesting case in the diplomatic and geopolitical consequences of the emerging global public understanding about US cyber operations. As the U.S. government increasingly talks about its cyber capabilities and their place in national security strategy, so too do U.S. adversaries accuse it of conducting cyber attacks. This diplomatic risk is explicitly recognised in one authoritative official U.S. statement about the shift in cyber strategy (US Cyber Command 2018, 10). The new cyber strategy — with its prescription of more frequent cyber operations against adversaries — developed organically and should not be associated with the politics or objectives of the Trump administration. Nevertheless, it unfolded against a backdrop of reduced public trust in the office of the presidency under the Trump administration, in light of its association with "fake news" and "alternative facts", its hostility towards journalism and even towards parts of the US federal government, such as the intelligence community, that Trump referred to derisively as the "deep state" and which he claimed were part of an effort to undermine his presidency (Rohde 2020). This created a less favorable information environment for the reception of this strategic shift, increasing the risk of misunderstanding about what the new strategy was trying to achieve.

THE UNCERTAINTY PRINCIPLE OF THE CYBER DOMAIN

In view of the complexity of physical and virtual layers that make up cyberspace, identifying causative activities and attributing them to specific

actors requires significant technical and analytical capabilities. These capabilities exist in both private (cybersecurity companies) and public sectors (most commonly in defense, intelligence and security agencies). But the level of sophistication and resourcing of cyber forensics differs widely, creating severe knowledge asymmetries both between governments and between governments and their publics.

This becomes more complicated when perpetrators go further than masking their acts, fabricating to mislead — even seeking to incriminate others in false flag operations. Given the inconclusiveness of certain forensic efforts, the attribution of actors often employs *cui-bono* logic, i.e.: given the political, economic, military and/or social context, the actor who would benefit the most from a cyber operation would be more likely to perpetrate it (Cavelty 2015, 93).

Thus, the uncertainty principle often implies a speculative context that weighs political issues. Sophisticated cyber actors can exploit this uncertainty for operational advantage, but, as the Venezuela case implies, uncertainty also has its costs. This is, of course, less straightforwardly the case in instances of cyber deterrence or compellence, when perpetrators presumably need to signal responsibility to achieve deterrence or compellence, a precondition for which is that the targeted state should understand the purpose of the attack, namely to dissuade/compel a specific response (Valeriano, Jensen, and Maness 2018, 47).

Cyberspace is operationally contested. State actors typically do not disclose their digital espionage activities, in order to retain surveillance access. Active digital surveillance, involving presence on a network, also affords the opportunity to develop an exploit of a vulnerability on that network to achieve a different effect, e.g. to degrade or destroy the network, wholly or in part. This duality is the cause of much of the policy debate and controversy surrounding the SolarWinds incident (Devanny 2021). Similarly, covert access to a network potentially enables criminal activities, e.g. data theft or ransoming individuals or organisations in exchange for re-enabling access to their devices or networks — a major consequence of the Microsoft Exchange incident (Alperovitch and Ward 2021; Poznansky and Perkoski 2018, 7–8). This duality of potential, juxtaposing cyber espionage and offensive cyber operations, creates uncertainty that could produce severe strategic consequences.

Medeiros and Goldoni (2020) see uncertainty, deterritoriality and multiplicity of actors as key elements to understand the operationalization of cyberspace. Acccordingly, when cyber operations are detected, widespread public acceptance of the attribution analysis will rest on the tension between *cui-bono* logic and (im)plausible deniability (Cormac and Aldrich

2018). Attribution occurs in a political context: it is not a neutral, purely technical exercise. The geopolitical competition of strategic narratives, exacerbated by digital media, is rendered more acute in cases of uncertainty over (alleged) cyber operations.

Cyber uncertainty and the potential to carefully calibrate operational effects, reducing the risk of casualties and managing the risk of escalation, have made cyber operations an increasingly attractive option in geopolitical competition. Recent reports of reciprocal cyber operations conducted by Iran and Israel highlight this practice (Baram and Lim 2020). As the world's most militarily capable state, the United States has also shaped behavior in the cyber domain, developing and using sophisticated digital espionage and offensive cyber capabilities (Harris 2014).

U.S. STRATEGY AND CYBER OPERATIONS

The United States has endorsed voluntary, non-binding norms of responsible state behavior in peacetime cyberspace, including "prohibitions against damaging civilian critical infrastructure" (US DOD 2018, 5). Notwithstanding, it is not an outlandish proposition to assert that there are circumstances in which the U.S. government might conduct a cyber operation against an adversary's critical infrastructure. For example, just three months after the Venezuelan energy outages, it was reported that the Trump administration had authorised penetration of the Russian energy network, signalling the sophistication of U.S. capabilities to conduct just such an attack (Sanger and Perlroth 2019). This operation's stated intent was to deter Russian operations against the United States. In contrast, the hypothetical value of cyber (or other covert) operations against Venezuelan energy infrastructure would be to exacerbate domestic socio-economic problems, intensifying opposition to Maduro and ultimately facilitating regime-change.

One operation was reportedly designed to deter, the other would have been designed to complement other, non-cyber measures implemented by the US government to bring about regime change in Venezuela. Whilst there is no evidence that the US conducted cyber operations in Venezuela, the problem is one of perception compounded by actual policy: the US was engaged in a broad-based effort to increase pressure on Maduro's regime, and has signaled the capability to conduct cyber operations against energy infrastructure in pursuit of other strategic objectives. The use of cyber operations in support of wider policy would follow the logic of "additive" cyber operations that "complement rather than replace traditional forms of coercion" (Valeriano, Jensen, and Maness 2018, 42). Perhaps for many

observers, without access to or comprehension of technical reports into the origins of energy outages in Venezuela, allegations of US complicity might not be so readily dismissed, particularly in light of a pre-existing pattern of strategic behavior arguably consistent with the conduct of such an operation. Another relevant factor shaping the information environment is the impact of history, particularly US policy towards Latin America during (and before) the Cold War (Crandall 2008; Grow 2008).

This aligns with Robert Jervis's observation about the polysemous nature of cyber operations, given the existence of multiple audiences within and between states: "Not only is no state completely unified, but the perceptions of numerous third parties are also important. What would seem like an under-reaction to some allies, for example, could be seen as a dangerous over-reaction by others" (Jervis 2016, 71). The combination of declaratory posture, rhetoric and reported US activities in cyberspace under the post-2018 strategy have collectively created the impression of a more permissive approach to cyber operations. This has implications for the ways in which other states and their publics will likely perceive the U.S. as a strategic actor.

The June 2019 reported signaling operation against Russian infrastructure was part of the new US strategy to "defend forward" in cyberspace and embrace "persistent engagement." Jacquelyn Scheider situates this turn towards a more assertive strategy in the context of an emerging pattern of behavior by US adversaries, which highlighted "the increasingly front-line role of critical infrastructure in state-led cyber attacks" (Schneider 2020, 161). The cases cited by Schneider include Russian interference in the 2016 US presidential election; cyber attacks against energy infrastructure in Ukraine; and cyber crime against financial networks reportedly conducted by Iran and North Korea. Schneider does not mention the U.S.-Israeli cyber operation against Iranian nuclear infrastructure, which pre-dates her examples and arguably deserves a more prominent place in the chronology of cases demonstrating the increasing number of infrastructure-targeted cyber operations conducted by state actors (Zetter 2014).

The intellectual justification for "persistent engagement" is closely associated with Michael Fischerkeller and Richard Harknett, who have argued that the previous US approach of deterrence and restraint was ill-suited to the cyber domain: "A strategy of deterrence seeks to avoid operational contact, whereas cyberspace participants are interconnected, and consequently, all operations in cyberspace always involve operational contact. Cyberspace is a perpetually contested space" (Fischerkeller and Harknett 2017, 386). Fischerkeller and Harknett's analysis of cyberspace

and consequent prescription for US responses is independent of U.S. policy objectives: the analyses and recommendations advanced by advocates of persistent engagement and defend forward are as adoptable by the Biden administration as they were by the Trump administration (Devanny 2021). They flow from an appraisal of the "offense-persistent" nature of cyberspace and the reality of "constant contact with the enemy" (Harknett and Goldman 2016, 86).

This analysis has heavily influenced U.S. Cyber Command, with its commander describing a shift from being a "response" force to becoming a "persistence" force, appropriate for a new reality in which: "Continuous action in cyberspace for strategic effect has become the norm, and thus the command requires a new strategic concept" (Nakasone 2019, 12). This shift is most visible in two documents produced by the U.S. government in 2018: the command vision for Cyber Command (US Cyber Command 2018) and the National Cyber Strategy (US DOD 2018). These documents explain a strategic shift to position the United States to succeed in cyberspace competition with its most capable adversaries. The new strategy is a "roadmap…to achieve and maintain superiority in cyberspace" (US Cyber Command 2018, 2). It is therefore a misapprehension to interpret the new strategy as evidence of greater likelihood that the U.S. would conduct cyber operations to sabotage non-cyber infrastructure of less cyber-capable adversaries such as Venezuela. Infrastructure-targeting is one example of cyber operations, but it is not the principal focus of the new turn in U.S. strategy.

The new strategy envisaged a higher tempo and greater risk appetite for US cyber operations — according to the Command Vision, the new approach is "risk aware, not risk averse" (US Cyber Command 2018, 7). This was conceived, however, as a specific response to the nature of competition in cyberspace. It did not imply reckless disregard for consequences and was rather calibrated to achieve specific effects. More broadly, the Trump administration continued the Obama administration's approach of using cyber operations to manage the risk of escalation, e.g. in responding to alleged Iranian attacks on oil tankers and an unmanned US surveillance drone in mid-2019 (Valeriano and Jensen 2019). This reflects the flexibility of cyber operations as an instrument of national strategy, a flexibility stemming partly from the aforementioned elements of cyber uncertainty.

The contemporary debate about U.S. strategy focuses understandably on its impact on stability and whether the broader strategy is overly focused on its offensive dimensions to the detriment of defense (Healey 2020). Holistic appraisal of the new strategy also requires analysis of its wider system effects, including its impact on the dynamics of policy issues

that were not considered as part of the process of strategic development (Jervis 1998).

One of these second-order effects is the potential impact of U.S. strategy on other states' (both allies' and adversaries') perceptions of false allegations regarding U.S. cyber operations. During the Trump administration, the combination of a broadly pro-active cyber strategy and a unpredictable White House prone to making seemingly provocative statements, injected an element of uncertainty and doubt about what the U.S. might or might not have been doing, in spite of the emerging body of policy-oriented literature — drawn from in this section — that explores and explains U.S. cyber strategy. This unusual conjuncture made the antagonism between the Trump and Maduro administrations an interesting case in the analysis of the implications of the Trump administration's approach to diplomacy and cyber operations.

THE TRUMP ADMINISTRATION, VENEZUELA AND CYBER UNCERTAINTY

In the context of severe economic crisis, the failure of Venezuelan energy infrastructure in March 2019 can plausibly be attributed to domestic shortcomings. These include the compound impact of years of underfunding and poor maintenance, possibly exacerbated by an exodus of skilled personnel from the sector as part of the wider sharp increase in emigration from Venezuela as many citizens try to escape from its crisis. This is a simpler explanation than the alternative of a protracted and expensive effort to develop and deploy U.S. cyber capabilities to undermine the electricity supply. There is a further doubt about the cyber explanation, when the U.S. might have been expected to have had cheaper, less high-tech options, such as non-cyber sabotage. Most relevantly, however, it is simply unclear precisely what strategic effect such an operation would have been intended to produce and how proportionate infrastructure-sabotage would have been as an instrument to achieve it.

Whilst the above will be sufficient to persuade many observers that the Trump administration probably did not conduct a cyber (or indeed a non-cyber) operation against Venezuelan critical infrastructure, the juxtaposition of two factors — (i) the Trump administration's discernible preference for a Venezuela under different governance and (ii) the second-order effects of the new cyber strategy — created the potential for a contested narrative, invoking the inherent uncertainty of cyberspace. This is particularly true in an era characterised by the proliferation of false narratives on social media and concerted efforts by state actors to pollute the information environment and undermine public confidence in the media.

In the context of John Bolton's rhetoric designating Venezuela as part of a "troika of tyranny", the Trump administration's policies towards Venezuela were inevitably evocative of the rhetorical inheritance of the "axis of evil." The latter phrase was coined during a previous US administration in which Bolton had served, namely the George W. Bush presidency. That presidency was indelibly associated with military intervention and regime-change (Mann 2004). Bolton's choice of rhetoric therefore generated an implicit expectation that more coercive instruments would be employed than had yet been employed by the Trump administration against Venezuela. Indeed, military action was explicitly stated to be "an option" by Trump himself, in apparently off-the-cuff remarks, both in August 2017 and February 2019 (Ellsworth 2019).

Moreover, the January 2019 appointment of the controversial neoconservative Elliott Abrams as the administration's special envoy for Venezuela provoked memories of an even earlier US administration. Abrams was assistant secretary of state for inter-American affairs during the Reagan administration. He was personally implicated in the Iran-Contra scandal (Borger 2019). When exploring global perceptions of the Trump administration's Venezuela strategy, it is important to contextualise debates about contemporary policies with reference to the substantial history of U.S. covert actions and regime-change policies in Latin America, for example during the Cold War (Grow 2008). Also relevant are tensions between the objectives of U.S. post-Cold War "democracy promotion" programmes and the domestic politics of specific states in the region, with Venezuela being a particularly acute and prominent case (Clement 2005).

The most plausible interpretation of the available evidence is that there was a counterproductive gap between the Trump administration's rhetoric and the policies it was prepared to pursue. As Hal Brands noted regarding Trump's 2017 comments about the military "option" in Venezuela: "the president's apparently improvised threats of military action against Venezuela served mainly to wrong-foot regional critics of President Nicolás Maduro's government (and to distract attention from that government's own failings) by raising the prospect of unwanted US intervention" (Brands 2017, 25–6). Throughout most of Trump's term in office, his Venezuela policy was coercive in intent, including significant economic sanctions (Main 2020, 34–5), but within limits notionally calibrated to facilitate negotiated settlement, most probably by splitting Maduro's constituency of support. Unsealed criminal indictments of Maduro and other senior figures in early 2020 appeared to indicate a loss of confidence that such an objective was achievable (Ramsey 2020). The juxaposition of bombastic rhetoric and loose talk about military options

did little to amplify or enhance the effectiveness of the administration's strategy: coercive economic sanctions undoubtedly had a severe impact on the Venezuelan economy, but the Maduro government entrenched itself and called the Trump administration's bluff regarding what appeared ultimately to be empty and ill-conceived threats of military action.

The blunt instrument of economic sanctions had increased pressure on Maduro's government, but the real victims were of course the millions of Venezuelan citizens who directly suffered from the impact of the economic crisis. In this sense, the hypothesis that the U.S. government would sabotage Venezuelan critical infrastructure did not appear to be a difference in kind: the human cost of the 2017 and 2019 economic sanctions arguably outweighed the specific consequences of the time-limited disruption to the electricity supply in March 2019. Just as the totality of instruments that comprised the Trump administration's Venezuela strategy militated against arguments that a limited cyber operation affecting critical infrastructure would cross an ethical line of conduct, the perceptual impact of "persistent engagement" — particularly reporting of U.S. pre-positioning of implants inside Russian energy infrastructure — perhaps contributed to already-fertile conditions in which counter-narratives could grow. This case-specific context arguably overshadowed in this instance the wider debate about the ethical implications of cyber operations targeting civilian infrastructure (Devanny 2020).

Cyber uncertainty is exacerbated by knowledge asymmetry, in which the circumstances surrounding incidents such as the Venezuelan energy outages are virtually impossible for most people to establish definitively. Such an assessment would require technical expertise to comprehend and would otherwise rely on diverse readerships' or audiences' willingness to trust the reliability of the secondary sources that explained it. Indeed, John Bolton himself recounts in his memoir that, on hearing of the outages, his "first thought was that Guaidó or someone had decided to take matters into their own hands…whatever the cause or the extent or duration of the outage, it had to hurt Maduro". Bolton quickly qualifies this equivocal note, however, highlighting that "the national power grid had disintegrated over two decades of Chavista rule" (Bolton 2020, 270).

In this era of disinformation operations and cyber uncertainty, the perceived benefits of "implausible deniability" should be weighed against the residual cost of a situation of "implausible culpability", in which the more assertive turn of U.S. cyber strategy combined with the Trump administration's broader policies of coercion and its use of threatening rhetoric, creating an opportunity for one U.S. adversary to seek to capitalize by

deflecting blame for domestic infrastructure failure onto the spectre of coercive U.S. behavior in cyberspace.

Following Jacquelyn Schneider (2020), this is arguably a reason for the U.S. government to review not only its declaratory posture in cyberspace, but also more broadly, the ways in which it publicly articulates its strategies and fuses its rhetoric and broad array of coercive policy instruments to pursue national strategic objectives. As mentioned above, this is an issue explicitly recognised by U.S. Cyber Command as requiring mitigation, partly through more effective communication (US Cyber Command 2018, 10). For the Biden administration, recalibrating rhetoric and reviewing the policy objectives that cyber and non-cyber instruments are used to pursue could mitigate shortcomings in the Trump administration's implementation of cyber strategy (Devanny 2021).

CONCLUSION

The last decade has seen an emerging pattern of cyber operations conducted by states against adversaries' critical infrastructure. It is this emerging pattern, or specifically the perceived failure of U.S. efforts to deter this behavior, that provided a significant part of the justification for U.S. adoption of a new cyber strategy in 2018. As states continue to develop and use national offensive cyber capabilities, it is likely that a continuation of existing policies will lead to further such operations.

Further complexity is added by the second-order effects of these operations. The system effects of this strategic turn in cyber operations are not limited to those that stem from the conduct of operations. They also include the effects of the competitive development process of offensive cyber capabilities by rival states, and indeed the very act of governments communicating about these capabilities. As persistent engagement's advocates argue, practice will shape the *de facto* norms of state behavior in cyberspace. This extends to the impact on perceptions caused by the potential complementarity of infrastructure-targeted cyber operations with other, non-cyber coercive instruments of policy or associated rhetorical threats. It also extends to the (unintended) strategic consequences of the duality between active cyber espionage and the potential to conduct offensive operations. This has been recently evident in the furore surrounding the SolarWinds breach.

As Robert Jervis has noted, the potential for misperceptions and corresponding errors of judgement in cyberspace is pronounced. This is particularly true in light of asymmetries of knowledge and the tendency for nuance to be winnowed out for decision-makers in the policy process (Jervis

2016). Another shaping factor is the distorted prism of the contemporary information environment. Competing narratives (both state narratives and proxy- or non-state narratives) proliferate more quickly and embed themselves more durably due to the analytical affordances and disintermediation of digital media platforms and the deterritoriality of the internet. The cumulative impact of these different strands is that states will likely struggle to control the perception of their intentions in cyberspace, not only amongst governments but across the many national audiences that comprise the global public sphere.

REFERENCES

Alperovitch, Dmitri, and Ian Ward. 2021. "How Should the U.S. Respond to the SolarWinds and Microsoft Exchange Hacks?" *Lawfare* 12 (March). https://www.lawfareblog.com/how-should-us-respond-solarwinds-and-microsoft-exchange-hacks.

Ball, James, Julian Borger, and Glen Greenwald. 2013. "Revealed: how US and UK spy agencies defeat internet privacy and security". *The Guardian.* https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

Baram, Gil, and Kevjn Lim. 2020. "Israel and Iran Just Showed Us the Future of Cyberwar with Their Unusual Attacks," *Foreign Policy* 5 (June). https://foreignpolicy.com/2020/06/05/israel-and-iran-just-showed-us-the-future-of-cyberwar-with-their-unusual-attacks/.

Bolton, John. 2020. *The Room Where it Happened: A White House Memoir.* New York: Simon and Schuster.

Borger, Julian. 2019. "US diplomat convicted over Iran-Contra appointed special envoy for Venezuela," *The Guardian* 26 (January). https://www.theguardian.com/us-news/2019/jan/26/elliott-abrams-venezuela-us-special-envoy.

Brands, Hal. 2017. "The Unexceptional Superpower: American Grand Strategy in the Age of Trump," *Survival* 59, no. 6: 7–40.

Casey, Nicholas. 2019. "Venezuela Was Crumbling. A Blackout Tipped Parts of It Into Anarchy," *New York Times* (March). https://www.nytimes.com/2019/03/15/world/americas/venezuela-blackout-maracaibo.html.

Cavelty, Myriam. 2015. "The normalization of cyber-international relations," *Strategic Trends 2015.* ETH Zurich: Center for Security Studies: 81–98.

Clement, Christopher I. 2005. "Confronting Hugo Chávez: United States 'Democracy Promotion' in Latin America," *Latin American Perspectives* 32, no. 3: 60–78.

Cormac, Rory, and Richard J. Aldrich. 2018. "Grey is the new black: covert action and implausible deniability," *International Affairs* 94, no. 3 (May), 477–94, https://doi.org/10.1093/ia/iiy067.

Crandall, Russell. 2008. *The United States and Latin America after the Cold War.* Cambridge: Cambridge University Press).

Daniels, Joe. 2019. "Venezuela: widespread blackouts could be new normal, experts warn," *The Guardian* 23 (July). https://www.theguardian.com/world/2019/jul/23/venezuela-blackouts-new-normal/.

Devanny, Joe. 2020. "The Ethics of Offensive Cyber Operations," *Foreign Policy Centre.* https://fpc.org.uk/the-ethics-of-offensive-cyber-operations/.

_____. 2021. "'Madman Theory' or 'Persistent Engagement'"? The Coherence of US Cyber Strategy under Trump. *Journal of Applied Security Research.* DOI: 10.1080/19361610.2021.1872359.

DeYoung, Karen, Anthony Faiola, and Alex Horton. 2020. "U.S. denies involvement in alleged Venezuela invasion attempt as details remain murky," *The Washington Post* (May). https://www.washingtonpost.com/national-security/trump-venezuela-invasion-attempt/2020/05/05/8b4d64ec-8ee7-11ea-9e23-6914ee410a5f_story.html?utm_campaign=wp_main&utm_medium=social&utm_source=twitter.

Egloff, Florian J., and Max Smeets. 2021. "Publicly attributing cyber attacks: a framework," *Journal of Strategic Studies.* DOI: 10.1080/01402390.2021.1895117.

Ellsworth, Brian. 2019. "UPDATE 3-Trump says U.S. military intervention in Venezuela 'an option', Russia objects". *The Washington Post* (February). https://www.washingtonpost.com/world/trump-us-military-intervention-in-venezuela-is-an-option/2019/02/03/27bb6d42-27ec-11e9-984d-9b8fba003e81_story.html

Faiola, Anthony. 2019a. "Inside the secret plot to turn Venezuelan officials against Maduro," *The Washington Pos*t (May). https://www.washingtonpost.com/world/the_americas/inside-the-secret-plot-to-turn-senior-venezuelan-officials-against-maduro/2019/05/13/5ad022a8-737e-11e9-8be0-ca575670e91c_story.html.

_____. 2019b. "Maduro's ex-spy chief lands in U.S. armed with allegations against Venezuelan government," *The Washington Post* (June). https://www.washingtonpost.com/world/the_americas/maduros-ex-spy-chief-lands-in-

us-armed-with-allegations-against-venezuelan-government/2019/06/24/b20ad508-9477-11e9-956a-88c291ab5c38_story.html.

_____. 2019c. "Juan Guaidó promised to save Venezuela. Now the flame he lit is petering out, and his U.S. backers are weighing their options". *The Washington Post* (December). https://www.washingtonpost.com/world/the_americas/juan-Guaidó-promised-to-save-venezuela-a-year-later-the-flame-he-lit-is-petering-out-his-us-backers-are-weighing-their-options/2019/12/17/48a1818-6-1495-11ea-80d6-d0ca7007273f_story.html.

Faiola, Anthony, Matt Zapotosky, and Karen DeYoung. 2020. "U.S. indicts Venezuela's Maduro on narcoterrorism charges, offers $15 million reward for his capture". *The Washington Post* (March). https://www.washingtonpost.com/world/the_americas/the-united-states-indicts-venezuelas-maduro-on-narco-terrorism-charges/2020/03/26/a5a64122-6f68-11ea-a156-0048b62cdb51_story.html.

Fischerkeller, Michael P. and Richard J. Harknett. 2017. "Deterrence is Not a Credible Strategy for Cyberspace". *Orbis* 61, no. 3: 381–93.

Grow, Michael. 2008. *U.S. Presidents and Latin American Interventions: Pursuing Regime Change in the Cold War*. Lawrence: University of Kansas Press.

Gunia, Amy. 2019. "Venezuela Blames U.S. For Blackout, Asks Diplomats To Leave". *Time*. https://time.com/5550481/venezuela-maduro-blackout-cyber-sabotage/.

Harknett, Richard J. and Emily O. Goldman, 2016. "The Search for Cyber Fundamentals," *Journal of Information Warfare* 15, no. 2: 81–8.

Harris, Shane. 2014. *@War: The Rise of Cyber Warfare*. London: Headline.

Harding, Luke. 2014. *The Snowden Files: The Inside Story of the World's Most Wanted Man*. London: Guardian Faber Publishing.

Healey, Jason. 2020. "The Cyber Budget Shows What the U.S. Values — And It Isn't Defense". *Lawfare* (June). https://www.lawfareblog.com/cyber-budget-shows-what-us-values%E2%80%94and-it-isnt-defense

Jervis, Robert. 1998. *System Effects: Complexity in Political and Social Life*. Princeton, NJ: Princeton University Press, 1998.

_____. 2016. "Some Thoughts on Deterrence in the Cyber Era," *Journal of Information Warfare* 15, no. 2: 66–73.

Jones, Sam. 2019. "Venezuela blackout: what caused it and what happens next?" *The Guardian* (October). https://www.theguardian.com/world/2019/mar/13/venezuela-blackout-what-caused-it-and-what-happens-next.

Krygier, Rachelle, and Anthony Faiola. 2020. "Venezuela's last democratic institution falls as Maduro attempts de facto takeover of National Assembly". *The Washington Post* (January). https://www.washingtonpost.com/world/the_americas/venezuelas-last-democratic-institution-falls-as-maduro-stages-de-facto-takeover-of-national-assembly/2020/01/05/8ba496fe-2d8f-11ea-bffe-020c88b3f120_story.html.

Leetaru, Kalev. 2019. "Could Venezuela's Power Outage Really Be A Cyber Attack?" *Forbes* (March). https://www.forbes.com/sites/kalevleetaru/2019/03/09/could-venezuelas-power-outage-really-be-a-cyber-attack/#581f687b607c.

Libicki, Martin. 2020. "Cyberwar is What States Make of It". T*he Cyber Defense Review* 5, no. 2, Special Edition: Information Operations/Information Warfare (Summer): 77–88.

Maduro, Nicolás. 2019. "La guerra eléctrica anunciada y dirigida por el imperialismo estadounidense en contra de nuestro pueblo será derrotada. Nada ni nadie podrá vencer al pueblo de Bolívar y Chávez. ¡Máxima unidad de los patriotas!". @NicolasMaduro, *Twitter* (March). https://twitter.com/NicolasMaduro/status/1103822286422003713.

Main, Alexander. 2020. "Out of the Ashes of Economic War: Sanctions and other forms of economic warfare have long caused serious harm for countries on the receiving end of Washington's efforts to impose its policy agenda. Could a progressive US administration marshal economic power at the service of people, not capital?". *NACLA Report on the Americas* 52, no. 1: 33–40.

Mann, James. 2004. *Rise of the Vulcans: The History of Bush's War Cabinet* (London: Penguin).

Medeiros, Breno Pauli, and Luiz Rogério Franco Goldoni. 2020. "The Fundamental Conceptual Trinity Of Cyberspace," *Contexto Internacional* 42, no. 1: 31–54. https://www.scielo.br/j/cint/a/WYHRGNsY5mpWzjCwsSfrTZv/?lang=en.

Nakashima, Ellen. 2019. "Trump approved cyber-strikes against Iranian computer database used to plan attacks on oil tankers," *The Washington Post* (June). https://www.washingtonpost.com/world/national-security/with-trumps-approval-pentagon-launched-cyber-strikes-against-iran/2019/06/22/250d3740-950d-11e9-b570-6416efdc0803_story.html.

Nakasone, Paul M. 2019. "A Cyber Force for Persistent Operations," *Joint Force Quarterly*, no. 92 (1st Quarter): 10–4, http://cs.brown.edu/courses/csci1800/sources/2019_01_22_JFQ_CyberRoleForPersistentOperations_Nakasone.pdf.

Pompeo, Mike. 2019. "No food. No medicine. Now, no power. Next, no Maduro," @SecPompeo, *Twitter* (March). https://twitter.com/SecPompeo/status/1103872530450771968.

Poznansky, Michael, and Evan Perkoski. 2018. "Rethinking secrecy in cyberspace: The politics of voluntary attribution". *Journal of Global Security Studies* 3, no. 4: 402–16.

Ramsey, Geoff. 2020. "By indicting Maduro, Trump is kneecapping a transition in Venezuela," *The Washington Post* 27 (March). https://www.washingtonpost.com/opinions/2020/03/27/by-indicting-maduro-trump-is-kneecapping-transition-venezuela/.

Rogin, Josh. 2018. "Bolton promises to confront Latin America's 'Troika of Tyranny'". *The Washington Post* (November). https://www.washingtonpost.com/opinions/global-opinions/bolton-promises-to-confront-latin-americas-troika-of-tyranny/2018/11/01/df57d3d2-ddf5-11e8-85df-7a6b4d25cfbb_story.html.

Rohde, David. 2020. *In Deep: The FBI, the CIA, and the Truth about America's "Deep State"*. New York: W.W. Norton.

Roth, Andrew, and Ellen Nakashima. 2017. "Massive cyberattack hits Europe with widespread ransom demands". *The Washington Post* (June). https://www.washingtonpost.com/world/europe/ukraines-government-key-infrastructure-hit-in-massive-cyberattack/2017/06/27/7d22c7dc-5b40-11e7-9fc6-c7ef4bc58d13_story.html?utm_term=.6f52ad40e788/.

Sanger, David E. 2012. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. New York City: Crown Publishing Group.

Sanger, David E., and Nicole Perlroth. 2019. "U.S. Escalates Online Attacks on Russia's Power Grid". *New York Times* (June). https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html.

Schneider, Jacquelyn. 2020. "A Strategic Cyber No-First-Use Policy? Addressing the US Cyber Strategy Problem". *The Washington Quarterly* 43, no. 2: 159–75.

Sequera, Vivian, and Deisy Buitrago. 2019. "Venezuela, blaming U.S. for six--day blackout, orders diplomats to leave". *Reuters* (March). https://www.reuters.com/article/us-venezuela-politics/venezuela-blaming-u-s-for-six-day-blackout-orders-diplomats-to-leave-idUSKBN1QT25W/.

Sheridan, Mary Beth, and Mariana Zuniga. 2019. "In Venezuela, massive blackout continues as Maduro blames U.S. for outages". *The Washington Post* (March). https://www.washingtonpost.com/world/the_americas/venezuelas-devastating-blackout-stretches-into-friday/2019/03/08/10ea8812-4198-11e9-9361-301ffb5bd5e6_story.html.

Spetalnick, Matt. 2019. "Russian Deployment in Venezuela Includes 'Cybersecurity Personnel': U.S. Official". *Reuters* (March). https://www.reuters.com/article/us-venezuela-politics-russians-idUSKCN1R72FX.

Tharoor, Ishaan. 2020. "A Bay of Pigs-style fiasco in Venezuela". *The Washington Post* (May). https://www.washingtonpost.com/world/2020/05/06/bay-pigs-style-fiasco-venezuela/.

U.S. Cyber Command. 2018. *Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command*. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf.

U.S. Department of Defense. 2018. *Summary: Department of Defense Cyber Strategy 2018*. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

Valeriano, Brandon, and Benjamin Jensen. 2019. "How cyber operations can help manage crisis escalation with Iran". *Washington Post* (June). https://www.washingtonpost.com/politics/2019/06/25/how-cyber-operations-can-help-manage-crisis-escalation-with-iran/.

Valeriano, Brandon, Benjamin Jensen, and Ryan C. Maness. 2018. *Cyber Strategy: The Evolving Character of Power and Coercion*. Oxford: Oxford University Press.

Volz, Dustin. 2018. "Trump, Seeking to Relax Rules on U.S. Cyberattacks, Reverses Obama Directive; Administration has faced pressure to show that it is taking seriously national-security cyberthreats". *The Wall Street Journal* (August). https://www.wsj.com/articles/trump-seeking-to-relax-rules-on-u-s-cyberattacks-reverses-obama-directive-1534378721.

Zetter, Kim. 2014. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown.

NOTAS

1. This article is part of the project 'Science, Technology and Innovation in Defense: Cybernetics and National Defense,' approved by Public Notice 27/2018, Support Program for Teaching and Scientific and Technological Research in National Defense – PRO-DEFENSE IV.

THE 2019 VENEZUELAN BLACKOUT AND THE CONSEQUENCES OF CYBER UNCERTAINTY

ABSTRACT

In March 2019, Nicolás Maduro claimed that the blackout in Venezuela was caused by U.S. cyber-attacks. This statement was promptly denied by Mike Pompeo, the U.S. Secretary of State. Irrespective of the truth of Maduro's allegation, this episode highlights the diplomatic challenges for states in the contemporary information environment, in which contested narratives proliferate and embed themselves more durably because of the deterritoriality and disintermediation of the Internet. This is particularly true in the context of an emerging pattern of state actors conducting cyber operations against critical infrastructure in other states. The cumulative impact of these different strands is that states will likely struggle to control the perception of their intentions in the cyber domain, not only amongst governments but across the many national audiences that comprise the global public sphere. Focusing on Maduro's allegation, this article analyses the political utility of cyber uncertainty, and its corresponding implications for states' cyber strategies and decisionmaking.

Keywords: Cyberspace; Uncertainty; Cyber Operations; Cyber Defense; Digital Diplomacy.

RESUMO

Em março de 2019, Nicolás Maduro afirmou que o blecaute na Venezuela foi causado por ciberataques perpetrados pelos EUA. Esta declaração foi prontamente negada por Mike Pompeo, Secretário de Estado norte-americano. Independentemente da verdade da alegação de Maduro, este episódio destaca os desafios diplomáticos para os Estados no ambiente de informação contemporâneo, no qual as narrativas contestadas proliferam e se incorporam de maneira mais durável por causa da desterritorialidade e desintermediação da Internet. Isso é particularmente verdadeiro no contexto de um padrão emergente de atores estatais que conduzem operações cibernéticas contra a infraestrutura crítica em outros Estados. O impacto cumulativo dessas diferentes vertentes é que os Estados provavelmente terão dificuldades para controlar a percepção de suas intenções no domínio cibernético, não apenas entre os governos, mas entre os diversos públicos nacionais que compõem a esfera pública global. Focando na alegação de Maduro, este artigo analisa a utilidade política da incerteza cibernética e suas implicações correspondentes nas estratégias e decisões cibernéticas dos Estados.

Palavras-chave: Ciberespaço; Incerteza; Operações cibernéticas; Defesa cibernética; Diplomacia digital.

Recebido em 29/06/2020. Aceito para publicação em 19/04/2021.

Cyberterrorism 2.0 or terrorist use of social media: the Islamic State case

Terrorismo cibernético 2.0 ou uso terrorista das redes sociais: o caso do Estado Islâmico

Rev. Bras. Est. Def. v. 7, nº 2, jul./dez. 2020, p. 59-80
DOI: 10.26792/RBED.v7n2.2020.75210
ISSN 2358-3932

GILLS VILAR-LOPES
MARCELO DE ALMEIDA MEDEIROS

INTRODUCTION

Cyberspace — and, more specifically, the Internet — becomes a common source of threats to national defence and international security (Brazil 2020; Costa 2012, 53–66), especially after the September 11 attacks. Besides, the rise and popularisation of so-called social media in the mid-2000s enhance the militancy of the most diverse social groups, including terrorist ones.

In this context, we problematise the international terrorism issue to point out which factors contribute to the emergence and development of new cyberterrorism 2.0. This article focuses on a particular recent aspect of cyberterrorism (thus, not about the entire phenomenon): new ways of using cyberspace, especially social media. Hence, we try to expose several inputs — and possible outputs — of social media usages by terrorists in terms of political[1]

Gills Vilar-Lopes — Lecturer in International Relations and Head of the Postgraduate Program in Aerospace Sciences (PPGCA) at the Brazilian Air Force University (UNIFA). PhD in Political Science from the Federal University of Pernambuco (UFPE). Specialised Course in Cybersecurity from the National Defense University (NDU), Washington D.C. Researcher at RedeCTIDC/Pró-Defesa IV (CAPES/MD), GEESI/UFPB and NEPI/UFPE. Editorial Advisor of the RBI/ABIN. This article is a result of research carried out in the Volunteer Service Program (PSV) of the Brazilian Ministry of Defence's Pandiá Calógeras Institute and complemented by discussions about "Terrorism and cyber threats in the 21st century" at a public hearing of the Foreign Relations Commission (CRE) of the Federal Senate in 2017.
Marcelo de Almeida Medeiros — Ph.D. in Political Science from the Institut d'Études Politiques de Grenoble and Habilitation Thesis from the Institut d'Études Politiques de Paris – Sciences Po. Full Professor of Comparative International Politics at the Federal University of Pernambuco – UFPE (Recife, Brazil) and PQ-1C Research Fellow of the National Council for Scientific and Technological Development – CNPq. He was Rio Branco International Relations Chair at St Antony's College, University of Oxford, Visiting Scholar at the Sciences Po, and Simon Bolivar Political Science Chair of the Institut des Hautes Études de l'Amérique Latine – Université Sorbonne Nouvelle – Paris III.

proposes, provided that we can better understand the complex current scenario of international security. Therefore, we do not ponder how and why terrorist groups use cyberspace or the Internet as a whole, but rather how they use specific and recent networks such as Facebook, Twitter, and YouTube.

Briefly, our main objective is to analyse the recent manifestations of cyberterrorism — which is an international phenomenon by itself — in the light of International Security Studies. In this regard, we try to promote a dialogue between specific data methods of collecting and analysing, as follows:

> Case study. Given the extraordinary international evidence the Islamic State (IS)[2] terrorist group has provoked the media, academy, and foreign policy of major great powers, we delve into a specific category of terrorist groups: paramilitary Islamic radicals/extremists. Here, we research and analyse the period between June 2014 and April 2015. The first period marks the IS self-proclamation, and the moment great powers start to pay more attention to the transnational claim of a caliphate in the Middle East. The second period (early 2015) is the apex of the terrorist use of social media worldwide.
>
> Discourse analysis. After monitoring social media during the cut time, as mentioned above, we sought to build an overview of the main subjects — Trending Topics (TTs) and hashtags — related to the terrorist activity on social media.

To bring the discussion of terrorism into cybersecurity, we describe and apply the qualitative framework so-called Stakeholders, Activities and Motives in the realm of cybersecurity (SAM), proposed by Kremer and Müller (2014, 41-58). we seek to understand the inputs around social media use by Islamic extremist groups, notably the IS case.

Accordingly, this work has three parts. The first one defines cyberterrorism 2.0 and social media, focusing on international relations. Subsequently, the inputs of cyberterrorism 2.0 are analysed; that is to say, we seek to identify by whom (Stakeholders), how (Activities), and why (Motives) social media are used with terrorist intentions. Social media use by specific terrorist groups has eventually engendered certain outputs in the secret services and National Defence bodies. In other words, we claim that states seek to combat such groups with the same virtual tools used to spread terror on the Internet and beyond, namely social media.

CYBERTERRORISM 2.0

As Hoffman (2017, 22) observed, "Like social media — another grossly overused term that has similarly become an indispensable part of the ar-

got of the early twenty-first century — most people have a vague idea or impression of what terrorism is [...]".

There is no consensus about terrorism, although some essential elements in these definitions are more common: political goals (Hoffman 2017, 25); violent unlawful acts or threats and actions to produce effects beyond the victims (Gonçalves and Reis 2017). The most classical definition comes from Hoffman (2017, 109), who stated that terrorism is "the deliberate creation and exploitation of fear through violence or the threat of violence in the pursuit of political change."

Nevertheless, to illustrate this conceptual difficulty, the United Nations (UN) itself struggles to define what terrorism is (Annan 2005). However, what we have is an old UN official statement that indirectly provides the following meaning to terrorism:

> criminal actions designed or calculated to provoke a state of terror in the general public, in a group of people or certain people, which have political ends and which are unjustifiable, regardless of their political, philosophical, ideological, racial, ethnic, religious claims or otherwise. (United Nations 1995, free translation).

As our work is directly related to the Internet — one of the main cyberspace facets — the analyses presented throughout this study refer specifically to the so-called cyberterrorism, a term made up in the 1980s by Barry Collin, a senior researcher at the Institute for Security and Intelligence in California (Cavelty 2007, 19-36).

In the same way, the term terrorism uncovers multiple definitions (Hoffman 2017, 22–5), and the concept of cyberterrorism is sometimes comprehensive and vague (Cavelty 2007, 20; Gercke 2009). Nevertheless, this theme's political and academic interest grows significantly, especially from the 2000s, when conceptual differences between policymakers and academics emerge (Crosston 2014, 253–67). However, there is practically a consensus about the most accepted meaning referred to as cyberattacks,[3] which generate fear and direct against national strategic structures,[4] such as hydroelectric, gas, energy, and air transport networks (ATN).

On the one hand, cyberspace promotes a high degree of decentralised, instantaneous, and sometimes anonymous sharing of information, which positively marks many societies' quotidian societies. On the other hand, it raises technical, logistical, and strategic risks for international security professionals and scholars (Demchak 2014, v-x). Regarding national security issues, this Manichaean trait of the Web lies in the fact that the concepts of internal and external enemies are merging more and more in this new domain. Otherwise stated, even though the era of social media has

emerged in the fields of humanitarian action, social activism, and development (Karlsrud 2014, 141–60), it also ends up being transformed into a strategic, operational environment for terrorists and jihadists influence (Kuehl 2014, 24–42).

In a global sense, social networks are not an exclusive issue to the Information Age. They have existed for centuries since they consist of many social groups whose individuals/elements interrelate by affinity. Nonetheless, with the spread of the Internet, especially in the mid-2000s, the term "social media" referred exclusively to websites and virtual applications that simultaneously support several social networks. Information sharing is one of the main particularities (Ferreira 2011, 208–31).

Despite the countless definitions of social media found in the most diverse areas of knowledge, there is still confusion related to them. An example of this conceptual imprecision is in Sterne's (2010) proposal, which differentiates six broad social media categories, precisely: (i) microblogs, (ii) media sharing, (iii) social media, (iv) blogs, (v) forums, (vi) bookmarking, and (vii) websites for opinions and recommendations. By separating the first three categories, the author also classifies different subcategories of websites and apps that have practically the exact characteristics of content sharing — such as Facebook, Twitter, and YouTube.

Aiming to standardise our analysis[5], we suggest a unique category of "social media", bringing together websites and applications such as Facebook, Twitter, and YouTube in the same group. Since these three web services perform practically the same tasks, differentiating one from the other only by technical limits — e.g., the number of characters or bytes. In conclusion, cyberspace incorporates the Internet because it is the only social media "many-to-many" (Sterne 2010, xvi) and is an interconnected digital infrastructure (Kremer and Müller 2014, 42).

As the years go by, social media leave the fields of leisure and work and incorporate more political aspects, i.e., creating a situation in which people and social groups can agree with their governments[6] and go against them (Karlsrud 2014, 154). Nevertheless, social media in the 21st century is not just about social revolutions and government repressions, as we usually see in papers and news, for instance, 2010/2012 Arab Spring and the 2019 Hong Kong Umbrella Movement.

Within the strategic uses of these tools, the term cyberterrorism is becoming popular in the scope of Defence and International Security Studies (Kuehl 2014, 5). Before putting them into context, it is necessary to remember the very definition of terrorism to understand how both terms apply to International Security Studies. From this, it is possible to assimilate the meaning of cyberterrorism 2.0.

Considering the association of cyberterrorism with cyberattacks, Cavelty (2010, 2) creates a hierarchical typology of cyber conflicts widespread in studies on the topic. Among the five types, cyberterrorism — involved in producing fear through some infrastructural damage — is in second place among cyber conflicts that can generate more potential damages to people, businesses, and states.

This mainstream position in the international security literature — which culmination is Cavelty's typology — does not entirely satisfy our objectives here. The reason for this is that, for instance, social media use by terrorist groups does not fit as an act of cyberterrorism in the eyes of this restricted meaning. Consequently, a broad enough concept is needed to, on one side, frame the extremist use of social media as a terrorist act along the lines of the UN definition; and, on the other, incorporate cyberattacks by terrorists to cause damage to strategic structures.

In this regard, our contribution intends to update the concept of cyberterrorism to what was practised by terrorist groups in cyberspace during the 2010s — now named cyberterrorism 2.0, that is, criminal cyber activities caused by a group or individual linked to a terrorist group, whose reasons or motivations are unjustified, to cause a state of terror to one or more people, *through psychological or physical damage.*

Typifying the crime of cyberterrorism 2.0 must comply with the judicial principle of the legal reserve. Hence, it must be previously defined as illegal; therefore, it is necessary to cultivate a law that guides it. Gagnon (2008, 46–65) recalled this when he stated that terrorism comprises both national security and criminal issues. Conversely, to legislate in an environment as unusual as cyberspace is complex, as reminded at (i) the 2001 Budapest Convention on Cyber Crimes and (ii) the fact that "several worrying criminal acts not officially defined by the authorities as terrorism may have been influenced, at least in part, by online terrorist propaganda" (Adl 2015a).

For instance, from this perspective, a posting of the video with decapitations of 21 Coptic Christians by an Islamic extremist group, as a direct message to other followers of that religion (*Folha de S. Paulo* 2015), for us, is an act of cyberterrorism 2.0. Additionally, the act of sharing and liking this type of content will also constitute a crime, even if practised by individuals who are not part of the original group of the post, if the justification/reason for this (cyber) action is the same as the original.

This forewarning is necessary because media outlets generally illustrate their reports with excerpts from videos posted by terrorist groups. In rare exceptions, these mass media provide links to videos and photos in full, under the argument of informing and often intentionally shocking

the public to call more attention to the reported case. In the Copts execution example, the act of liking or sharing the original post can be framed as a type of crime: an apology to terrorism or another correlate, but it is not defined as cyberterrorism 2.0 in the terms we defend here. Only those who encourage and support the message shared initially to cause psychological damage to a specific person or group are those who practice the act of cyberterrorism in its updated version 2.0.

Therefore, we define cyberterrorism 2.0, which analyses how terrorists or terrorist groups use social media to spread fear inside and, mainly, outside the Internet. Thus, it is a type of the cyberterrorism 2.0 genre that can cover other subareas, such as encrypted means — e.g., mobile telephone, electronic mail, and SMS services, to articulate terrorist cells. Along with the mapping of potential terrorist targets using geolocation software and online maps, the terrorist performance on the Deep Web; and financial support received via cryptocurrency.

In this sense, Terrorism Studies involve different areas and fields of knowledge to explain this violent phenomenon. At the international security level, we can see how cyberspace and specifically social media have boost terrorist activities such as recruitment and propaganda (Ford 2020) to achieve the main goal of spreading terror. Figure 1 shows the logic behind our argument, situating, at the same time, both the epistemic and operational position around cyberterrorism 2.0.

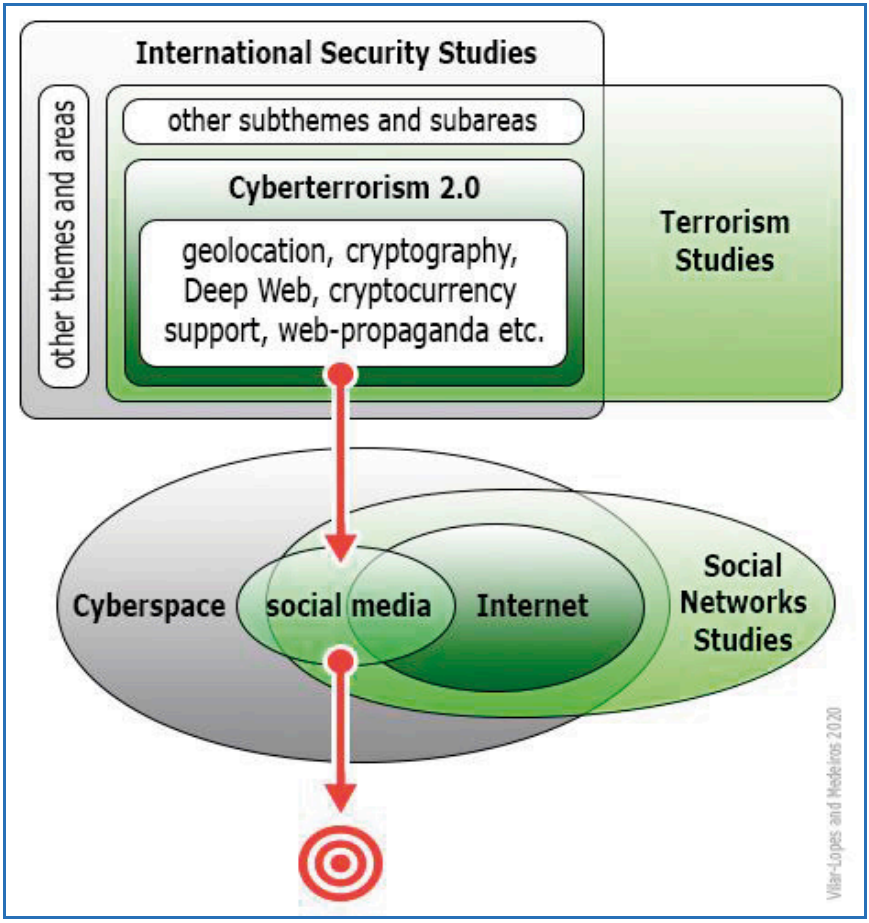


Figure 1 — Cyberterrorism 2.0 definition.
Source: the authors.

As Figure 1 shows, cyberterrorism 2.0 has its logic, explicitly: to demonstrate that social media can also be used for non-peaceful purposes. An example of this is comparing such a negative form of operation with a positive defence one in peacekeeping processes:

> There is a mushrooming of efforts to make use of big data and social media in countries in crisis. [...]Concurrently, social media is strengthening the opportunities of rebels to communicate their mes-

> sage internally, to domestic and external supporters, and directly to traditional media outlets. (Karlsrud 2014, 147).

When analysing the idea behind cyberterrorism 2.0, we see that it is contrary to Karlsrud's. In other words, while there are efforts to operate social media constructively, for example, in countries experiencing conflict, it becomes a means for terrorist groups to spread their message to the whole world through social media to bring terror to their targets. This is the hypothesis that the analyses of the following section seek to corroborate.

INPUTS OF CYBERTERRORISM 2.0 IN THE LIGHT OF THE SAM FRAMEWORK

This section seeks to highlight (i) who cyber terrorists are, (ii) how they act, and (iii) what leads them to use social media to promote cyberterrorism 2.0. These three issues are in strict accordance with the three variables set of the qualitative analysis tool named Stakeholders, Activities and Motives (SAM), by Kremer and Müller (2014), which applies to specific cybersecurity and international relations cases.

As seen in the previous section, most of the literature tends to associate cyberterrorism with cyberattacks by terrorists. Accordingly, the link between cybersecurity and international relations seems clear. As we advocate, it is necessary to broaden the concept of cybersecurity when discussing studies on terrorism, including logical/informational and psychological attacks — such as the publication of content on social media. Radical religious groups have recognised, for years, the multifaceted role that images, audio and videos play in psychological warfare (Katz 2015).

Even though the SAM's creators indicated that it aims to deal with the conceptual challenges of categorising stakeholders, activities, and motives within the scope of cybersecurity (Kremer and Müller 2014, 44), such a framework fits perfectly into this section's objectives, as it has a holistic character. However, when we deal with cybersecurity, the authors are more concerned with property and political damage caused to strategic structures — e.g., cyberattacks and intrusions into networks and computers.[7]

This thinking is very similar to the scholars' first cyberterrorism conception (cyberterrorism 1.0) seen in the previous section. Also, as with cyberterrorism 2.0, we adapt SAM to make it fit into the terrorist use of social media problems — and not the other way around — and involve cyber incidents (Kremer and Müller 2014, 45) as well as an international

phenomenon related to cyberspace, as the cyberterrorism 2.0 case shows us. In this sense, Table 1 presents three dimensions behind SAM.

Table 1
SAM framework

Stakeholder	Who?	Who is mandating, who is executing and who is affected?
Activities	What?	What activities they carried out, and what are the results in terms of defects?
Motives	Why?	Why have the activities been carried out, what are the underlying motivations and intentions?

Source: Kremer and Müller 2014, 46.

As we notice, the three sets of SAM responses correspond, essentially, to the three inputs of cyberterrorism 2.0. The research design excels in this endeavour, and we divide it into three smaller parts. The first one aims to find out who the stakeholders of cyberterrorism 2.0 are, through a quantitative survey of the profiles of terrorist groups on social media, and with the help of Webometrics methodology. The second part investigates the actions and effects on the terrorist targets through discourse analysis (DA) of the leading virtual profiles in the first phase of the research. Finally, the third part seeks to list the reasons for these activities. In doing so, we could complete the SAM framework.

Accordingly, we consider Webometrics, which includes all content accessible from the Internet and its web search engines — such as Bing, Google, Yahoo! — and other online tools. One of the webometric species is big data, which refers to the large volume of publications on virtual social media websites, videos, and blogs (Demchak 2014, viii; Karlsrud 2014, 142).

Although less than half of the terrorist groups had websites in 1998, almost all of them, including Al-Qaeda, had a space on the Internet around five years later. Shortly after that milestone, YouTube starts to function as a tool favouring fundamentalist advertisements (Gercke 2009, 53). In June 2014, the terrorist group that calls itself the Islamic State (IS) acts in an even more radical way concerning those opposed to creating a caliphate in parts of Iraq and Syria. One way to draw the world's attention and supporters to its cause is social media use. Other groups quickly followed this way of acting. The three main paramilitary Islamic fundamentalist groups operating in the Middle East and Africa — Al-Shabab, Al-Qaeda and Boko Haram — began to copy it.

Therefore, chart 1 shows the interest of Internet users in these groups between 2014 and 2015. It provides accurate data regarding the general research interest of four terrorist groups, ranging from 0 to 100 in that period. Nevertheless, we take into account the relative interest rather than the absolute. That is why, even though it does not appear in Chart 1, in relative terms, Al-Qaeda is by far the most searched terrorist group in the last 15 years. For this reason, it is natural that the peak (100) remained with that group in May 2004 — a few weeks after the attacks on the Madrid Metro, which allegedly attributed to it. However, once the research is from June 2014, it is noted that Al-Qaeda lost prominence on the Internet for Boko Haram and IS, and only in mid-April 2015, for example, it regained prominence.

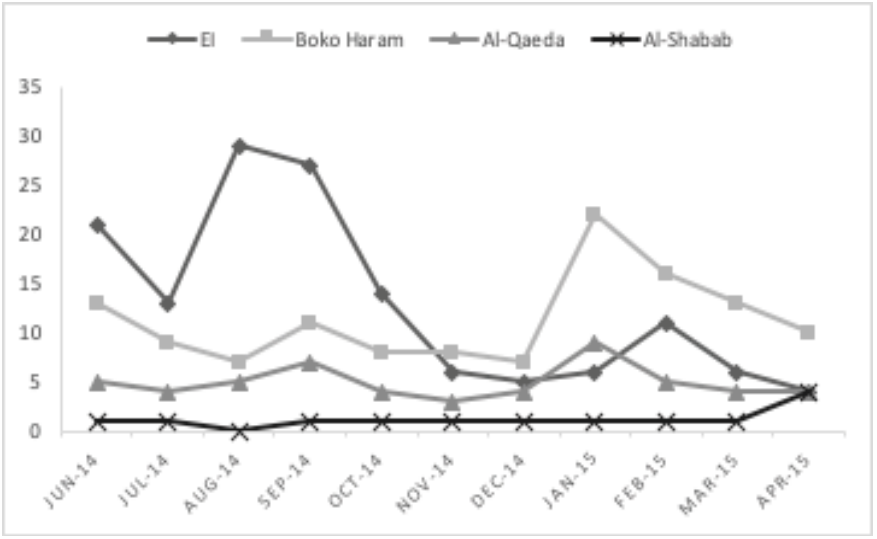


Chart 1 — Internet interest in terrorist groups (2014-2015)
Source: the authors based on data obtained in Google (2015)

Based on the first SAM variable, Stakeholder, we aim to identify who is in charge of cyberterrorism 2.0 between 2014 and 2015. For this purpose, we carry research out on the social medium used mainly by extremist Islamist groups such as IS, namely, Twitter (Adl 2015a, 10; 2012).[8] Through this aggressive social media strategy, IS transforms how terror-

ist groups and their supporters reach, influence, and recruit worldwide (Adl 2015a, 10).

IS Twitter numbers are impressive. In 2014, more than 12 official accounts were just for the organisation's central leadership, with the @alItisam account gaining over 50,000 followers. To get a comparative idea, the website Topsy (2015) shows the list of tweets per day on a given topic or over the last month. Consequently, we verify that between March 27 and April 26, 2015,[9] IS maintained its position as the most mentioned terrorist group on Twitter, according to Chart 2.

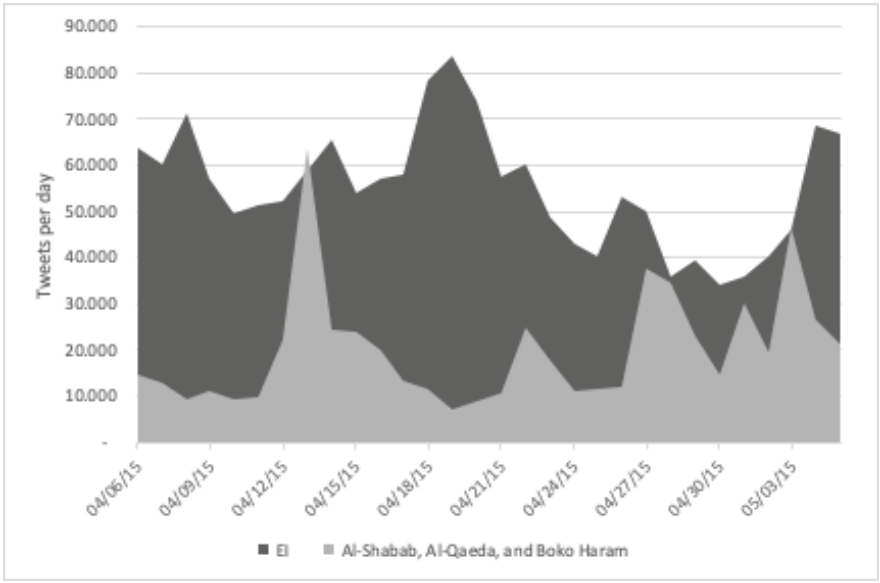


Chart 2 — Daily tweets about terrorist groups (April 6.- May 5, 2015).
Source: the authors based on data obtained in Topsy (2015).

Chart 3, in turn, shows the hashtags that refer to each of the four terrorist groups under analysis, in one month, between April 6 and May 5, 2015.

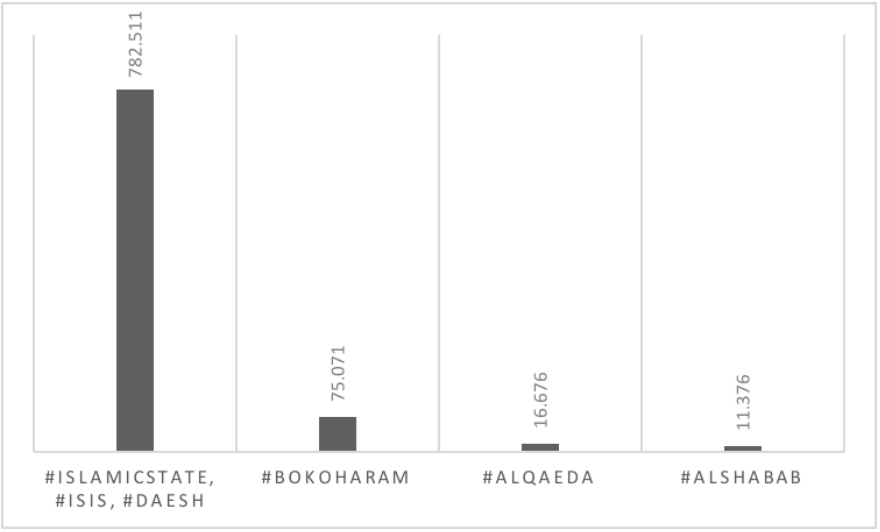


Chart 3 — Hashtags from terrorist groups on Twitter (April 6. — May 5, 2015).
Source: the authors, based on data obtained in Topsy (2015).
Note: Once IS is best known for ISIS and DAESH, the following amounts of hashtag citations are combined: #ISIS (605,670), #DAESH (113,510) and #ISLAMICSTATE (63,331).

Through Charts 2 and 3, it is possible to highlight two critical findings. Firstly, both the tweets and the hashtags about IS alone surpass all three other terrorist groups together within the proposed interval.[10] Secondly, as in the real world, the reactions of Twitter users follow the repercussions of the activities and physical attacks of these terrorist groups. For example, the only time IS loses its first position in the ranking shown in Graph 2 is on April 14, 2015, when Amnesty International reports — and the mainstream media reflects — that Boko Haram has already kidnapped at least 2,000 women (*Al Jazeera* 2015) — including 270 Nigerian Catholics in 2014.[11] Another example is the summit (49,721 tweets per day) of this time series that happened precisely on April 19, 2015, when ISIS releases a video about the execution of 30 Ethiopian Christians in Libya (*Folha de S. Paulo* 2015).

Significantly, we can say that one of the main objectives of these groups, which is to attract attention, is being achieved. However, it is challenging to measure the extent to which the contents (videos, texts, and images) shared on social media by such groups cause psychological damage, especially because Twitter, for example, is more used in Western countries. Nonetheless, it is possible to measure some perception or feeling from this

medium. For instance, the Topsy Sentiment Score[12] seeks to define how Twitter users react to specific subjects on a 0-to-100 scale. The closer a subject or hashtag is to 100, the more well-received or approved by social media. In other words, above 50 points, a positive score is attributed to the subject or hashtag.

When searching for the scores of the hashtags listed in Chart 3,[13] we observe there is a negative feeling towards all terrorist groups, as shown in Chart 4.

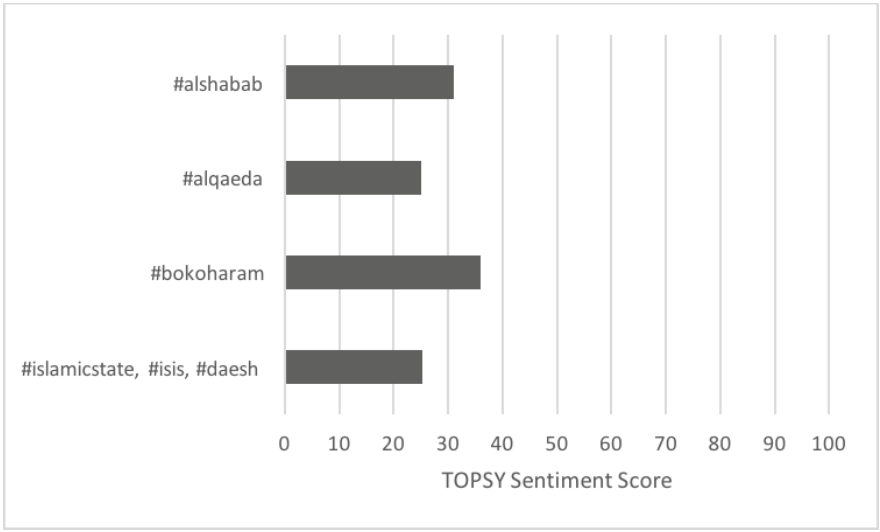


Chart 4 — "Sentiment" towards terrorist groups on Twitter on April 6 — May 5, 2015)
Fonte: the authors, based on data obtained in Topsy (2015).
Note: As IS is well known by ISIS and DAESH, the average score of its hashtags is taken, namely: #ISIS (26), #DAESH (32) and #ISLAMICSTATE (18).

Based on the cyberterrorism 2.0 definition, Chart 4 does not point out to whom and what psychological damage the contents posted by terrorist groups on Twitter causes. However, it demonstrates, in a way, that there is a tendency for users affected by the messages to disapprove of those terrorist activities, such as the sharing of execution videos, slogans, information about the city taken. In this bias, we can infer the score proposed by Topsy, which reflects the rejection of the shared content or aversion to terrorist groups by most Twitter users. Therefore, the score shown in

Chart 4 dialogues with SAM framework points to the disapproval of the messages' content by most affected users (stakeholders).

As stated, Islamic State is the terrorist group that best manages social media, especially Twitter and YouTube, to spread its messages, recruit followers, including Westerners, and encourage its supporters to take part in this process. However, it is impossible to say social media play a sufficient role in this recruitment (Adl 2014).

There are several motivations behind the terrorist use of the Internet, such as: disseminating advertisements, describing and publishing the reason for its activities, and recruiting or contacting members and donors for their cause (Gercke 2009, 53). However, the following question arises concerning recruitment: is it possible to have such activity on the Internet?

Aiming to clarify this doubt, the European Convention on the Prevention of Terrorism, signed in 2005 and applicable since 2009, must be referred. This international treaty defines *recruitment* for terrorism as the request for someone to commit or participate in a terrorist act or participate in an association or group to contribute to the practice of one or more terrorist acts on behalf of that association or group (European Council 2005).

As above-mentioned, many Westerners nations, including American (Adl 2015a, 16–7), have enlisted in the paramilitary forces of these groups, mainly in IS, whose propaganda machine not only attracted thousands of recruits but also helped Syria and Iraq to emerge as the preferred destinations of this new generation of extremists (Adl 2015a, 1).

This new generation of future terrorists permits closing the panorama of the inputs of cyberterrorism 2.0. Table 2 presents the final version of the SAM adapted and filled with what we expose so far.

Table 2
SAM Framework applied to cyberterrorism 2.0

Stakeholder	*Who* is ordering the use of social media for terrorist purposes?	*terrorist* groups such as: - Al-Shabab - Al-Qaeda - Boko Haram and, mainly, - IS
	Who is executing the terrorist activities on social media?	- *individuals* directly linked to terrorist groups. - *individuals* supporting the causes contained in messages shared on social media.
	Who is affected by the terrorist use of social media?	- even though it is challenging to measure psychological damage on social media, it can be said that the majority (approximately 70%) of *individuals* who have Twitter accounts disapprove of such groups.
Activities	*What* activities the terrorist use of social media carries out?	*non-destructive*, to *influence* public opinion and potential recruits.
	What are the results in terms of damage from the terrorist use of social media?	- *empirically*, Westerners will fight on the field and funding is sent to terrorist groups. - *psychologically and inductively*, about 70% of tweets show a high sense of disapproval for the four groups analysed. - *physically*, no strategic structure was damaged directly or indirectly.
Motives	*What* motivations lead carrying terrorist activities out on social media?	- *ideologically*: proliferating the Islamic faith. - *psychologically*: recruiting followers. - *financially*, empower supporters to take part in their activities. - *politically*, support the idea of the foundation of an Islamic State between Iraq and Syria.

Source: the authors.

CONCLUSION

The terrorist use of social media has engendered, in addition to the inputs seen in this work, some technological and political outputs. A technological example is that companies that own social media websites, such as Twitter, blocked (Garcia 2015) and closed (Adl 2014b) accounts that supported followers and even members of Al-Shabab and IS. However, by excluding accounts associated with terrorist groups, companies seem to stimulate a sort of Procrustean dilemma applied to cyberterrorism 2.0;

namely, the fewer accounts there are, the fewer potential intelligent sources of terrorist activity will exist (Adl 2012).

We can speculate that the mimicry the military will use is in two stages. The first is the observation of how terrorist groups use social media for massive recruiting. The second stage concerns a needed blend between different methods of espionage and sabotage, something very close to a junction between social[14] and reverse engineering, in what we can call "reverse social engineering". This seems to be a very complex task since the Internet — an environment in which social media are inserted — has a potential not yet measurable and in self-expansion. This seems to be the ideal scenario for the proliferation of cyber benefits and ills — the case of cyberterrorism 2.0.

Briefly and strategically speaking, there are some motivations for the use of social media by terrorist groups that we can summarise:

Make it impossible, in most cases, the consecutive charge for the content and publication, since the publisher's anonymity can be guaranteed with a simple fake profile or by use of more technical devices to mask or even hide the actual upload location where a post is.

Make it possible to reach many people practically across the globe.

Transmit various media types for free and instantaneously (text, image, voice, and video).

By applying the SAM framework in the IS case, we could have a big picture about who is responsible for manipulating social media to promote terror for political purposes, what are the results in terms of damage from the terrorist use of social media and, finally, what motivations lead terrorist activities out on these online tools.

Therefore, it is evident that the terrorist use of social media — the inputs this article sought to discuss — by paramilitary fundamentalist groups, such as IS, prove to be quite effective in their attempts, despite the strategic action of civilian and military intelligence services have emerged as an output that sates have found out to fight against cyberterrorism 2.0.

REFERENCES

Adl. 2011. "Al Shabab launches apparent Twitter campaign". http://www.adl.org/combating-hate/international-extremism-terrorism/c/shabaab-launches-twitter.html.

_____. 2012. "Tweeting for terror". http://www.adl.org/combating-hate/international-extremism-terrorism/c/tweeting-for-terror.html.

_____. 2014a. "Hashtag Terror: how ISIS manipulates social media". http://www.adl.org/combating-hate/international-extremism-terrorism/c/isis-islamic-state-social-media.html.

_____. 2014b. "ISIS faces resistance from social media companies". https://www.adl.org/blog/isis-faces-resistance-from-social-media-companies.

_____. 2015. "Homegrown Islamic Extremism in 2014: the rise of ISIS & sustained online recruitment". https://www.adl.org/sites/default/files/documents/assets/pdf/combating-hate/homegrown-islamic-extremism-in-2014-the-rise-of-isis-and-sustained-online-recruitment.pdf.

Al Jazeera. 2015. "Report: At least 2,000 women abducted by Boko Haram". http://www.aljazeera.com/news/2015/04/nigeria-boko-haram-150414043301574.html.

Annan, Kofi. 2005. "Uma estratégia mundial de combate ao terrorismo." *Público*, Lisboa, 12 Mar, http://www.publico.pt/espaco-publico/jornal/uma-estrategia-mundial-de-combate-ao-terrorismo-10842.

Barreto, Eduardo M. 2007. "Terrorismo Cibernético e cenários especulativos". *Revista Brasileira de Inteligência* 3, no. 4: 63–76.

Brazilian Institutional Security Office, GSI. 2019. "Glossário de Segurança da Informação." *Brazil's Republic Presidency*, https://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663.

_____. 2020. "National Cybersecurity Strategy." *Brazil's Republic Presidency*, http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm.

Cavelty, Myriam D. 2007. "Cyber-Terror — Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate". *Journal of Information Technology & Politics* 4, no. 1: 19–36.

_____. 2010. "Cyberwar: concept, status quo, and limitations". *CSS Analysis in Security Policy* 71: 1–3.

Costa, Carlos E. B. 2012. "Tendências mundiais e seus reflexos para a defesa brasileira". *Revista Brasileira de Inteligência* 7: 53–66.

Crosston, M. 2014. "Phreak the speak: the flawed communications within cyber intelligentsia". In *Cyberspace and International Relations: theory, prospects and challenges*, edited by J. Kremer and B. Müller, 253–67. Heidelberg: Springer.

Demchak, Chris C. 2014. "Foreword". In *Cyberspace and International Relations: theory, prospects and challenges*, edited by J. Kremer and B. Müller, v–x. Heidelberg: Springer.

European Council. 2005. "Convention on the prevention of terrorism". https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/196.

Ferreira, Gonçalo C. 2011. "Redes sociais de informação: uma história e um estudo de caso." *Perspectivas em Ciência da Informação* 16, no. 3: 208–31.

Folha de S. Paulo. 2015. "Estado Islâmico divulga vídeo que mostra a execução de cristãos etíopes". *Folha de S. Paulo* (Abr.). http://www1.folha.uol.com.br/mundo/2015/04/1618601-estado-islamico-divulga-video-que-mostra-a-execucao-de-cristaos-etiopes.shtml.

Ford, Peter. 2020. "Combatting terrorist propaganda". *Journal of Policing, Intelligence and Counter-Terrorism* 15, no. 2: 175–86. DOI: 10.1080/18335330.2020.1780298.

Gagnon, Benoît. 2008. "Cyberwars and cybercrimes". In *Technocrime: technology, crime and social control*, edited by Stéphane Leman-Langlois: 46–65. London: Willan Publishing.

Garcia, Gabriel. 2015. "Estado Islâmico ameaça de morte fundador do Twitter". *Info* (Mar.). https://exame.com/tecnologia/estado-islamico-ameaca-de-morte-fundador-do-twitter.

Gercke, Marco. 2009. *Understanding cybercrime: a guide for developing countries*. Geneva: UN/ITU.

Gonçalves, Joanisval Brito, and Marcus Vinícius Reis. 2017. *Terrorismo: conhecimento e combate*. Niterói: Ímpetus.

Google. 2015. "Google Trends." http://goo.gl/3fh9Wd.

Hoffman, Bruce. 2017. *Inside terrorism*. 3rd ed. New York: Columbia University Press.

Karlsrud, J. 2014. "Peacekeeping 4.0: harnessing the potential of Big Data, social media, and cyber technologies". In *Cyberspace and International Relations: theory, prospects and challenges*, edited by J. Kremer and B. Müller, 141–60. Heidelberg: Springer.

Katz, Rita. 2015. "Follow ISIS on Twitter: a special report on the use of social media by jihadists". *SITE Intelligence Group*. http://news.siteintelgroup.com/

blog/index.php/entry/192-follow-isis-on-twitter-a-special-report-on-the-use-of-social-media-by-jihadists.

Kremer, J., and B. Müller. 2014. "SAM: a framework to understand emerging challenges to states in an interconnected world". In *Cyberspace and International Relations: theory, prospects and challenges*, edited by J. Kremer and B. Müller: 41–58. Heidelberg: Springer.

Kuehl, Daniel T. 2014. "From cyberspace to cyberpower: defining the problem". In *Cyberspace and International Relations: theory, prospects and challenges*, edited by J. Kremer and B. Müller: 24–42. Heidelberg: Springer.

Nicol, Mark. 2015. "We can't find enough whizzkids, says British Army as it struggles to recruit technical experts for secret unit intended to combat ISIS". *Daily Mail* (April). http://www.dailymail.co.uk/news/article-3035191/We-t-whizzkids-says-British-Army-struggles-recruit-technical-experts-secret-unit-intended-combat-ISIS.html.

Raposo, Álisson C. 2007. "Terrorismo e contraterrorismo: desafio do século XXI". *Revista Brasileira de Inteligência* 3, no. 4: 39–55.

Sterne, Jim. 2010. *Social media metrics*. New Jersey: John Wiley & Sons.

Topsy. 2015. "Topsy Sentiment Score". http://topsy.com.

United Nations. 1995. "A/RES/49/60". http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/49/60.

Wendt, Emerson. 2011. "Ciberguerra, inteligência cibernética e segurança virtual: alguns aspectos." *Revista Brasileira de Inteligência* 6: 15–26.

NOTAS

1. When we talk about political meanings social media use by terrorist groups, we are bringing the classic Hoffman (2017)'s terrorism conception.
2. It is also known as the Islamic State of Iraq and the Levante (ISIS) or its Arabic version DAESH.
3. A cyberattack can be defined in many ways. One of the most famous in Brazil is provided by the Republic Presidency: a deliberate and unauthorized attempt to access or manipulate information or make a system inaccessible, non-integral, or unavailable (Brazilian Institutional Security Office 2019).
4. See Barreto (2007, 63–76), Cavelty (2007, 19–20; 2010, 1–3), Gercke (2009, 51), Raposo (2007, 39–55) and Wendt (2011, 15–26).
5. It is also considered that Sterne's reference work on social media is from 2010. Since then, all online sharing and relationship websites and services have incorporated each other's functions. For example, Facebook and Instagram share videos, as well as being used as a microblog.
6. Google Transparency Report can measure some results of this bias change in social media use.
7. Cybersecurity turns to best practices to prevent the security attributes of information — availability, integrity, confidentiality, and authenticity — from being put in check. However, when such a subfield of Computer Science is brought to the analysis of International Relations, its concept ought to be extended to examine issues other than computational — for example, policies — in the same sense that the Copenhagen School proposes the extension of the Security concept.
8. Facebook and YouTube have acted quickly to delete content published by such groups, making it difficult to investigate these two social media accurately.
9. This is one of the limitations of that website: it allows comparative research in a short period; between the day it is researched and exactly 30 days before.
10. The website Topsy allows checking such information only for the last 30 days.
11. The reaction of the international media was the creation of the #BringBackOurGirls campaign on social media, calling the attention of political leaders to the fact that the case had been neglected.
12. Such a score can only be seen and measured in the last thirty days, individually for each of the hashtags, at www.topsy.com. That is why the limitation of this part of the research and why the analysis was restricted to the period from April 6 to May 5, 2015. However, the index proposed by Topsy is quite accurate, especially when comparing the negative scores of the groups analyzed with those of other more "accepted" international

themes, such as certain sports teams, which have, on average, positive scores above 75.

13. #slamicstate, #isis, #daesh, #alshabab, #bokoharam and #alqaeda, the first three are combined into one for the same reasons listed in the note of Chart 3.
14. In the scope of Information Security, social engineering is the ability to access denied information through persuasion; that is, it is presumed that the asset that most exposes Information Security to risks is the human element.

CYBERTERRORISM 2.0 OR TERRORIST USE OF SOCIAL MEDIA:
THE ISLAMIC STATE CASE

ABSTRACT

Cyberspace has become a common source of international security threats, especially after September 11. The emergence and popularisation of so-called social media have enhanced the militancy of the most diverse groups, including terrorist ones. This article problematises international terrorism, pointing out the causes and effects of this 21st-century phenomenon that we name cyberterrorism 2.0. Thus, we focus on the cyberterrorism studies that analyse social media usage's inputs and outputs by terrorist groups. Through Webometrics and the framework Stakeholders, Activities and Motives in the realm of cybersecurity (SAM), we aim to explain, in the light of International Security Studies and through the Islamic State case study, how cyberterrorism 2.0 arises, develops and impacts national security.

Keywords: Cyberterrorism; International Politics; International Security; Social Media.

RESUMO

O ciberespaço tem se tornado uma fonte corriqueira de ameaças para a segurança internacional, sobretudo após o 11 de setembro de 2001. O surgimento e a popularização das chamadas redes sociais *on-line* potencializaram a militância dos mais diversos tipos de grupos, inclusive terroristas. Este texto problematiza o tema do terrorismo internacional, no sentido de apontar quais as causas e efeitos desse fenômeno inerente ao século XXI que aqui nominamos de Terrorismo Cibernético 2.0. Foca-se, assim, na vertente dos estudos sobre Terrorismo Cibernético voltada para a análise dos *inputs* e *outputs* da utilização das redes sociais pelos grupos terroristas. Por meio da webometria e da ferramenta de análise *Stakeholders*, Ações e Motivos na Segurança Cibernética (SAM), objetivamos explicar, à luz dos Estudos de Segurança Internacional e por meio do estudo de caso do Estado Islâmico, como esse fenômeno surge, desenvolve-se e se reflete na segurança internacional.

Palavras-chave: Mídias Sociais; Relações Internacionais; Segurança Internacional; Terrorismo Cibernético.

Recebido em 01/07/2020. Aceito para publicação em 21/04/2021.

Israel e defesa cibernética: estudo da vinculação Estado, setor privado e academia

Israeli cyberdefense: State, private sector and academy sector

Rev. Bras. Est. Def. v. 7, nº 2, jul./dez. 2020, p. 81-101
DOI: 10.26792/RBED.v7n2.2020.75206
ISSN 2358-3932

JÚLIA LOOSE
GRACIELA DE CONTI PAGLIARI

INTRODUÇÃO[1]

O avanço de tecnologias de informação e comunicação (TICs) e a popularização do acesso à Internet criaram processos inseridos em um ambiente complexo nas discussões das Relações Internacionais: o espaço cibernético. Sua complexidade se dá pelo exercício de se pensar em uma dimensão que não existe materialmente, mas que permeia todos os espaços físicos que se compreende por reais. Trata-se de uma dimensão virtual que se sustenta em primeiro lugar pela ação humana, portanto, é primordial pensá-la como um recurso de poder de quem a prioriza.

Em face deste cenário de transformação tecnológica, o presente artigo propõe analisar o tema a partir do seu estudo em um Estado relevante em matéria de defesa cibernética, o Estado de Israel. Sua capacidade tecnológica e a importância da cibernética do ponto de vista militar, bem como as regulamentações condutoras das políticas na área, justificam um estudo mais aprofundado sobre o tema. O objetivo do artigo é apresentar quais são os elementos que compõem a infraestrutura de defesa cibernética do Estado de Israel bem como sua evolução, e para este feito, busca-se analisar os documentos e marcos de referência em matéria cibernética, incluindo o atual documento de defesa nacional divulgado em 2015, *The Israel Defense Forces Strategy*, quanto à interpretação do Estado em relação ao ciberespaço e construção de capacidades tecnológicas militares.

Júlia Loose — Doutoranda do Programa de Pós-Graduação em Relações Internacionais da Universidade Federal de Santa Catarina (UFSC). Mestra em Relações Internacionais pela Universidade Federal de Santa Catarina.
Graciela De Conti Pagliari — Professora Associada da Universidade Federal de Santa Catarina. Doutora em Relações Internacionais pela Universidade de Brasília.

O artigo está dividido em duas partes devido à quantidade de informações do tema. O período temporal adotado para esta análise, 2010 a 2015, justifica-se por duas características: i) surgimento do *worm* Stuxnet (2010) e ii) criação do *National Cyber Boureau* (NCB), que ao serem exploradas demonstram a relevância da implementação da prioridade cibernética por Israel. Inicialmente aborda-se, como uma forma de apresentar o estado da arte no tema, o ciberespaço no seu espectro de novas ameaças, demonstrando os ataques cibernéticos a Israel que permearam o período temporal abordado. Na segunda parte será apresentado o mapeamento da infraestrutura de defesa cibernética do país quanto a seus organismos, e legislações de referência nas três esferas: estatal, privada e acadêmica-científica. Contata-se que Israel atribui prioridade para o setor cibernético em seu plano de defesa multidimensional, a partir do elemento de cooperação tripartite, tendo sua infraestrutura de defesa composta por Estado, setor privado e academia. Prioridade a qual, se condiciona devido à sua específica dinâmica securitária regional representada pela presença efetiva de atividades cibernéticas realizadas majoritariamente por fontes não tradicionais provenientes de grupos militares armados e sociedade civil.

Ademais, salienta-se que se desconhecem publicações em português com o mapeamento aqui realizado, cuja temática se torna relevante para o planejamento de defesa cibernética no Brasil, tanto no âmbito institucional das Forças Armadas, quanto nos âmbitos privado e acadêmico-científico. Tanto Israel quanto Brasil se constituem como duas potências regionais inseridas em sistemas regionais periféricos, dotados de particularidades próprias, e, portanto, capazes de exercer poder regionalmente, inclusive na esfera cibernética. Israel demonstra-se como um exemplo robusto de articulação de cooperação tripartite interagências, o que favorece a inserção do debate acerca do desenvolvimento deste tipo de cooperação, em nível doméstico, já existente no Brasil que pode ser aprimorada.

CIBERESPAÇO: BREVE APRESENTAÇÃO

Ciberespaço no espectro das novas ameaças

A literatura apresenta diferentes definições do ciberespaço não havendo consenso. Para Kuhel (2009, 29), o ciberespaço trata-se de um domínio operacional marcado "pelo uso da eletroeletrônica e do espectro eletromagnético com a finalidade de criação, armazenamento, modificação e/ou troca de informações através de redes interconectadas e interdependentes". O ciberespaço precede o surgimento da Internet, a qual por sua vez, é um elemento que compõe este espaço, sendo um condicionante para os

processos que nele ocorrem — espionagem, hacktivismo, guerra cibernética, entre outros. Observa-se, nesse sentido, que se trata de um domínio já existente dependente do desenvolvimento tecnológico, utilizado tanto nas relações domésticas para comunicação entre pares quanto no âmbito estatal para coleta de informações de inteligência.

Uma das definições é a proposta por Ventre (2011, 34), que critica a ideia de que o ciberespaço é sinônimo de Internet, mas sim argumenta que se trata de um escopo muito mais amplo que envolve diferentes camadas. Em suas palavras: "o ciberespaço é representado em três camadas: camada inferior: infraestrutura (*hardware*); camada intermediária (*software*) e a camada superior cognitiva". A essência da definição de Ventre (2011) é a característica de transversalidade do ciberespaço entre os espaços virtual e real. Todas as dimensões que são compreendidas como convencionais: terra, ar, mar e espaço sideral fazem parte do espaço real e são compostas pela existência de sistemas de telecomunicações, internet, infraestrutura, ordenadores, IPs, etc. Na dimensão virtual encontra-se o ciberespaço — e é quando essas duas dimensões se entrelaçam e interagem que ocorrem os ataques cibernéticos.

Os ataques cibernéticos, portanto, são atos agressivos que partem da dimensão real, e por meio da dimensão virtual alcançam determinado objetivo cujo impacto não se limita apenas ao ciberespaço. Podem ocorrer nas três camadas: hardware, quando direcionado a redes; software quando direcionado a espionagem e na camada humana cognitiva quando o objetivo é transmitir uma mensagem, comunicar ou informar. Já a Guerra cibernética é definida "como a dimensão cibernética de um conflito armado" (Ventre 2011, 37), fator o qual alavancou aos Estados o investimento de infraestrutura e estratégias de ciberdefesa e cibersegurança, o que também ocorreu aos atores não estatais conforme explorado por Barker (2019).

Para Barker (2019, 4) os mesmos conceitos trabalhados na Guerra, como ataque, defesa, privacidade, segurança foram transpostos para o "mundo cibernético". Nesse processo, além do engajamento dos Estados, os grupos não estatais expandiram seu escopo da guerra tradicional para a esfera cibernética, o que gera uma relação de igualdade perante a capacidade dos Estados Nações. Ou seja, o ponto de Barker (2019) é salientar que as atividades cibernéticas podem ser avançadas de forma equiparada tanto por Estados quanto por atores não estatais, tendo os últimos menos riscos do que os Estados, devido sua baixa infraestrutura para ataque (Barker 2019, 4). Embora os atores não-estatais demonstrem baixa capacidade cibernética, esse elemento na configuração da guerra cibernética interessa a este artigo, dado que Israel pertence a um entorno regional com alta presença relativa de atores não estatais, bem como considera o ciberespaço como uma quarta dimensão na estratégia de defesa e proteção, conforme

destacado em sua política declaratória de defesa "[...] Defense in all four dimensions (land, sea, air and cyber)." (IDF 2016, 18).

ISRAEL: ATAQUES E RESPOSTAS CIBERNÉTICAS NO PERÍODO DE 2010 — 2015

Autodeclarado como um Estado judeu, em meio a um "núcleo árabe fragmentado em múltiplos territórios" (Hinnebusch 2003, 3), o investimento de Israel em inovação tecnológica para defesa é uma prioridade. Não obstante, essa prioridade foi impulsionada pelos recorrentes ataques cibernéticos que o Estado enfrentou a partir dos anos 2000, especialmente após a acusação do seu suposto envolvimento — nunca autodeclarado — no *Worm Stuxnet*.

O entorno regional israelense caracteriza-se por uma configuração com correlação de forças estatais e não estatais que investem em medidas de infraestrutura cibernética[2]. Quanto à primeira ameaça de cunho estatal, Israel enfrentou ataques em sua maioria protagonizados pelo Irã, mas também por Turquia, África do Sul, Rússia e China (Cohen, Freilch, and Siboni 2015), como se verá no desenvolvimento dessa seção. Os atores não estatais apresentam duas categorias: os grupos armados e a sociedade civil. Aqueles compreendem como principais, Hezbollah e Hamas, o primeiro com sede no Líbano e o segundo com sede na Palestina. Já a atuação da sociedade civil, inclui-se nesse processo por meio da atuação de hackers ativistas.

A disseminação do Stuxnet (2010) foi um fator importante regionalmente, para o estudo da relevância dos ataques cibernéticos realizados contra Israel posteriormente. O Stuxnet é um sofisticado *worm* de computador criado especificamente para se infiltrar em sistemas de controle industrial. O ataque mais significativo foi o ataque ao sistema desenvolvido pela Siemens, para girar as centrífugas de enriquecimento de urânio do Irã, na usina de Bushehr (Tabansky 2016, 61). O *worm* foi detectado em junho de 2010 pela Microsoft — que também foi atacada em todos os sistemas Windows — e pela companhia Symantec Norton Security (Fildes 2010). Estimou-se que o *W32.Stuxnet*, seu nome técnico, atingiu em um período de 48 horas cerca de 14.000 endereços de IP de instalações de diversos países conforme mostra a Figura 1.

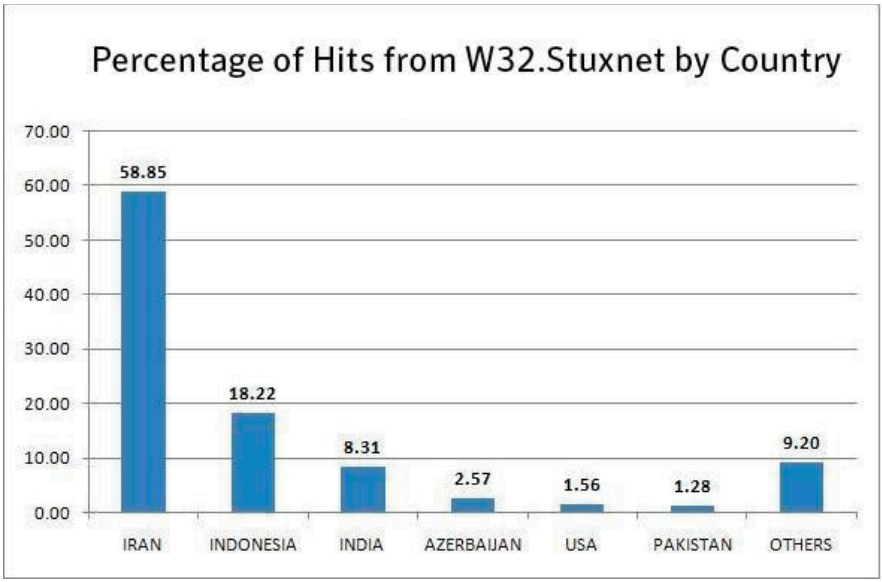


Figura 1 — Porcentagem de ataques do Stuxnet por país
Fonte: Retirado do Relatório "*W32.Stuxnet — Network Information*", elaborado pela Symantec Corporation (2010).

A partir do Stuxnet, compreendeu-se que um ataque realizado no ciberespaço poderia criar danos extremos no espaço físico com dano nuclear, embora esse objetivo não tenha sido concretizado[3]. Conforme aponta Milevski (2011, 65. Tradução nossa), pela primeira vez no "submundo do ciberespaço que um pacote abrangente foi capaz de se espalhar por si mesmo e ser empregado contra uma meta específica para alcançar ou facilitar um objetivo político", em sua duração de 48 horas. O autor destaca a importância que deve ser dada ao caso do Stuxnet, mesmo que não tenha atingido seu fim, dado sua complexidade e possibilidade de sucesso:

> O Stuxnet (*Malware*), no contexto internacional, em última análise, não afetou a vontade política iraniana de obtenção de um programa nuclear soberano. Então como o Stuxnet poderia ser bem sucedido? Esse tipo de ataque teria que ser destrutivo o suficiente, ao impactar as capacidades iranianas de fato ao acabar com o material disponível para seus programas nucleares. Além disso, também deveria ser capaz de superar o aumento da eficiência nuclear iraniana. Esse sucesso poderia ser possível, visto que o Stuxnet tem uma vantagem significativa sobre as operações físicas: ao contrário das pessoas reais, um malware pode estar em múltiplos lugares ao mesmo tempo, centenas de milhares, milhões ou mais. (Mileviksy 2011, 69, Tradução Nossa).[4]

Por ser criado com o objetivo de atingir sistemas industriais de infraestruturas críticas do espaço físico (centrais elétricas, usinas hidrelétricas e unidades industriais nucleares), o Stuxnet foi apontado como o mais sofisticado ataque cibernético já realizado e por esse motivo associa-se sua criação com algum Estado (Fildes 2010). Nunca houve autoria declarada, no entanto o governo iraniano apontou que sua criação teve motivação governamental, acusando Estados Unidos e Israel. Segundo Barker (2019), nos casos em que armas cibernéticas parecem ter sido usadas por atores estatais, dificilmente algum Estado aceitou a responsabilidade de usá-las e o caso do Stuxnet é um exemplo, pois se acusa o envolvimento de Israel e Estados Unidos, mas nunca houve uma declaração por parte de ambos (Barker 2019, 8). Aqui salienta-se a dificuldade da pesquisa em classificar a autoria dos ataques, devido a particular característica de anonimato que o ciberespaço proporciona.

No cenário israelense, nesse mesmo contexto, foi criado em 2011 o NCB, já mencionado, uma agência governamental que atua em parceria tanto com o setor privado, quanto com o setor acadêmico para o desenvolvimento de políticas de cibersegurança e liderança global. O NCB é um órgão fundamental para a pesquisa e mapeamento dos ataques cibernéticos ao país e no fomento do desenvolvimento de tecnologia para combatê-los (Cohen, Freilch, and Siboni 2015, 4).[5]

Conforme apontam Cohen, Freilch e Siboni (2015), estima-se que Israel sofra ataques com origem de grupos estatais e não-estatais, Hezbollah e Hamas, os quais, segundo o governo israelense, são liderados pelo Irã. Em 2011, Israel acusou o Irã de liderar a Operação *newscaster* contra si mesmo e Estados Unidos. A Operação consistiu na criação de falsas identidades virtuais com laços de funcionários do governo e repórteres. O ataque comprometeu mais de dois mil computadores e foi descoberto somente em 2014. Dois anos antes (2012), Israel havia acusado novamente o Irã, Hamas e Hezbollah como responsáveis por uma série de ataques que se sucederam aos sistemas nacionais vitais do país, como água, energia e bancos (Cohen, Freilch, and Siboni 2015, 4).

No período aqui abordado, um dos ataques mais significativos foi a Operação *#OpIsrael*, coordenada pelo grupo *Anonymous* e demais hacktivistas pró-Palestina. A Operação iniciou em 2013 e consistiu em um ataque programado para que fossem retirados do ar todos os sites do governo no dia do *Holocaust Remembrance Day* (27 de janeiro). Foi retirada do ar uma gama de sites governamentais, incluindo sites de bancos e agências financeiras e do Museu Nacional do Holocausto. Durante grande parte do dia, Tel Aviv ficou sem conexão de Internet. Estimou-se que o dano causado foi de três bilhões de dólares de prejuízo para o país. Os sites eram retirados

com a utilização da *hashtag #Opisrael*, que também estava sendo disseminada nas redes sociais como o Twitter (Pitts 2017).

Durante a Operação Margem Protetora (2014), ofensiva contra o Hamas que durou mais de um mês, outro ataque cibernético retirou do ar o site das FDI por diversas vezes. Aqui cabe mencionar o contexto da operação, que gerou uma comoção internacional, dado que acarretou a baixa de palestinos mortos — civis confome caracterização do conflito israelo-palestino — em sua maioria, jovens[6]. Um aspecto curioso desta operação que corrobora o propósito deste artigo foi sua narração direta feita no Twitter, pelo perfil das FDI, que oscilava entre estar disponível ou fora do ar (Cohen, Freilch, and Siboni 2015, 4).

Os eventos acima mencionados representam um contexto regional que além de altamente militarizado, dispõe de ameaças cibernéticas, o qual justifica o investimento em infraestrutura aprimorada. Israel é um exemplo que priorizou em seu projeto de grande estratégia nacional o desenvolvimento de capacidades tanto ofensivas quanto defensivas em matéria cibernética. Essas capacidades resultaram em sua estrutura em defesa cibernética, desenvolvida a partir do investimento em inovação em ciência e tecnologia com a cooperação tripartite entre Estado, setor privado e academia, conforme trabalhado a seguir.

ISRAEL: INFRAESTRUTURA EM DEFESA CIBERNÉTICA

Israel é reconhecido mundialmente pelo seu envolvimento com tecnologias de inovação, fomento à pesquisa cientifica e desenvolvimento de startups. Segundo dados do centro israelense *Central Bureau of Statistics*, em 2014, dentro do escopo de países da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) o Estado de Israel, considerando a porcentagem do PIB nacional, ocupou o segundo lugar de liderança dos gastos em pesquisa e inovação tecnológica, conforme aponta o relatório desenvolvido no NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Estão incluídos nesse processo de desenvolvimento, a instalação de tecnologias avançadas de infraestrutura de comunicação, que incluem cabos fixos e a construção de fibra ótica (CCDCOE, 2017 6).

Conforme aponta Tabanksy (2016), o alto investimento em tecnologia sob iniciativa do Estado, fez com que o país se utilizasse do ciber poder[7] na aplicação do *hard power* e dissuasão da sua política defesa, especialmente frente ao Irã nuclear. No que tange ao investimento de ciber tecnologia para defesa nacional, Tabansky (2016, 51) aponta que a tecnologia cibernética oferece ferramentas novas e acessíveis para o alcance mais rápido de seus interesses no conflito, isso inclui arquitetura de rede e de sistema,

criptografia, amostras de malware, comandos militares e indicadores de defensores cibernéticos. Para que se possa dimensionar o investimento na esfera do Estado, do setor privado e da academia, apresenta-se a seguir um rigoroso levantamento destes investimentos[8].

Estado

Nesta subseção, serão apreciadas três iniciativas do Estado, que cresceram em importância conforme a política de prioridade do tema foi sendo implementada. Essas iniciativas dividem-se em dois grandes momentos: fim da década de 1990, com criação da plataforma *Tehila*, e a partir de 2010 com a criação de dois órgãos: o NCB, já mencionado, e o *National Cyber Secutiry Authority*.

No fim da década de 1990, Israel criou a plataforma eletrônica *Tehila*, *Government Infrastructure for the Internet Age*. A plataforma consistia em uma ferramenta de proteção destinada à garantia de conexões seguras de acesso à Internet dos escritórios governamentais e aos sites do governo. A criação da *Tehila* foi a primeira iniciativa do país para proteção das redes nacionais, que, posteriormente e de maneira mais sofisticada tecnologicamente, tornou-se a National Information Security Authority (NISA), criada para a proteção da infraestrutura nacional em matéria de informação (Cohen, Freilch, and Siboni 2015, 5). Atualmente a *Tehila* evoluiu para a o portal do governo (gov.il) de acesso ao público, que contém uma ampla gama de orientações das políticas promovidas pelo Estado em saúde, emprego, educação, investimento estrangeiro, além do fornecimento de serviços eletrônicos utilizados pela população como o portal de atividade fiscal e o sistema jurídico. O portal do governo é disponível em hebraico, árabe e inglês.

Em 2010, a segurança cibernética se tornou publicamente um objetivo prioritário. O Primeiro Ministro, Benjamin Netanyahu, lançou a Iniciativa Cibernética Nacional sob os cuidados do Ministério da Ciência, no conselho Nacional de Pesquisa e Desenvolvimento. Essa atividade foi uma força tarefa composta por mais de oitenta funcionários das FDI, setor privado e academia. O objetivo era a promoção da liderança israelense na segurança cibernética em nível global e resultou na Resolução 3611 (2011) do Governo intitulada de "Promoção das Capacidades Nacionais do Ciberespaço" (CCDCOE 2017, 8).

A Resolução 3611 foi o prelúdio para a criação do já mencionado NCB: primeiro órgão nacional de consultoria e consolidação para segurança cibernética. Conforme aponta o relatório da CDCOE, a Resolução 3611 indica quatro prioridades de domínio do ciberespaço para Israel. São elas:

(1) o avanço das capacidades nacionais e a melhoria da gestão dos atuais e futuros desafios do ciberespaço.
(2) melhorar a defesa das infraestruturas nacionais essenciais para a manutenção de uma vida estável e produtiva no Estado de Israel.
(3) avançar o status do país como um centro global para o desenvolvimento de tecnologias de informação.
(4) incentivar a cooperação interdisciplinar entre a academia, setor privado e ministérios. (CCDCOE 2017, 8).

Com o avanço do debate sobre o desenvolvimento cibernético no país, em 2015 o NCB estabeleceu um segundo órgão nacional de segurança cibernética, a *National Cyber Secutiry Authority*. Ambos os órgãos são os pilares institucionais da Direção Nacional de Defesa Cibernética (*Ma'arach)* que incluiu outras Resoluções para além da 3611. A atual estrutura governamental em matéria cibernética está sintetizada no organograma a seguir:

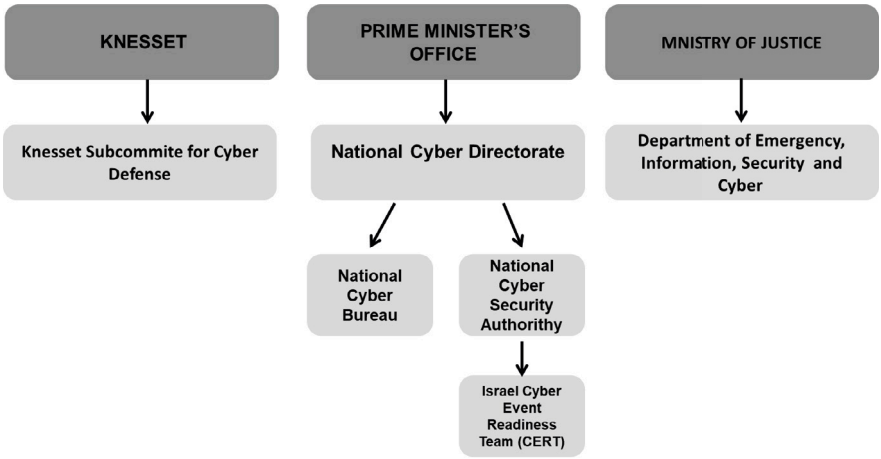


Figura 2: Estrutura de Defesa Cibernética de Israel
Fonte: Elaboração própria baseada em informações coletadas no site do governo israelense e documento da Política Declaratória de Defesa (2016).

Mencionado no relatório, a Mossad, Agência de Inteligência israelense supostamente desenvolve em cooperação com o *National Cyber Directorate*, capacidades cibernéticas defensivas para abordar uma ampla gama de ameaças. No entanto, ressalta-se que as informações não estão disponíveis

por se tratar de uma agência de inteligência da magnitude da Mossad. A seguir apresentaremos as agências em matéria cibernética ainda pertencentes a esfera estatal, no âmbito das FDI.

Forças de Defesa Israelenses

Apresenta-se as FDIs como subtópico à parte, pois as mesmas não se confundem com as demais iniciativas políticas dos governos, exceto pela dinâmica prioritária que é estabelecida para a área cibernética. As FDI, compostas pelo Chefe do Estado Maior Geral, Alto Comando e efetivos do exército, força aérea e marinha (IDF, online), representam uma das estruturas mais importantes do Estado israelense em face de seu entorno conflitivo e das ameaças e relações de desconfiança regionais. As mesmas estão incluídas no *National Cyber Directorad*, ao desenvolver capacidade cibernética na defesa de redes de comunicação, sistemas de armamento e coleta de informações sobre o inimigo que possui tecnologia e capacidade de ataque as suas redes de Defesa (Cohen, Freilch, and Siboni 2015, 6).

Em 2012, as FDI implementaram o *IDF Cyber Defender Training Course*, um amplo programa de treinamento militar para segurança cibernética. O treinamento consiste no recrutamento de militares por meio de exames técnicos em parceira com o Centro de Computação e Informação de Sistemas (*Computing and Information System*) e a Escola de Profissionais de Computação (*School for Computer Professions*) — outras duas agências do escopo das FDI. A partir deste sistema organizacional criaram-se diversas unidades militares especializadas em defesa cibernética. Em sua maioria, as unidades não são divulgadas pelo Estado e não aparecem nos sites oficiais, o que torna um tema difícil de ser explorado. No entanto, as duas unidades divulgadas, embora com defasagem de dados, são a Unidade 8200 e a Unidade C4I.

A Unidade 8200 consiste em uma unidade de inteligência composta por um grupo militar de elite que desenvolve tecnologias de defesa. Em muitos aspectos, conforme apontam Coheh, Freilch e Siboni (2015) a unidade se equipara à Agência de Segurança Nacional dos Estados Unidos (NSA), e, portanto, as informações também são classificadas. Contudo, segundo os relatórios da Oitava Conferência Internacional de Cyber Conflito em Israel (2016), a Unidade 8200 foi responsável pela resposta de Israel à ataques cibernéticos mencionados na seção anterior, tal qual o ataque às facilidades nucleares da Síria, conhecido como a *Operação Orchard* em setembro de 2007 (Tabansky 2016).

Cabe destaque a esta Operação pois se tratou de um exemplo da combinação de elementos militares tradicionais (enfoque para a Força Aérea)

e elementos de ciberataque que paralisaram a Força Aérea Síria. Segundo (Raska 2015, 6. Tradução Nossa): "a operação Orchard é o primeiro exemplo do tipo de capacidades que as nações terão de alavancar no futuro com a utilização do ciberespaço como multiplicador de força". Aqui se tangenciou a capacidade das FDI em atuar no campo de batalha com tecnologia cyber e obter êxito. Além dessa Operação, Israel utilizou suas capacidades tecnológicas em outras ações ofensivas: como na Operação Margem Protetora em Gaza (2014).

O segundo corpo, o C4I consiste na Unidade Tecnológica de elite da FDI. A unidade é responsável por toda a defesa cibernética das FDI, o que inclui a reponsabilidade de todas as formas de comunicação das FDI, onde atuam no fornecimento de tecnologia aos militares que estão em campo para o gerenciamento de situações de risco. Conforme mencionado pelo próprio corpo, seu objetivo é "iniciar, desenvolver, explorar e fortalecer o sistema de integração tecnológica da FDI" (IDF, online).

Dentro do plano multidimensional de defesa, o Documento de Defesa Nacional, *The Israel Defense Forces Strategy*, foi divulgado ao público em 2015. Na própria apresentação da doutrina dá-se proeminência às ameaças cibernéticas que são classificadas em "ciberterrorismo associado a grupos não-estatais e de espionagem" (IDF, 2016, p. 2). Outro ponto relevante é a inclusão do ciberespaço como uma quarta dimensão na estratégia de defesa e proteção junto às demais dimensões "reais". Nas palavras do documento: "(...) Defense in all four dimensions (land, sea, air and cyber)." (IDF 2016, 18). Segundo o documento a interpretação do Estado sobre o ciberespaço se define por:

> O ciberespaço se configura como um domínio de combate adicional. Este domínio deve apresentar ações defensivas, ofensivas e de coleta de informações. A capacidade da FDI neste domínio deve ser baseada nos seguintes termos: a) estabelecimento de um cyber arm, o qual servirá de Comando Principal, subordinado ao Chefe do Estado Maior, destinado a operações no ciberespaço; b) desenvolvimento de capacidades tecnológicas de defesa cibernética para as capacidades operacionais e de apoio (pessoal e logística de sistemas). (IDF 2016, 42, Tradução Nossa). [9]

Nesta afirmação retirada do documento, cabe destaque para o termo *cyber arm* — exército cibernético. No qual conforme aponta Barker (2019), se define por um exército que se utiliza de *cyberweapons* — algo difícil de ser definido dado sua atualidade. Para tanto, considera-se que se a guerra cibernética é a extensão de um conflito armado para o ciberespaço, as armas utilizadas também são particulares, tais quais: *malware*, *botnets* e qualquer outro meio que possibilite ataques cibernéticos. A existência de

cyberweapons pressupõe a existência de um ciberarsenal, responsável pela defesa das infraestruturas críticas cibernéticas do Estado (Barker 2019, 5).[10] Conforme demonstrado no documento (IDF 2016, 37), embora não havendo registros de uma divisão de "cyberarm" Israel publicita seu interesse no desenvolvimento de capacidades cibernéticas, que sinalizariam a criação de um *cyber arm*, a partir das suas FDI, sendo elas: utilização para inteligência, responsabilidade logística, investigação e influência cognitiva nas operações, entre outras.

A partir do compilado do setor público e das especificidades desenvolvidas para as Forças Armadas, a partir das quais demonstra-se a relevância que a cooperação tripartite na dimensão ciber assumiu no Estado israelense, cumpre desenvolver as iniciativas e construções responsivas à ciber dimensão que o setor privado desenvolveu.

Setor privado

O setor privado é um pilar fundamental para a cooperação tripartite. Segundo dados do World Economic Forum, Israel ocupa o segundo lugar no ranking dos dez maiores países inovadores do mundo (World Economic Forum Report 2015-2016). Conhecido como a "nação das startups", esse dado corrobora com a quantidade de empresas startups no país. Segundo relatório da CCDCOE existem aproximadamente 360 empresas de cibersegurança e o número de exportações de produtos desenvolvidos beira seis bilhões de dólares (CCDCOE 2017, 16).

A mais importante iniciativa tripartite, com forte presença do setor privado é o *Israel Inovation Cyber Arena*, o *Cyber Spark*. Uma arena de pesquisa em cyber tecnologia localizada no deserto de Bee-Sheva. Embora com investimento do setor privado, a organização é estatal e compõe a cooperação entre o NCB, indústria cibernética e as Universidades de Negev e Ben-Gurion University, especialmente com a implementação de incubadoras (Cyberspark, *online*).

Outra iniciativa, dirigida por diferentes corporações multinacionais foi o estabelecimento de mais de vinte sedes em Israel. Empresas de tecnologias como PayPal, IBM, General Electric, McAfee fazem parte desse pacote. Além disso, a criação do *Israeli Companies Consortium* (IC3), liderado pela indústria aeroespacial israelense, consiste em um grupo composto somente por empresas de cibersegurança, criado em 2016 com apoio do Ministério da Economia (CCDCOE 2017, 16).

Observa-se que ambas as iniciativas são de caráter dual, mesclando os investimentos do setor público e privado. Diante deste vasto cenário de startups de cibersegurança no setor privado, privilegiou-se nessa seção a

apresentação de duas principais iniciativas desenvolvidas, as quais, a partir dos seus relatórios anuais, demonstram o papel que exercem na incorporação do tema ciber na agenda do governo israelense.[11]

Academia

A ligação de Israel com a educação como elemento aglutinador do Estado é presente desde sua autoproclamação. Já no projeto de unificação do exército de Ben-Gurion[12] a educação foi elemento fundamental para o processo de construção das FDI com o estabelecimento de ensino militar nas escolas (Cohen 2008, 31). A partir das décadas de 1950 e 1960 o apoio e investimento às Universidades foi crescente. Esse histórico de investimento estatal na esfera acadêmico-científica é transpassado para a cooperação tripartite na esfera cibernética, a partir da criação de institutos de pesquisa direcionados e incubadoras tecnológicas.

Israel possui atualmente nove Universidades públicas as quais possuem departamentos de computação. Destacam-se nesta seção, institutos com coordenação do NCB, como no caso da Universidade Hebraica de Jerusalém e o *Technion-Israel Institute of Tecnology*, localizado em Haifa. Em 2012 o Ministério de Ciência e Tecnologia priorizou o financiamento de estudos acadêmicos de segurança cibernética dentro do escopo de coordenação do NCB. A iniciativa resultou em acordos de cooperação entre Estado e Universidades para a criação de centros cibernéticos de excelência. O primeiro deles foi o Centro Interdisciplinar de Pesquisa Cibernética (ICRC), na Universidade de Tel Aviv. O ICRC se organiza em três pilares de pesquisa: era da informação; transformação digital e segurança cibernética, e opera na concessão de bolsas de estudos para pesquisadores locais e estrangeiros (IRCS, online).

Cabe ressaltar como elemento da cooperação tripartite que para além da esfera acadêmica universitária, o Estado criou Programas para o nível escolar de ensino: Programa *Magshimim* e *Nitzanei Magshimin*, que incluem na grade curricular a disciplina de segurança cibernética, além de informática como obrigatórias. Ambos os programas além do financiamento partir do Ministério da Educação, também parte das FDI, que vêm objetivando cada vez mais a busca de militares especializados em T.I para atuação em Inteligência.

CONSIDERAÇÕES FINAIS

Este trabalho se propôs a sinalizar os aspectos possíveis de serem mapeados, em virtude da escassez de fonte sobre o assunto anteriormente

justificada, da infraestrutura de defesa israelense em matéria cibernética. Na primeira parte do texto, destacamos que o ciberespaço se insere no espectro das novas ameaças, portanto, considerou-se que no âmbito da guerra, este espaço se caracteriza como um ambiente de combate propulsor ao conflito, que se intersecciona com os ambientes dados como reais nos termos de Ventre (2011), a lembrar: mar, terra, ar e espaço sideral. O que corrobora com o argumento de Barker (2019), ao afirmar que o avanço das atividades cibernéticas propicia uma nova configuração para o conflito, caracterizada pela presença de *ciberweapons* e *ciberarms*. Essa configuração por sua vez, gera uma relação de igualdade de capacidade dos Estados Nação e atores não estatais.

Ainda neste momento buscou-se apresentar os ataques e respostas cibernéticos a Israel no período de 2010 a 2015, tal qual escolhido a partir do ano de fundação do NCB e da influência conjuntural do *worm* Stuxnet. Constatou-se que o âmbito regional israelense se configura por uma correlação de forças estatais e não estatais que não somente operam no espaço real, mas transferem suas capacidades ao operar no ciberespaço. Dado que o ciberespaço não possui fronteiras de poder delimitadas, essa característica amplia a possibilidade de ameaças. Como a principal delas, sem autoria confirmada, destacou-se a criação do *worm* Stuxnet, o qual conforme as evidências demonstram se constituiu como um ponto originário para o fortalecimento de infraestrutura em defesa cibernética por parte do Estado.

No segundo momento, apresentou-se o mapeamento acerca dessa infraestrutura. Constatou-se na pesquisa que ao contrário do esperado, o desenvolvimento de capacidades em ciência e tecnologia agregadas à defesa cibernética não se restringe somente a esfera das FDl, mas sim, tal processo faz parte de um plano de desenvolvimento ousado encabeçado por Estado, setor privado e academia resultado de uma cooperação tripartite, tendo a Resolução 3611 como marco. A seguir, apresenta-se dois quadros conclusivos do mapeamento dos resultados obtidos desta pesquisa sobre a cooperação tripartite:

Quadro 1
Estrutura Tripartite de Defesa Cibernética de Israel

Setor	Organismo	
ESTATAL	AGÊNCIAS ESTATAIS	National Cyber Directorate National Cyber Bureau National Cyber Security Authorithy
	FORÇAS ARMADAS (Forças de Defesa Israelenses)	Computing and Information System School for Computer Professions Unit 8200 C4I Directorate
PRIVADO	Israel Inovation Cyber Arena Israel Aerospace Industries (IAI) Israeli Companies Consortium (IC3) CyberGym[13]	
ACADÊMICO	Technion-Israel Institute of Tecnology (Haifa) Blavtnink Interdisciplinary Cyber Research Centre (ICRC) Israel Inovation Cyber Arena — Universidade de Nege/ Ben-Gurion University Magshimim e Nitzanei Magshimin Programs	

Fonte: Elaboração própria baseada em informações coletadas no site do governo israelense e sites das organizações privadas aqui trabalhadas.

Quadro 2
Documentos e Legislações de referência de Israel

Documento/ Legislação	Ano
Computers Low	1995
Resolução nº. 3.611	2011
Resolução nº 2.443, "Advancing National Regulation and Governmental	2015
Resolução nº 2.444 "Advancing the National Preparedness for Cyber Defense".	2015
Israel Defense Forces Srategy (IDF)	2015
Resolução nº 3.270	2017
Memorandum: Cyber Defense Law and the National Cyber System	2018[14]

Fonte: Elaboração própria baseada em informações coletadas no site do governo israelense.

O quadro 1 sintetiza o mapeamento realizado neste artigo ao apresentar os organismos responsáveis pela esfera cibernética nos âmbitos estatal, privado e acadêmico. Com exceção das FDI que são responsáveis pelo campo tático-operacional de Defesa e possuem suas informações restritas como de Segurança Nacional, todos os demais organismos exercem trans-

parência quanto ao investimento em cibernética. Na criação de tecnologias de inovação como no caso das empresas privadas listadas; no planejamento organizacional da inserção da cibernética como política de Estado como no caso das agências estatais e nos institutos de pesquisa de ensino superior que recebem investimentos público e privado para realização das pesquisas.

O quadro 2, por sua vez, apresenta as legislações de referência do Estado no tema da cibernética. Observa-se que a partir de 2011 o Knesset aprovou três resoluções que foram incorporadas a criação do NCB com suas subdivisões sequentes, sendo a Resolução 3611 seu marco de criação. Tais legislações são um marco de referência importante para que em 2015, com a divulgação do documento de Defesa Nacional, Israel demonstrasse publicamente, especialmente para seu entorno regional de rivalidade, suas intenções em investimento de cibernética para Defesa.

Neste sentido, por meio dos quadros acima apresentados, coaduna-se a dependência das três esferas para desenvolvimento da cibernética em Israel, o qual aponta-se ser um indicativo de cooperação tripartite. O resultado encontrado nesta análise demonstra, portanto, que é imprescindível, que para verificar a posição de destaque de Israel na esfera cibernética, em nível mundial de análise, seja necessária sua investigação a partir das três esferas de maneira conjunta.

Frente ao exposto, conclui-se que Israel, a partir da consolidada cooperação entre Estado, empresas privadas e Institutos de Pesquisa mencionados, se trata de um exemplo de Estado com alta capacidade de defesa cibernética, tanto para fins ofensivos quanto defensivos. Destaca-se ainda, que todos os organismos mencionados estão em atividade, dado que muitas das fontes coletadas se tratam de dados de 2018 e 2019. Ao que tudo indica, se os ditos "*cyberarms*" são o futuro, Israel lançou sua cartada no passado e a está lançando no presente.

REFERÊNCIAS

Barker, Ken. 2019. "Cyber attack: what goes around comes around". *The School of Public Policy Publications. SPP Briefing Paper* 12, no. 17. Canadian Global Affair Institute Institute. University of Calgary.

Blavatnik Interdisciplinary Cyber Research center, ICRC. *Activity Report: 2014-2016*. https://icrc.tau.ac.il/home.

CCDCOE, NATO. 2017. Couriel-Housen. Deborah. *National Cyber Security Organisation: Israel*. NATO Cooperative Cyber Defence Centre of Excellence. Tallinn.

Cohen, Matthew S., Charles Freilich, and Gabi Siboni. 2015. "Israel and Cyberspace: Unique Threat and Response". *International Studies Perspectives*: 1–15 (December).

Cohen, Stuart A. 2008. *Israel and its Army: from cohesion to confusion*. New York: Routledge.

Fildes. Jonathan. 2010. "Stuxnet *Worm* 'targeted high-value Iraninan Assets'". *BBC News* (Setembro). https://www.bbc.com/news/technology-11388018.

Hinnebusch, Raymond. 2003. *The International Politics of the Middle East*. Manchester; Nova York: Manchester University Press.

Israel Cyber Police Portal. *Cyber Security Policy*. http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Documents/Advancing%20National%20Cyberspace%20Capabilities.pdf.

Israel Defense Forces. IDF. 2016. *C4I and Cyber Defense Directorate*. Disponível em> <https://www.idf.il/en/minisites/c4i-and-cyber-defense-directorate/> Acesso: junho de 2019.

Israel National Cyber Directorate. 2016. *The Government Services and Information Website — Gov.il* . https://www.gov.il/en/Departments/israel_national_cyber_directorate.

Israel. 2016. *The Israel Defense Forces Strategy*. Translation by Susan Rosenberg. Research Assistance by Henry Rome.

Israeli Cyber Innovation Arena. 2019. *Cyberspark*. http://cyberspark.org.il/.

Kuehl, Daniel. 2009. *From Cyberspace to Cyberpower: defining the problem*. In *Cyberpower and National Security*, edited by Franklin Kramer, Starr Stuart, and Larry Wentz: 24–42. Duller: National Defense University Press.

Milevski, Lukas. 2011. *Stuxnet and Strategy: A special operation in cyberspace?* 63 (4th quarter): 64–9.

Pitts, Vanessa. 2017. *Cyber Crimes: History of World's Worst Cyber Attacks*. Alemanha: Alpha Editions.

Raska, Michael. 2015. *Confronting Cybersecurity challenges: Israel's envolving cyber Defence Strategy. Policy Report. S. Rajaratnam School of International Studies*. Nanyang Technological University (NTU). Singapore.

Symantec Cooportation (NASDAQ: SYMC). *W.32. Stuxnet.* https://www.symantec.com/security-center/writeup/2010-071400-3123-99.

Tabansky, Lior. 2016. *Towards a Theory of Cyber Power: The Israeli Experience with Innovation and Strategy.* 8th International Conference on Cyber Conflict. Tallinn: NATO CCDCOE Publications.

Ventre. Daniel. 2011. Ciberguerra. In: *Academia General militar. Seguridad global y potências emergentes em um mundo multipolar.* XIX Curso Internacional de Defensa. Espanha: Universidad Zaragoza.

World Economic Forum Report 2015-2016. *The Most Inovatives Countries in the World*, https://www.weforum.org/agenda/2016/11/the-most-innovative-countries-in-the world/.

NOTAS

1. Este texto foi desenvolvido como parte da pesquisa vinculada ao Pró-Defesa IV: "Ciência, Tecnologia e Inovação em Defesa: cibernética e defesa nacional".
2. Israel enfrenta um cenário de legitimidade contestada no seu entorno desde sua fundação, 1948, até aos dias atuais. Conforme relatório apresentado pelo CSIS (2003), o Médio Oriente é a região mais militarizada do mundo, por possuir: alta porcentagem de gasto em armamento por país, alta porcentagem de exportação de armas de grande porte, proliferação nuclear, guerra assimétrica, guerra proxy, presença de atores não estatais, coalizações externas e regionais e guerra de informação.
3. Cabe destacar a discussão presente na literatura que considera o ataque preliminar ao Stuxnet, ocorrido na Geórgia, em 2008, reconhecido como o primeiro ataque que coincidiu em uma guerra real, no entanto, sem possibilidade de consequências nucleares imediatas.
4. No original: *"The Stuxnet malware, in the context of international sanctions, ultimately has not affected Iranian political will to a sovereign nuclear program or Iranian capabilities sufficiently that their goal cannot be pursued regardless of intent. What would a strategically successful Stuxnet look like? That sort of attack would have to be destructive enough to at least leave a permanent mark on Iranian capabilities by overwhelming the material redundancy available to their nuclear programs. It would also have to be able to overcome increased Iranian nuclear efficiencies. Such success may be possible, since malware such as Stuxnet has one significant advantage over physical special operations: unlike actual people, a program can be in multiple places at once — hundreds of thousands, millions, or more — if necessary"*.
5. Importante ressaltar que os ataques à Israel são realizados, em sua maioria, no mesmo período das Operações Militares lideradas pelas Forças de Defesa Israelense (FDI), no território da Faixa de Gaza. No entanto, esse fato não é uma regra. Conforme apontam Cohen, Freilch e Siboni (2015), algo interessante a ser notado no rastreamento dos ataques contra Israel é que nem sempre há uma motivação direcionada a um período ou acontecimento, mas sim a motivação geral é a desestabilização interna do país para um "cessar fogo" de suas políticas ofensivas.
6. O Objetivo da operação era a destruição do armazenamento de armas e túneis subterrâneos do Hamas utilizados para romper o bloqueio da Faixa de Gaza. Por ser realizada no âmbito urbano, as consequências foram um índice extremo de baixas de palestinos, que não ocorria desde as Intifadas da década de 1980.
7. Poder que se manifesta no espaço cibernético.
8. O mapeamento aqui apresentado foi feito a partir do levantamento minucioso de relatórios das próprias agências estatais israelenses, institutos de pesquisa e empresas privadas. No entanto, ressalta-se que o material di-

vulgado ao público sobre as políticas israelenses em matéria de defesa cibernética é bastante escasso, dado que muitas informações são restritas ao Estado, o que denota o cuidado e a importância que Israel atribui ao tema.

9. No original: *"The cyberspace is an additional combat domain. This domain shall feature defensive, intelligence gathering and offensive actions. IDF force buildup in this domain shall be based on the following: a. Establishing a Cyber Arm, which will serve as a Principal Command, subordinate to the Chief of the General Staff, for operations and force buildup of the IDF's cyberspace capabilities. It will be in charge for planning and implementing the cyber domain campaign.b. Development of technological capabilities for cyber defense for the operational capabilities and for supporting capabilities (personnel, logistical systems)".*
10. A discussão sobre "cyberarsenal" é incipiente. A dificuldade está na categorização e diferenciação entre arma cibernética e arma eletrônica. Para mais informações, ver Barker (2019).
11. Cabe mencionar nesta seção a dificuldade em separar as startups que são direcionadas especificamente para defesa nacional, visto que em todas as fontes trabalhadas menciona-se apenas a esfera de cibersegurança. Um apontamento por parte das autoras infere essa configuração como uma opção estratégica do Estado, inserida no campo tático-operacional de Defesa, o qual possui, portanto, informações restritas como de Segurança Nacional.
12. No projeto de unificação do exército Nacional de Ben-Gurion (1948) as Forças militarizadas judaicas presentes no território desde o Mandato Britânico (Haganah) unificam-se em um exército nacional, as FDI.
13. Nessa rede de startups se incluem cerca de 360 companhias especializadas em cibersegurança. Para mais informações consultar: https://www.startupnationcentral.org/.
14. Em progresso, sujeito à aprovação do Parlamento.

ISRAEL E DEFESA CIBERNÉTICA: ESTUDO DA VINCULAÇÃO ESTADO, SETOR PRIVADO E ACADEMIA

RESUMO

O contínuo avanço das tecnologias de informação e comunicação intensificou o desenvolvimento de um espaço complexo, o ciberespaço, o qual se tornou objeto referente de securitização, proveniente da vinculação entre Estado, corporações privadas e sociedade civil. Em face deste cenário, os Estados passam a compreender a esfera cibernética como uma ameaça contemporânea existencial, necessitando o desenvolvimento de medidas de infraestrutura de defesa, como no caso de Israel. Busca-se neste artigo analisar quais são as medidas tomadas pelo Estado israelense em termos de infraestrutura de defesa cibernética. A metodologia empregada será de técnica de pesquisa de revisão bibliográfica, a partir de fontes primárias, que compreendem uma inicial análise do documento de defesa nacional (publicado ineditamente em 2015) e demais marcos de referência, bem como fontes secundárias. Como conclusões preliminares, infere-se que Israel atribui prioridade para o setor cibernético em seu plano de defesa multidimensional, tendo uma infraestrutura de defesa formulada a partir da cooperação tripartite entre Estado, setor privado e academia, condicionada devido à sua específica dinâmica regional securitária de legitimidade contestada com presença efetiva de ameaças cibernéticas de fontes não tradicionais e tradicionais.

Palavras chave: Israel; Defesa Cibernética; Política de Defesa.

ABSTRACT

The rise of ICTs (information and communication technology) has intensified the development of cyberspace research in International Politics in the last years. Cyberspace became an object of securitization, that includes State, private corporations, and civil society. In this way, States began to recognize the cyber sphere as a contemporary threat, which demanded the development of a qualified defense infrastructure by them. This research seeks to understand the measures taken by Israel in its cyber defense infrastructure. The following methodology applied includes bibliographic reviews (primary and secondary sources which includes the preliminary analysis of the national defense document published for the first time in 2015). In the end of the article, we apply as some conclusions, that Israel allocates priority to the cyber sector, by having a defense infrastructure formulated from tripartite cooperation between the State, the private sector and the academic sector, as a part of its multidimensional defense plan. We assume that this situation is related to the regional security context of Israel in Middle East, defined by a contested legitimacy and the existence of cyber threats from non-traditional and traditional actors.

Keywords: Israel; Cyber Defense; Defense Policy.

Recebido em 30/06/2020. Aceito para publicação em 20/04/2021.

Guerra cibernética, ameaças às infraestruturas críticas e a defesa cibernética do Brasil

Cyber war, threats to critical infrastructure and Brazil's cyber defense

Rev. Bras. Est. Def. v. 7, nº 2, jul./dez. 2020, p. 103-131
DOI: 10.26792/RBED.v7n2.2020.75178
ISSN 2358-3932

DANIELLE JACON AYRES PINTO
JÉSSICA MARIA GRASSI

INTRODUÇÃO

Nos conflitos contemporâneos os meios não-tradicionais de ataque têm evoluído constantemente, isso se deve a busca constante pelo distanciamento do soldado do *front* de batalha e da automação cada vez mais acentuada da guerra. Nessa perspectiva, o espaço cibernético vem nos últimos anos tornando-se cenário central da dinâmica securitária dos Estados tanto interna como externamente. Infraestruturas críticas, tanto as ligadas ao setor privado quanto as do setor público, passaram a ser alvo principal de uma nova maneira de violência, que apesar de não ser direta, causa danos efetivamente sérios a sociedade e aos Estados. A partir da relevância dessa temática nos dias atuais, um questionamento central que surge e motiva o desenvolvimento deste artigo é: de que forma esses novos moldes e dinâmicas ligadas aos recursos cibernéticos poderiam ser compreendidos diante de um potencial cenário de ciberguerra?

Para analisar tal questão, este estudo corrobora a maioria dos debates acadêmicos nessa seara que afirmam que uma verdadeira ciberguerra ainda não existiu. Apesar do uso do ciberespaço em conflitos, dos crescentes ataques cibernéticos e das preocupações futuras quanto ao seu desenvolvi-

1 **Danielle Jacon Ayres Pinto** — Coordenadora da Pós-Graduação em Relações Internacionais da Universidade Federal de Santa Catarina – UFSC. Pós-Doutora em Ciências Militares na Escola de Comando e Estado-Maior do Exército – ECEME, Doutora em Ciência Política, na linha de Política Internacional, pela UNICAMP. Vice-Presidente da ABED - gestão 2020-2022. Líder do Grupo de Pesquisa em Estudos Estratégicos e Política Internacional Contemporânea - GEPPIC.
2 **Jéssica Maria Grassi** — Doutoranda em Relações Internacionais na Universidade Federal de Santa Catarina – UFSC e Bolsista da CAPES. Mestra em Integração Contemporânea da América Latina pela Universidade Federal da Integração Latino-Americana – UNILA. Pesquisadora do Grupo de Pesquisa em Estudos Estratégicos e Política Internacional Contemporânea – GEPPIC.

mento, a materialização da guerra movida por esse recurso de poder digital ainda é uma nebulosa na realidade da política internacional.

No entanto, os atores estatais já pensam em estratégias específicas para lidar com esse fenômeno tanto numa dinâmica defensiva e resiliente, como ofensiva. Entre os fatores que poderiam permitir uma retaliação imediata e legítima a um ciberataque, levando a uma guerra cibernética, elenca-se a possibilidade concreta e precisa de identificação do ator agressor, a regulamentação dos comportamentos no ciberespaço dando ao Estados a capacidade de demarcar seus limites soberanos e a delimitação das ações legais e sanções possíveis ao transgressor para que possam assim responder com atos repressivos aos atores que venham lhe atacar intencionalmente e ferir sua soberania no espaço cibernético. Já na ordem defensiva e resiliente a proposta é aumentar a segurança efetiva de seus aparatos tecnológicos das infraestruturas críticas e planejar maneiras rápidas e eficazes de colocar a funcionar novamente as infraestruturas estratégicas atacadas de forma a não gerar pânico na sociedade e debilidades prolongadas no serviço afetado.

Frente a esse cenário, com a emergência dessas novas dinâmicas, ao observarmos o Brasil vemos que ele é um dos países que mais sofre ataques cibernéticos no mundo — e o que mais sofre ataques cibernéticos na América Latina. Essa realidade demonstra a importância de se investigar como o país vem inserindo a temática na sua política de defesa e como lida com as possibilidades estabelecidas nesse novo espaço de atuação e com as vulnerabilidades crescentes diante do aperfeiçoamento tecnológico, principalmente no sentido de estabelecer meios eficazes de segurança de suas infraestruturas críticas. Desse modo, este estudo pensa ser importante entender como o Brasil vem construindo sua ação na esfera da defesa cibernética e da segurança de suas infraestruturas críticas para entender suas pretensões estratégicas em relação a uma possível ciberguerra.

Portanto, o objetivo da pesquisa é discutir sobre os novos moldes de atuação estabelecidos diante de ações ofensivas e defensivas no ciberespaço de modo a compreender algumas dinâmicas envolvidas diante das potencialidades de cenários de ciberguerra. A partir disso, serão investigadas as ações que têm sido tomadas pelo Brasil no âmbito de seus documentos sobre defesa nacional para enfrentar essa nova ameaça.

Para isso, o artigo será articulado em três seções, que delimitam os objetivos específicos desta pesquisa. Em um primeiro momento serão discutidos aspectos introdutórios ao tema e delimitados os conceitos principais do âmbito da cibernética nas relações internacionais. Após, concentrar-se-á em analisar acerca da guerra cibernética, discutindo conceituações, o que poderia levar um ataque cibernético tornar-se uma ciberguerra e dificuldades de regulação de comportamentos no nível cibernético. Por fim, pre-

tende-se explorar como o Brasil vem trabalhando com as problemáticas levantadas pelo ciberespaço, com especial atenção no que diz respeito às suas infraestruturas críticas, analisando, para isso, seus principais documentos de segurança e defesa.

Utiliza-se aqui a técnica de pesquisa bibliográfica, consultando fontes secundárias como livros, artigos, teses e dissertações sobre o tema proposto, e fontes primárias, ao analisar documentos de segurança e defesa do Brasil. Além disso, caracteriza-se como uma pesquisa exploratória e qualitativa.

O CIBERESPAÇO NO CONTEXTO DOS CONFLITOS CONTEMPORÂNEOS

A transformação contemporânea nas formas de se fazer as guerras envolve o distanciamento do embate direto em campo de batalha, utilizando-se, para isso, meios não tradicionais. É dentro deste contexto que surge o debate acerca da revolução dos assuntos militares (RAM), sendo o domínio do espaço cibernético compreendido como primordial nessa nova forma de conflito (Olson 2012; Teixeira Júnior, Vilar-Lopes, and Freitas 2017).

Nessa perspectiva, Olson (2012, 73) assevera que a guerra hodiernamente inclui ataques contra infraestruturas nacionais, como as econômicas, e recursos cibernéticos são considerados armas estratégicas para tais fins. Desse modo, enfatiza-se aqui o papel do ciberespaço nos conflitos contemporâneos. O ciberespaço, ou espaço cibernético, é definido pelo Pentágono como "o domínio global dentro do ambiente de informações que consiste na rede interdependente de infraestruturas de tecnologia da informação, incluindo a Internet, redes de telecomunicações, sistemas de computadores e processadores e controladores incorporados."[1] (Singer and Friedman 2014, 13, tradução nossa).

De modo simplificado, o espaço cibernético é a "rede global de infraestruturas de tecnologias de informação interligadas entre si, especialmente as redes de telecomunicações e os sistemas de processamento dos computadores." (Fernandes 2012b, 12). Da mesma maneira, Singer e Friedman (2014, 13, tradução nossa) definem o ciberespaço como "o domínio das redes de computadores (e dos usuários por trás delas) em que as informações são armazenadas, compartilhadas e comunicadas on-line"[2]. Os autores ainda acrescentam:

> O ciberespaço é, antes de tudo, um ambiente de informação. É composto de dados digitalizados que são criados, armazenados e, mais importante, compartilhados. Isso significa que não é apenas um lugar físico e, portanto, desafia a medição em qualquer tipo de dimensão física. Mas o ciberespaço não é puramente virtual. Ele com-

> preende os computadores que armazenam dados, além dos sistemas e infraestrutura que permitem que ele flua. Isso inclui a Internet de computadores em rede, intranets fechadas, tecnologias de celular, cabos de fibra ótica e comunicações baseadas em espaço. (Singer and Friedman 2014, 13–4, tradução nossa).[3]

No imaginário da sociedade há uma ideia de que ciberespaço e internet sejam a mesma coisa, todavia, essa ideia é errônea e quando se pensa em ciberguerra é muito importante entender essa diferença. Assim, como afirmam Lobato e Kenkel (2015, 25) "o ciberespaço e a internet não são sinônimos: o primeiro é um domínio operacional eletrônico / eletromagnético, o segundo é a rede central do domínio operacional baseada em computadores." O primeiro existe sem o segundo, mas o segundo só existe porque o primeiro existe. Assim, o ciberespaço e a sua possibilidade como cenário e recurso de guerra é algo muito mais alargado, já a internet é uma ferramenta que pode ser utilizada para um conflito, mas que ainda não teve sua efetiva dimensionalidade bélica determinada, ou mesmo, efetivamente consensualizada entre o meio acadêmico e militar.

Outro ponto relevante a se destacar é a errônea interpretação do ciberespaço como um "patrimônio global" uma vez que, da mesma forma que se divide as fronteiras físicas dos países, o ciberespaço também deve ser compreendido a partir da aplicação das noções de nacionalidade, soberania e propriedade (Singer and Friedman 2014).

Destaca-se que no mundo virtual algumas características são distintivas e trazem dificuldades no que diz respeito à segurança e à defesa, entre estas, apontam-se que os atores podem atuar anonimamente, o que dificulta o rastreamento dos ataques, a distância física não existe, as ameaças podem avançar rapidamente e ser, até mesmo, invisíveis, bem como uma ação ofensiva é relativamente mais barata, fazendo com que aquele que promova o ataque fique em uma posição mais favorecida do que o que precisa se defender (Araújo Jorge 2012; Lobato and Kenkel 2015).

Abaixo, no quadro 1, pode-se ver a síntese dos principais conceitos utilizados quando se trata do ciberespaço nas relações internacionais.

Quadro 1
Principais conceitos relacionados à cibernética
nas relações internacionais

Termo	Autor	Definição
Cibernética	Ministério da Defesa (2015, 62)	"Termo que se refere à comunicação e controle, atualmente relacionado ao uso de computadores, sistemas computacionais, redes de computadores e de comunicações e sua interação. No campo da Defesa Nacional, inclui os recursos de tecnologia da informação e comunicações de cunho estratégico, tais como aqueles que compõem o Sistema Militar de Comando e Controle (SISMC2), os sistemas de armas e vigilância, e os sistemas administrativos que possam afetar as atividades operacionais."
***Cyberspace* / Ciberespaço / Espaço cibernético**	Fernandes (2012b, 12)	"[...] rede global de infraestruturas de tecnologias de informação interligadas entre si, especialmente as redes de telecomunicações e os sistemas de processamento dos computadores."
	Singer e Friedman (2014, 13)	"[...] o domínio das redes de computadores (e dos usuários por trás delas) em que as informações são armazenadas, compartilhadas e comunicadas on-line. [...] não é apenas um lugar físico [...] não é puramente virtual."
	Ministério da Defesa (2015, 106)	"Espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas."

(Continua)

(Continuação)

Termo	Autor	Definição
***Cyberpower* / Ciberpoder / Poder cibernético**	Nye Jr. (2011, 123)	"[...] um conjunto de recursos relacionados a criação, controle e comunicação da informação eletrônica e computacional — infraestrutura, redes, software e habilidades humanas. Isso inclui não apenas a Internet de computadores em rede, mas também Intranets, tecnologias móveis e comunicações espaciais."[4]
	Ministério da Defesa (2015, 211)	"Capacidade de utilizar o Espaço Cibernético para criar vantagens e eventos de influência neste e nos outros domínios operacionais e em instrumentos de poder".
Software Power	Vilar-Lopes (2016, 98)	"[...] a capacidade político-estratégica de que dispõem Estados para intervir na política internacional ou externa de outro Estado via utilização de software."
***Cyberdefense* / Ciberdefesa / Defesa cibernética**	Oliveira *et al.* (2017, 13).	"[...] ato de defender o sistema crítico das TICs [Tecnologias de Informação e Comunicação] de um Estado", além de englobar "as estruturas e questões cibernéticas que podem afetar a sobrevivência de um país."
	Ministério da Defesa (2015, 85)	"Conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente."

(Continua)

(Continuação)

Termo	Autor	Definição
***Cybersecurity* / Cibersegurança / Segurança cibernética**	Oliveira *et al.* (2017, 14).	"[...] aborda questões políticas, gestão de riscos, melhores práticas de garantia e tecnologias usadas para proteger o ambiente cibernético de um país e suas organizações. De forma mais direta, a segurança cibernética trata de temas relacionados à segurança pública."
	Ministério da Defesa (2015, 249)	"Arte de assegurar a existência e a continuidade da sociedade da informação de uma nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas."
***Ciberthreats* / Ciberameaça / Ameaça cibernética**	Ministério da Defesa (2015, 27)	"Causa potencial de um incidente indesejado, que pode resultar em dano ao Espaço Cibernético de interesse."
***Cyber-attack* / Ciberataque / Ataque cibernético**	Gandhi *et al.* (2011, 29)	"[...] qualquer ato de um *insider* ou *outsider* que compromete as expectativas de segurança de um indivíduo, organização ou nação."[5]
	Lobato e Kenkel (2015, 27)	"[...] uma ação humana que explora as vulnerabilidades da esfera virtual, conseguindo prejudicar os sistemas informacionais ou mesmo, à luz da dependência on-line da vida moderna, da vida diária material."[6]
	Ministério da Defesa (2015, 39)	"Ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais em dispositivos e redes computacionais e de comunicações do oponente."
***Cyberhacktivism ou Cybervandalism* / Ciber-hacktivismo ou Cibervandalismo**	Cavelty (2010, 01)	"[...] envolve modificação virtual ou destruição de conteúdo, por exemplo, invadir websites ou desativar um servidor por sobrecarga de dados. [...] os efeitos de tais incidentes são limitados no tempo e relativamente inofensivos."[7]
***Cyberterrorism* / Ciberterrorismo / Terrorismo cibernético**	Curran, Concannon e McKeever (2008, 01)	"[...] é um ataque premeditado e politicamente motivado contra informações, sistemas de computadores, programas de computador e dados que resultam em violência contra alvos não combatentes por parte de grupos subnacionais ou agentes clandestinos."[8]

(Continua)

(Continuação)

Termo	Autor	Definição
Resiliência cibernética	Ministério da Defesa (2015, 241)	"Capacidade de manter as infraestruturas críticas de tecnologia da informação e comunicações operando sob condições de ataque cibernético ou de restabelecê-las após uma ação adversa."
***Cyberwar* / Ciberguerra / Guerra cibernética**	Ministério da Defesa (2015, 134)	"Corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C² [comando e controle] do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC2) do oponente e defender os próprios STIC2. Abrange, essencialmente, as Ações Cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação à TIC."

Fonte: quadro elaborado pelas autoras

No Quadro 1 é possível perceber a complexa lista de conceitos que permeiam a dimensão cibernética na área da defesa e como tais definições são elementos essenciais para compreender as estratégias dos Estados quando pensam essa nova seara como um meio para a existência da guerra. Assim, tomando como ponto de partida os diferentes conceitos apresentados, este estudo irá concentrar-se mais enfaticamente acerca da percepção de guerra cibernética, também denominada de ciberguerra, e sua aplicação nas relações internacionais.

Não há ainda um consenso entre os pesquisadores para a definição e caracterização de uma ciberguerra, existindo assim, diferentes definições com graus de abrangência e delimitações distintas para o termo. O termo tem sido frequentemente usado para descrever várias ações cibernéticas, indo desde uma campanha de cibervandalismo, ciberterrorismo e ataques cibernéticos no geral (Singer and Friedman 2014).

Mas compreender de forma mais efetiva possível esse termo, mais do que uma necessidade conceitual para erigir meios de proteção e controle no sistema internacional, é o caminho para entender com os atores internacionais o estão utilizando e perceber se o estão manipulando para que ele atenda aos seus interesses individuais.

Nesse sentido, a seção seguinte terá como objetivo discutir mais profundamente acerca do conceito e da utilização do termo guerra cibernética, assim como compreender as condições para que um ataque cibernético escale para a condição de guerra cibernética. Além disso, serão apresentadas algumas das dificuldades que imperam na regulação das ações e comportamentos internacionais no nível cibernético.

CIBERGUERRA: ATAQUES CIBERNÉTICOS E AS AMEAÇAS ÀS INFRAESTRUTURAS CRÍTICAS

O termo ciberguerra, ou guerra cibernética, vem sendo utilizado para uma série de acontecimentos, inclusive sobrepondo-se aos termos já definidos na seção anterior, frequentemente usado para designar qualquer tipo de conflito no ciberespaço. Isso leva a uma abrangência de significados, divergências quanto a sua ocorrência e consequências e dificuldades ao lidar com as situações advindas do ciberespaço.

Frente a esse cenário, Cavelty (2010, 1, tradução nossa) aponta ser necessário uma categorização conceitual mais precisa, sendo esta "uma pré-condição indispensável para avaliar o perigo concreto e sua importância, alocar responsabilidades, implementar contramedidas preventivas e reativas e conduzir investigações criminais".[9]

Ressalta-se que, pela definição de Clausewitz (2010), a guerra segue alguns princípios: é um ato violento; tem um propósito fundamentalmente político; tem um meio sério e um fim sério; e não é apenas um ato isolado. Partindo dessa perspectiva, Rid (2013) afirma que não há ainda uma ofensa cibernética que atenda a todos esses três critérios.

> Até agora não há nenhum ato conhecido de "guerra" cibernética, quando a guerra é adequadamente definida. Isto, obviamente, não significa que não haja ofensas cibernéticas políticas. Mas todas as ofensas cibernéticas políticas conhecidas, criminosas ou não, não são crime comum nem guerra comum. Seu objetivo é subverter, espionar ou sabotar[10] (Rid 2013, 10, tradução nossa).

Deve-se levar em consideração que as novas formas de se fazer a guerra podem estar fugindo, em certa medida, dos termos postos por Clausewitz. Contudo, Singer e Friedman (2014) frisam que, independentemente do es-

paço — terra, mar, ar, ou ciberespaço —, a guerra tem essencialmente um objetivo e um modo político, o que a distingue do crime, e o elemento da violência está sempre presente.

Nye (2012, s. p.) distingue ciberataque como "uma ampla variedade de ações, que vão de simples tentativas para apagar dados até danos a websites, negação de serviço, espionagem e destruição". Enquanto a ciberguerra é designada pelo autor, de maneira ampla, como "uma ação hostil no ciberespaço cujos efeitos ampliam ou são equivalentes a uma enorme violência física."

Já Teixeira Júnior, Vilar-Lopes e Freitas (2017, 31), retratam a guerra cibernética, de maneira mais aberta, "como um estado de coisas em que o poder militar utiliza meios, estratégias e ferramentas no ciberespaço para alcançar seus objetivos". Os autores acrescentam que a guerra cibernética se caracteriza pela atuação beligerante no ambiente cibernético, buscando obter informações privilegiadas, desestabilizar ou destruir sistemas computadorizados do país alvo (Teixeira Júnior, Vilar-Lopes, and Freitas 2017).

A guerra cibernética estratégica é compreendida por Libicki (2009, 117, tradução nossa) como "uma campanha de ataques cibernéticos lançada por uma entidade contra um estado e sua sociedade, principalmente, mas não exclusivamente, com o objetivo de afetar o comportamento do estado-alvo"[11]. A ciberguerra também pode ser definida como "uma ação ou conjunto associado de ações com uso de computadores ou rede de computadores para levar a cabo uma guerra no ciberespaço, retirar de operação serviços de internet e/ou de uso normal da população (energia, água, etc.) ou propagar códigos maliciosos pela rede" (Wendt 2011, 16, 21) e, para além de ataques às infraestruturas críticas, também visa afetar a soberania da nação atacada.

Já Dipert (2010, 398, tradução nossa) pontua que "se os ataques entre entidades políticas forem suficientemente 'generalizados', poderemos então falar de uma guerra cibernética"[12]. Levando essas conceitualizações em consideração, é importante ressaltar que nem todo ataque cibernético tem origem militar ou faz parte de uma guerra cibernética (Cavelty 2010).

Nessa perspectiva, Cavelty (2010) distingue níveis de ataques cibernéticos, o que ele chama de *cyberladder* (escada cibernética), sendo que quanto mais acima da escada estiver maior será seu dano potencial (Figura 1).

No primeiro degrau da escada de Cavelty (2010, 1, tradução nossa) está o cibervandalismo, ou ciber-hacktivismo. Este se caracteriza pela ação de modificar ou destruir conteúdos, invadindo sites ou desativando servidores, por exemplo. No segundo degrau está o crime de internet e, no terceiro, a ciberespionagem, os quais já ocorrem de forma rotineira, indepen-

dentemente de conflitos, tendo como vítima principal o setor corporativo, embora as redes governamentais também sejam alvos dessas atividades (Cavelty 2010).

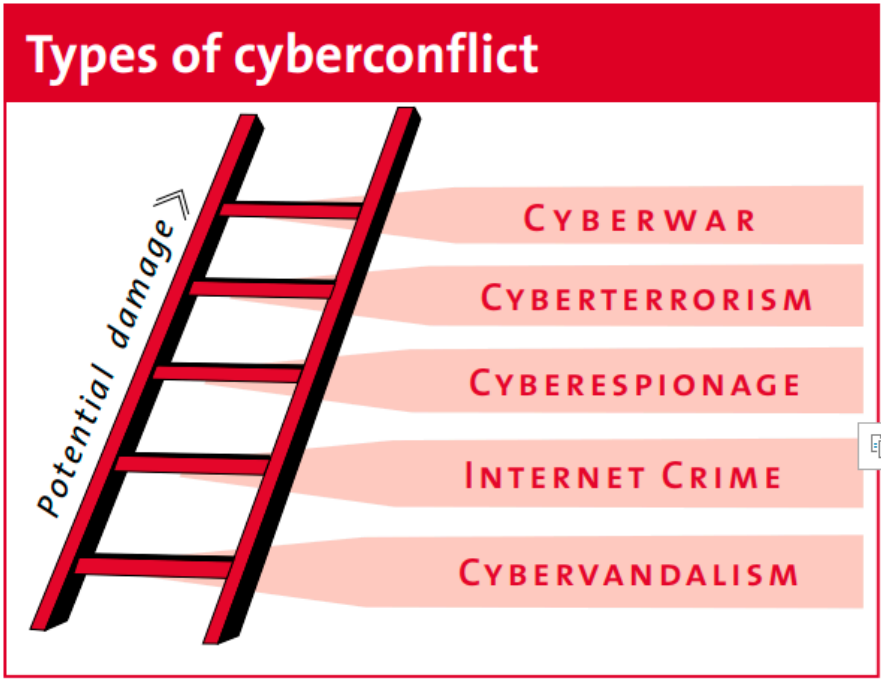


Figura 1 — Tipos de conflitos — escada cibernética *(Cyberladder)*.
Fonte: Cavelty (2010).

No quarto degrau está o ciberterrorismo que pode ser compreendido como "ataques ilegais de atores não estatais contra computadores, redes e as informações armazenadas nele, realizadas com o intuito de intimidar um governo (ou população) ou para obrigar determinado comportamento" (Cavelty 2010, 1, tradução nossa). Por fim, no último degrau da escada cibernética está a guerra cibernética. O termo, conforme Cavelty (2010, 2, tradução nossa), refere-se a uma guerra que ocorre no espaço virtual, envolvendo principalmente meios de tecnologia da informação, apesar de ponderar também que "cenários para uma guerra cibernética estratégica, ou seja, um conflito conduzido exclusivamente no mundo virtual, permanecem irrealistas neste momento".

Nas definições apresentadas podemos perceber um importante determinante da ideia de ciberguerra que é a falta de relação direta com o conceito tradicional de guerra, principalmente com o conceito clausewitziano. Essa não ligação nos faz constatar que a utilização do termo ciberguerra é feita com pouco cuidado conceitual e atende muito mais a interesses específicos dos atores do sistema, do que efetivamente a um complexo de características que definem uma guerra. Assim, a ciberguerra parece ser algo novo e que ainda está em construção, sendo possível até argumentar que tal fenômeno não existiu ainda, mas nem por isso deve-se desconsiderar as ameaças reais que os recursos cibernéticos produzem hodiernamente.

Apesar disso, deve-se considerar que um objetivo primordial na guerra cibernética deve ser possibilitar que as informações obtidas pelo meio cibernético possam trazer as possibilidades de ultrapassar esse domínio. Assim, para Silva (2014), nos domínios físicos e cognitivo da guerra pretende-se atacar as infraestruturas críticas de um país levando a paralisação ou a destruição de seus sistemas. A partir disso, o autor ressalta que, estrategicamente, a guerra cibernética teria como propósito atacar sistemas relacionados às infraestruturas nacionais de energia, ao sistema financeiro e à infraestrutura social, dificultando aos Estados manter sua capacidade de defesa e reação (Silva 2014).

Por outro lado, taticamente, teria como alvo os sistemas de comunicação, de controle e os de apoio à decisão, o que diminuiria a capacidade operacional e logística das Forças Armadas do país. Já operacionalmente, a ciberguerra teria como objetivo os sistemas de controle e a comunicação operacional, uma vez que, afetando ou destruindo estes, levaria ao comprometimento da capacidade de coordenação e manobra de um grupo das Forças Armadas. (Silva 2014).

Portanto, as guerras cibernéticas poderiam comprometer ou destruir infraestruturas críticas dos países, ameaçando os sistemas de segurança e colocando em risco a soberania, além de se caracterizar por avançar também em alvos civis. Todavia, é possível entender que mais do que um fim em si mesma a guerra cibernética poderia ser mais uma etapa da guerra tradicional, ou talvez mais um recurso de poder ao invés de um sistema de conflitualidade específico. Essa dinâmica é que, ainda hoje, provoca divergências sobre a existência ou não da possibilidade de uma ciberguerra.

Sobre as Infraestruturas Críticas Nacionais, o Artigo 2º da Portaria nº 2, de 8 de fevereiro de 2008, do Gabinete de Segurança Institucional da Presidência da República do Brasil, define Infraestruturas Críticas (IEC) como "as instalações, serviços e bens que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança nacional". Na referida portaria, em seu Artigo

3º, expõe-se que são consideradas áreas prioritárias de IEC: "I - Energia; II - Transporte; III - Água; IV - Telecomunicações; e V — Finanças." (Gabinete De Segurança Institucional 2008, s. p.).

Portanto, os alvos preferenciais dos ataques em uma ciberguerra seriam os programas de computador que controlam ou gerem os setores econômico-empresarial e/ou de serviços públicos (Fernandes 2012a), ou seja, as infraestruturas críticas, sendo estas:

> i) comando das redes de distribuição de energia elétrica; ii) comando das redes de distribuição de água potável; iii) comando das redes de gestão dos caminhos de ferro; iv) comando das redes de gestão do tráfego aéreo; v) comando das redes de informação de emergência; vi) comando das redes bancárias, possibilitando a inabilitação das contas, ou seja, apagando o dinheiro registado em nome dos cidadãos; vii) comando das redes de comunicações em geral e em particular (incluindo as redes de estações de rádio e de televisão); viii) comando dos links com sistemas de satélites artificiais (incluindo fornecedores de sistemas telefônicos, de sinais para tv, de previsões de tempo e de sistemas gps); ix) comando da rede do Ministério da Defesa (incluindo também outros ministérios-chave, como o do Interior e da Justiça, e o próprio Banco Central); x) comando dos sistemas de ordenamento e recuperação de dados nos sistemas judiciais, incluindo os de justiça eleitoral. (Fernandes 2012a, 58).

O *malware Stuxnet* é considerado um marco no que diz respeito ao nível alcançado pelos ataques cibernético, já que foi o primeiro que teve como alvo uma infraestrutura crítica de um Estado, no caso as instalações nucleares do Irã, também afetando outros países como Indonésia, Índia, Estados Unidos, Austrália, Inglaterra, Malásia e Paquistão. Dessa forma, este mudou a noção de vulnerabilidades no ciberespaço (Demchak and Dombrowski 2011; Silva 2014; Wendt 2011).

A utilização dessas ferramentas como armas cibernéticas para uso em infraestruturas críticas dos países, ou de modo a ameaçar a soberania dos Estados é uma preocupação no que diz respeito à evolução para uma guerra cibernética. O *Stuxnet* demonstrou que "armas cibernéticas" estão sendo desenvolvidas também para alvos civis, objetivando efeitos estratégicos (Olson 2012, 73). Porém, ainda não é possível entender o ataque feito com esse *malware* com uma guerra cibernética em si, talvez um ato de guerra, mas não como um novo modelo virtual e tecnológico da guerra. Ainda assim, não há informações suficientes para atestar que ataques cibernéticos tenham resultado em danos de grandes proporções contra infraestruturas estratégicas ou centros de comando e controle (Teixeira Júnior, Vilar-Lopes, and Freitas 2017). A partir do abordado, é importante compreen-

der as possibilidades e as dificuldades que ainda imperam na regulação de comportamentos no nível cibernético e nas sanções a serem aplicadas aos transgressores, pontos relevantes para se discutir acerca da evolução de ataques cibernéticos para uma ciberguerra.

Uma questão a ser discutida trata da legislação internacional no que diz respeito ao ciberespaço e a legalidade de atos repressivos. Diante das regras, normativas e regimes para a atuação internacional e para a qualificação da guerra há dificuldades para abranger a lógica da cibernética. Apesar de iniciativas individuais por parte dos Estados e institucionalmente, como no caso da OTAN, para tratar da problemática (Demchak and Dombrowski 2011; Lobato and Kenkel 2015), não existem resoluções ou acordos internacionais que regulamentem como lidar com as novas dinâmicas envolvidas no ciberespaço (Dipert 2010). Tal lacuna muitas vezes parece ser proposital, visto que essa nova seara de atuação bélica é bastante complexa e quanto mais aberta sua regulação for, mais os estados poderão utilizar-se desse meio para atingir seus objetivos no espaço interacional sem sofrer tal pressão em relação aos seus atos, e o *Stuxnet* é um bom exemplo dessa suposta liberdade.

Nesse sentido, a indefinição do conceito de guerra cibernética e a falta de bases legais para uma adequada atuação internacional na área também trazem dificuldades em termos de segurança jurídica, para os decisores políticos agirem adequadamente em caso de ciberataques ou em uma ciberguerra (Fernandes 2012a).

Para ilustrar a problemática da falta de uma legislação que regule o âmbito da guerra cibernética, Fernandes (2012a, 54) aponta alguns questionamentos, entre eles, como "saber se um determinado ciberataque poderá ser considerado um ato de guerra?", ou "se os seus protagonistas poderão, ou deverão, ser tratados de forma similar aos combatentes ou se as ciberarmas poderão ser legalmente equiparadas a armas físicas?". Portanto, é fundamental haver certas disposições em tratados internacionais que os Estados possam seguir, o estabelecimento de parâmetros de atuação no ciberespaço, definindo quais ações configuram ataques a soberania estatal e, assim, sustentar suas ações diante de um ato de ciberguerra (Fernandes 2012a). Sem tais regulações o uso indiscriminado e deturpado desse recurso tende a crescer a favorecer os Estados mais tecnológicos e desenvolvidos.

Contudo, uma questão essencial diz respeito à necessidade da identificação precisa do agressor, para poder fazer inferências seguras e, assim, efetuar a represália ao ator transgressor. No entanto, diante da estrutura do ciberespaço, é muito difícil identificar as fontes dos ataques cibernéticos. Isso é chamado de "problema de atribuição" e leva a negação de credibilidade aos ciberataques, especialmente porque os países podem alegar que,

apesar de originados em seus territórios, os ataques não foram perpetrados por seus governos (Dipert 2010, 385).

Ao abordar o tema, Olson (2012) avalia o fato de que grupos independentes podem ser controlados por uma grande potência, dificultando a atribuição de responsabilidade diante de ataques cibernéticos. Nesse sentido, o autor, alertando os Estados Unidos para esse cenário, propõe:

> O valor da utilização de "fantoches" na guerra cibernética é que eles complicam ainda mais a possibilidade de atribuir responsabilidade. Uma potência pode identificar e mapear vulnerabilidades e, em seguida, coordenar ataques usando intermediários. Mapeamentos passados de vulnerabilidades de rede e infraestrutura não foram tratados como um ato de guerra. Assim, contanto que a potência hostil utilize "fantoches", haverá poucas medidas diretas que os EUA poderão tomar, ainda que se conheça a fonte de informações que possibilita os ataques. (Olson 2012, 77).

Logo, o que no começo poderia ser um problema para o Estado — a dificuldade em identificar os perpetradores dos ataques — passa, após uma percepção estratégica de interesses, a ser talvez uma benesse para conquistar o que se deseja no sistema internacional sem ser punido por eventuais ilegalidades cometidas ao longo desse ato.

Outro ponto importante relacionado a questão da ciberguerra diz respeito à soberania dos países no ciberespaço. Como definir o espaço soberano de cada país de modo que este possa agir diante de um ataque cibernético justificando este ameaçar sua soberania? Diante das incertezas postas no espaço cibernético, as ameaças invisíveis, a facilidade do anonimato e a falta de regulação tem se justificado a necessidade de impor limites soberanos no mundo virtual (Demchak and Dombrowski 2011).

O estabelecimento de fronteiras cibernéticas possibilitaria aos Estados desenvolverem capacidades de controle soberano desse território de modo a melhorarem suas capacidades de cibersegurança e ciberdefesa. Desta forma, criaria condições dos Estados identificarem e, se fosse o caso, retaliarem agressores externos (Demchak and Dombrowski 2011). A interconectividade dos sistemas e a ausência de regulamentação no ciberespaço facilitam ataques que possam promover rupturas políticas e militares, principalmente devido ao potencial desse cenário de controlar objetos físicos e a dificuldade de rastreamento do agressor (Lobato and Kenkel 2015).

No entanto, essas questões de limites, controles e fronteiras geram uma série de críticas sobre as implicações destas como ferramentas de controle dos fluxos internos dos países e as possibilidades de uso autoritário por parte dos governos, estabelecendo limites mais rígidos na esfera ciberné-

tica, podendo levar a violações dos direitos e da liberdade dos cidadãos e demais agentes internos, ou mesmo modificar a noção do que é compreendido como um direito. Ademais, geram receios sobre as possibilidades de intervenção em territórios apontados como fontes de ataques cibernéticos, além das críticas acerca da utilização de uma lógica Westfaliana para tratar de questões de uma complexidade que talvez demandassem análises e soluções diferentes do que se está acostumado no sistema internacional atual (Ayres Pinto, Freitas, and Pagliari 2018).

Entretanto, segundo Demchak e Dombrowski (2011), há um consenso sobre a necessidade de regulamentação do ciberespaço, seja pelos Estados individualmente, seja por meio de regimes internacionais. Essas iniciativas estão tomando forma nas estratégicas norte-americana e chinesa e nas ações institucionais observadas, por exemplo, nas iniciativas no âmbito da OTAN (Demchak and Dombrowski 2011; Lobato and Kenkel 2015).

Tendo em vista todas as questões levantadas nesta seção, com as preocupações crescentes com relação a ataques às infraestruturas críticas e as possibilidades do desencadear de uma ciberguerra, Olson (2012) propõe que as vulnerabilidades persistentes e as ameaças de um ataque contínuo e coordenado levam a impossibilidade de defender completamente uma rede vasta - como as redes de abastecimentos de petróleo, as quais dependem de sistemas computacionais - contra um inimigo invisível. Desse modo, alerta que "o potencial prejuízo econômico de uma campanha cibernética coordenada por uma grande potência contra gargalos nos sistemas mundiais (ou nacionais) seria incalculável" (Olson 2012, 80). Mas a pergunta é: isso seria guerra? A reposta pode ser: diretamente não, mas poderia ser parte de um contexto maior de conflitualidade que chegaria ao tradicional enfretamento bélico.

Ainda hoje existe a preocupação de que um "filho do *Stuxnet*" possa estar sendo desenvolvido para atingir alguma infraestrutura crítica, ou estar flutuando por algum tempo, aparentemente inofensivo e despercebido até ser desencadeado em uma data específica ou em um tipo programa. Esse *malware* poderia parar milhões de computadores ao mesmo tempo, enviar comandos de destruição a outros, substituir dados, afetar redes de energia, água, transportes ou sistemas financeiros (Demchak and Dombrowski 2011), mas nada de real e concreto ainda foi vivenciado

Por fim, devido ao potencial destrutivo de uma possível guerra cibernética nos campos econômico, social e físico, Olson (2012) alerta para a necessidade de lhe conferir o grau de importância e preocupação, assim como incentivar estudos na área, do mesmo modo que é dado às armas nucleares. Porém, para isso, é essencial que novas conceituações de guerra,

baseadas na sociabilidade efetiva do século XXI trazida especialmente pela globalização, sejam elementos centrais desses novos conceitos.

Assim, tendo em vista a imprecisão do conceito de guerra cibernética, o aumento dos ataques no âmbito cibernético, as possibilidades de ataques escalarem para uma guerra cibernética, o potencial destrutivo de armas cibernéticas, bem como o aumento da dependência dos recursos de tecnologia da informação pelos Estados e pelas empresas, tem-se, por consequência, um aumento das vulnerabilidades dos Estados frente as ameaças cibernéticas.

Para entender essa dinâmica conceitual no contexto nacional, o tópico seguinte investigará brevemente como o Brasil vem inserindo e trabalhando com a temática do setor cibernético em suas políticas e estratégias de defesa.

PREOCUPAÇÃO COM AS NOVAS AMEAÇAS: A DEFESA CIBERNÉTICA DO BRASIL E A SEGURANÇA DAS INFRAESTRUTURAS CRÍTICAS

Como mencionado, os avanços tecnológicos, os novos meios e ameaças nos conflitos contemporâneos, fazem com que o ciberespaço se torne elemento essencial ao se pensar a política de defesa dos Estados. No contexto da América Latina, o Brasil é o país que mais sofreu ataques cibernéticos nos últimos anos e, por outro lado, é o terceiro país que mais faz ataques cibernéticos no mundo (Oliveira *et al.* 2017). Os ataques sofridos demonstram "tanto a fragilidade brasileira em defesa cibernética como sua força, pois em uma guerra a possibilidade de neutralizar o oponente é primordial" (Oliveira *et al.* 2017, 67).

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. Partindo disso, essa seção enfatizará as medidas que estão sendo adotadas pelo país, trabalhando principalmente com seus documentos de defesa e como esses entendem a ideia de ciberguerra.

O Livro Branco de Defesa do Brasil (LBDB) salienta que "a ameaça cibernética se tornou uma 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" (Ministério da Defesa 2012b, 69).

Assim, o país inseriu o setor cibernético no tripé estratégico para a defesa nacional, juntamente com o aeroespacial e o nuclear, e, a partir disso, estaria estimulando o desenvolvimento de pesquisas e novas tecnologias, assim como a capacitação de recursos humanos, de modo a elevar seus mecanismos de defesa nacional e buscar a maximização da segurança de

infraestruturas e informações. Nesse sentido, para o projeto de defesa cibernética, o LBDB prevê a destinação de valor estimado de R$ 839,90 milhões até 2031 (Ministério da Defesa 2012b).

> A implantação do Setor Cibernético tem como propósito conferir: confidencialidade, disponibilidade, integridade e autenticidade dos dados que trafegam em suas redes, os quais são processados e armazenados. Esse projeto representa um esforço de longo prazo, que influenciará positivamente as áreas de ciência e tecnologia e operacional. Sob a coordenação do Exército, significativos avanços têm se concretizado na capacitação de pessoal especializado e no desenvolvimento de soluções de elevado nível tecnológico. (Ministério da Defesa 2012b, 69).

Desse modo, no que diz respeito ao setor cibernético, a Estratégia Nacional de Defesa (END) dispõe da necessidade de capacitação no amplo espectro de usos industriais, educativos e militares, incluindo como prioritária as tecnologias de comunicação entre todos os contingentes das Forças Armadas. Nesse sentido, aponta a necessidade de desenvolver o aparato tecnológico do país assim como a formação de recursos humanos, frisando sobre a importância de se estabelecer uma política de formação de cientistas para atuar na área cibernética - do mesmo modo na espacial e na nuclear - com a aproximação entre a produção científica e as atividades relativas ao desenvolvimento tecnológico da Base Industrial de Defesa (Ministério da Defesa 2012a).

Ressalta-se entre prioridades apontadas na END: fomentar a pesquisa científica e estruturar a produção de conhecimento na área, além de incrementar medidas de apoio tecnológico por meio de laboratórios específicos; desenvolver sistemas computacionais de alto desempenho e tecnologias que permitam o planejamento e a execução da Defesa Cibernética; fortalecer o Centro de Defesa Cibernética, para que possa evoluir para o Comando de Defesa Cibernética das Forças Armadas; aprimorar a Segurança da Informação e Comunicações (SIC), principalmente no que diz respeito à Infraestrutura de Chaves-Públicas da Defesa (ICP-Defesa); e desenvolver a capacitação para a proteção das infraestruturas estratégicas. Ademais, prevê a criação da Escola Nacional de Defesa Cibernética (Ministério da Defesa 2012a).

Dessa maneira, para contribuir com a Segurança Nacional no que se refere ao setor cibernético, a END prevê o desenvolvimento de medidas para a segurança das infraestruturas estratégicas (energia, transporte, água, finanças e comunicações), assim como o aperfeiçoamento dos dispositivos e procedimentos de segurança que possam reduzir a vulnerabilidade dos sistemas de Defesa Nacional. Também é previsto a intensificação de par-

cerias estratégicas com o entorno geográfico de modo a contribuir com a estabilidade regional (Ministério da Defesa 2012a).

Salientando sobre a proteção das infraestruturas estratégicas nacionais, o documento incentiva as seguintes ações para o desenvolvimento de soluções nacionais inovadoras:

> [...] sistema integrado de proteção de ambientes computacionais; simulador de defesa cibernética; ferramentas de conteúdo web; ferramentas de inteligência artificial; algoritmos criptográficos e autenticação próprios; sistema de chaves-públicas da Defesa; sistema de análise de artefatos maliciosos; ferramentas de análise de interesse para o setor cibernético (voz, vídeo, idioma e protocolos); sistema de certificação de Tecnologias da Informação; sistema de apoio à tomada de decisão; sistema de restabelecimento do negócio; sistemas de gestão de riscos; sistema de consciência situacional; computação de alto desempenho; rádio definido por software; e pesquisa científica por meio da Escola Nacional de Defesa Cibernética, de instituições acadêmicas no âmbito do Ministério da Defesa e demais instituições de ensino superior nacionais e internacionais. (Ministério da Defesa 2012a, 39).

Todavia, a END traz também em seu corpo, quando trabalha a ideia de flexibilidade, a compreensão que os meios digitais não irão substituir os meios tradicionais da guerra. Vejamos o texto: "[A END] [...] rejeita a tentação de ver na alta tecnologia, alternativa ao combate, assumindo-a como um reforço da capacidade operacional" (Ministério da Defesa 2012a, 75). Ou seja, apesar de reconhecer a importância de tais tecnologias, a coloca como um patamar abaixo dos meios tradicionais.

A Política de Defesa Cibernética (PDC), aprovada no final de 2012, visa coordenar e integrar as ações de defesa cibernética no âmbito do Ministério da Defesa nas áreas de inteligência, ciência e tecnologia, operacional, doutrina e recursos humanos. Assim, esta dispõe da criação do Sistema Militar de Defesa Cibernética (SMDC), na qual participam civis e militares da Marinha, do Exército e da Aeronáutica (Ministério da Defesa 2012c).

Já a Doutrina Militar de Defesa Cibernética (DMDC) aborda aspectos mais técnicos e operacionais de modo a coordenar as ações militares no âmbito da defesa cibernética (Oliveira *et al.* 2017). No que se refere à guerra cibernética, a DMDC define alguns processos gerais de coordenação, planejamento e conduções de operações de ciberguerra (Ministério da Defesa 2014).

No âmbito da segurança cibernética, ressalta-se a elaboração do Livro Verde de Segurança Cibernética (LVSC), o qual objetiva reunir propostas e

diretrizes básicas sobre a temática (Oliveira *et al.* 2017). Este livro destaca os desafios presentes no âmbito da segurança das infraestruturas críticas nacionais:

> Falta de clareza e de identificação das interdependências nas infraestruturas críticas e entre infraestruturas críticas, e seus respectivos graus de criticidade e impactos; Ausência de integração das várias políticas setoriais, iniciativas e investimentos de segurança das infraestruturas críticas; Movimentos tardios de definição de prioridades estratégicas da Nação e harmonização das estratégias, com foco na prevenção; Limitado leque das infraestruturas críticas nacionais já priorizadas; Crescentes riscos de ataques cibernéticos a Sistemas SCADA; Insuficiente número de equipes de resposta e tratamento de incidentes em rede computacionais nos vários segmentos da sociedade, bem como insuficiente número de especialistas com competência para desempenhar tais atividades. (Mandarino Júnior and Canongia 2010, 40–1).

Além disso, o LVSC aponta as diretrizes a serem contempladas na Política Nacional de Segurança Cibernética no que se refere às infraestruturas críticas nacionais. Entre as diretrizes, pode-se mencionar a iniciativa para a formulação da Política Nacional de Segurança das Infraestruturas Críticas e o mapeamento do grau de vulnerabilidade dos sistemas de informação e das infraestruturas críticas do país, de modo a definir os requisitos de segurança e desenvolver um sistema de monitoramento de ameaças cibernéticas (Mandarino Júnior and Canongia 2010).

Também abrange, entre suas diretrizes, a elaboração de uma metodologia para avaliações de risco, identificando o grau de interdependência dos serviços das infraestruturas críticas do país, de modo a desenvolver ou adaptar uma metodologia comum para avaliar as vulnerabilidades das infraestruturas críticas, dos seus sistemas e serviços e, assim, criar um sistema dinâmico que contemple medidas preventivas, proativas e reativas contra as ameaças e ataques cibernéticos. Por fim, prevê o desenvolvimento de um programa de capacitação dos gestores atuantes nas infraestruturas críticas, o qual contemplaria tópicos como "análise e gestão de riscos, segurança das infraestruturas críticas da informação, resiliência operacional e organizacional, monitoramento e resposta a ataques cibernéticos." (Mandarino Júnior and Canongia 2010, 47).

Em suma, apesar da necessidade de maior aporte financeiro para investimentos em pessoal, material e pesquisa, sendo que as vulnerabilidades ainda são marcantes no setor, devem-se destacar os avanços obtidos nos últimos anos (Lobato and Kenkel 2015; Silva 2014). Nesse sentido, obser-

va-se, antes de tudo, a prioridade dada ao setor cibernético considerado um dos três setores estratégicos nos documentos de defesa do país.

A partir disso avanços foram observados, como a implantação do Simulador Nacional de Operações Cibernéticas (Simoc), voltado ao treinamento de militares em combate cibernético, que oferece também simulações para a academia, buscando despertar o interesse de profissionais para a pesquisa e capacitação na área. Outro avanço foi a criação do Centro de Defesa Cibernética (CDCiber), em 2010, dentro do Exército, que atualmente compreende uma das estruturas do Comando de Defesa Cibernética das Forças Armadas (ComDCiber), que coordena o SMDC (Lobato and Kenkel 2015; Silva 2014).

Ademais, foi criada a Escola Nacional de Defesa Cibernética (ENaDCiber), inaugurada em fevereiro de 2019, a qual já funcionava como núcleo desde janeiro de 2015. 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" (Ministério da Defesa 2019, s. p.).

Por fim, quando olhamos para os documentos brasileiros que versam sobre sua defesa, em especial dos que tratam da área cibernética, é possível perceber que há um valioso esforço em construir elementos sólidos para o desenvolvimento das atividades das forças armadas nessa seara. Porém, os documentos não trazem efetivamente um entendimento específico e direto sobre guerra cibernética, dando ao Estado brasileiro maior flexibilidade de ação quando entenda necessário no mundo virtual.

CONSIDERAÇÕES FINAIS

Este artigo pretendeu discutir alguns aspectos referentes aos ataques cibernético e à ciberguerra, bem como compreender as ações que estão sendo tomadas pelo Brasil nesse setor. Assim, distinguiu-se alguns dos principais conceitos discutidos ao abordar a cibernética nas relações internacionais, explorou-se fatores que poderiam levar um ataque cibernético desencadear uma ciberguerra e as dificuldades enfrentadas na regulamentação de ações e comportamentos no âmbito cibernético, bem como identificou-se os avanços obtidos pelo Brasil diante das novas ameaças e ataques advindos do ciberespaço.

Nesse sentido, ao debruçar-se em discutir as conceitualizações de guerra cibernética, buscou-se deixar claro como essa deve ser compreendida e diferenciada dos demais ataques cibernéticos. A partir disso, alguns pontos

devem ser observados. Uma guerra cibernética pode vir a ocorrer com a constatação de ataques cibernéticos coordenados, efetuados com propósitos políticos e militares, que venham a afetar as infraestruturas críticas, a população ou os organismos de defesa de uma nação, ou que visem atacar diretamente a soberania de um Estado. Esses ataques, para serem considerados atos de guerra cibernética, deveriam equivaler a um ato de violência contra o Estado atacado.

A ciberguerra deve ser compreendida no contexto da revolução dos assuntos militares, e especula-se como a guerra do futuro. Uma ameaça que se tornou uma das grandes preocupações das defesas nacionais devido as vulnerabilidades inerentes de todas as infraestruturas que dependem dos sistemas computacionais. Além disso, salienta-se a consideração do potencial de se efetuar ataques imprevisíveis, anônimos, até mesmo, invisíveis e, talvez, destrutíveis às infraestruturas críticas dos Estados por meio do ciberespaço, principalmente se usado como arma combinada, destacando-se a facilidade em coordenar ataques a longa distâncias com o domínio do poder cibernético.

Outro ponto discutido diz respeito a falta de regulamentação internacional quanto às ações, comportamentos e a legalidade de atos repressivos no ciberespaço. Essas dificuldades se estabelecem pelo fato de não haver previsão jurídica e normativa nos regimes e instituições internacionais acerca das ações no ciberespaço. Nesse sentido, alguns Estados têm buscado encontrar soluções individualmente com tentativas de estabelecer limites soberanos ou fronteiras no espaço cibernético de modo a facilitar a identificação de agressores e garantir a punibilidade das ações que julgam transgredir sua soberania.

A dificuldade de rastreamento do agressor, a questão da atribuição de responsabilidade, a dificuldade em delimitar espaços soberanos e a falta de regulamentação internacional são considerados importantes entraves para sanções ou represálias em casos de ataques cibernéticos. No entanto, vários questionamentos se acercam e novas críticas surgem - como os mencionados na segunda seção do artigo - a partir das possibilidades apresentadas. Além disso, observa-se a falta de alternativas novas que fujam da lógica utilizada para a resolução dos problemas tradicionais nas relações internacionais. Isso tudo dificulta tanto a tomada de ações adequadas diante de ataques ou diante da possibilidade de uma guerra cibernética quanto em termos de segurança jurídica.

Um conflito do nível apontado para uma ciberguerra ainda não ocorreu, apesar de poder tornar-se uma realidade diante do constante e rápido aperfeiçoamento tecnológico, que levam a interconexão dos sistemas, e do alcance exponencial do poder cibernético entre os atores, estatais e não-es-

tatais, sendo que os Estados estão cada vez mais investindo tanto em meios defensivos como ofensivos no âmbito ciberespaço.

Assim, ao se explorar a atuação brasileira na área, salientam-se as vulnerabilidades presentes e a necessidade de maior atenção e aporte financeiro de modo a desenvolver pesquisas e ferramentas avançadas para a área. O treinamento e a capacitação de profissionais, as pesquisas na área e o desenvolvimento de programas e mecanismos que visem melhorar as capacidades de defesa e segurança cibernética do Brasil devem ser constantemente aperfeiçoados. Ademais, torna-se importante, diante da acelerada digitalização dos dados da população e do Estado, repensar estratégias de proteção destes, tanto no nível governamental quanto no que diz respeito ao setor privado.

Aponta-se, contudo, que desde que o setor cibernético foi considerado prioritário para a defesa do país, este vem se destacando e recebendo consideráveis recursos financeiros, principalmente no contexto das Forças Armadas, bem como tem-se buscado, até certo ponto, incentivar as pesquisas e a capacitação de pessoal no âmbito militar e no meio acadêmico. Do mesmo modo, os documentos de segurança e defesa enfatizam a preocupação acerca das infraestruturas críticas, buscando identificar os principais desafios, potencialidades e meios para a redução das vulnerabilidades nos sistemas de segurança e defesa. Desde então, alguns projetos tomaram forma como o SMDC, o Simoc, o CDCiber e o ComDCiber e a ENaDCiber, os quais devem ser estudados mais profundamente em trabalhos futuros.

REFERÊNCIAS

Araújo Jorge, Bernardo Wahl G. de. 2012. "Das guerras cibernéticas". *XI Ciclo de Estudos Estratégicos da Escola de Comando e Estado-Maior do Exército (ECEME)*: 1–26 (Maio). Rio de Janeiro.

Ayres Pinto, Danielle Jacon, Riva Sobrado Freitas, and Graciela de Conti Pagliari. 2018. "Fronteiras virtuais: um debate sobre segurança e soberania do estado". In *Fronteiras contemporâneas comparadas: desenvolvimento, segurança e cidadania*, edited by Danielle Jacon Ayres Pinto, Maria Raquel Freire, and Daniel Chaves: 40–53. Macapá: Editora da UNIFAP.

Cavelty, Myriam Dunn. 2010. "Cyberwar: concept, status quo, and limitations". *Center for Security Studies (CSS)* 71: 1–3 (Abril).

Charap, Samuel. 2015. "The ghost of hybrid war". *Survival* 57, no. 6: 51–8.

Clausewitz, Carl Von. 2010. *Da guerra*. São Paulo: Ed. Martins Fontes.

Curran, Kevin, Kevin Concannon, and Sean Mckeever. 2008. "Cyber terrorism attacks". In *Cyber warfare and cyber terrorism*, edited by Lech J.Janczewski, and Andrew M. Colarik. New York: Information Science Reference: 1–6.

Demchak, Chris, and Peter Dombrowski. 2011. "Rise of cybered westephalian wge". *Strategic Studies Quarterly 5*, no. 1: 32–61.

Dipert, Randall. 2010. "The ethics of cyberwarfare". *Journal of Military Ethics* 9, no. 4: 384–410.

Fernandes, Hugo Miguel Moutinho. 2016. "As novas guerras: o desafio da guerra híbrida". *Revista de Ciências Militares* 4, no. 2 (Nov.): 13–40. Lisboa.

Fernandes, José Pedro Teixeira. 2012a. "A ciberguerra como nova dimensão dos conflitos do século XXI". *Relações Internacionais*: 53–69 (Março).

_____. 2012b. "Utopia, Liberdade e Soberania no Ciberespaço". *Revista Nação e Defesa* 133: 11–31. Portugal: Instituto de Defesa Nacional.

Gabinete de Segurança Institucional. 2008. *Portaria GSIPR Nº 2, de 8 de Fevereiro de 2008*. Institui Grupos Técnicos de Segurança de Infraestruturas Críticas (GTSIC) e dá outras providências. https://contadores.cnt.br/legislacoes/portaria-gsipr-no-2-de-8-de-fevereiro-de-2008.html.

Gandhi, Robin, Anup Sharma, William Mahoney, William Sousan, Qiuming Zhu, and Phillip Laplante. 2011. "Dimensions of cyber-attacks: social, political, economic and cultural**".** *IEEE Technology and Society Magazine*: 28–38 (Spring).

Hoffman, Frank G. 2007. *Conflict in the 21st century: the rise of hybrid wars*. Virginia: Potomac Institute for Policy Studies Arlington.

Libicki, Martin. 2009. *Cyberdeterrence and cyberwar*. Pittsburgh: RAND Corporation.

Lobato, Luísa Cruz, and Kai Michel Kenkel. 2015. "Discourses of cyberspace securitization in Brazil and in the United States". *Revista Brasileira de Política Internacional* 58, no. 2: 23–43. http://dx.doi.org/10.1590/0034-7329201500202.

Mandarino Júnior, Raphael, and Claudia Canongia (Org.). 2010. *Livro Verde: Segurança Cibernética do Brasil*. Departamento de Segurança da Informação e Comunicações. Brasília: GSIPR/SE/DSIC.

Ministério da Defesa. 2012a. *Estratégia Nacional de Defesa - END*. Brasília. https://www.defesa.gov.br/arquivos/2012/mes07/end.pdf.

_____. 2012b. *Livro Branco de Defesa Nacional*. Brasília. https://www.defesa.gov.br/arquivos/2012/mes07/end.pdf.

_____. 2012c. *Política de Defesa Cibernética — PDC*. Brasília. https://www.defesa.gov.br/arquivos/File/legislacao/emcfa/publicacoes/md31_p_02_politica_cibernetica_de_defesa.pdf.

_____. 2014. *Doutrina Militar de Defesa Cibernética — DMDC*. Brasília. https://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_2014.pdf.

_____. 2015. *Glossário das Forças Armadas*. 5. ed. Brasília. http://bdex.eb.mil.br/jspui/bitstream/123456789/141/1/MD35_G01.pdf.

_____. 2019. *Escola Nacional de Defesa Cibernética é inaugurada em Brasília*. Notícia. Brasília, 11 de fevereiro de 2019. https://www.defesa.gov.br/noticias/52690-escola-nacional-de-defesa-cibernetica-e-inaugurada-em-brasilia.

Nye, Joseph. 2012. "Guerra e paz no ciberespaço". *O Estado de S. Paulo* (Abril). Internacional. http://www.estadao.com.br/noticias/impresso,guerra-e-paz--no--ciberespaco-,861242,0.htm.

Nye Jr., Joseph S. 2011. *The future of power*. New York: Public Affairs.

Oliveira, Marcos Aurelio Guedes, Graciela De Conti Pagliari, Adriana A. Marques, Lucas Soares Portela, and Walfredo Bento Ferreira Neto. 2017. *Guia de defesa cibernética da América do Sul*. Recife: Ed. UFPE.

Olson, Soren. 2012. "'Treino de Sombra': a guerra cibernética e o ataque econômico estratégico". *Military Review*: 73–83 (Set./Out.).

Rid, Thomas. 2013. *Cyberwar will not take place*. New York: Oxford University.

Silva, Júlio Cezar Barreto Leite da. 2014. "Guerra cibernética: a guerra no quinto domínio, conceituação e princípios". *Revista da Escola de Guerra Naval* 20, no. 1: 193-211 (Jan./Jun.). Rio de Janeiro.

Singer, Peter Warren, and Allan Friedman. 2014. *Cybersecurity and cyberwar: what everyone needs to know*. 1. ed. New York: Oxford University Press.

Teixeira Júnior, Augusto W. M., Gills Villar Lopes, and Marco Túlio Delgobbo Freitas. 2017. "As três tendências da guerra cibernética: novo domínio, arma combinada e arma estratégica". *Carta Internacional* 12, no. 3: 30–53. Belo Horizonte.

Vaczi, Nobert. 2016. *Hybrid warfare: how to shape special operations forces.* 103 p. Dissertação (Mestre em Ciência e Arte Militar) — Faculdade da Escola de Comando e Estado-Maior do Exército dos Estados Unidos, Fort Leavenworth, Kansas.

Vilar-Lopes, Gills. 2016. *Relações Internacionais Cibernéticas (CiberRI): uma defesa acadêmica a partir dos estudos da segurança internacional.* 171 p. Tese (Doutorado em Ciência Política) — Universidade Federal de Pernambuco, Recife.

Wendt, Emerson. 2011. "Ciberguerra, inteligência cibernética e segurança virtual: alguns aspectos". *Revista Brasileira de Inteligência* 6: 15–26 (Abril). Brasília.

NOTAS

1. "[...] the global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers." (Singer and Friedman 2014, 13).
2. "[...] cyberspace is the realm of computer networks (and the users behind them) in which information is stored, shared, and communicated online." (Singer and Friedman 2014, 13).
3. "Cyberspace is first and foremost an information environment. It is made up of digitized data that is created, stored, and, most importantly, shared. This means that it is not merely a physical place and thus defies measurement in any kind of physical dimension. But cyberspace isn't purely virtual. It comprises the computers that store data plus the systems and infrastructure that allow it to flow. This includes the Internet of networked computers, closed intranets, cellular technologies, fiber-optic cables, and space-based communications." (Singer and Friedman 2014, 13).
4. "[...] a set of resources that relate to the creation, control and communication of electronic and computer-based information — infrastructure, networks, software, human skills. This includes not only the internet of networked computers, but also intranets, cellular technologies, and space--based communications." (Nye Jr. 2011, 123).
5. "[...] as any act by an insider or an outsider that compromises the security expectations of an individual, organization, or nation." (Gandhi *et al.* 2011, 29).
6. "[...] is hence a human deed that explores the vulnerabilities of the virtual sphere, managing to harm informational systems or even, in light of modern life's online dependency, material daily life." (Lobato and Kenkel 2015, 27).
7. "0[...] involves virtual modification or destruction of content, e.g., hacking websites or disabling a server by data overload. [...] the effects of such incidents are limited in time and relatively harmless." (Cavelty 2010, 01).
8. "Cyber terrorism is the premeditated, polically motivaded attacks against information, computer systems, computer programs, and data which result in violence against non-combatant targets by sub-national groups or clandestine agents." (Curran, Concannon, and McKeever 2008, 01).
9. "[...] an indispensable precondition for assessing the concrete danger and its importance, allocating responsibilities, implementing preventive and reactive countermeasures, and conducting criminal investigations." (Cavelty 2010, 01)
10. "So far there is no known act of cyber "war," when war is properly defined. This of course does not mean that there are no political cyber offenses. But all known political cyber offenses, criminal or not, are neither com-

mon crime nor common war. Their purpose is subverting, spying, or sabotaging." (Rid 2013, 10).

11. "A campaign of cyberattacks launched by one entity against a state and its society, primarily but not exclusively for the purpose of affecting the target state's behavior, would be strategic cyberwar." (Libicki 2009, 117).
12. If the attacks between political entities are sufficiently "widespread" we might then speak of a cyberwar." (Dipert 2010, 398).

GUERRA CIBERNÉTICA, AMEAÇAS ÀS INFRAESTRUTURAS CRÍTICAS E A DEFESA CIBERNÉTICA DO BRASIL

RESUMO

Diante das dinâmicas emergidas com as novas tecnologias, esse estudo propõe debater sobre os novos moldes de ações ofensivas e defensivas no ciberespaço, buscando compreender algumas dinâmicas envolvidas diante das potencialidades de um cenário de ciberguerra. Nessa perspectiva, a pergunta central que este artigo procura responder é: de que forma esses novos moldes e dinâmicas ligadas aos recursos cibernéticos poderiam ser compreendidos diante de um potencial cenário de ciberguerra? Os atores estatais têm desenvolvido estratégias específicas para lidar com as novas dinâmicas impostas pelo ciberespaço, tanto numa dinâmica defensiva e resiliente, como ofensiva. Contudo uma série de fatores característico deste espaço precisam ser melhor compreendidos frente as vulnerabilidades enfrentadas pelos Estados. Assim, após o debate teórico-conceitual sobre ciberguerra, o artigo analisa o posicionamento do Brasil frente a tais dinâmicas tendo como base de análise os documentos estratégicos de defesa do país.

Palavras-chave: Ciberespaço; Ciberguerra; Infraestruturas Críticas; Segurança Internacional; Defesa.

ABSTRACT

In view of the dynamics that emerged with the new technologies, this study will discuss about the new forms of offensive and defensive actions in cyberspace, seeking to understand its dynamics involved ahead of the potential occurrence of a cyberwar scenario. In this perspective, the central question that this article seeks to answer is: how could these new patterns and dynamics linked to cyber resources be understood in the face of a potential cyberwar scenario? State actors have developed specific strategies to deal with the new dynamics imposed by cyberspace, both in a defensive and resilient and offensive dynamic. However, a series of factors characteristic of this space need to be better understood in view of the vulnerabilities faced by States. So, after this theoretical-conceptual debate on cyberwar, the article aims to understand Brazil's position in face of such dynamics, based on the country's defense strategy documents.

Key-words: Cyberspace; Cyberwar; Critical Infrastructures; International Security; Defense.

Recebido em 02/03/2020. Aceito para publicação em 22/02/2021.

Armas inteligentes no ciberespaço: oportunidades inovadoras e desafios prementes

Intelligent weapons in cyberspace: innovative opportunities and pressing challenges

Rev. Bras. Est. Def. v. 7, nº 2, jul./dez. 2020, p. 133-157
DOI: 10.26792/RBED.v7n2.2020.75211
ISSN 2358-3932

ANA CAROLINA DE OLIVEIRA ASSIS
NATHALIA VIVIANI BITTENCOURT
SANDRA MARIA BECKER TAVARES

INTRODUÇÃO

As definições de espaço cibernético e de inteligência artificial (doravante, IA) são controversas e difusas, cada qual à sua maneira. O ciberespaço é, via de regra, um domínio de exploração, criação e tráfego de informações através do uso de eletrônicos em redes interconectadas de sistemas de computadores,[1] enquanto o conceito de IA abrange uma diversidade de técnicas de computação capazes de executar tarefas e resolver problemas antes limitados à cognição humana[2] (Boulanin *et al.* 2019). No contexto contemporâneo, as tecnologias de informação e comunicação estão massivamente presentes na sociedade, desde os computadores pessoais a infraestruturas críticas que dependem do funcionamento remoto de redes (por exemplo, eletricidade, redes de esgoto, sistema financeiro). Da mesma forma, podemos observar a aplicação de IA em diversos setores da vida

Ana Carolina de Oliveira Assis — Doutoranda no Programa de Pós-Graduação em Ciência Política pela Universidade Federal de Pernambuco. Graduada no curso de Relações Internacionais da Universidade Federal da Paraíba e Mestrado em Ciência Política pela Universidade Federal de Pernambuco. Membro do Grupo de Pesquisa O Brasil e as Américas (UFPE) e Grupo de Pesquisa sobre Estratégia e Segurança Internacional (UFPB).
Nathalia Viviani Bittencourt — Doutoranda em Ciência Política com ênfase em Relações Internacionais pela Universidade Federal de Pernambuco. Graduada em Direito pela mesma Universidade e advogada. Membro do Grupo de Pesquisa O Brasil e as Américas (UFPE) e pesquisadora da Rede de Ciência e Tecnologia e Inovação em Defesa: Cibernética e Defesa Nacional (Pró-Defesa IV).
Sandra Maria Becker Tavares — Doutora em Bioética, Ética Aplicada e Saúde Coletiva pela Fundação Oswaldo Cruz (2014). Professora Adjunta 3 da Universidade Federal do Rio de Janeiro. Coordenadora Adjunta (vice-diretora) do Instituto de Relações Internacionais e Defesa (IRID/UFRJ) e Coordenadora de Extensão da Decania do Centro de Ciências Jurídicas e Econômicas (CCJE/UFRJ). É membro titular do Conselho de Extensão Universitária da UFRJ.

cotidiana, como aplicativos que otimizam nossas escolhas e a produção de artefatos de reconhecimento facial e de voz. No que concerne às suas aplicações na esfera Estatal, ambos os termos podem ser considerados em ampla ascensão estratégica à segurança e à defesa nacional.

Nessa perspectiva, governos estão dedicando mais possibilidades para questões referentes ao espaço cibernético — tanto na criação de instituições, subdivisões e meios para defesa/ataque aos inimigos, como também ao emprego da IA para, *inter alia*, construção de armas crescentemente autônomas, sistemas robóticos, sensores responsáveis para identificar alvos (Morgan *et al.* 2020). A título ilustrativo, o Departamento de Defesa dos Estados Unidos (***DOD —Department of Defense***), em 2018, teve o seu Comando Cibernético (CyberCom) unificado para um Comando de Combate, o que significa mais autonomia na condução de operações, considerando que o domínio cibernético está mudando muitos aspectos da guerra (Ferdinando 2018). Por seu turno, as capacidades da IA têm influenciado muitos Estados a elaborarem documentos estratégicos que incentivem seus investimentos em setores de interesse nacional, a exemplo da China, Rússia, Índia, Canadá, União Europeia, Reino Unido e Estados Unidos (EUA) (Future of Life Institute 2020).

No que tange ao governo brasileiro, algumas iniciativas coordenadas têm recentemente atribuído grande relevância ao ciberespaço e à IA. O Ministério da Tecnologia, Ciência e Inovações (MCTIC) está elaborando um documento que identifica as áreas prioritárias que podem ter seus processos aperfeiçoados pelos benefícios dessa tecnologia (Brasil 2019). Ademais, em fevereiro de 2020 foi aprovada a Estratégia Nacional de Segurança Cibernética (E-Ciber) pelo Decreto nº 10.222. Dentre os seus objetivos de tornar o espaço cibernético mais resiliente e seguro, o documento apresenta a necessidade do desenvolvimento de mecanismos avançados que maximizem o combate a ameaças cibernéticas, a saber:

> As ameaças cibernéticas [...] têm o escopo de alcançar grande número de organizações, inclusive as representantes das infraestruturas críticas, que, por prestarem serviços essenciais à sociedade, possuem elevado nível de criticidade. Por isso, essas organizações necessitam de meios para identificar, proteger, detectar, avaliar, responder, recuperar e assim gerenciar o risco das ameaças cibernéticas, e também de ferramentas de automação de segurança que usam inteligência artificial e aprendizado de máquina, que permitam analisar, identificar e conter os ataques cibernéticos. (Brasil 2020, 6)

Diante disso, a exploração da IA seria um desses meios que poderiam contribuir na segurança e resiliência cibernética. Segundo Taddeo *et al.*

(2019), estima-se que os investimentos em IA com a finalidade de cibersegurança pelos países vão ter um salto de US$1 bilhão para US$ 34 bilhões no intervalo de nove anos (entre 2016 e 2025). Ainda sobre esse aparato, os autores demonstram que o fenômeno é de tamanha relevância que as Estratégias de Segurança e de Defesa Cibernética de alguns países como a Austrália, Japão, Singapura, Estados Unidos, China e Reino Unido já mencionam a utilização de IA para aprimorar a proteção de suas infraestruturas críticas. De fato, o pensamento de Morgan *et al.* (2020) assenta que essa tecnologia tem o potencial de auxiliar na identificação de *malwares* e das próprias vulnerabilidades das redes — o que permite, assim, o aprimoramento da defesa — e na localização de brechas dos sistemas de inimigos a fim de explorá-las para, eventualmente, promover um ataque.

Isso posto, o objetivo do presente artigo é descrever como o emprego de IA tem influenciado no ataque e ao combate de ameaças cibernéticas pela Defesa, assim como inserir o leitor no debate acerca dos benefícios e dos perigos do uso dessa tecnologia no ciberespaço. A questão investigativa que norteia este estudo é: quais são as oportunidades e desafios que a expansão do uso das tecnologias de IA proporciona ao armamento e à segurança cibernética no ramo militar? Acredita-se que o presente estudo seja relevante devido a fatores de duas ordens. No âmbito teórico, a consulta bibliográfica permitiu inferir ser ainda incipiente o debate nas academias de Relações Internacionais (RIs) e de Defesa Nacional sobre a interseção da Inteligência Artificial no espaço cibernético, de modo que se busca contribuir à literatura, especialmente aos estudos de segurança das RIs e de Defesa. De ordem prática, é significativo apontar a importância estratégica que Estados têm conferido a esse assunto.

Para atender ao objetivo do estudo, optou-se pela abordagem qualitativa. No primeiro momento, foi utilizada uma revisão bibliográfica da literatura dos Estudos de Segurança e de Defesa sobre o espaço cibernético e a exploração da IA. Em sequência, foi realizada, com o auxílio da Teoria da Balança Ofensiva-Defensiva Cibernética, uma análise das relações internacionais em relação ao emprego da IA neste domínio, introduzindo conceitos como poder cibernético (*cyberpower*), dissuasão cibernética (*cyberdeterrence*) e dilema da segurança cibernética (*cyber security dilemma*). Com efeito, entendemos que os pressupostos trazidos pela Teoria à análise dos custos das operações de ataque e de defesa revelou-se pertinente ao objetivo do artigo, sendo este a descrição das oportunidades e desafios que as aplicações de IA introduzem às operações realizadas no domínio cibernético. Por fim, foram levantadas, com apoio também de uma revisão bibliográfica e de documentos oficiais, as limitações e oportunidades da IA para Segurança e Defesa Cibernética.

Como resultados, entendemos que o desenvolvimento de IA no espaço cibernético é uma faca de dois gumes: ao mesmo tempo em que o processamento rápido de grande volume de dados e o reconhecimento de padrões pela programação computacional podem ser grandes aliados na antecipação e combate de ameaças a redes, por outro, novas vulnerabilidades exigem cautela em sua operacionalização. Além disto, acreditamos que, no que tange à Teoria da Balança Ofensiva-Defensiva Cibernética, as capacidades da referida tecnologia podem promover o favorecimento da defesa em detrimento da primazia do ataque.

A REVOLUÇÃO DA INFORMAÇÃO E A MILITARIZAÇÃO DO ESPAÇO CIBERNÉTICO

A partir da ideia de que a informação sempre foi um recurso de poder para os Estados, Nye (2010) assume que o poder cibernético (*cyberpower*) possui idiossincrasias que tornam o seu conceito mais difuso e volátil. Ao contrário dos domínios tradicionais, o ciberespaço é uma criação artificial do homem que permite a redução de custos no emprego de ataques, dificulta a atribuição de responsabilidade e facilita a proliferação de ofensivas por atores não-estatais e por Estados considerados menos influentes na política internacional. Nessa acepção, o autor define o poder cibernético como a capacidade dos Estados em manipular, criar e explorar informações eletrônicas e baseadas em sistemas de computador que podem promover vantagens neste domínio ou influenciar eventos em outros ambientes operacionais (Nye 2010)

Nessa perspectiva, a capacidade das operações cibernéticas afetarem outros âmbitos da esfera social e militar, bem como as suas singularidades de ataques e do anonimato de atores promovem, inevitavelmente, a sua securitização na agenda política dos Estados (Waever *et al.* 1993; Waever 1995; Buzan *et al.* 1998; Cavelty 2008). Sob esse prisma, destaca-se o trabalho pioneiro de Hansen e Nissenbaum (2009), cuja análise dos ataques cibernéticos de negação de serviços (DDoS — Distributed Denial of Service[3]) na Estônia, em 2007, foi realizada à luz da Escola de Copenhague. Dessa forma, as autoras situam a questão cibernética como um setor específico de segurança — não apenas subordinado a um problema econômico, técnico ou criminal — mas que se apresenta de forma independente e que provoca consequências de ordens políticas e normativas próprias. Ato contínuo, concluem que existe a necessidade premente de que os Estudos de Segurança adotem uma perspectiva interdisciplinar na abordagem teórica do fenômeno cibernético. Com efeito, a avaliação das operações neste domínio exige que a abordagem seja

multifacetada, inovadora, e que inclua outros ramos do conhecimento para sua compreensão.

Outrossim, a securitização e a consequente politização do espaço cibernético tornam as suas operações matérias de grande interesse e mudanças no setor militar. Em verdade, na literatura (Schneider 2019, Cavelty 2012) argumenta-se que a revolução da informação exerce influência de modo decisivo ao seu *modus operandi*, tendo em vista o crescente desenvolvimento de tecnologias que tornam a sociedade e governos cada vez mais dependentes de serviços que envolvem processos digitais em infraestruturas críticas. Krepinevich (1994), ao fazer uma análise histórica sobre as Revoluções Militares e o fator decisivo de tecnologias emergentes como recurso de poder, argumenta que a Guerra do Golfo pode ser considerada precursora de uma nova Era no campo de batalha, haja vista a coordenação e integração das operações proporcionadas pela informação em redes.

Ao debruçar-se sobre o estudo cronológico e argumento desse autor, Schneider (2019) aponta que a exploração das atuais tecnologias de ponta pela Defesa, a exemplo da IA, computação quântica e armazenamento em nuvem torna o recurso de dados como uma recente etapa da Revolução Militar[4], ao lado do marco da Infantaria, Artilharia, dentre outros. Ademais, a autora conclui que existe um paradoxo de vulnerabilidade\vantagem ao espaço cibernético militarizado, tendo em vista que o aumento da dependência de redes ao funcionamento de serviços pode provocar brechas de segurança que permitem ataques ocultos e a escalada, por consequência, das tensões em conflitos. Esse argumento também é explorado por Liff (2012), ao afirmar que a rapidez nos processos de tecnologias de informação e comunicação e a expansão da digitalização nas operações podem representar um verdadeiro "calcanhar de Aquiles" em campanhas militares dos EUA (Liff 2012).

ARMAS CIBERNÉTICAS, AUTONOMIA E IA

De modo geral, pode-se afirmar que as armas cibernéticas (*cyber weapons*) são aplicações da tecnologia de informações que buscam criar efeitos negativos na disponibilidade, integridade e\ou confidencialidade nos dados de um computador individual ou de sistemas complexos de comunicação (Lin 2016). Além disso, o autor salienta que enquanto os ataques cibernéticos (*cyberattacks*) têm como objetivo afetar a disponibilidade e integridade dos dados e do funcionamento de sistemas, a exploração ou espionagem cibernética (*cyber exploitation*) se refere à busca por informações sigilosas e confidenciais. Por último, torna-se relevante destacar dois mecanismos comumente utilizados no emprego das armas cibernéticas: para Lin (2016, 115), intrusão (*penetration*) e carga útil (*payload*), os quais significam, respectivamente, a

obtenção do acesso a sistemas de computadores a partir das vulnerabilidades encontradas e a execução programada para agir após a intrusão, o que pode, a depender do canal de comunicação, ser remotamente atualizada.

Além disso, Kello (2013) revela alguns termos técnicos comuns a respeito do alcance das armas cibernéticas e suas complicações em estratégias de defesa cibernética. Ao indicar argumentos de pesquisadores sobre a vantagem da ofensiva ou da defesa em operações neste meio, o autor assinala perigos que desafiam o equilíbrio da balança. Assim, a imprevisibilidade de ataques que atingem vulnerabilidades dia-zero (*zero-day vulnerabilities*), por exemplo, torna o ataque muito difícil de ser rastreado em função da capacidade do *malware* de mascarar os seus efeitos danosos ao computador (Kello 2013). A título ilustrativo, o amplamente conhecido *worm Stuxnet* é um exemplo desse tipo de ataque, o qual foi capaz de explorar uma brecha de segurança dos sistemas de enriquecimento de urânio do Irã que não tinha cobertura (*patch*) para corrigir a sua vulnerabilidade.

Ademais, o autor identifica outros fatores de desequilíbrio, como o ataque de distribuição de negação de serviços, a complexidade da superfície de defesa (associada ao atual desenvolvimento intrincado dos sistemas de software e hardware, os quais exigem mais *expertise* na implementação de ataques e na defesa) e a presença maciça da indústria privada na cadeia de suprimentos e na infraestrutura críticas de computadores, o que dificulta a elaboração de políticas coesas no espaço cibernético pelos governos. Diante dessas assimetrias, tem-se que a atribuição de valor e custo a essas problemáticas podem conferir vantagens ao mecanismo de ataque. Entretanto, conforme poderemos observar nas próximas seções, avanços em IA na segurança cibernética podem oferecer razões que desafiam a primazia da ofensiva neste meio.

No que concerne à implementação de IA no ramo militar, Johnson (2019) aponta que não há dúvidas de que o uso de processos habilitados para essa tecnologia pode promover vantagens decisivas, haja vista a sua capacidade de fomentar, por exemplo, o sensoriamento remoto e a compressão do ciclo de tomada de decisão, sobretudo em casos de situações hostis que exijam respostas rápidas. De modo amplo, o autor categoriza em diferentes áreas de atuação as possibilidades do aumento de performance de sistemas automáticos e autônomos pela IA, sendo as mais relevantes para o nosso escopo do artigo: área de raciocínio e de tomada de decisão, as quais se relacionam com resolução de problemas e planejamento; a de representação de aprendizagem e conhecimento (aprendizagem de máquina e aprendizagem profunda[5]) e a de autonomia.

Há importante debate em setores acadêmicos e em Organizações Internacionais acerca da definição de autonomia e de suas diferenças em

relação a sistemas automáticos. Os sistemas automáticos são considerados processos que respondem a regras pré-programadas, além de apresentarem resultados previsíveis, com pouca ou nenhuma capacidade para lidar com variâncias. Autonomia, por seu turno, possui um grau mais complexo e inteligente de autocontrole, tendo em vista que pode selecionar diferentes caminhos para alcançar um objetivo (Boulanin *et al.* 2019; Morgan *et al.* 2020). Nesse contexto, tal distinção possui relevância às operações desempenhadas no ciberespaço em razão da crescente autonomia das armas desenvolvidas nesse meio, seja por intermédio de IA ou não, conforme afirmam Liivoja *et al.* (2019). A partir de alguns exemplos de capacidades cibernéticas autônomas, como o *Stuxnet*, os autores trazem à tona questões do *jus ad bellum* e *jus in bello* ao debate do *compliance* dessas operações às normas e princípios do Direito Internacional, bem como argumentam que as matérias de sistemas de armas autônomas (*autonomous weapons systems*) e das intervenções cibernéticas não podem ser tratadas de forma isolada pela comunidade internacional. Diante dessas discussões que a IA suscita nas relações internacionais, assim como as suas possibilidades de otimizar processos e decisões em diversas tecnologias no meio militar, alguns Estados, especialmente a China, Rússia e EUA têm aplicado e aprimorado algumas de suas capacidades cibernéticas por intermédio da IA com finalidade de alcançar as vantagens do pioneiro (*first-mover*) (Johnson 2019).

Nessa perspectiva, a respeito da China, sua indústria de defesa tem desenvolvido armas com considerável capacidade de inteligência e autonomia, as quais permitem alto grau de precisão nas operações, o que soma à sua capacidade de dissuasão, conforme pontua Kania (2019). Utiliza-se como exemplo dessas habilidades o uso de algoritmos inteligentes ao processamento de imagens de satélites e a criação de armas hipersônicas. Além disso, a autora afirma que o Exército de Libertação Popular, por intermédio de sua Força de Apoio Estratégico, tem integrado suas práticas relativas à guerra cibernética, eletrônica e espacial, bem como explorado pesquisas de tecnologias de IA para aprimorar a sua segurança e defesa cibernética.

No que tange à indústria de defesa do governo russo, Thornton e Miron (2020) destacam a relevância estratégica da IA ao fortalecimento de duas facetas da guerra cibernética que são levantadas pela perspectiva russa: a psicológica (*cyber-psychological*) e a técnica (*cyber-technical*). Quanto à primeira, armas cibernéticas impulsionadas pela IA seriam capazes de disseminar informações a um escopo e velocidade maiores, a exemplo das *fake news* e da produção de *deepfakes*,[6] com o intuito de exercer maior influência na consecução de seus interesses. Quanto à perspectiva técnica, aludem os autores que essa faceta configura o uso de espionagem e desenvolvimento

de malwares inteligentes que buscam vulnerabilidades em sistemas de tecnologia da informação.

Os EUA, por seu turno, têm demonstrado preocupação com a aplicação generalizada de IA no espaço cibernético. Em 2018, o evento CyCon US (2018) promoveu um debate acerca do uso da IA na segurança cibernética, oportunidade na qual dois oficiais das Forças Armadas discutiram sobre os mais recentes avanços dessa tecnologia e seus limites. Na ocasião, o Major Nathaniel D. Bastian e o Brigadeiro-General Matthew Easley defenderam que a IA tem sido muito útil na descoberta e correção automática de *malwares* e anomalias de forma rápida e eficaz, mas acreditam que essa tecnologia ainda não é capaz de proteger sistemas de ataques mais complexos, como os de dia-zero. Além disso, afirmaram que a aprendizagem de máquina tem demonstrado avanços na análise e classificação de padrões, porém também permite que novos ataques com essa estrutura sejam mais sofisticados (*adversarial-learning attacks*[7]) (Bastian and Easley 2018).

Diante do exposto, percebe-se que as tecnologias de IA têm sido amplamente utilizadas no domínio cibernético. Entretanto, as suas capacidades ofensivas e defensivas tornam o debate acerca dos custos de suas operações complexo à medida que novos tipos de ataque e de defesa baseados nessa tecnologia são desenvolvidos. Na próxima seção, vamos abordar com mais profundidade a Teoria da Balança Ofensiva-Defensiva no Ciberespaço para, em seguida, analisar algumas oportunidades e desafios que a IA possibilita à indústria de Defesa Cibernética.

TEORIA DA BALANÇA OFENSIVA-DEFENSIVA NO ESPAÇO CIBERNÉTICO

Uma vez que as pesquisas sobre as dinâmicas no ciberespaço nas Relações Internacionais são recentes, parte dos autores tenta adaptar diversos conceitos e teorias tradicionais utilizadas nos Estudos Estratégicos, nas RIs e em outras disciplinas para o novo contexto em que se inserem. Alguns estudiosos, por exemplo, utilizam a teoria da guerra proposta por Clausewitz em estudos sobre cibernética. Outros dedicam-se à própria concepção da guerra à análise de seus aspectos fundamentais e da sua natureza para travar o debate se a guerra cibernética é um fenômeno bélico de fato (Rid 2012; Liff 2012; Stone 2013), ou até para entender como a tecnologia cibernética pode transformar as estratégias e táticas no campo de batalha (Teixeira Júnior *et al.* 2017).

Além dessa perspectiva sobre o fenômeno cibernético, alguns estudos passaram a abordar a questão da securitização e politização do espaço cibernético de modo semelhante ao trabalho de Hansen e Nissenbaum

(2009). Dentre eles, citamos o de Lacy e Price (2018) e pesquisas até mais específicas que se destinam a tratar do caso brasileiro (Muggah *et al.* 2014; Medeiros *et al.* 2019).

Outro conceito afeito aos estudos das RIs refere-se à questão do Dilema de Segurança. Inicialmente, essa concepção foi elaborada por Jervis (1978) em *Cooperation under the Security Dilemma*, no qual o autor vai abordar as dinâmicas que levam à percepção de ameaça entre os atores no nível internacional e como isso impacta a relação entre eles. No que tange ao Dilema de Segurança Cibernética, é argumentado de forma inovadora por Buchanan (2017) que os princípios levantados por Jervis aplicam-se a vários momentos da história mundial, inclusive no contexto atual da era da informação. De acordo com o referido autor, no que concerne à segurança cibernética, assim como em outras esferas, as características estruturantes do sistema internacional, assim como as particularidades de cada tipo de operação, geram apreensão nos atores; por conseguinte, esse pavor pode escalar conflitos.

Por sua vez, Jervis (1978), em seu estudo seminal, complementa a sua discussão trazendo a Teoria Ofensiva-Defensiva, na qual avalia o efeito de cada uma das abordagens para escalada do conflito ou sobre os incentivos à Corrida Armamentista — por exemplo, no momento em que a balança pende para a ofensiva, o dilema de segurança tende a se intensificar, o que pode, por consequência, levar a conflitos (Garfinkel and Dafoe 2019). Sobre a Teoria da Balança Ofensiva-defensiva, uma definição mais tradicional, também atrelada aos estudos de RI pode ser apontada como:

> a razão dos custos das forças que o atacante requer para tomar o território ao custo das forças do defensor emprega. Isto é, se o defensor investir X em ativos militares, quão maior deve ser o investimento Y do atacante para adquirir as forças necessárias para tomar o território: A balança ofensiva-defensiva é a razão Y/X. Razões maiores indicam uma balança mais favorável à defesa (Glaser and Kaufmann 1998, 3).[8]

Embora a definição acima descreva como o objetivo final a tomada de território, as finalidades definidas pelos atores envolvidos podem ser distintas. De forma mais informal, a balança ofensiva-defensiva relaciona-se com os custos ou facilidades em realizar um ataque ou adotar uma postura defensiva. Ou seja, os tomadores de decisão levam em consideração nos cálculos racionais a influência da tecnologia militar nos dispêndios da defensiva e da ofensiva. (Garfinkel and Dafoe 2019, Slayton 2017).

No que tange à aplicação ao setor cibernético, Rebecca Slayton (2017) aponta para três principais perspectivas implícitas do que seria a Balança

Ofensiva-Defensiva Cibernética — implícitas porque muitos dos autores não apresentam diretamente uma definição, mas a avaliam empiricamente. Nesse sentido, a primeira perspectiva se refere aos custos relativos da ofensiva e defensiva. Dominante na academia, essa abordagem abrange a atribuição de valores (principalmente materiais) a cada operação para medir a sua equação. Já a perspectiva da Ofensiva Cibernética concentra-se mais nos resultados (*payoff*) em detrimento dos custos, na medida em que a balança está relacionada com a eficácia das operações. Por fim, a perspectiva da vantagem do pioneiro identifica as vantagens de ser o primeiro a tomar iniciativas de conflito.

Em termos gerais, a Balança Ofensiva-Defensiva Cibernética está relacionada com a análise dos custos para empreender ataques cibernéticos em relação aos custos para edificar uma estratégia de resiliência. Cada opção estratégica terá investimentos e resultados diferenciados e cabe ao tomador de decisão optar pelo caminho a seguir. Algo recorrente e que transpassa a literatura sobre a Balança Ofensiva-Defensiva é a questão do *culto à ofensiva* ou *primazia do ataque*.[9] Para adeptos dessa argumentação, a postura ofensiva normalmente é tida como a melhor opção, uma vez que os custos são menores em relação à defesa e até a própria configuração das tecnologias atuais facilitam um ataque em detrimento da defesa — um exemplo disso é a questão da vulnerabilidade dos Sistemas e a facilidade dos 'atacantes' para encontrar apenas uma fragilidade e partir para ação, em contrapartida da defesa, a qual tem que identificar todas as vulnerabilidades possíveis e mesmo assim pode ser que não seja a que o atacante vai explorar (Slayton 2017).

Entretanto, alguns acadêmicos não concordam que a ofensiva permaneça como vantagem. Slayton (2017) lança uma proposta com quatro argumentos para explicar por que as reivindicações abrangentes sobre as vantagens da ofensiva no ciberespaço são equivocadas. Em primeiro lugar, nos estudos que defendem a primazia do ataque, a Balança Ofensiva-Defensiva é analisada apenas em relação aos custos das operações, entretanto, há a necessidade de avaliar também o valor atribuído pelos tomadores de decisão aos objetivos (caso uma postura agressiva tenha consequências mais dispendiosas para os tomadores de decisão, eles devem optar por uma postura defensiva). Em segundo lugar, a tecnologia não é o fator determinante único das vantagens da defensiva e da ofensiva, sendo imprescindível avaliar o processo organizacional que rege as relações entre tecnologia e operadores habilidosos. Em outras palavras, a Balança é determinada tanto pelas habilidades possuídas pelos atores em comparação com seus adversários, como pelas complexidades dos objetivos (não adianta ter um objetivo complexo sem habilidade e vice-versa, ou sem a organização do processo da tradução dos objetivos em ações).

Em terceiro lugar, a autora demonstra que a ofensiva é colocada como superior porque em grande parte das análises, o sucesso dessa estratégia é resultado de objetivos mais limitados e da má gestão dos adversários, isto é, em muitos casos a vantagem da ofensiva recai sobre fragilidades do inimigo ao invés da superioridade tecnológica nos ataques. Por fim, a autora realiza um estudo de caso sobre o *Stuxnet*, calcula em termos materiais o custo-benefício tanto para os atacantes como para os defensores e obtém que a defensiva seria menos custosa, financeiramente, do que a ofensiva (Slayton 2017).

Garfinkel and Dafoe (2019), por seu turno, argumentam que a defensiva apresenta vantagens superiores à ofensiva conforme a quantidade de investimentos aplicados às tecnologias. Inicialmente, quando os investimentos ainda são discretos, a ofensiva é mais vantajosa, pois necessita de menos recursos, uma vez que os defensores não conseguem cobrir todos os pontos de vulnerabilidade (o que o autor denomina como *gap exploitation*). Entretanto, para os autores, à medida que as aplicações aumentam, a defesa é mais vantajosa porque os pontos de ingressão (vulnerabilidades) vão sendo cerceados gerando o desgaste ou uma *deffensive saturation.*

Ademais, Schneier (2018) pontua que a IA pode favorecer a defensiva na medida em que suas tecnologias realizam a segurança em sistemas de informação de forma mais rápida e em maior escala do que os humanos. Sendo assim, ainda que suas capacidades no espaço cibernético também favoreçam o escopo de ataques, o autor acredita que a IA tornará a defesa mais eficaz ao combate de *malwares* e anomalias tendo em vista o seu potencial de analisar um grande volume de dados a uma velocidade superior à humana.

Por último, outro conceito também relacionado à Teoria da Balança Ofensiva-Defensiva é o de dissuasão (*deterrence)*. Quanto à sua influência no espaço cibernético, autores como Taddeo (2018) e Nye (2017) argumentam que a sua concepção tradicional não é adequada para abordar as questões singulares de alcance global, anonimidade e interconectividade atribuídas a esse domínio. Nye (2017), por exemplo, entende que existem quatro meios de emprego da dissuasão no ciberespaço: a ameaça de punição (*threat punishment)*; a defesa por negação (*defense denial*), emaranhamento (*entanglement)* e taboos normativos (*normative taboos)*. Quanto ao primeiro, o autor baseia-se na obra pioneira de Libicki (2009) para defender a possibilidade do emprego de punição como forma de dissuasão no espaço cibernético, ainda que o problema de atribuição persista. O segundo se refere à redução de incentivos a ataques em razão de a defesa ser capaz de torná-la ineficaz. Acerca deste ponto, Nye (2017) entende que as novas tecnologias terão papel fundamental na mudança da primazia da ofensiva no espaço

cibernético pelo emprego da dissuasão por meio da defesa por negação. Quanto aos aspectos do emaranhamento e os *taboos* normativos, o autor entende que o fenômeno da interdependência poderá tornar os custos de um ataque muito superiores do que seus benefícios devido a retaliações por outros meios, como respostas econômicas e diplomáticas.

Taddeo (2018), por sua vez, fornece argumentos para uma Teoria da dissuasão cibernética. Assim, a dissuasão *cyber* é composta por três elementos centrais: Identificação do alvo; Retaliação; e Demonstração. Primeiramente, a identificação dos sistemas que realizaram o ataque é essencial para que ocorra a dissuasão — independentemente do conhecimento ou não de quem são os agressores — pois, dessa forma, o defensor pode isolar a ameaça, contra-atacar e obter a retaliação almejada. Acerca da Retaliação, a autora afirma que apenas a intimidação do oponente não é suficiente. Para deter novos ataques a seus sistemas, o ator envolvido deve infringir danos nos sistemas do inimigo para que ele perca a intenção de atacar novamente. Nesse sentido, a imprevisibilidade e inevitabilidade de ataques podem tornar a retaliação aconselhada como forma de defesa. Com efeito, se tradicionalmente os Estados realizam demonstrações públicas nas relações internacionais com armamentos ou ataques para intimidação e ameaça ao oponente, isso não teria efeito dissuasório no domínio cibernético em razão de que Estados não divulgam muitas informações quando são vítimas ou quando atacam. O argumento geral de sua teoria pode ser resumido através da Figura 1:

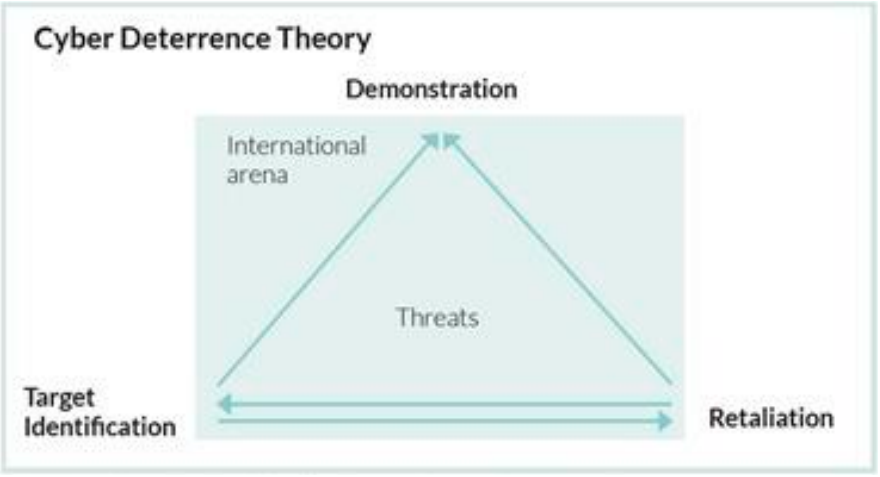


Figura 1 — Teoria da Dissuasão Cibernética
Fonte:Taddeo 2018, 5.

OPORTUNIDADES E DESAFIOS PROPORCIONADOS PELO NEXO CYBER-IA

Nesta seção, vamos apresentar algumas das oportunidades que as tecnologias de IA proporcionam à segurança cibernética, bem como seus riscos inerentes às operações e às possibilidades de ataques coordenados a esses sistemas. Sendo assim, torna-se relevante destacar, neste primeiro momento, recente White Paper sobre Segurança e Inteligência Artificial publicado por um think thank do Ministério da Indústria e Tecnologia da Informação da China, em 2018, no qual uma estrutura de segurança em IA foi analisada sob a perspectiva de três áreas estratégicas, como explicitado na Figura 2:

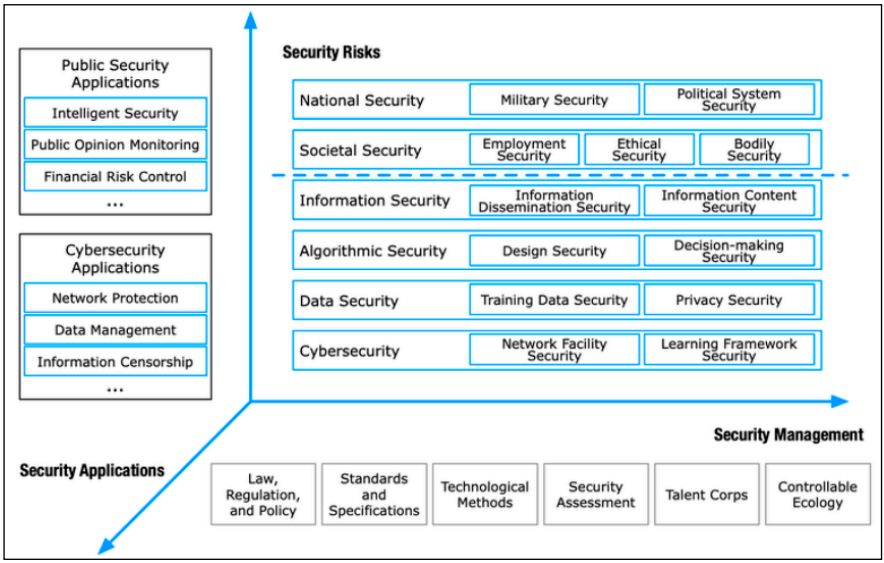


Figura 2 — Quadro do Sistema de Segurança em Inteligência Cibernética
Fonte: China Academy of Information and Communications Technology (CAICT), 2018, traduzido por *Kania et al.* (2019).

No âmbito da relação entre cibernética e IA, dentro do quesito de riscos de segurança (*Security Risks*), podemos observar que o grupo de pesquisa chinês verifica quatro ameaças que a IA pode influenciar no espaço cibernético. Em relação à segurança na informação (*Information Security*), considera-se fator de atenção a forma pela qual a IA potencialmente afeta

a velocidade na disseminação e manipulação de seu conteúdo. Além disso, a segurança algorítmica (*Algorithmic Security*) requer mais estudos acerca de seu *design* (maturidade técnica do algoritmo) e da sua tomada de decisão segura (*decision-making security*) no que tange a questões de explicação dos processos dos algoritmos de caixa-preta.[10] Quanto à segurança dos dados (*Data Security*), levantam-se problemas em matéria de privacidade dos indivíduos e do seu tratamento pela programação. Por último, no que se refere a questões de cibersegurança, revela-se a preocupação sobre as vulnerabilidades na infraestrutura das redes e riscos sistêmicos causados por aplicações maliciosas da IA.

Por outro lado, a Figura 2 compartilhada acima também apresenta algumas aplicações de IA (*Security Applications*) em segurança cibernética que têm demonstrado avanços na detecção e neutralização de *malwares* de forma automática. Sendo assim, a IA pode envolver formas dinâmicas de defesa de elementos maliciosos nas redes a partir do seu potencial de aprendizagem. Algumas empresas já utilizam essas aplicações de IA para segurança cibernética, a exemplo da *Darktrace*, proveniente do Reino Unido, que propõe um método de antivírus inovador que reconhece aspectos de softwares maliciosos sem a necessidade de confiar em uma lista predefinida, já que os métodos tradicionais dependem de ameaças históricas que se baseiam em "assinaturas" de vírus (Babuta *et al.* 2020, 10).

Ademais, torna-se importante apresentar os resultados de entrevistas a especialistas em IA sobre benefícios e malefícios gerais que suas aplicações promovem ao setor militar (Morgan *et al.* 2020). A Figura 3 reflete as principais concordâncias acerca das suas oportunidades, a saber:

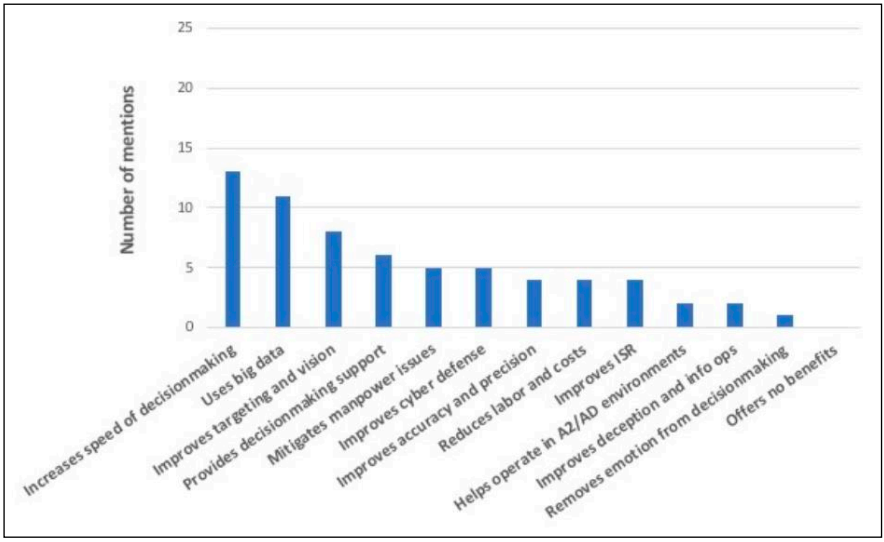


Figura 3 — Benefícios Potenciais de Aplicações Militares de Inteligência Artificial Identificadas nas Entrevistas Estruturadas
Fonte: Morgan et al. 2020, 16.

Dentre elas, destacam-se o aumento da velocidade da tomada de decisão e seu suporte, o uso de *big data*, o aprimoramento da precisão e acurácia de equipamentos, bem como o aperfeiçoamento da segurança cibernética. De fato, a IA é capaz de promover mais eficiência ao fortalecimento da robustez, resposta e resiliência dos sistemas de computadores, conforme assentam Taddeo *et al.* (2019). Na visão dos autores, o primeiro potencial torna o sistema capaz de continuar a se comportar conforme previsto mesmo com estímulos anômalos em seus *inputs*, o que pode reduzir o impacto de ataques de dia-zero, enquanto o segundo significa o aumento da capacidade de autonomia na defesa e em contra-ataques, a exemplo dos *honeypots*. Quanto à resiliência, a IA enriquece a capacidade dos sistemas a suportarem ataques, o que facilita a análise de detecção de ameaças. Tendo em vista essas vantagens táticas e estratégicas, o artigo argumenta que há muita expectativa acerca de suas aplicações à segurança cibernética, porém isso não garante que o sistema se torne totalmente imune a ameaças.

Nessa perspectiva, apresentamos as respostas acerca dos riscos que a IA provoca no ramo militar respondidas pelos especialistas, as quais podem ser conferidas na Figura 4:

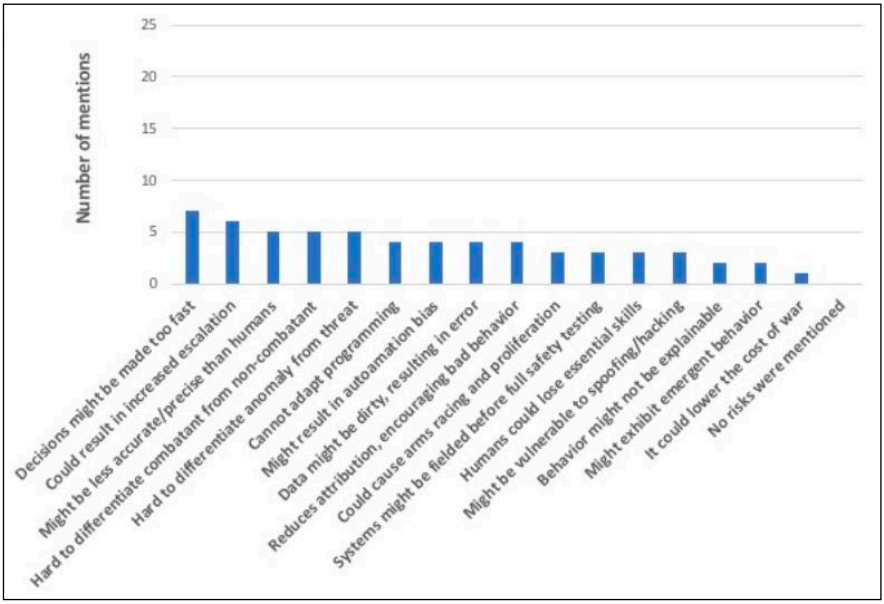


Figura 4 — Riscos das Aplicações Militares da Inteligência Artificial Identificadas nas Entrevistas Estruturadas
Fonte: Morgan et al. 2020, 21

Dentre os riscos mencionados, nota-se o incremento da escalada de conflitos, da corrida armamentista, dos erros surgidos em decorrência da manipulação errada de dados e da vulnerabilidade a *hacking* e a ataques de *spoofing*. Brundage *et al.* (2018) fazem uma análise acerca das ameaças de segurança de IA em três domínios: o digital, físico e político. O relatório menciona a necessidade de tornar os modelos de IA mais maduros a fim de mitigar a sua exploração maliciosa. Além disso, no que concerne aos riscos identificados no âmbito digital, os autores enfatizam o envenenamento de dados (*data poisoning*) e o aprendizado de máquina adversário como possíveis ataques que tentarão acessar os sistemas de forma sorrateira.

Diante dessas oportunidades e desafios, Johnson (2019) argumenta que as características disruptivas da IA podem provocar uma corrida armamentista, especialmente no atual cenário de competição entre a China e os EUA por influência na política internacional. Além disso, as questões de dilema de segurança assinaladas também estimulam Estados a se protegerem por intermédio de um aumento de suas capacidades cibernéticas, sendo a IA uma dessas opções. Com efeito, as suas ferramentas que fortalecem os sistemas de segurança da informação são aliadas importantes no aspec-

to da dissuasão por negação (*defense denial*), o que poderá desestimular o emprego de ataques no ciberespaço. Contudo, para que as tecnologias de IA tenham impacto relevante na segurança cibernética, especialmente em relação à proteção de redes de infraestruturas críticas dos Estados, torna-se fundamental que sejam desenvolvidas políticas coordenadas acerca da exploração da IA na defesa de sistemas de computadores.

CONSIDERAÇÕES FINAIS

Nosso artigo buscou ilustrar algumas das oportunidades que as tecnologias de IA têm proporcionado ao espaço cibernético, sobretudo em relação às expectativas de avanços no combate a *malwares* em uma velocidade e escala notáveis. Entretanto, também foram demonstrados alguns desafios quanto ao desenvolvimento de ataques mais sofisticados às redes de computadores, o que aumenta a complexidade na aferição da relação dos aspectos ofensivos e defensivos nos conflitos cibernéticos.

Quanto às oportunidades promovidas pela IA, mencionou-se a sua capacidade de fortalecer mais robustez, tempo de resposta e resiliência aos sistemas de computadores sobre ameaças do espaço cibernético, na medida em que os seus modelos podem auxiliar na manutenção e resistência dos programas, bem como no combate a anomalias. Quanto aos desafios, por sua vez, identificamos o envenenamento de dados (*data poisoning)* e os ataques de aprendizado adversário (*adversarial-learning attacks)* como riscos que essa tecnologia pode provocar no meio digital, especialmente em relação ao funcionamento de sistemas.

Outrossim, no que concerne à concepção da primazia do ataque ou culto à ofensiva no mundo cibernético, entendemos que esta nem sempre deve ser considerada opção estratégica superior à defensiva, uma vez que os danos causados podem ser muito inferiores ao seu custo material e político. Além disso, sugerimos que os avanços dos modelos e técnicas de IA podem favorecer a segurança dos sistemas em razão de sua eficiência em termos de escala e velocidade no combate a ataques. Diante dessas razões, programas computacionais impulsionados pela IA podem fazer a balança pender para a defesa. Sobre a possibilidade de se investir em políticas cibernéticas retaliatórias como forma de dissuasão, salientamos que essa alternativa pode levar à escalada do dilema de segurança e de conflitos entre os atores.

Nessa esteira, acreditamos que seja necessário tornar os sistemas de IA mais confiáveis (*reliability*) e explicáveis (*explainability*) para garantir que suas tarefas sejam executadas em consonância com o planejado e para permitir que seus processos autônomos de segurança cibernética sejam mais robustos (Taddeo *et al.* 2019) na mitigação de vulnerabilidades e neu-

tralização de ataques. Contudo, isso torna fundamental a implementação de regulamentações e estandardizações profissionais para aqueles que produzem e administram ferramentas com IA, de modo a criar uma cultura padronizada e, por consequência, mais segura acerca do desenvolvimento de suas aplicações.

Em arremate, entendemos que as políticas de ataque e defesa no espaço cibernético tornam indispensáveis a colaboração multissetorial de técnicos, pesquisadores e militares para que as suas formulações sejam coordenadas e estratégicas ao interesse nacional. Além disso, recomendamos que as questões de *compliance* às normas e princípios do Direito Internacional sejam contempladas por intermédio de medidas didático-pedagógicas em conteúdos teórico-práticos, baseadas em conhecimentos de Psicologia, Ética e Sociologia ao longo da formação profissional do combatente virtual.

REFERÊNCIAS

Babuta, Alexander, Marion Oswald, and Ardi Janjeva. 2020. "Artificial Intelligence and UK National Security". *RUSI Occasional Paper*. Royal United Services Institute.

Bastian, Nathaniel D., and Matthew Easley. 2018. "Artificial Intelligence in Cyber Security". Filmed 2018 at CyCON US, Army Cyber Institute. Vídeo, 1:14:22. https://www.youtube.com/watch?v=YEejuT2s5QQ&t=2582s

Battaglia, Rafael. 2020. "Afinal, o que são *deepfakes*?". Revista *Superinteressante*. https://super.abril.com.br/tecnologia/afinal-o-que-sao-deepfakes/.

Boulanin, Vincent, Lora Saalman, Petr Topychkanov, Fei Su, and Moa Carlsson. 2019. *Artificial Intelligence, Strategic Stability and Nuclear Risk*. Solna: SIPRI Publications.

Boulanin, Vincent, and Maaike Verbruggen. 2017. *Mapping the Development of Autonomy in Weapon Systems*. Solna: SIPRI Publications.

Boulanin, Vincent, Neil Davison, Netta Goussac, and Moa Carlsson. 2020. *Limits on Autonomy in Weapon Systems: Identifying Practical Elements of Human Control*. Solna: SIPRI Publications.

Brasil. Ministério da Ciência, Tecnologia e Inovações. 2019. "Estratégia Brasileira de Inteligência Artificial". www.mctic.gov.br/mctic/opencms/inovacao/paginas/politicasDigitais/Inteligencia/Artificial.html.

_____. 2020. "Decreto nº 10.222, de 5 de fevereiro de 2020". Diário Oficial da União (DOU). http://www.in.gov.br/web/dou.

Brundage, Miles, *et al.* 2018. *The Malicious Use February 2018 of Artificial Intelligence: Forecasting, Prevention, and Mitigation.* https://maliciousaireport.com/.

Buchanan, Ben. 2017. *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations.* New York: Oxford University Press.

Buzan, Barry, Ole Wæver, and Jaap de Wilde. 1998. *Security: A New Framework for Analysis.* Boulder: Lynne Rienner.

Cavelty, Myriam Dunn. 2008. *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age.* London: Routledge.

_____. 2012. "The Militarization of Cyber Security as a Source of Global Tension". *Cyber Security* 22: 103–24.

Coady, C.A.J. 2012. The Jus Post Bellum. In *New wars and new soldiers: military ethics in the contemporary world*, edited by P. Tripodi, and J. Wolfendale. Farnham: Ashgate

Ferdinando, Lisa. 2018. "Cybercom to Elevate to Combatant Command". U.S. Department of Defense. www.defense.gov/Explore/News/Article/Article/1511959/cybercom-to-elevate-to-combatant-command/.

Future of Life Institute. 2020. "National and International AI Strategies". *Future of Life Institute Organization.* https://futureoflife.org/national-international-ai-strategies/.

Garfinkel, Ben, and Allan Dafoe. 2019. "How does the offense-defense balance scale?". *Journal Of Strategic Studies* 42, no. 6: 736–63. http://dx.doi.org/10.1080/01402390.2019.1631810.

Glaser, Charles L., and Chaim Kaufmann. 1998. "What is the Offense-Defense Balance, and Can We Measure it?". *International Security* 22, no. 4: 44–82.

Hansen, Lene, and Helen Nissenbaum. 2009. "Digital Disaster, Cyber Security, and the Copenhagen School". *International Studies Quarterly* 53, no. 4: 1155–75.

Jervis, Robert. 1978. "Cooperation under the Security Dilemma". *World Politics* 30, no. 2: 167–214.

Johnson, James. 2019. "The AI-Cyber Nexus: Implications for Military Escalation, Deterrence and Strategic Stability". *Journal of Cyber Policy* 4, no. 3: 442–60.

Kania, Elsa B. 2019. "Chinese Military Innovation in the AI Revolution". *The RUSI Journal* 164, no. 5–6: 26–34.

Kania, Elza, Dahlia Peterson, Lorand Laskai, and Graham Webster. 2019. "Translation: Key Chinese Think Tank's 'AI Security White Paper' (Excerpts)". *New America.* http://newamerica.org/cybersecurity-initiative/digichina/blog/translation-key-chinese-think-tanks-ai-security-white-paper-excerpts/.

Kello, Lucas. 2013. "The Meaning of Cyber Revolution. Perils to Theory and StateCraft". *International Security* 38, no. 2: 7–40.

Krepinevich, Andrew. 1994. "Cavalry to Computer: The Pattern of Military Revolutions". *National Interest* 37: 29–40. https://nationalinterest.org/article/cavalry-to-computer-the-pattern-of-military-revolutions-848?page=0%2C2.

Kuehl, Dan. 2009. "From Cyberspace to Cyberpower: Defining the Problem". In: *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry Wentz: 24–42. Washington D.C.: National Defense University Press.

Lacy, Mark, and Daniel Prince. 2018. "Securitization and the global politics of cybersecurity". *Global Discurse* 8, no. 1: 101–15.

Libicki, Martin C. 2009. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND

Liff, Adam. 2012. "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War". *Journal of Strategic Studies* 35, no. 3: 401–28.

Liivoja, Rain, Maarja Naagel, and Ann Väljataga. 2019. "Autonomous Cyber Capabilities Under International Law". *NATO CCDCOE Publications.* https://ccdcoe.org/library/publications/autonomous-cyber-capabilities-under-international-law/

Lin, Herbert. 2016. "Governance of Information Technology and Cyber Weapons". *Governance of Dual-Use Technologies: Theory and Practice*, edited by Elisa D. Harris: 112–58. American Academy of Arts & Sciences.

Lynn, William J. 2010. "Defending a New Domain: The Pentagon's Cyberstrategy". *Foreign Affairs* 89, no. 5: 97–108.

Maness, Ryan C., and Brandon Valeriano. 2016. "The Impact of Cyber Conflict on International Interactions". *Armed Forces & Society* 42, no. 2: 301–23.

Medeiros, Breno P., Alessandra C. Carvalho, and Luiz R. F. Goldoni. 2019. "Uma análise sobre o processo de securitização do ciberespaço". *Coleção Meira Mattos* 13, no. 46: 45–66.

Morgan, Forrest E., Benjamin Boudreaux, Andrew J. Lohn, Mark Ashby, Christian Curriden, Kelly Klima, and Derek Grossman. 2020. *Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World*. Santa Monica: Rand Corporation.

Muggah, Robert, Misha Glenn, and Gustavo Diniz. 2014. "Securitização da cibersegurança no Brasil". *Cadernos Adenauer* 15, no. 4: 69–109.

Nye, Joseph S. 2010. *Cyber Power*. Cambrige: Belfer Center for Science and International Affairs.

_____. 2017. "Deterrence and Dissuasion in Cyberspace". *International Security* 41, no. 3: 44–71.

Rid, Thomas. 2012. "Cyber War Will Not Take Place". *Journal of Strategic Studies* 35, no. 1: 5–31.

Schneider, Jacquelyn. 2019. "The Capability/Vulnerability Paradox and Military Revolutions: Implications for Computing, Cyber, and the Onset of War". *Journal of Strategic Studies* 42, no. 6: 841–63.

Schneier, Bruce. 2018. "Artificial Intelligence and the Attack/Defense Balance". *IEEE Security & Privacy* 16, no. 2: 96-96. Institute of Electrical and Electronics Engineers (IEEE).

Shires, James, and Max Smeets. 2017. *Contesting "Cyber"*. Washington: New America.

Slayton, Rebecca. 2017. "What is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment". *International Security* 41, no. 3: 72–109.

Stone, John. 2013. "Cyber War Will Take Place!". *Journal of Strategic Studies* 36, no. 1: 101–8.

Taddeo, Mariarosaria. 2018, "How to Deter in Cyberspace". *The European Centre of Excellence for Countering Hybrid Threats* 6: 1–10.

Taddeo, Mariarosaria, Tom Mcctcheon, and Luciano Floridi. 2019. "Trusting artificial intelligence in cybersecurity is a double-edged sword". *Nature Machine Intelligence* 1, no. 12: 557–60.

Teixeira Júnior, Augusto, Gills Villar-Lopes, and Marco T. Freitas. 2017. "As três tendências da guerra cibernética: novo domínio, arma combinada e arma estratégica". *Revista Carta Internacional* 12, no. 3: 30–53.

Thornton, Rod, and Marina Miron. 2020. "Towards the 'Third Revolution in Military Affairs': The Russian Military's Use of AI-Enabled Cyber Warfare". *The RUSI Journal*: 1–10 (Maio).

Turing, A. 1950. "Computing Machinery and Intelligence". *Mind, New Series* 59, no. 236: 433–60.

Wæver, Ole. 1995. "Securitization and Desecuritization". In *On Security*, edited by Ronnie Lipschutz. New York: Columbia University Press.

Wæver, Ole, Barry Buzan, Morten Kelstrup, and Pierre Lemaitre. 1993. *Identity, Migration and the New Security Agenda in Europe*. London: Pinter.

Whyte, Christopher. 2020. "Problems of Poison: New Paradigms and 'Agreed' Competition in the Era of AI-Enabled". 12th International Conference on Cyber Conflict. *NATO CCDCOE Publications*.

NOTAS

1. Neste artigo, consideramos a proposta de Kuehl (2009) para atribuir significado ao espaço cibernético. Utilizamos também a concepção de Smeets e Shires (2017), que trazem uma perspectiva acerca de como o entorno dos avanços da interconectividade de sistemas de computadores passou de um entusiasmo inicial de mundo sem fronteiras para um ambiente de constantes ameaças, crimes e espionagem.
2. Alan Turing é amplamente considerado como o pioneiro na criação de sistemas inteligentes, os quais teriam capacidade de substituir os seres humanos em algumas atividades. A partir de um jogo de imitação, Turing (1950) investiga a capacidade de uma máquina de responder a certas perguntas da mesma forma que um indivíduo. Devido aos rápidos avanços da computação neste aspecto, sobretudo em relação aos programas de aprendizagem de máquina (*machine learning)* e aprendizagem profunda (*deep learning)*, capazes de processar e identificar padrões em um grande volume de dados, adotamos o conceito geral de que IA constitui uma série de aplicações que reproduzem tarefas que geralmente requerem inteligência humana (Morgan *et al.* 2020).
3. Maness e Valeriano (2016) argumentam que o ataque de negação de serviços é um dos únicos métodos sorrateiros que afetam as dinâmicas de relações internacionais, na medida em que tem um efeito psicológico e público na sociedade conectada que exige uma resposta Estatal coordenada. No caso da Estônia (2007), sites oficiais do governo, da mídia e de bancos ficaram fora do ar, bem como diversas difamações foram direcionadas ao Primeiro Ministro. Apesar de a origem dessas ofensivas ser atribuída à Rússia, ela permanece desconhecida.
4. A autora não utiliza o termo Revolução dos Assuntos Militares (RAM) em razão de não querer se comprometer com as políticas de defesa específicas que o conceito, muito em voga nos anos 90 e 2000, exigem (Schneider 2019, 844). Dessa forma, prefere utilizar a expressão genérica de Revolução Militar para categorizar a potencialidade dessas tecnologias em promover transformações no setor.
5. De acordo com Boulanin e Verbruggen (2017, 16), aprendizagem de máquina é um método de IA capaz de executar mudanças em sua estrutura, programa ou dados de acordo com os insumos recebidos, motivo pelo qual é esperado que a sua performance tenha um melhor desempenho à medida que seu funcionamento avance. A aprendizagem profunda, por seu turno, é um tipo de aprendizagem de máquina que transforma os dados brutos em representações. Por exemplo, esta se refere a técnicas de reconhecimento facial, enquanto a primeira se relaciona com artefatos que fazem reconhecimento de voz.
6. *Deepfake* é uma aplicação da tecnologia de IA de *deep learning* capaz de manipular o conteúdo de vídeos de tal modo que torna muito difícil de serem desmascarados (Battaglia 2020).

7. Whyte (2020) afirma que o termo aprendizado adversário se refere a algoritmos de modelos de aprendizado de máquina (*machine learning*) capazes de se adaptar em diferentes ambientes hostis de sistemas de computadores. Um *malware* desenvolvido com essa aplicação poderia perturbar os dados de entrada nos sistemas, o que causaria problemas de falsos positivos ou negativos, por exemplo.
8. Do original: "the ratio of the cost of the forces the attacker requires to take territory to the cost of the forces the defender has deployed. That is, if the defender invests X in military assets, how large an investment Y must the attacker make to acquire the forces necessary for taking territory? The offense-defense balance is the ratio Y/X. Larger ratios indicate a balance more in favor of defense" (Glaser and Kaufmann 1998, 3).
9. A ideia de que a ofensiva é mais vantajosa em relação à defesa é compartilhada não apenas entre acadêmicos, mas também por militares e políticos, a exemplo do Ex Secretário de Defesa William Lynn, em 2010, o qual demonstra que os EUA não devem utilizar uma postura defensiva (o autor faz alusão à Linha Maginot, Estratégia defensiva francesa que fracassou na Segunda Guerra mundial) e que a ofensiva é superior (Lynn 2010).
10. O problema relacionado à caixa preta (*black box problem*) dos algoritmos se insere no contexto de que a complexidade de seus sistemas não oferece explicações plausíveis acerca dos caminhos percorridos ao encontro dos seus resultados. À medida que se ampliam as aplicações desse tipo de IA na vida cotidiana, há uma crescente preocupação sobre o direito dos indivíduos a uma explicação do processo de tomada de decisão algorítmica, e a respeito da confiabilidade do modelo pelos operadores.

ARMAS INTELIGENTES NO CIBERESPAÇO: OPORTUNIDADES INOVADORAS E DESAFIOS PREMENTES

RESUMO

A característica disruptiva e inovadora da Inteligência Artificial (IA) tem provocado uma miríade de benefícios e especulações em múltiplos setores da sociedade, em especial no militar. O presente artigo busca trazer à tona o debate das oportunidades e desafios que a IA pode promover em relação a ataques e à segurança no espaço cibernético. Com efeito, argumenta-se que essa nova modalidade de capacidade cibernética possui a característica de faca de dois gumes: se, por um lado, o processamento rápido de grande volume de dados e o reconhecimento de padrões pela programação computacional podem ser grandes aliados na antecipação e combate de ameaças a redes, por outro, novas vulnerabilidades exigem cautela em sua operacionalização. Em termos metodológicos, foi realizada revisão bibliográfica e documental de abordagens sobre a interseção da inteligência artificial no ramo da segurança e defesa cibernética. Além disso, nosso arcabouço teórico debruça-se sobre alguns conceitos das Relações Internacionais, em especial o da Teoria da Balança Ofensiva-Defensiva Cibernética para elucidar como as capacidades dessa tecnologia podem influenciar na dissuasão e favorecimento da defesa em detrimento da primazia do ataque.

Palavras-chave: Ciberataque; Defesa Cibernética; Vulnerabilidade Cibernética; Inteligência Artificial.

ABSTRACT

The disruptive and innovative feature of Artificial Intelligence (AI) has provoked a myriad of benefits and speculation in multiple sectors of society, especially in the military. This article seeks to bring up the debate about the opportunities and challenges that AI can promote in relation to cyberattacks and cybersecurity. Indeed, it is argued that this new type of cyber capability has a double-edged sword feature: if, on the one hand, the rapid processing of large volumes of data and the recognition of patterns by computer programming can be great allies in anticipation and combating network threats, on the other hand, new vulnerabilities require caution in their operation. In methodological terms, a bibliographic and documentary review of approaches on the intersection of artificial intelligence in the field of cyber security and defense were carried out. In addition, our theoretical framework focuses on some concepts of International Relations, especially that of the Theory of Cyber-Offensive-Defensive Balance to elucidate how the capabilities of this technology can influence deterrence and favoring defense over the primacy of attack.

Keywords: Cyberattack; Cyberdefense; Cyber Vulnerability; Artificial Intelligence.

Recebido em 01/07/2020. Aceito para publicação em 20/04/2021.

Ensaio

Por que o Brasil deveria adotar uma *distro* Linux própria?

Why should Brazil adopt its own Linux distro?

Rev. Bras. Est. Def. v. 7, nº 2, jul./dez. 2020, p. 161-183
DOI: 10.26792/RBED.v7n2.2020.75248
ISSN 2358-3932

MARCELO ANTONIO OSLLER MALAGUTTI
RICARDO BORGES GAMA NETO

INTRODUÇÃO

Este trabalho analisa o uso de software de código aberto, em particular distribuições Linux, por motivação de segurança e defesa. É utilizado o método descritivo, do tipo *associations* (Gerring 2012, 721–46). Primeiro descrevemos as características do objeto de estudo, concentrando nas condições prevalentes e subjacentes as unidades de análise. A pesquisa é associada a estudos de caso de nações comumente apontadas como superpotências cibernéticas (EUA, China, Rússia e Coreia do Norte) e também de potências regionais relevantes (Índia, Turquia e Coreia do Sul). O argumento é que a maior parte dos casos aponta que a adoção do Linux ocorre por questões de segurança e defesa. A introdução de sistemas operacionais (SO[1]) de código aberto se dá pelo receio de imposição de restrições ao acesso a tecnologias e/ou uso de *backdoors* ou exploração de falhas do tipo *zero-day*. Por esta razão defendemos que o Brasil deve adotar a mesma estratégia, selecionar uma *distro* Linux para emprego em sistemas associados à defesa. Dessa forma pode-se reduzir os riscos de dependência tecnológica em cibernética e tecnologia da informação (TI).

O trabalho foi dividido da seguinte forma: esta introdução, depois uma brevíssima conceituação sobre software aberto e um pequeno histórico do Linux, seguido do contexto histórico do desenvolvimento da TI, riscos postos pela dependência tecnológica externa, exemplos de adoção do uso do Linux por forças armadas e governos de diferentes países, recomendações e argumentos exortando o Ministério da Defesa a adotar uma me-

Marcelo Antonio Osller Malagutti — Doutor em Ciências Militares pela Escola de Comando e Estado-Maior do Exército; Mestre em War Studies pelo King's College London.
Ricardo Borges Gama Neto — Professor Doutor do Departamento de Ciência Política da Universidade Federal de Pernambuco.

ta-distribuição para o desenvolvimento de um Linux nacional. Por fim, a conclusão e as referências bibliográficas.

SOFTWARE ABERTO

Historicamente, a contratação de softwares era realizada de duas maneiras distintas: pela contratação do desenvolvimento sob especificação do cliente, ajustada às suas necessidades; e pela aquisição de licenças e serviços associados. Com o passar dos anos, novas formas de uso de software foram criadas por *novos entrantes* na busca pela abertura de mercados entre fornecedores já consolidados. Alguns softwares passaram a ter seus executáveis distribuídos gratuitamente (*freeware*) ou licenciados a preços irrisórios (*shareware*).

No início dos anos 1980, a ARPANET, precursora da Internet, ainda engatinhava, com menos de 1.000 servidores conectados, e restrita a militares e pesquisadores de universidades e centros de pesquisa (Rid 2016, 190). Não obstante, o usuário comum já podia *discar* (utilizando um modem) para uma Bulletin Board Service (BBS) e *baixar* softwares. Em alguns casos até mesmo software *pirata* (o mercado negro sempre existiu). Posteriormente evoluiu-se para iniciativas denominadas de software aberto (*Open Source Software*, OSS), cujo código-fonte, e não apenas seus executáveis, eram disponibilizados para usuários licenciados. OSS também é conhecido como software livre (*free*), mas não no sentido de que não tenha custo. O *livre* do nome advém da liberdade do usuário de não depender do fornecedor, e não necessariamente da *gratuidade* do uso (U.S. DoD n.d.).

O conceito de OSS é frequentemente confundido pelo grande público com aquele de software grátis (U.S. DoD n.d.). Em grande medida, pelo fato de que boa parte do OSS é, de fato, disponibilizada sem a cobrança de taxas de licenciamento e, portanto, sem custos. Mas OSS não é necessariamente *freeware*, que embora gratuito, não precisa ser aberto. De fato, dezenas de *freewares* são distribuídos apenas na forma de seus executáveis, verdadeiras *caixas-pretas* que podem implicar riscos à segurança dos dados e dispositivos de seus usuários. OSS, embora aberto, não necessariamente significa gratuito. É perfeitamente possível que o software OSS seja licenciado ao usuário por meio da cobrança de serviços associados (tipicamente treinamento e suporte).

Para fins legais e de aquisição, o governo dos EUA define OSS como "software para o qual o código fonte legível por humanos está disponível para uso, estudo, reutilização, modificação, aprimoramento e redistribuição pelos usuários desse software" (Wennergren 2009). Seja o software comercial (licenciamento pago) ou não (U.S. DoD n.d.).

Cada um desses tipos de software possui um modelo de negócios distinto. *Freewares* em geral são patrocinados por anúncios publicitários (*advertisements* ou *ads*) apresentados durante a utilização do software, e geralmente associados à *invasão de privacidade* dos usuários. Por vezes, alternativamente ou complementarmente, cobram seu preço por meio da captura e revenda de informações privilegiadas dos usuários, para uso em ações frequentemente não éticas ou legais. Já o OSS, em geral tem diferentes formas de rentabilização. Software comercial é remunerado pela venda de licenças, bem como dos serviços associados. Mas seu código aberto aufere transparência ao fornecedor, e ao cliente a percepção de liberdade e independência daquele fornecedor (o *livre* acima mencionado). Quando o OSS é licenciado sem custos, a remuneração pode se dar por meio da prestação dos serviços associados. Uma terceira forma de remuneração pode ser o licenciamento de *add-ins* ou *versões profissionais*: em sua versão básica é gratuito, mas incrementos de funcionalidades são licenciados comercialmente[2].

Dentre os muitos Softwares Abertos disponíveis no mercado, destaca-se o Linux, SO concorrente do Microsoft Windows e do Mac OS X, que além de aberto é também de licenciamento gratuito.

UMA (MUITO BREVE) HISTÓRIA DO LINUX

A origem do Linux está associada ao Unix. Em fins dos anos 1960, o Bell Labs, que fazia parte da AT & T, iniciou o desenvolvimento de um SO para uso em minicomputadores PDP-7 da Digital Equipment Corporation. Sua migração, em fins dos anos 1970, para o modelo PDP-11, confirmou o que viria a ser um dos pontos-fortes do Unix: a portabilidade para diferentes tipos de equipamentos (Hosch 2008b).

Em meados dos anos 1970 um dos projetistas temporariamente se afastou do projeto para lecionar na Universidade da Califórnia em Berkeley. Professores e alunos passaram a realizar incrementos ao sistema original, desenvolvendo uma nova versão que se tornou também popular, o Berkeley Software Distribution (BSD). Paralelamente o trabalho continuava no Bell Labs, e em 1983 foi finalizada a versão Unix System V (Hosch 2008b). Posteriormente essas *distros* foram unificadas em diferentes versões produzidas por diversas companhias para seus minicomputadores: Solaris da Sun Microsystems; IRIX da Silicon Graphics; HP-UX da HP; AIX da IBM, dentre outras.

As características do Unix interessaram também ao mercado de microcomputadores. Em fins dos anos 1970 a Microsoft licenciou junto à AT&T a comercialização do sistema, e por anos foi a maior distribuidora do Unix, fosse seu próprio Xenix, ou outras denominações (*distros*) da Siemens,

Santa Cruz Operation (SCO) e "dúzias e dúzias de sublicenciados" (Gates 1996). Dificuldades comerciais com a AT&T levaram a Microsoft a vender o Xenix para a SCO, que o comercializou até 2007 sob o nome SCO Unix, e a focar no desenvolvimento do Windows NT, com arquitetura muito influenciada pelas características do Unix (Gates 1996). Do Unix FreeBSD derivou o Rhapsody DR2, base do Mac OS X da Apple, do qual descende o iOS que opera nos iPhones e iPads (Singh 2007, 32).

A guinada do Unix para OSS se deu com o advento do Linux, um k*ernel* (núcleo) Unix inteiramente reescrito, cuja primeira versão data de 1994. No mesmo período a Free Software Foundation (FSF) desenvolvia esforços para o desenvolvimento do GNU, um sistema baseado no Unix, mas de código aberto. Conquanto o Linux tivesse iniciado pelo núcleo do sistema, o GNU iniciou-se pela criação de utilitários do sistema. Esses utilitários foram então incorporados ao Linux criando o GNU/Linux, popularizado apenas pelo nome do núcleo (Hosch 2008a). Inicialmente, por ter uma interface gráfica menos amigável que a do Microsoft Windows ou do Mac OS, embora sendo mais confiável e robusto a falhas, o uso do Linux ficou mais restrito a servidores corporativos e da Internet. No entanto, sendo de código aberto, o sistema foi sendo adaptado por diferentes fabricantes, criando novas *distros*, como no caso da SUSE (antes Novell Linux), Red Hat, Debian e Slackware (Hosch 2008a). A incorporação de interfaces mais amigáveis (Gnome, KDE, WindowMaker), de servidores web e de aplicações foi tornando o sistema mais popular. O Android, da Google, que hoje equipa a maior parte dos smartphones, derivou de modificações no *kernel* original do Linux.

A IMPORTÂNCIA DA INFORMÁTICA PARA A DEFESA E SEGURANÇA NACIONAIS

A inteligência de comunicações sempre desempenhou papel relevante em questões de segurança e defesa. *Signals Intelligence* (SIGINT) tornou-se cada vez mais relevante com a popularização das telecomunicações, e ainda mais importante para os militares. Em Bletchley Park, em 1941, Alan Turing e sua equipe criaram a *Bombe*, o primeiro computador da história, ainda que eletromecânico, que ajudou a decifrar o código Enigma, utilizado pelas forças armadas nazistas. No mesmo local, a equipe de Tommy Flowers criou o Colossus Mark I, o primeiro computador eletrônico, de 1943, que decifrou o ultrassecreto código Lorenz. Ambas foram ativos importantes para a vitória na Segunda Guerra Mundial (GCHQ 2016).

Não apenas para SIGINT o uso de processamento automatizado de informações foi relevante para os militares. Em 1943 o exército ameri-

cano encomendou à Universidade da Pensilvânia o desenvolvimento de uma máquina capaz de computar alvos balísticos, resultando no desenvolvimento do ENIAC, o primeiro computador eletrônico programável, entregue em 1946. O medo da repetição da *blitz* (bombardeio de Londres durante a WWII) em território norte-americano levou à criação do Semi-Automatic Ground Environment (SAGE), integrando centenas de estações de radar com processamento em 23 supercomputadores distribuídos pelos EUA, cujo protótipo foi demonstrado já em 1951 (Rid 2016, 76–7). O sistema foi contratado à IBM, que utilizava linhas de comunicação comerciais da AT&T para integrar toda a rede, que em 1958 foi centralizada no mítico North-American Air Defense Command (NORAD) no Colorado, ao custo total (em 15 anos) de mais de 500 bilhões de dólares em valores atuais (Rid 2016, 76–7). Similarmente, por meio da Advanced Research Projects Agency (ARPA), o Pentágono custeou o desenvolvimento da ARPANET, a "famosa precursora da Internet" (Rid 2016, 111). O objetivo era melhorar sistemas de comando e controle militares e prover redundância de rotas em casos de falhas de algum nó da rede (Rid 2016, 147).

No Brasil o desenvolvimento da informática também esteve ligado a interesses militares. Foi por influência das ideias do Capitão de Corveta Geraldo Maia, que retornara dos EUA, que o Conselho de Desenvolvimento Nacional do Governo Juscelino Kubitscheck propôs a criação de um grupo para avaliar o uso de computadores (Moreira 1995, 24). No ano seguinte, a equipe tornou-se o Grupo Executivo para Aplicação de Computadores Eletrônicos (GEACE), e autorizou a importação dos três primeiros computadores brasileiros: um para a Pontifícia Universidade Católica do Rio de Janeiro; um para o Instituto Brasileiro de Geografia e Estatística; e um para a Listas Telefônicas Brasileiras (Moreira 1995, 23).

Em 1972 criou-se a Coordenação das Atividades para o Processamento Eletrônico de Dados (CAPRE), vinculada ao Ministério do Planejamento (Moreira 1995, 24; Figueiredo 1986, 288; Tonooka 1992, 274–6). À CAPRE foi atribuída a responsabilidade pelo desenvolvimento de uma política nacional de informática, e uma de suas primeiras determinações foi a restrição à importação de hardware estrangeiro por instituições governamentais (Moreira 1995; Figueiredo 1986; Tonooka 1992, 274–78). Iniciava-se uma Reserva de Mercado que duraria 20 anos. Em 1979 a CAPRE foi substituída pela Secretaria Especial e Informática (SEI), vinculada então ao Conselho de Segurança Nacional, e fortemente influenciada pelo Serviço Nacional de Informações (SNI) (Moreira 1995, 28–9; Tonooka 1992).

Em 1984, implementou-se a Lei de Informática[3]. Esta estabeleceu a Política Nacional de Informática, pela qual somente produtos *Made in*

Brazil (ou estrangeiros autorizados) poderiam ser comercializados. A ideia era a de se criar um mercado visando o desenvolvimento de uma indústria nacional que pudesse ser competitiva internacionalmente. O modelo adotado baseava-se em três pilares: capacitação de pessoal; estímulo ao investimento privado; e numa empresa estatal, a Computadores Brasileiros (COBRA). Contudo, tais esforços foram infrutíferos, e até mesmo contraproducentes, dado que submeteram o país a um considerável atraso na adoção de novas tecnologias que rapidamente emergiam no mercado externo, mas que não entravam no Brasil e dos elevados valores que os usuários nacionais pagavam pelos produtos nacionais comparados aos preços internacionais (Moreira 1995; Tonooka 1992). Em 1993, com o fim da reserva de mercado, as empresas brasileiras optaram pelo licenciamento de produtos estrangeiros.

RISCOS DA DEPENDÊNCIA TECNOLÓGICA EM TI

Backdoors

Uma das maiores preocupações com a utilização de ativos importados é a existência de *backdoors* (portas dos fundos) desconhecidas que possam ser utilizadas contrariamente aos interesses dos clientes. Já em 2001, autoridades de inteligência dos EUA acreditavam que "certos equipamentos importados" estavam infectados com dispositivos capazes de "ler dados ou destruir sistemas" (Adams 2001). Posteriormente, hardware falsificado foi identificado em sistemas adquiridos pelo Departamento de Defesa dos EUA (Lynn 2010). Um relatório do Comitê Permanente de Inteligência da Câmara dos EUA, em 2012, recomendou restrições à aquisição de equipamentos de rede das empresas chinesas Huawei e ZTE por órgãos do governo americano e seus contratados, devido à possibilidade de vazamento de informações sigilosas por meio de *backdoors* (Banach 2012).

No Caso Snowden revelou-se que a empresa norte-americana Cisco, maior fabricante mundial de ativos de rede, tinha seus roteadores e servidores interceptados e manipulados pela National Security Agency (NSA), sem no entanto haver evidências de que a empresa estivesse envolvida (Greenwald 2014, 142). Em dezembro de 2015, a Juniper Networks, segunda maior fabricante de ativos de rede do mundo, anunciou a descoberta de uma *backdoor* secreta em seus *firewalls* (Zetter 2015). Posteriormente, a Cisco confirmou que uma vulnerabilidade *zero-day*[4] fora explorada por software ligado à NSA durante anos (Goodin 2016). Ao menos outras oito *backdoors* foram encontradas pela Cisco em 2017 e 2018 (Cisco n.d.; Cimpanu 2018).

Nem mesmo empresas de países tradicionalmente neutros são insuspeitas. Recentemente revelou-se que a suíça Crypto AG, fabricante de criptógrafos utilizados em mais de 120 países pertenceu, entre 1970 e 2018, a uma parceria altamente secreta da CIA com o serviço de inteligência alemão BND, e que os equipamentos vendidos pela companhia eram sabotados para que aquelas agências tivessem acesso às informações neles criptografadas AG (Miller 2020).

O governo norte-americano acusa a Huawei, líder mundial em telefonia 5G, de possuir ligações obscuras com a inteligência chinesa. Os EUA também pressionaram seus aliados a vetarem o uso de tecnologia chinesa de 5G. Em maio o Reino Unido anunciou a proibição da empresa atuar naquele país. Os EUA argumentam preferir o uso de equipamentos da sueca Ericsson e da finlandesa Nokia, mesmo que mais caros, e personalidades do governo dos EUA até sugeriram a aquisição do controle acionário dessas empresas (Kharpal 2020).

Classificação de Itens como *Tecnologias Sensíveis*

Desde 2015 a Intel foi impedida pelo governo dos EUA de revender para a China seus processadores mais modernos, sob o argumento de que os mesmos seriam utilizados para testes nucleares (Clark 2015). Em 2018 os EUA reassumiram a liderança da lista de supercomputadores, pertencente anteriormente a China, e nela permaneceram com os dois maiores equipamentos até fins de 2020, quando foram superados pelos Japoneses (TOP500.org n.d.). A diferença dos processadores americanos e chineses se reflete nos números. Enquanto o Sierra, dos EUA, atinge 200 PFLOPS[5] com 2,4 milhões de núcleos (*cores*) e consome 10MW de energia, o chinês TaihuLight, duas posições atrás, utilizando processadores chineses, atinge 125 PFLOPS com 10,6 milhões de núcleos e consome 15MW (TOP500.org n.d.).

Após a proibição de uso de componentes norte-americanos pela Huawei em 2019, a gigante chinesa passou a trabalhar pela substituição desses componentes por versões chinesas (Strumpf 2020). Mas mesmo essa estratégia ficou ameaçada quando o Departamento de Comércio dos EUA subiu o tom em maio de 2020 e proibiu que fabricantes de componentes de todo o mundo, que utilizem tecnologia norte-americana, vendam produtos à Huawei (U.S. Dept. of Commerce 2020). Essa nova dificuldade pode mesmo tirar a empresa da posição dominante na corrida pelo 5G, e mesmo prejudicar a manutenção de redes de telefonia de outras gerações fornecidas pela empresa e já em uso em diversos países (Strumpf 2020).

Os EUA ainda consideram bloquear o fornecimento de tecnologia norte-americana para cinco empresas chinesas de vigilância por vídeo (Shidong 2019).

O Brasil também enfrenta dificuldades na importação de computadores e outros materiais *sensíveis*, e até na compra de computadores *Made in Brazil* por empresas americanas beneficiadas por isenções fiscais do governo brasileiro (Angelo 2007). O maior supercomputador brasileiro está ranqueado na posição 192 da lista, com 1,9 PFLOPS (TOP500.org n.d.).

Restrições ao uso não se referem apenas a hardware, mas também a software. O banimento imposto pelo governo dos EUA à Huawei impede que a Google licencie o uso do SO Android em aparelhos telefônicos da empresa (Moon 2019). Ainda que o núcleo do mesmo seja de código aberto, e assim possa continuar a ser usado pela empresa chinesa, diversos serviços associados são fornecidos pela Google e deixariam de estar disponíveis, limitando a utilidade dos smartphones (Moon 2019).

Em meio ao embargo dos EUA a fornecimento de tecnologia para a China, Pequim ordenou a todos os escritórios governamentais e instituições públicas que removam equipamentos e softwares estrangeiros até 2022 (Yang and Liu 2019). A medida faz parte de uma campanha para reduzir a dependência chinesa de tecnologias estrangeiras, provavelmente terá um efeito de *desacoplamento* das cadeias de fornecimento dos EUA e China, e pode representar um duro golpe para empresas estadunidenses (Yang and Liu 2019). As novas sanções impostas acrescentaram urgência ao projeto, diferentemente dos esforços anteriores por autossuficiência em tecnologia, e seu objetivo é que no futuro próximo as empresas e o governo estejam livres de ameaças (Yang and Liu 2019).

Mas a substituição de hardware e software norte-americano por equivalentes chineses também apresenta problemas. A chinesa Lenovo utiliza processadores fabricados pela Intel e discos rígidos produzidos pela sul-coreana Samsung (Yang and Liu 2019). A China fica atrás dos EUA em algumas das tecnologias mais avançadas, incluindo design e fabricação de chips. Os principais componentes usados por algumas das maiores empresas de tecnologia do país são fabricados pela Intel ou pela Qualcomm. Os SO mais usados em dispositivos produzidos na China são Google Android, em smartphones e tablets, ou Microsoft Windows, em computadores (Shidong 2019).

EXEMPLOS DE ADOÇÃO DO LINUX

Em princípios dos anos 2000, governos e empresas pelo mundo se preocupavam com a possibilidade de que o uso de OSS os abrisse para *bugs*, brechas de segurança e, consequentemente, ações judiciais. Mas, apesar

desses medos iniciais, o código aberto passou a dominar o cenário digital (Finley 2016). Hoje, praticamente todas as principais tecnologias com as quais interagimos diariamente - da *Web* ao telefone e ao carro - foram construídas usando pelo menos alguma forma de OSS, muitos deles gratuitos (Finley 2016).

Estados Unidos

Em 2003 o Departamento de Defesa dos EUA (DoD) encomendou uma pesquisa à MITRE Corporation[6] sobre o uso de OSS em sistemas de defesa (MITRE 2003). Essa pesquisa mostrou que diversos OSS já eram utilizados, e apontou sugestões para sua institucionalização. Em 2009, o DoD emitiu uma diretiva sobre o uso de OSS, dando preferência ao mesmo dentro de regras bem estabelecidas (Wennergren 2009). Em 2016 a Casa Branca lançou sua primeira política oficial de código fonte, detalhando um programa que exige que as agências governamentais liberem como software de código aberto 20% de qualquer novo código que encomendarem, o que significa que o mesmo estará disponível para qualquer um examinar, modificar e reutilizar em seus próprios projetos (Scott and Rung 2016). As agências governamentais também compartilharão códigos entre si, adotando essencialmente práticas de OSS em seu próprio universo governamental (Scott and Rung 2016). Agências como a NASA e o serviço postal (USPS) estão entre os grandes usuários.

Embora tendo sido precursor no uso de OSS, o Pentágono não atendeu ao estipulado pela política governamental (Eversden 2019). Ainda assim, o uso de OSS pelos militares dos EUA se intensifica, e aqui destacamos exemplos emblemáticos.

A novíssima classe de destroieres USS Zumwalt incorporou Linux Red Hat em seus sistemas de navegação, manutenção, armamentos e monitoração (Gallagher 2013). Sistemas originalmente não construídos para serem conectados a uma rede IP são integrados por meio de processadores de adaptação distribuídos (DAPs). Tais adaptadores são computadores de placa única usando o Lynx RTOS (Real Time Operating System), uma *distro* de Linux para dispositivos e sensores em tempo real, que conectam à rede dispositivos da embarcação, como sistemas de engenharia e de combate a incêndio, lançadores de mísseis e equipamentos de comunicação de rádio e satélite, para que possam ser controlados por aplicativos na rede (Gallagher 2013; Lynx.com n.d.). Dessa forma, os aplicativos não precisam estar instalados em computadores localizados em pontos determinados do navio, mas podem ser utilizados a partir de qualquer estação de trabalho do navio, provendo mais resiliência (Gallagher 2013). Cada estação de traba-

lho pode executar várias máquinas virtuais Linux particionadas por nível e finalidade de segurança (Gallagher 2013).

Noutra iniciativa, uma arquitetura de segurança Linux foi customizada pela NSA. O Security-Enhanced Linux, ou SELinux, incorpora controles de segurança aprimorados. Ele impõe políticas de controle de acesso mandatórias que limitam os programas de usuários e os servidores do sistema à quantidade mínima de privilégios necessários para realizar suas tarefas. Dessa forma, a capacidade de programas de usuário e do sistema causarem danos quando comprometidos é reduzida ou eliminada.

A Iniciativa de Proteção de Software (SPI), sob a direção do Laboratório de Pesquisa da Força Aérea e do Departamento de Defesa dos EUA, criou o Lightweight Portable Security (LPS). Trata-se de uma distribuição Linux que, como o nome indica, é pequena e pode ser usada a partir de um dispositivo removível, em qualquer computador, sem, no entanto, armazenar ou registrar qualquer informação nesse computador (Vaughan-Nichols 2011).

A Marinha dos EUA contratou a Raytheon para instalar o software de controle em sua frota de drones de decolagem e aterrissagem vertical (VTOL) em plataforma Linux (Thomson 2012). Possivelmente, em decorrência da revelação de um ataque de malware ao sistema de controle de drones baseado em Windows da Força Aérea dos EUA (Thomson 2012). Comentando sobre o incidente, Mikko Hypponen, respeitado pesquisador de segurança cibernética, teria declarado: "Se eu precisasse escolher entre o Windows XP e um sistema baseado em Linux durante a construção de um sistema militar, não duvidaria nem um segundo de qual seria" (Thomson 2012).

China

Em meio às restrições impostas pelos EUA, a China estimula o crescimento da oferta de produtos nacionais; fabricantes de semicondutores e empresas de software têm isenção total de impostos por dois anos e de 50% nos três anos seguintes, à medida que a guerra comercial migra para "um ataque à tecnologia chinesa" (Shidong 2019).

Mesmo com a Microsoft tendo produzido uma "Edição do Governo Chinês" do Windows 10 em 2017, em conjunto com sua joint venture chinesa, empresas chinesas de cibersegurança informam que o governo deve migrar para SO *nacionais* (Yang and Liu 2019). Existem ao menos dois SO caseiros da China derivados do Linux: o Kylin OS e o Red-Flag Linux.

O Kylin OS é desenvolvido desde 2001 pela National University of Defense Technology in China (Kirin Software n.d.). Suas versões iniciais eram baseadas no FreeBSD, mas a partir de 2010 ele tornou-se ba-

seado em Linux. Um projeto separado, denominado Ubuntu Kylin, foi anunciado em 2013. Por mais de uma década o Kylin tem sido amplamente utilizado pelos setores de defesa, governo, energia, transporte e aeroespacial da China, entre outros (Li, Liao, and Ma 2017, 66). Oferece compatibilidade com diversos processadores chineses independentes ou compatíveis com o Intel x86. Para reduzir a carência de aplicativos para ambiente Linux, o Kylin oferece compatibilidade para a execução de mais de 2.000 aplicativos Android. Possui também um sistema de segurança com proteção integrada dentro e fora do núcleo, gerenciamento e controle compatíveis com controle de acesso forte de código aberto e incorpora software que pode identificar e impedir automaticamente violações ilegais e evitar que dados privados sejam indevidamente acessados. Suporta métodos de autenticação biométrica como impressões digitais, veias, íris e impressões de voz.

O Red-Flag iniciou-se em 2000 sob os auspícios do Software Research Institute da Chinese Academy of Sciences (Zhongke Hongqi n.d.). Foi desenvolvido a partir do Red Hat Linux. O projeto, uma iniciativa governamental, tinha três motivações: baixo custo, fomento à indústria nacional, e desconfiança do "imperialismo americano", com possíveis *backdoors* no Windows (Pan and Bonk 2007, 2–3). Dentre suas funcionalidades de segurança destacam-se: adequação a padrões internacionais, separação de privilégios, reforço à autenticação de identidade, isolamento do domínio da operação, controle de acesso obrigatório, controle de acesso autônomo, sistema de arquivos criptografado, auditoria de segurança no nível do *kernel*, gerenciamento centralizado de segurança e auditoria, monitoramento e alarme de segurança, controle de sessão e recursos, assistente automatizado de políticas de segurança de aplicativos, e "boa compatibilidade" de hardware e software.

Rússia

Os russos possuem sua própria versão de Linux, denominada Astra Linux (Astra Linux n.d.), e derivada do Debian. O sistema tem uma versão Edição Especial, com melhorias no tocante à segurança. Esta versão é certificada em conformidade com os requisitos de segurança do Ministério da Defesa Russo desde 1996, e pelo FSB, o Serviço Federal Russo de Segurança, sucessor da antiga KGB. Dentre suas funções de segurança destacam-se: controle de acesso obrigatório, isolamento do núcleo, limpeza da memória interna e externa, exclusão garantida de arquivos, marcação de documentos, registro (*logging*) de eventos, mecanismos de segurança da informação no subsistema gráfico, modo de restrição de

ação do usuário, proteção do espaço de endereço dos processos (acesso dos programas à memória), controle de integridade, ferramentas de organização de domínio, gerenciador de banco de dados relacional seguro e servidor de e-mail seguro.

Visando escapar do monopólio de Android e iOS em dispositivos móveis, os russos estão desenvolvendo seu próprio SO móvel como alternativa. De acordo com o ministro Nikolai Nikiforov, do Ministério da Comunicação da Rússia, o novo SO móvel será construído a partir do Sailfish OS, desenvolvido pela empresa finlandesa Jolla, formada por antigos engenheiros da Nokia e registrada em Hong Kong (Hanson 2015; Mohit Kumar 2016).

Índia

Desde 2007 a Índia possui o Bharat Operating System Solution, (BOSS), apresentado como um SO alternativo ao Windows (Ganguli 2017; CDAC n.d.). Derivado do Debian, foi desenvolvido pelo National Resource Centre for Free and Open Source Software (NRCFOSS), órgão do Centre for Development of Advanced Computing (CDAC). Foi inicialmente anunciado como uma proposta para reduzir a desigualdade digital (*digital divide*) na Índia, por ser gratuito e suportar diversas línguas daquele país. Após o Caso Snowden, mostrando a Índia como objeto de grande interesse da NSA, e diante dos contínuos incidentes de ciberataques chineses à Índia, o governo daquele país decidiu adotar o BOSS como o SO nacional (Manan Kumar 2015). O sistema implementa diferentes opções de segurança. Uma versão Secured Operating System (algo como Sistema Operacional Seguro) foi criada com foco nos "clientes do setor de defesa", que exigem um SO livre de invasões e ataques cibernéticos. Implementa medidas específicas usadas para proteger o sistema contra ameaças, vírus, *worms*, malware e ataques cibernéticos, e técnicas de controle preventivo que protegem os dados no computador de serem editados ou excluídos. Inclui controle de acesso mandatório e atualizações regulares de segurança e do banco de dados antivírus. O BOSS oferece ainda um servidor de e-mail seguro, mecanismos de comando e controle para *smart-cities* (integração de componentes IoT — Internet das Coisas — para gestão urbana), armazenamento em "nuvem segura", integração com dispositivos móveis para coleta de dados distribuída, um "cofre eletrônico seguro" (*secured electronic vault*) para o armazenamento de documentos digitais e um scanner de reconhecimento facial que pode identificar pessoas num vídeo e gerar relatórios.

Coreia do Norte

Red Star OS é um SO baseado em Linux, derivado do Fedora (portanto Red Hat) desenvolvido pelo Korean Computer Center (Schiess 2017, 1–2). Além de evitar eventuais *backdoors* em SO norte-americanos, o Red Star visa monitorar o comportamento digital dos cidadãos norte-coreanos (Hoffman 2014). Embora a maior parte de sua funcionalidade seja igual aos SO padrão, o Red Star contém recursos úteis à segurança do Regime vigente. Por exemplo, insere uma marca d'água digital rastreável em todos os documentos que o percorrem, visando combater a distribuição da mídia sul-coreana e dificultar o compartilhamento de informações (Pauli 2015; Schiess 2017, 2). O Red Star possui também um mecanismo para evitar violações, retornando uma mensagem de erro ou encerrando a execução se alguma violação dos arquivos do sistema for detectada (Wagstaff and Pearson 2015; Schiess 2017). Por fim, o Red Flag também não pode ser conectado à Internet, mas possui um navegador interno, baseado no FireFox, que funciona apenas na intranet norte-coreana, destinado a monitorar a atividade *online* (Hoffman 2014).

Turquia

O Pardus é uma distribuição Linux turca, que desde 2013 é baseada no Debian GNU/Linux (Pardus n.d.). É desenvolvido desde 2004 pelo Instituto Nacional de Pesquisa em Eletrônica e Criptologia (UEKAE) daquele país, com o apoio do Conselho de Pesquisa Tecnológica da Turquia (TUBITAK), Ministério da Defesa e do Gabinete do Primeiro Ministro. O objetivo foi o de pesquisar a viabilidade de uma *distro* de um SO nacional para independência de países estrangeiros e para garantir a segurança de informações militares (Karakoç and Varol 2016, 26). Não foram encontradas informações sobre implementações específicas de segurança do Pardus.

Coreia do Sul

Com o suporte ao Windows 7 vivendo seus momentos derradeiros, o governo sul-coreano estuda desistir do Windows. Em maio de 2019, o Ministério do Interior do país anunciou planos de migrar aproximadamente 3,3 milhões de computadores de Windows para Linux (Vaughan-Nichols 2020). Os motivos seriam os custos de licenciamento de software e a dependência do governo no tocante ao Windows. O custo da atualização do Windows 7 para o Windows 10 foi estimado em cerca de US$ 655 milhões (Vaughan-Nichols 2020).

O Ministério da Defesa Nacional e o Ministério da Administração Pública e Segurança já utilizam o SO coreano Gooroom Cloud, baseado no Linux Debian (Vaughan-Nichols 2020). Este sistema implementa algumas extensões de segurança (Gooroom n.d.). O Trust Boot assegura que o carregador de inicialização ou o próprio SO não sejam infectados antes de carregados os módulos de segurança, verificando a integridade do sistema e garantindo sua inicialização sem infecções. O núcleo também é protegido com um mecanismo de verificação baseado em virtualização para monitorar a falsificação ou adulteração de elementos chave do sistema, impedindo a operação de malware com acesso privilegiado ao sistema. Um sistema de proteção de integridade verifica *assinaturas de código* antes de ativar os principais arquivos executáveis, como serviços do sistema e bibliotecas, evitando instalações não autorizadas ou a execução de programas forjados ou alterados ilegalmente. O navegador incluído no sistema aplica diferentes políticas de segurança para limitar possíveis ações (reprodução de mídia, download, etc.) ao acessar sites não confiáveis.

O Ministério da Defesa Nacional e a Agência Nacional de Polícia usam também o Harmonica OS 3.0, baseado no Ubuntu, mas com muitas características da *distro* Mint (HarmoniKR n.d.). O Harmonica também inclui o navegador Naver Whale, criado em coreano (Vaughan-Nichols 2020).

RECOMENDAÇÕES PARA O BRASIL

O aumento da segurança cibernética demanda que o Brasil siga os exemplos dos países citados e internalize softwares de código aberto em suas estruturas governamentais, especialmente na defesa. Esse processo naturalmente seria gradual, mas os casos estudados demonstram que já em dois anos é possível colher os primeiros resultados. Propõe-se, aqui, a Criação de um Núcleo de Software Básico da Defesa (NSBD). Mas não apenas a segurança e defesa do Estado são determinantes. A economia na aquisição de licenças também é motivo relevante, assim como a ampliação da inclusão digital. Observe-se que não se pretende aqui uma reserva de mercado, mas a simples oferta de uma alternativa viável, com ganhos de segurança, não mensuráveis, mas também econômicos e sociais, facilmente mensuráveis.

A criação desse NSBD é consoante com o eixo estratégico cibernético da Estratégia Nacional de Defesa (END), e permitiria que o país desenvolvesse tecnologia própria para proteger-se de certas classes de problemas. Ainda que, nos primeiros anos, não se desenvolva tecnologia genuinamente nacional, a internalização de plataformas OSS e o controle de acesso aos códigos fonte já reduziria significativamente a possibilidade de existência de *backdoors*.

Esse núcleo deveria ser vinculado ao Comando de Defesa Cibernética, no Ministério da Defesa (MD), responsável pela ciberdefesa e mais bem estruturado que o Gabinete de Segurança Institucional (GSI), responsável pela cibersegurança. O NSBD seria composto por militares e civis, necessariamente contendo representantes da iniciativa privada (componentes da Base Industrial de Defesa) e da academia. Essa necessidade advém do fato de que a dinâmica da carreira militar leva a constantes movimentações e transferências, dificultando o processo de retenção e transferência de conhecimento. A participação da iniciativa privada e da academia assegurariam essa retenção e repasse. Ressalte-se que todos os componentes propostos aqui têm emprego dual, tanto militar quanto civil, e assim atendem ao disposto na END.

O NSBD selecionaria uma versão do SO de código livre Linux a ser definida como padrão oficial brasileiro. Baseado nos exemplos dos países citados, as *distros* Debian ou Red Hat/Fedora seriam boas opções, embora o Ubuntu também pudesse sê-lo. Os códigos-fonte desse sistema seriam *internalizados* pela equipe, que os estudaria e providenciaria eventuais modificações necessárias. Seriam geradas versões periódicas desse sistema, distribuídas livremente. Esse procedimento levaria ao domínio completo do sistema, reduzindo a possibilidade de existência de códigos indesejados ou secretos, ou *backdoors* desconhecidas potencialmente exploráveis em situações de crise ou conflito. Além disso, em caso de ataques cibernéticos ou violações, a comunidade teria facilidade em identificar e corrigir os problemas.

Numa segunda fase, plataformas como servidores de e-mail e gerenciadores de banco de dados, navegadores web, e mesmo de automação de escritório, de código aberto, poderiam ser internalizadas e incorporadas à distribuição, com configurações padrão que atendam aos interesses de segurança e defesa do país.

A partir da *nacionalização* de cada plataforma, melhorias de segurança poderiam ser incorporadas, tornando-as mais robustas e incorporando tecnologias desenvolvidas nacionalmente.

CONCLUSÃO

Diversos países, com regimes políticos e culturas distintos, optaram, por motivos de segurança, econômicos ou sociais, pela utilização de Software de Código Aberto para utilização em seus sistemas de missão crítica, relacionados à defesa, segurança, inteligência e governo, ou ainda para sua população. Claramente, razões de segurança nacional prevalecem sobre outros interesses nessa opção. A possibilidade de dispor de independência tecnológica, mesmo que limitada ao software, onde as barreiras de entrada

são consideravelmente menores que aquelas de hardware, tem um grande peso. E oferece alternativas viáveis quando se observa a imposição de restrições de acesso a tecnologias, presentes nas sanções à China, Rússia, Irã e Coreia do Norte, por exemplo. Além dessa, há também a questão da espionagem política e comercial, da qual o Brasil é obviamente um alvo de grande interesse, seja dos EUA, como ficou patente no Caso Snowden, ou de outros.

Mas não apenas questões de segurança justificam a adoção de uma *distro* Linux nacional. Interesses econômicos também são significativos, com a redução da exportação de divisas às empresas multinacionais de software, bem como de redução do déficit fiscal, dados os valores dispendidos pelos governos, em todas as suas instâncias, no licenciamento de SO comerciais estrangeiros. Não menos relevantes, interesses sociais também estão atrelados a essa decisão, posto que a disponibilização de um sistema nacional gratuito permitiria que a população não precisasse gastar recursos limitados na aquisição de produtos importados de elevado custo, ou que, na impossibilidade de fazer esse desembolso, fique sujeita ao *digital divide* ou compelida ao uso de software pirata, sem suporte e sujeita a vulnerabilidades potencialmente exploradas por criminosos.

Outrossim, são muitos os benefícios, e significativamente baixos os custos, para a adoção gradual de OSS, em particular o aqui proposto, num projeto coordenado pelo MD no Brasil.

REFERENCIAS

Adams, James. 2001. "Virtual Defense". *Foreign Affairs* 80, no. 3: 98. https://doi.org/10.2307/20050154.

Angelo, Cláudio. 2007. "'Eixo Do Mal' Científico: Ministério Pede Explicações à Dell Sobre Exigências a Físicos". *Folha de São Paulo* (September). http://www1.folha.uol.com.br/fsp/ciencia/fe1409200703.htm.

Astra Linux. n.d. "Astra Linux - Универсальная Операционная Система". Astra Linux Website. http://www.astralinux.ru/en/.

Banach, William. 2012. "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE". https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE Investigative Report (FINAL).pdf.

CDAC. n.d. "BOSS Linux". BOSS Linux Website. Accessed June 25, 2020. https://bosslinux.in/.

Cimpanu, Catalin. 2018. "Cisco Removed Its Seventh Backdoor Account This Year, and That's a Good Thing". *ZDNet* (November). https://www.zdnet.com/article/cisco-removed-its-seventh-backdoor-account-this-year-and-thats-a-good-thing/.

Cisco. n.d. "Cisco Prime Home Authentication Bypass Vulnerability - Cisco". https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-20170201-prime-home.html.

Clark, Don. 2015. "U.S. Agencies Block Technology Exports for Supercomputer in China". *The Wall Street Journal*. http://www.wsj.com/articles/u-s-agencies--block-technology-exports-for-supercomputer-in-china-1428561987.

Eversden, Andrew. 2019. "Why Can't the Pentagon Use More Open Source Code?" *Wired* (September). https://www.fifthdomain.com/civilian/omb/2019/09/11/why-cant-the-pentagon-use-more-open-source-code/.

Figueiredo, Nice. 1986. "Legislação de Informática No Brasil". *Revista de Biblioteconomia de Brasília* 34, no. 81.

Finley, Klint. 2016. "Open Source Won. So, Now What?" *Wired* (November). https://www.wired.com/2016/08/open-source-won-now/.

Gallagher, Sean. 2013. "The Navy's Newest Warship Is Powered by Linux". *Ars Technica* (October).

Ganguli, Subrata. 2017. "Computer Operating Systems: From Every Palm to the Entire Cosmos in the 21st Century Lifestyle". *CSI Communications*: 5–8.

Gates, Bill. 1996. "Unix Expo Remarks by Bill Gates, October 9, 1996". Wayback Machine (October). https://web.archive.org/web/20010818203946/http://www.microsoft.com/billgates/speeches/industry&tech/uexpo.asp.

GCHQ. 2016. "GCHQ History". http://www.gchq.gov.uk/history/Pages/index.aspx.

Gerring, John. 2012. "Mere Description". *British Journal of Political Science* 42: 721–46. https://doi.org/10.1017/S0007123412000130.

Goodin, Dan. 2016. "Cisco Confirms NSA-Linked Zeroday Targeted Its Firewalls for Years". *Ars Technica*. https://arstechnica.com/security/2016/08/cisco-confirms-nsa-linked-zeroday-targeted-its-firewalls-for-years/.

Gooroom. n.d. "Cloud Platform Forum". Gooroom Website. https://www.gooroom.kr/.

Greenwald, Glenn. 2014. *No Place to Hide: Edward Snowden, the NSA and the Surveillance State*. Penguin Books.

Hanson, Matt. 2015. "Russia's Making Its Own Mobile OS to Boot out Apple and Google | TechRadar". *TechRadar* (May). https://www.techradar.com/uk/news/phone-and-communications/mobile-phones/russia-s-making-its-own-new-mobile-os-to-boot-out-apple-and-google-1294258.

HarmoniKR. n.d. "Linux Community HarmoniKR". HarmoniKR Website. https://hamonikr.org/.

Hoffman, Chris. 2014. "Meet Red Star OS, the North Korean Linux Distro That Apes Apple's OS X | PCWorld". *PCWorld* (December). https://www.pcworld.com/article/2862737/meet-red-star-os-the-north-korean-linux-distro-that-apes-apples-os-x.html.

Hosch, William. 2008a. "Linux | Operating System | Britannica". *Encyclopaedia Britannica* (November). https://www.britannica.com/technology/Linux.

_____. 2008b. "UNIX | Operating System | Britannica". *Encyclopaedia Britannica* (December). https://www.britannica.com/technology/UNIX.

Karakoç, Mehmet, and Asaf Varol. 2016. "National Distribution Project and Pardus Operating System". *Turkish Journal of Science and Technology* 11, no. 2: 25–34.

Kharpal, Arjun. 2020. "US Should Take Stake in Nokia, Ericsson to Counter Huawei in 5G: Barr". *CNBC* (February). https://www.cnbc.com/2020/02/07/us-should-take-stake-in-nokia-ericsson-to-counter-huawei-in-5g-barr.html.

Kirin Software. n.d. "Kirin Software". KylinOS Website. http://www.kylinos.cn/.

Kumar, Manan. 2015. "Make In India: Now Government to Have Its Own Operating System, May Replace Microsoft Windows in Future". *DNA* (September). https://www.dnaindia.com/india/report-make-in-india-now-government-to-have-its-own-operating-system-may-replace-microsoft-windows-in-future-2125014.

Kumar, Mohit. 2016. "Russia to Get Rid of Android and IOS by Launching Its Own Mobile Operating System". *The Hacker News* (June). https://thehackernews.com/2016/06/russian-mobile-os.html.

Li, Jia-Qi, Xiang-Ke Liao, and Jun Ma. 2017. "A Typical Commercial Application for Kylin Operating System". In *2017 3rd International Conference on Computer Science and Mechanical Automation*: 66–70. Wuhan. https://doi.org/10.12783/dtcse/csma2017/17323.

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

Lynx.com. n.d. "LynxOS | POSIX Real Time Operating System | Lynx Software Technologies". Lynx.Com Website. https://www.lynx.com/products/lynxos-posix-real-time-operating-system-rtos.

Miller, Greg. 2020. "How the CIA Used Crypto AG Encryption Devices to Spy on Countries for Decades – Washington Post". *The Washington Post* (February) https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/?fbclid=IwAR1ydM24snbzKUpHz1fsNny7LkLVScUwmUNAuiQMDWtsB4LUYTVopqyWOxg.

MITRE. 2003. "Use of Fre and Open-Source Software (FOSS) in the U.S. Department of Defense".

Moon, Angela. 2019. "Exclusive: Google Suspends Some Business with Huawei after Trump Blacklist - Source - Reuters". *Reuters* (May). https://www.reuters.com/article/us-huawei-tech-alphabet-exclusive/exclusive-google-suspends-some-business-with-huawei-after-trump-blacklist-source-idUSKCN1SP0NB.

Moreira, José de Albuquerque. 1995. "Informática: O Mito Política Nacional de Informática". *Revista de Biblioteconomia de Brasília* 19, no. 1: 23–50.

Pan, Guohua, and Curtis J. Bonk. 2007. "The Emergence of Open-Source Software in North America". *International Review of Research in Open and Distance Learning* 8, no. 3: 1–18. https://doi.org/10.19173/irrodl.v8i3.496.

Pardus. n.d. "Pardus – TÜBİTAK ULAKBİM". Pardus Website. https://www.pardus.org.tr/.

Pauli, Darren. 2015. "North Korea's Red Star Linux Inserts Sneaky Serial Content Tracker". *The Register* (July). https://www.theregister.com/2015/07/20/north_korea_red_star_linux_inserts_sneaky_serial_content_tracker/.

Rid, Thomas. 2016. *Rise of the Machines*. London: Scribe Publications.

Schiess, Niklaus. 2017. "Governmental Control of Digital Media Distribution in North Korea: Surveillance and Censorship on Modern Consumer Devices". https://dprktech.info/media/governmental_control_of_digital_media_distribution_in_north_korea-nschiess.pdf.

Scott, Tony, and Anne Rung. 2016. "Federal Source Code Policy". Federal Source Code Policy (August). https://sourcecode.cio.gov/.

Shidong, Zhang. 2019. "China Offers Five-Year Tax Breaks to Chip Makers, Software Developers to Bolster Industry as Trade War Stretches to Tech | South China Morning Post". *South China Morning Post* (May). https://www.scmp.com/business/article/3011377/china-offers-five-year-tax-breaks-chip-makers-software-developers-bolster.

Singh, Amit. 2007. *Mac OS X Internals: A Systems Approach*. Boston: Pearson Education.

Strumpf, Dan. 2020. "Huawei's 5G Dominance Threatened by U.S. Policy on Chips – WSJ". *The Wall Street Journal* (June). https://www.wsj.com/articles/huawei-struggles-to-escape-u-s-grasp-on-chips-11592740800.

Thomson, Iain. 2012. "US Navy Buys Linux to Guide Drone Fleet". *The Register* (June). https://www.theregister.co.uk/2012/06/08/us_navy_linux_drones/.

Tonooka, Eduardo. 1992. "Política Nacional de Informática: Vinte Anos de Intervenção Governamental". *Estudos Econômicos* 22, no. 2: 273–97.

TOP500.org. n.d. "Top500". TOP500.Org. https://www.top500.org/lists/.

U.S. Dept. of Commerce. 2020. "Department of Commerce Announces the Addition of Huawei Technologies Co. Ltd. to the Entity List | U.S. Department of Commerce". Dept. of Commerce Press Releases (May). https://www.commerce.gov/news/press-releases/2019/05/department-commerce-announces-addition-huawei-technologies-co-ltd.

U.S. DoD. n.d. "DoD Open Source Software (OSS) FAQ". DOD CIO Web Site. https://dodcio.defense.gov/Open-Source-Software-FAQ/#Q:_Under_what_conditions_can_GPL-licensed_software_be_mixed_with_proprietary.2Fclassified_software.3F.

Vaughan-Nichols, Steven. 2011. "The Air Force's Secure Linux Distribution". *ZDNet* (September). https://www.zdnet.com/article/the-air-forces-secure-linux-distribution/.

_____. 2020. "South Korea's Government Explores Move from Windows to Linux Desktop". *ZDNet* (February). https://www.zdnet.com/article/south-koreas-government-explores-move-from-windows-to-linux-desktop/.

Wagstaff, Jeremy, and James Pearson. 2015. "Paranoid: North Korea's Computer Operating System Mirrors Its Political One – Reuters". *Reuters* (December). https://www.reuters.com/article/northkorea-computers-idUSKBN0UA0GF20151227.

Wennergren, David. 2009. "Clarifying Guidance Regarding Open Source Software (OSS)". http://www.defenselink.mil/cio-nii/cio/oss/.

Yang, Yuan, and Nian Liu. 2019. "Beijing Orders State Offices to Replace Foreign PCs and Software | Financial Times". *Financial Times* (December). https://www.ft.com/content/b55fc6ee-1787-11ea-8d73-6303645ac406.

Zetter, Kim. 2015. "Suite of Sophisticated NationState Attack Tools Found With Connection to Stuxnet". *Wired*. https://www.wired.com/2015/02/kapersky-discovers-equation-group/.

Zhongke Hongqi. n.d. "Zhongke Hongqi Website and Application". Zhongke Hongqi Website. http://www.chinaredflag.cn/.

NOTAS

1. Ou OS, acrônimo de Operating System.
2. Exemplos desses métodos de remuneração podem ser encontradas nos antivírus e serviços de Virtual Private Network (VPN) gratuitos, que ou fazem publicidade ou oferecem uma versão inicial limitada, com a versão profissional, mais completa, sendo paga.
3. Lei nº 7.232/1984.
4. Zero-day ou 0-day são vulnerabilidades decorrentes de falhas existentes na codificação do , desconhecidas do público e do fabricante do produto, demandando a publicação e instalação de correções do programa ou biblioteca de (*patches*).
5. PetaFLOPS, or 10^{15} FLoating-point Operations Per Second.
6. Um instituto privado de pesquisas com histórico de atuação em pesquisas militares e sociais.

POR QUE O BRASIL DEVERIA ADOTAR UMA *DISTRO* LINUX PRÓPRIA?

RESUMO

Na tentativa de se escapar da dependência tecnológica externa em sistemas relacionados à defesa, por conseguinte de missão-crítica, bem como de elevados custos de licenciamento, alguns países evitam o uso de softwares comerciais desenvolvidos fora de suas fronteiras, utilizando sistemas abertos ou versões compatíveis desenvolvidas autonomamente. Este artigo argumenta que o Brasil deveria buscar tal autonomia, adotando uma versão própria de sistema operacional, a partir de uma distribuição Linux. É empregada uma metodologia descritiva, baseada em estudos de casos, para análise das opções feitas por diferentes nações. A adoção dessa opção permitiria que o país superasse a desconfiança existente quanto à existência de *backdoors* criadas por parte de serviços de inteligência estrangeiros nos softwares produzidos em seus países de origem. Adicionalmente, alinha-se à Estratégia Nacional de Defesa, permitindo a aquisição de tecnologia de uso dual pela indústria nacional.

Palavras-chave: Autonomia Tecnológica; Distribuições Linux; Software de Código Aberto.

ABSTRACT

In an attempt to escape external technological dependence on defense-related systems, therefore mission-critical, as well as high licensing costs, some countries avoid using commercial software developed outside their borders, using open systems or compatible versions developed autonomously. This article argues that Brazil should seek such autonomy, adopting its own version of the operating system, based on a Linux distribution. A descriptive methodology, based on case studies, is used to analyze the options made by different nations. The adoption of this option would allow the country to overcome the existing mistrust regarding the existence of backdoors created by foreign intelligence services in the software produced in their countries of origin. Additionally, it is in line with the National Strategy of Defense, allowing the acquisition of dual-use technology by the national industry.

Keywords: Technological Autonomy; Linux Distributions; Open Source Software.

Recebido em 03/05/2021. Aceito para publicação em 03/05/2021.

Artigos

Limitações das reformas para o controle civil sobre as forças armadas nos governos do PT (2003-2016)

The limits of civilian control reforms in Brazil during the Workers' Party Administrations (2003-2016)

Rev. Bras. Est. Def. v. 7, nº 2, jul./dez. 2020, p. 187-216
DOI: 10.26792/RBED.v7n2.2020.75239
ISSN 2358-3932

JULIANO DA SILVA CORTINHAS
MARINA GISELA VITELLI

INTRODUÇÃO[1]

Este artigo pretende contribuir para o debate sobre a evolução do controle civil sobre as forças armadas brasileiras durante os governos do Partido dos Trabalhadores (PT). Apesar de considerar que o controle civil se estabelece a partir de um esforço complexo que envolve a criação de diversas estruturas e iniciativas de vários agentes sociais e governamentais, além da mudança cultural de civis e militares, a análise terá um foco específico: a evolução do Ministério da Defesa (MD), tanto em sua estrutura quanto em sua composição.

Como se verá, a maioria da literatura teórico-conceitual que trata do controle civil sobre os militares, principalmente quando desenvolvida internacionalmente, destaca positivamente as medidas adotadas naquele período. Contrariando tais visões, este artigo defende que o período foi marcado pela permanência e, em certa medida, pelo aumento da autonomia institucional das forças armadas.

Essa discrepância decorre de lacunas ontológicas e metodológicas dos modelos tradicionais, que deixam de captar questões relevantes das relações civis-militares no Brasil. Ontologicamente, tais modelos privilegiam o estudo da estrutura do Ministério da Defesa, em detrimento do exame do perfil dos agentes que a compõem. Metodologicamente, a maioria uti-

Juliano da Silva Cortinhas — Professor do Instituto de Relações Internacionais da Universidade de Brasília. Doutor em Relações Internacionais (UnB). Coordenador do Grupo de Estudos e Pesquisas em Segurança Internacional (GEPSI/UnB).
Marina Gisela Vitelli — Doutora em Relações Internacionais (Universidad Nacional de Rosario/Argentina). Professora visitante na EPPEN/Unifesp e pesquisadora do GEDES (Grupo de Estudos de Defesa e Segurança Internacional).

liza a comparação, mas as tentativas de mensurar a qualidade do controle civil sobre os militares em toda a América Latina deixam de considerar peculiaridades de cada país, levando a conclusões sobre os casos que não se ajustam à realidade.

O artigo tem dois objetivos principais. Primeiramente, contribuir para a correção das lacunas acima descritas de dois modos: a) ontologicamente, adiciona ao debate sobre a estrutura do MD uma análise sobre o perfil dos agentes que atuavam no ministério; b) metodologicamente, o artigo se concentra exclusivamente na discussão específica do caso brasileiro, incluindo dados mais detalhados que os utilizados pelos estudos existentes. O segundo objetivo é apontar que os avanços estruturais no Ministério da Defesa brasileiro ao longo dos governos do PT foram insuficientes e não consolidaram o controle civil sobre as forças armadas, característica fundamental para o bom funcionamento das democracias.

O artigo começa por uma revisão bibliográfica das principais obras sobre as relações civis-militares que têm o Brasil como um dos países estudados. A partir dessa revisão, o artigo propõe uma complementação dos modelos examinados a partir de três variáveis: a) a evolução da estrutura organizacional do Ministério da Defesa; b) perfis dos ministros da Defesa; c) equilíbrio entre civis e militares no Ministério da Defesa. Enquanto a primeira variável se concentra na estrutura do Ministério, a segunda e a terceira se referem aos agentes que lá atuavam.

OS DEBATES SOBRE AS RELAÇÕES CIVIS-MILITARES NO BRASIL

A literatura acerca do processo de democratização do aparato de defesa e do estabelecimento do controle civil sobre as forças armadas é vasta. Para os autores que tratam do tema, a prevalência dos civis é fundamental para contrapor as tendências antidemocráticas das instituições militares, que tendem a resistir às ordens das autoridades democráticas na defesa da sua autonomia institucional (Desch 2001, 4–6). Além disso, a estrutura das forças armadas — separadas em três armas — enviesa o olhar dos militares sobre a defesa, pois o espírito de corpo que deles é exigido ao longo da carreira os leva a ter o foco predominante na sua força, dificultando a formulação de uma perspectiva nacional.

A democratização da defesa, a partir desses pressupostos, envolve dois tipos de reformas. Em primeiro lugar, é necessário manter os militares em suas funções prioritárias, ligadas à defesa contra ameaças externas. Isso possibilita eliminar todas as demais formas de interferência militar nos processos políticos, incluindo sua remoção dos espaços de tomada de decisão (presidência, gabinete de ministros, chefia de empresas estatais, etc.), de

modo a permitir que as lideranças civis desenvolvam o projeto político para o qual foram eleitas. Em um segundo nível, é necessário garantir a liderança das autoridades civis na formulação da política de defesa e em algumas decisões sobre as forças armadas. Parte importante dessas transformações se consolida com reformas organizacionais, principalmente no Ministério da Defesa, mas que também incluem os Conselhos de Segurança Nacional, as agências de inteligência e o Congresso. Nesses espaços, é necessário reduzir a autonomia das forças armadas, o que se dá com o *incremento da presença de civis*.

A literatura sobre relações civis-militares nos países sul-americanos, ao longo das últimas décadas, prestou especial atenção a essas *reformas institucionais*. Um dos modelos mais utilizados para avaliar o progresso das reformas tendentes ao controle civil é o quadro das prerrogativas militares de Alfred Stepan (1988, 93-127). O autor identificou onze quesitos que indicam se o grau de prerrogativas das forças armadas continua alto, ou se passou para um patamar moderado ou baixo. A situação ideal seria um quadro de prerrogativas militares de nível baixo, no qual o presidente é *de jure* e de fato comandante em chefe, o Ministério da Defesa é coordenado por um funcionário do gabinete (normalmente um civil que comande uma equipe de servidores civis e militares) e que a situação se repita em outras instituições do setor de defesa. Por sua parte, o Legislativo tem importantes atribuições para influenciar e monitorar decisões nas áreas orçamentária, estrutura das forças e compra de armamento, entre outras.

O arcabouço construído por Stepan foi retomado por Bruneau e Tollefson (2014) em artigo sobre as relações civis-militares no Brasil contemporâneo. Utilizando a mesma matriz conceitual, os autores argumentaram que o Brasil tinha evoluído de um nível de prerrogativas moderado/alto para um nível baixo, apontando grandes progressos em termos de controle civil. A avaliação dos autores contrasta com análises mais céticas feitas pelo próprio Stepan em 1988, assim como de outros trabalhos de autores que defenderam que as possíveis melhorias nas normas funcionaram de forma apenas duvidosa na prática (Fuccille 2006; Marques 2004; Martins Filho 2010; Winand and Saint-Pierre 2010).

Dois exemplos reforçam este argumento. Primeiro, a criação do Ministério da Defesa por um governo democrático, em 1999, e a escolha de civis para o cargo foram apontadas pelos autores como indicador de melhora do controle civil sobre as forças armadas, mas o compromisso dos ministros com tal objetivo apresentou, mesmo nos anos de governos mais progressistas, limitações importantes. Segundo, apesar de os autores entenderem que a existência de comissões de defesa nacional no Congresso sinaliza o papel ativo do Legislativo na formulação e supervisão da política,

não há pesquisas para aferir em que medida tais comissões cumprem seu papel. Ao contrário, as análises sobre a questão costumam destacar o baixo envolvimento do Congresso na definição e supervisão da política de defesa (Amorim Neto 2010; Madruga 2015; Rocha, Saint-Pierre, and Silva 2004).

Seguindo nos exemplos de trabalhos que privilegiem a estrutura em detrimento do estudo sobre os agentes, dois outros importantes trabalhos podem ser mencionados.

Sintetizando as recomendações de um conjunto de autores preocupados com a institucionalização do controle civil, Pion-Berlin (2009) construiu um modelo típico-ideal sobre o desenho institucional do setor de defesa que garanta o controle civil democrático, minimizando a autonomia dos militares com base em quatro princípios: 1) fortalecer a presença civil; 2) empoderar o Ministério da Defesa; 3) reduzir a autoridade militar vertical (*lowering military vertical authority*); e 4) fragmentar o poder militar. De acordo com ele, o desenho institucional ótimo é aquele que coloque civis nos espaços de decisões estratégicas e operacionais mais importantes, que insira intermediários civis para criar distância institucional entre as autoridades eleitas e a corporação militar e que evite que as forças armadas unifiquem seu poder para determinar as escolhas dos civis. Em contraste, deve-se evitar o modelo que, mesmo com presença civil no Ministério da Defesa, não lhe atribua funções de planejamento, comando e supervisão. Pion-Berlin chama os modelos que mantêm essas desarticulações de modelos com *estrutura de comando dual*, pois apesar de incluir civis, mantêm com os militares as funções estratégicas e não os distancia das autoridades democráticas. O autor avalia os avanços obtidos por dezesseis países da América Latina e, quanto ao Brasil, entende que o desenho institucional do setor de defesa se aproximou do ideal a partir das reformas dos anos anteriores.

Anos mais tarde, Pion-Berlin e Martinez (2017) construíram uma proposta conceitual mais ampla[2] para avaliar o estado das relações civis-militares de Argentina, Brasil, Chile e Uruguai. Entre os quatro, veem o Brasil como o país com menor avanço na construção de relações civis-militares democráticas,[3] principalmente pela performance fraca na dimensão das instituições de defesa, que inclui o Ministério da Defesa, o Estado-Maior Conjunto das Forças Armadas (EMCFA) e as comissões de defesa do Congresso. Os autores julgam que o MD brasileiro ainda está na fase de transição, porém próximo de passar para a fase de consolidação democrática. Como principais avanços, mencionam a aprovação da Lei Complementar 97/1999, que inseriu o ministro da Defesa na cadeia de comando, aumentou o poder do ministro na seleção e promoção de oficiais e determinou que cada força prepare sua proposta orçamentária junto ao

MD, que formula a versão final do orçamento e supervisiona sua execução. No entanto, os autores advertem que — revisando a avaliação feita por um deles em 2009 — na prática, a defesa no Brasil tem um desenho institucional caracterizado por uma estrutura de trabalho dual: os civis fazem a administração e os militares a estratégia e operação, quadro que vai persistir enquanto não houver uma carreira civil de defesa bem estruturada.

Apesar de existirem algumas diferenças nas conclusões de cada autor, os estudos mencionados adotam uma abordagem similar, que denominamos de institucional formal: por meio da análise das normativas aprovadas pelos governos, as pesquisas buscam avaliar os países com base em modelos ideais de controle civil. Essa escolha metodológica se reforça nos trabalhos que adotam a metodologia comparada, os quais escolhem aumentar o número de casos e reduzir a complexidade das variáveis e dos dados empregados para facilitar mensurações. Embora as variáveis estruturais e comparações sejam importantes, muitas vezes escondem realidades que somente análises de dados mais específicos e a utilização de variáveis agenciais poderiam revelar.

No Brasil, entender a evolução do controle civil sobre as forças armadas exige examinar o que ocorre no interior das burocracias, observando quais são os atores que estão inseridos nas estruturas decisórias. Como descrito na introdução, este artigo relativiza os resultados obtidos pelos trabalhos centrados em variáveis estruturais a partir de três variáveis. Primeiramente, são descritas algumas limitações do próprio organograma do Ministério da Defesa. A seguir, com o intuito de ampliar a ontologia dos debates tradicionais acerca do tema, são observadas duas variáveis agenciais: os perfis dos ministros e dos servidores do Ministério da Defesa entre 2003 e 2016.

A EVOLUÇÃO DAS ESTRUTURAS ORGANIZACIONAIS DO MINISTÉRIO DA DEFESA DE 2003 A 2016

Com base nos modelos conceituais discutidos acima, é possível argumentar que as gestões do Partido dos Trabalhadores (2003-2016) fizeram progresso para estabelecer o controle civil sobre os militares e fortalecer o MD. Em contraste, nesta seção, demonstra-se que, apesar de o PT ter robustecido o ministério, fez muito pouco para empoderar os funcionários civis da pasta.

Em 2003, quando Luiz Inácio Lula da Silva assumiu a Presidência, a composição do Ministério da Defesa era regida pelo Decreto 3.466, de 17 de maio de 2000. O Decreto previa muitas competências para o Ministério, mas a estrutura organizacional era precária. Como é possível observar no

quadro 1, o ministério era composto por poucos órgãos, todos com estrutura simplificada. Havia apenas 1091 posições previstas para servidores, entre cargos em comissão, gratificações de representação, cargos de confiança e funções. A distribuição de cargos privilegiava os militares, com a previsão de 566 gratificações exclusivas para eles e 525 cargos e gratificações que podiam ser ocupadas tanto por civis quanto por militares.

A reformulação seguinte do Ministério da Defesa ocorreu ainda no primeiro ano da gestão Lula, com o Decreto 4.735, de 11 de junho de 2003. Entre as modificações mais importantes, estava o fortalecimento do Estado-Maior de Defesa, que passou a ter quatro subchefias. Além disso, destaca-se a criação da Secretaria de Estudos e Cooperação (SEC), que tinha como principais atividades a realização de pontes com a academia e a elaboração de estudos sobre matérias afetas à defesa. O Decreto previu 1174 posições, com a manutenção da prevalência de militares.

As próximas reformulações foram realizadas ainda na gestão Lula, pelo Decreto 5.201, de 2 de setembro de 2004, pelo Decreto 6.223, de 04 de outubro de 2007, e pelo Decreto 7.364, de 23 de novembro de 2010. Entre as três, somente a última trouxe mudanças mais substantivas, pois se deu a partir da influência da Lei Complementar 136, aprovada em agosto de 2010.

Pelas diversas alterações advindas dela, a LC 136/2010 ficou conhecida como a Lei da Nova Defesa. Muitos autores já debateram sua importância para a aquisição de produtos de defesa (Moreira 2011) e para o processo de planejamento da defesa nacional (Cortinhas and Okado 2015), entre outros temas. Sua influência sobre a estrutura decisória do MD, que também foi bastante relevante, se deu por meio do Decreto 7.364/2010, que consolidou algumas das mudanças previstas na LC 136/2010. O Decreto acrescentou competências ao Ministério da Defesa e estabeleceu a estrutura e as competências do Estado-Maior Conjunto das Forças Armadas (EMCFA), criado pela LC 136/2010. Além disso, estabeleceu a Secretaria de Produtos de Defesa (SEPROD) e a Secretaria de Pessoal, Ensino, Saúde e Desporto (SEPESD). Para suprir as necessidades de uma estrutura mais complexa que as anteriores, foram designados 1391 cargos, gratificações e funções para o MD.

O mais importante dos novos órgãos era o EMCFA, cujas competências foram previstas pela LC 136/2010 e se resumiam a planejar o emprego conjunto das FA e assessorar o ministro em exercícios conjuntos e Operações de Paz. Para realizar suas funções, o Decreto reservou 310 cargos e funções para o EMCFA, destinando, portanto, praticamente ¼ de todos os servidores da Defesa para o órgão. Importante mencionar que, apesar de ter representado uma evolução relevante, a criação do EMCFA

não deu ao seu chefe condições de construir meios de interoperabilidade e de racionalizar as operações das forças armadas. Meses antes da consolidação de sua estrutura, e no mesmo dia da publicação da LC 136/2010, foi editado o Decreto 7276/2010, que ao tratar aprovou a estrutura militar da Defesa e posicionou o chefe do EMCFA hierarquicamente abaixo dos comandantes das forças armadas.

A próxima reforma do Ministério da Defesa somente foi aprovada no terceiro ano do primeiro mandato de Dilma Rousseff, por meio do Decreto 7974, de 1º de abril de 2013. Como no Decreto anterior, houve modificações importantes. A principal delas foi a criação de um órgão central de direção: a Secretaria-Geral (SG), que passou a congregar, abaixo de si, todas as demais secretarias do ministério. A importância da SG se encontra no fato de que foi pensada para ser ocupada por servidor da total confiança do ministro da Defesa e que pudesse contrabalançar a importância do chefe do EMCFA. Desse modo, abaixo do ministro, os dois principais órgãos do ministério seriam, em paralelo, a Secretaria-Geral e o Estado-Maior Conjunto das Forças Armadas. Enquanto o ministro da Defesa fosse civil, imaginava-se que o secretário geral também seria, o que não se consolidou no tempo. Percebe-se, com isso, que o fortalecimento do Ministério da Defesa pela criação de uma estrutura com três posições principais (ministro, secretário geral e chefe do EMCFA) não levou automaticamente ao estabelecimento de meios de reduzir a autonomia das três forças armadas. Elas continuaram posicionadas em paralelo à estrutura do Ministério, estando ligadas diretamente ao ministro de Estado.

Além da SG, uma outra adição importante à estrutura do MD foi a criação do Instituto Pandiá Calógeras, um órgão pequeno, mas com competência para refletir sobre temas de defesa nacional e estabelecer pontes entre o ministério e a academia. Quando criado, o instituto era, em toda a estrutura do MD, o único órgão composto exclusivamente por civis e funcionou, ao menos de 2013 ao início de 2016, como *think tank* do ministério, estabelecendo parcerias nacionais e internacionais[4].

O quadro abaixo faz uma comparação entre o organograma do Ministério da Defesa quando o Partido dos Trabalhadores assumiu o poder e quando o deixou. Percebe-se que houve poucas alterações, apesar da relevância de algumas delas:

Quadro 1
Comparação entre as estruturas do MD em 2003 e 2016

2003 (Decreto 3466/2000)	**2016 (Decreto 7974/2013)**
Órgãos de assistência direta e imediata ao Ministro de Estado da Defesa	
- Gabinete do Ministro - Consultoria Jurídica - Assessoria Especial - Secretaria-Executiva do Conselho Deliberativo do Sistema de Proteção da Amazônia	- Gabinete - Assessoria Especial de Planejamento - Consultoria Jurídica - Secretaria de Controle Interno - Instituto Pandiá Calógeras
Órgão de assessoramento superior	
Conselho Militar de Defesa	
Órgão setorial	
Secretaria de Controle Interno	
Órgão de assessoramento	
Estado-Maior de Defesa	- Conselho Militar de Defesa - Estado-Maior Conjunto das Forças Armadas
Órgão Central de Direção	
	Secretaria-Geral
Órgãos específicos singulares	
- Secretaria de Política, Estratégia e Assuntos Internacionais - Secretaria de Logística e Mobilização - Secretaria de Organização Institucional	- Secretaria de Organização Institucional - Secretaria de Produtos de Defesa - Secretaria de Pessoal, Ensino, Saúde e Desporto - Centro Gestor e Operacional do Sistema de Proteção da Amazônia
Órgãos de estudo, de assistência e de apoio	
- Escola Superior de Guerra - Hospital das Forças Armadas - Ordinariado Militar - Representação Brasileira na Junta Interamericana de Defesa - Centro de Catalogação das Forças Armadas	- Escola Superior de Guerra - Representação Brasileira na Junta Interamericana de Defesa - Hospital das Forças Armadas
Forças Armadas	
Comando da Marinha Comando do Exército Comando da Aeronáutica	Comando da Marinha Comando do Exército Comando da Aeronáutica

Fonte: elaboração dos autores

Como já mencionado, as maiores inovações foram a criação da Secretaria-Geral e do EMCFA. A estrutura organizacional básica do Ministério da Defesa ao final dos governos do Partido dos Trabalhadores pode ser observada no seguinte organograma.

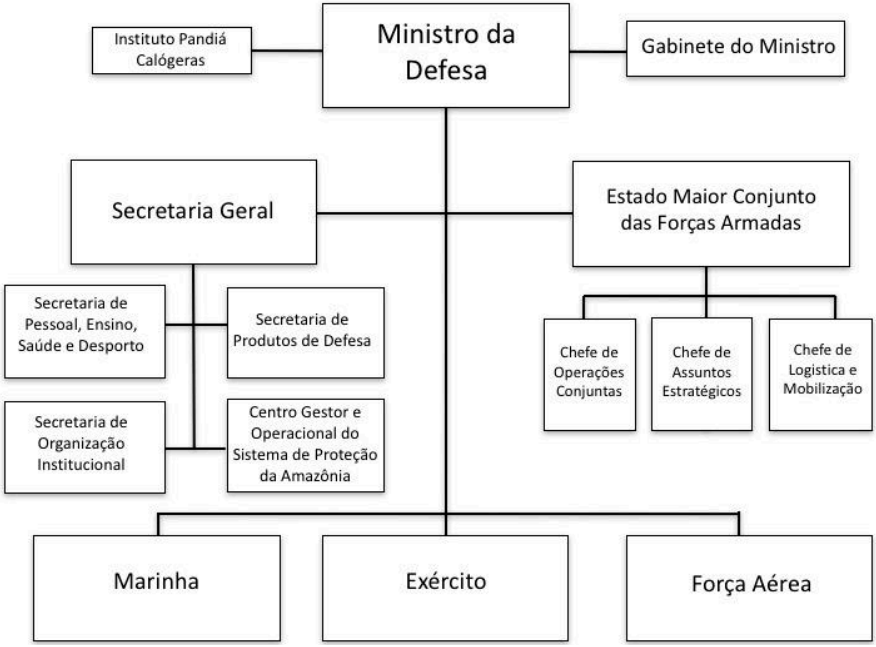


Figura 1 — Organograma do md em 2016
Fonte: elaboração dos autores

Percebe-se, pela análise acima, por que modelos que se concentram somente na análise de variáveis estruturais defendem que o PT ampliou o controle civil. De fato, o país, em 2016, possuía uma estrutura mais consolidada na Defesa. Por outro lado, as limitações dessas alterações são muito importantes. A criação do EMCFA sem prevalência hierárquica sobre as forças armadas manteve a autonomia do poder militar. Além disso, ao colocar a SG e o EMCFA em paralelo, e não garantir o caráter civil da primeira, o PT não conseguiu reduzir a autoridade militar vertical sobre decisões orçamentárias e administrativas.

Essas lacunas são ainda mais evidentes quando analisadas os perfis dos ministros da Defesa e dos servidores que compuseram a estrutura do MD no período.

OS AGENTES DO PROCESSO DECISÓRIO DO MINISTÉRIO DA DEFESA AO LONGO DOS GOVERNOS DO PT

Desde a introdução, traçou-se o objetivo de complementar a ontologia essencialmente institucional utilizada pela literatura sobre as relações civis-militares a partir da análise do perfil dos agentes que ocupam cargos no Ministério da Defesa. Ao longo dos últimos anos, vários autores já reconheceram a importância de dar a mesma relevância, em análises sobre quaisquer realidades sociais, aos agentes e às estruturas (Wight 2006; Dessler 1989; Wendt 1987; Carlsnaes 1992). Apesar disso, os avanços ontológicos advindos do debate agente-estrutura ainda não foram absorvidos pela literatura sobre as relações civis-militares no Brasil.

Nesta seção, apontamos que as evoluções estruturais referidas na seção anterior não levaram a uma alteração relevante na caracterização dos agentes que atuavam no Ministério da Defesa. O próximo subtítulo examina, mais especificamente, o perfil agencial dos ministros da Defesa e como possam ter contribuído para a maior ou menor aceitação de sua liderança. Além disso, também será observada a agência dos servidores do MD nas gestões do Partido dos Trabalhadores, de modo a demonstrar que não houve alteração na distribuição entre civis e militares no órgão, anulando o possível resultado prático das mudanças estruturais ocorridas.

Idealmente, em uma estrutura de defesa equilibrada, há o comando decisivo de um ministro civil que conhece a área e é respeitado pelos seus subordinados. Por sua parte, os servidores do MD civis e militares atuam conjuntamente, mas com responsabilidades diferentes. Em geral, o sistema tende a funcionar mesmo que essas características não estejam totalmente presentes, mas a importância dessa discussão aumenta quando não há consenso entre militares e civis. Nesses casos, um bom controle democrático sobre as forças armadas existe quando os civis que representem o projeto político eleito prevaleçam sobre os militares.

Os perfis dos ministros da defesa de 2003 a 2016

A literatura sobre relações civis-militares é clara quanto à necessidade de que, entre o chefe do Executivo e o comando das forças armadas, seja colocado um funcionário civil[5] que — de baixo para cima — consiga filtrar os elementos corporativistas presentes no assessoramento das forças e —

de cima para baixo — transmitir às lideranças militares as orientações políticas decididas pelo poder político. O consenso sobre esse ponto, porém, não significa que o comando civil automaticamente gere efeitos positivos nas duas dimensões centrais das relações civis-militares democráticas: subordinação das forças armadas ao poder civil e efetiva direção política da defesa. Apesar dessa insuficiência, boa parte das análises atribui peso excessivo para o perfil do ministro da Defesa, defendendo que houve avanço na subordinação das forças armadas apenas por presidentes brasileiros terem nomeado ministros publicamente identificados com posicionamentos ideológicos de esquerda ou funcionários diplomáticos — duas filiações malvistas pelas forças armadas. Para este artigo, contudo, o caráter civil, a orientação ideológica e a profissão, por si sós, não constituem indicadores eficientes de supremacia civil.

O exercício da direção política da defesa em democracias é responsabilidade dos civis, com papel central do ministro. O grau de eficiência na condução da defesa e na execução dos principais objetivos traçados está diretamente atrelado à vontade política de investir recursos humanos, materiais e políticos nesse objetivo (Pion-Berlin 2005). Essa decisão repercute nos militares, pois não é viável exigir obediência das forças armadas sem oferecer em troca uma autoridade com intenção real de exercer liderança. Diversos estudos estabelecem que as chances de os militares apoiarem a liderança civil aumentam quando o ministro da Defesa tem conhecimento e experiência sobre o tema (Bruneau 2005). Assim, dois indicadores para analisar a escolha de chefes da pasta da Defesa são a familiaridade com a área e a sinalização de comprometimento com decisões que contribuam para alcançar os objetivos políticos traçados.

Para além do perfil do ministro, a segunda dimensão que reflete a existência do controle democrático é a subordinação das forças armadas ao chefe civil. Enquanto o chefe deve demonstrar a vontade política de exercer o comando, os militares devem mostrar deferência à autoridade ministerial, obedecendo suas ordens — pois se trata de representante do chefe do Executivo — e se abstendo de manifestar resistências e questionamentos.

Por isso, é interessante examinar, no momento da nomeação de ministros, a reação das forças armadas. Quando há expressão de contrariedade com a escolha pelas autoridades militares, percebe-se uma tentativa de exercer poder de veto incompatível com as relações civis-militares democráticas. É necessário, ainda, considerar reações mais sutis de intolerância ao comando por civis com características ideológicas ou profissionais contrárias às preferências das forças. Por fim, é relevante observar possíveis manifestações de descontentamento das forças com decisões do governo que visem fortalecer a pasta vis-à-vis às organizações militares.

Quadro 2
Dimensões das relações civis-militares democráticas

Dimensão 1 **Direção política da defesa** (responsabilidade de civis)	*Dimensão 2* **Subordinação das forças armadas às autoridades civis** (obrigação das forças armadas)
- Ministro com conhecimento sobre defesa	- Tolerância a ministros com preferências políticas e/ou organizacionais contrárias às das forças armadas
- Manifestações de exercício da liderança	- Abstenção de manifestar contestação de decisões que empoderem o MD

Fonte: elaboração dos autores

Quadro 3
Ministros da Defesa dos Governos Do PT (2003-2016)

Período	Ministro	Profissão
01/2003 — 11/2004 (23 meses)	José Viegas Filho	diplomata
11/2004 — 03/2006 (17 meses)	José Alencar	político
04/2006 — 06/2007 (16 meses)	Francisco Waldir Pires	político
06/2007 — 08/2011 (51 meses)	Nelson Jobim	político e jurista
08/2011 — 01/2015 (41 meses)	Celso Amorim	diplomata
01/2015 — 09/2015 (9 meses)	Jaques Wagner	político
09/2015 — 05/2016 (9 meses)	Aldo Rebelo	político

Fonte: elaboração dos autores

Durante os dois mandatos do presidente Lula e os dois mandatos da presidenta Dilma Rousseff, houve sete ministros da defesa. O primeiro deles, o diplomata José Viegas Filho, pediu demissão pouco antes de cumprir dois anos à frente da pasta após embate com o comandante do Exército Brasileiro[6]. Com a saída, Lula nomeou o vice-presidente, José Alencar, que passou a exercer concomitantemente os cargos de ministro da Defesa e vice-presidente durante um ano e meio, até a nomeação de Waldir Pires (perfil político), que deixou a Controladoria-Geral da União para chefiar o ministério. Pires permaneceu até a maior crise aérea da história do país. Lula, então, substituiu Pires pelo ex-ministro do Supremo Tribunal Federal, Nelson Jobim, que se transformou no ministro mais longevo na pasta. Após o pedido de demissão de Jobim, a presidenta Dilma Rousseff nomeou o ex-chanceler Celso Amorim, que comandou o ministério até o

início de seu segundo mandato. Em janeiro de 2015, Amorim foi substituído pelo ex-governador da Bahia, Jaques Wagner. Em decorrência da crise institucional que começou a tomar força no segundo semestre de 2015, Wagner foi substituído pelo então ministro da Ciência e Tecnologia, Aldo Rebelo, que permaneceu até o impedimento de Rousseff em maio de 2016.

Se a medida do compromisso dos governos do PT com a construção de um Ministério da Defesa que fortalecesse o regime democrático fosse mensurada simplesmente pela escolha de civis, eles atingiriam a nota mais alta: nenhum dos sete ministros era militar. No entanto, a utilização dos indicadores mencionados acima leva a um resultado menos positivo. Nenhum dos ministros chegou ao cargo pelo seu conhecimento em temas de defesa. A ligação institucional dos dois ministros de origem diplomática — Viegas e Amorim — poderia indicar certa proximidade com temas de segurança internacional e defesa nacional (Marque 2004, 46), mas suas carreiras na chancelaria não indicam aproximação especial com o tema. Dos ministros políticos, apenas Rebelo possuía familiaridade com o tema, pois havia presidido a Comissão de Relações Exteriores e Defesa Nacional (CREDEN) e participado da Frente Parlamentar de Defesa. Em suma, durante os 14 anos em que o PT ocupou o Executivo, nenhum dos ministros nomeados era especialista na área, o que indica que o partido não teve boa performance nas suas escolhas se considerada a capacidade de direção política da Defesa.

Quanto às manifestações de exercício de liderança, duas nomeações de ministros podem indicar falta de interesse do governo no estabelecimento do controle civil sobre as forças armadas, concentrando-se apenas no "*political management of the military*":[7] José Alencar e Aldo Rebelo. Há, ainda, casos mais ambíguos: Viegas, Pires, Jobim, Amorim e Wagner.

Viegas foi visto como uma tentativa do recém-eleito presidente Lula de hierarquizar a defesa e efetivamente demonstrou intenção de liderar quando submetido crises. No entanto, o presidente não respaldou o ministro no conflito com as forças armadas surgido a partir do caso Herzog (Martins Filho 2010, 300), apontado por analistas como um claro sinal de acomodação política em um episódio de contestação militar.

José Alencar não exerceu o comando da pasta com dedicação exclusiva e não houve grandes movimentações em sua gestão, além de ter declarado publicamente que carecia de conhecimento básico sobre o tema (Martins Filho 2010, 287).

Waldir Pires também não possuía experiência na área da Defesa e na relação com as forças armadas, mas, se posicionou de modo claro na maior crise que enfrentou. Após o acidente aéreo em que um avião da Gol colidiu com um jato Legacy em 29 de setembro de 2006, ocasionando a morte de

154 pessoas, os controladores de tráfego aéreo (em sua maioria, sargentos da Aeronáutica) fizeram uma operação padrão que levou ao atraso ou ao cancelamento de diversos voos por todo o país, ocasionando o chamado "apagão aéreo". Como solução para a crise, Pires passou a defender o fim da militarização do controle aéreo, posição frontalmente contrária à do comandante da Aeronáutica, Juniti Saito. O comandante entendia que a operação padrão era uma insubordinação e Pires, por divergir da Aeronáutica, chegou a receber representantes dos controladores. Pires e Saito discordaram abertamente em audiência pública, realizada em 10 de abril de 2007, na Câmara dos Deputados (Monteiro and Scinocca 2007). Devido à continuidade da crise aérea, o ministro foi demitido em junho daquele ano e o controle do espaço aéreo permanece militarizado até hoje. O chefe do Executivo novamente optou por não defender a posição de seu representante junto às forças armadas.

Pires foi substituído por Nelson Jobim, cuja importância política poderia significar uma tentativa de estabelecer o controle civil sobre as forças armadas.[8] Jobim comandou a pasta durante o lançamento de diversas iniciativas relevantes na área da defesa: a Estratégia Nacional de Defesa (END), a LC 136/2010, a criação do CDS-Unasul e o acordo com a França para a construção dos submarinos de propulsão nuclear, entre outras. É preciso notar, porém, que todos os projetos capitaneados por Jobim atendiam aos interesses das forças armadas. A END, para alguns autores, apenas resumia o que as forças queriam (Saint-Pierre 2009, 21). A LC 136/2010 ampliou poderes do MD, mas teve efeitos práticos limitados, já que a nova estrutura não criou um nível civil intermediário de autoridade entre o ministro e as forças armadas, como já apontado. Jobim não avançou temas mais controversos, entre outros, como a criação da carreira civil de defesa, que teria ampliado efetivamente a presença civil no MD. Em suma, a gestão de Jobim simboliza a vontade do Executivo de dar importância à Defesa, mas sem reduzir a autonomia das forças armadas. No caso em que o Executivo — porém fora do Ministério da Defesa — estava impulsando uma medida relativa aos militares em direto confronto com os interesses dos militares — a Comissão Nacional da Verdade (CNV) — o ministro tomou posição em favor das forças em lugar de defender a política do governo cujo presidente ele representava, o que levou à sua saída.

A nomeação de Celso Amorim é outro caso ambíguo, pois também parecia representar uma tentativa de avanço devido ao grande sucesso que obteve como chanceler. Apesar disso, o novo ministro não possuía experiência na área e não fez menção de desafiar as forças. Quando criou a Secretaria-Geral, por exemplo, nomeou para a função o senhor Ari Matos Cardoso, que anteriormente ocupava o cargo de secretário de Organização

Institucional (SEORI) e era servidor do MD desde 2003. O primeiro secretário-geral era conhecido no ministério por seu perfil apaziguador, tendo evitado conflitos com os militares ao longo de toda a sua extensa passagem pelo órgão. Na nova função, o padrão foi mantido.

Jaques Wagner era uma figura importante do PT, o que pode demonstrar interesse de dar relevância à pasta. Assumiu, porém, em meio ao agravamento da crise política, sendo rapidamente deslocado à Casa Civil para tentar conter as pressões parlamentares que levaram ao impedimento de Dilma Rousseff.

No auge da crise, foi nomeado Aldo Rebelo, que apesar de ter alguma aproximação com o tema, foi o segundo caso de ministro nomeado apenas para realizar o "*political management of the military*", buscando atender aos interesses das forças armadas em um período conturbado. Rebelo gerou o mais grave retrocesso do controle civil sobre as forças armadas durante os mandatos do PT. Em sua gestão, o general Silva e Luna foi nomeado secretário-geral do Ministério, tendo, a partir daí, controle sobre o orçamento de defesa, o pessoal do MD e das forças e sobre diversos outros processos decisórios inerentes à defesa nacional. Tratou-se de um passo atrás que levou, anos depois, à chegada do próprio general à posição de primeiro militar a ocupar o cargo de ministro da Defesa do Brasil. A partir dele, nenhum outro civil foi elevado a tal condição.

Passando para a dimensão da subordinação das forças armadas à autoridade civil, apesar de aparentemente nunca ter chegado a articular institucionalmente a rejeição da escolha de um ministro ou uma determinada medida que visasse fortalecer o MD vis-a-vis os comandos, existiram episódios nos quais as forças armadas indevidamente manifestaram insatisfação.

O episódio mais grave ocorreu com Amorim. A imprensa reportou a insatisfação dos militares em razão da origem diplomática — supostamente contrária à Defesa — pelo fato de a diplomacia se basear na negociação e a defesa no potencial emprego da força. Alguns generais da ativa, após a nomeação, chegaram a questionar: "desde quando um diplomata gosta de guerra? É como botar médico para cuidar de necrotério. Parece brincadeira" (Costa 2011). Outra manifestação de alto oficial demonstra claramente a insatisfação: "é quase como nomear o flamenguista Márcio Braga para o cargo de presidente do Fluminense ou do Vasco, ou o vascaíno Roberto Dinamite como presidente do Flamengo" (Redação NSC 2011). Por fim, outro oficial afirmou que, enquanto chanceler, Amorim "contrariou princípios e valores dos militares" (Redação NSC 2011), havendo inclusive menções sobre a suposta ideologia bolivariana do novo ministro (Gedes 2011). Como se verá na próxima seção, essas pressões sobre um ministro de perfil negociador, como foi Amorim, parecem ter

alcançado resultados importantes. Os militares aumentaram muito a presença no ministério em sua gestão.

Por outro lado, chama a atenção a ausência de rejeição à nomeação de Aldo Rebelo, pelo seu histórico de filiação ao PCdoB. Essa ausência de contrariedade pode ter relação com o fato de que ele prontamente nomeou um militar para a Secretaria-Geral.

No que se refere à resistência por parte das autoridades militares a medidas tomadas por autoridades civis, não seria viável abordar aqui todas as instâncias em que as forças armadas manifestaram oposição. É possível, contudo, selecionar alguns episódios.

Além dos embates entre o ministro Viegas e o comandante do Exército e entre o ministro Pires e o comandante da FAB, já abordados, interessam para este trabalho outros dois episódios. O primeiro se trata de um processo que é iniciado pela publicação no Diário Oficial da União (DOU) do 3º Plano Nacional de Direitos Humanos, em dezembro de 2009, e culmina com a Comissão Nacional da Verdade (2011-2014), decisões duramente resistidas pelas forças armadas. Já na publicação do Plano, os comandantes das forças se reuniram com o ministro Jobim para expressar sua indignação (Cantanhêde and Iglesias 2009). Em lugar de tentar convencer os oficiais a aceitarem a decisão do governo, ou pelo menos negociar sua aquiescência, o ministro da Defesa apoiou as preocupações dos comandantes: alguns meses depois, em audiência pública no Congresso, Jobim afirmou que tinha considerado renunciar se o governo insistisse na proposta (Moraes 2010).

Por fim, o segundo episódio ocorreu em 3 de setembro de 2015, último mês em que Jaques Wagner chefiou a pasta. Naquele dia, foi publicado no DOU o Decreto 8515, que delegava ao ministro da Defesa competências para a edição de atos relativos ao pessoal militar, tais como transferência para a reserva remunerada de oficiais, reforma de oficiais da ativa e da reserva e promoção aos postos de oficiais superiores. Apesar da normativa prever a possibilidade de subdelegação aos comandantes, que até o momento exerciam tais competências, o decreto provocou a imediata reação das forças armadas. O ministro rapidamente buscou acalmá-las, emitindo uma portaria que neutralizou os efeitos do decreto, anulando um claro avanço nas capacidades de o ministério exercer a direção superior das forças armadas. Mais uma vez, um ministro civil precisou recuar na tentativa de ampliar o controle civil sobre a pasta (Gedes 2015).

Em resumo, examinar a adequação de ministros nomeados pelos governos do PT apenas pela sua condição de civis obscurece dois fatores que têm impacto negativo sobre o controle civil sobre as forças armadas. Em primeiro lugar, não diz nada acerca da preparação desses funcionários para liderar uma pasta dominada por burocracias definidas pelo espírito de corpo

e acostumadas a mandar. Empossar ministros legitimados não apenas pela decisão da Presidência da República, mas também por seu conhecimento, incrementa sensivelmente as chances de controle civil. Em segundo, a obediência dos militares ao ministro não pode ser condicional, motivo pelo qual os estudos precisam considerar as atitudes de contestação das forças armadas à escolha dos ministros e às decisões ministeriais que reduzam prerrogativas militares. De forma similar, ministros civis — conhecedores da área da defesa ou não — que evitem tomar decisões que incomodem as forças armadas, não permitem identificar a subordinação dos militares às autoridades democráticas. Os verdadeiros testes da supremacia civil são os casos de ministros que tomem decisões contrárias às preferências das forças armadas e que permaneçam no posto apesar de enfrentarem contestação militar. Nenhum dos sete Ministros de Defesa dos governos do PT passou nesse teste.

O perfil dos servidores do ministério da defesa nos governos do PT

Os subtítulos anteriores mostraram que os governos do PT aumentaram o número de servidores do MD e criaram instituições que atenderam aos padrões gerais definidos pelas principais obras que tratam do controle civil sobre as forças armadas. Por outro lado, o perfil dos ministros da Defesa do período indica que o partido evitou investir capital político na Defesa, deixando de nomear ministros capacitados e com vontade política de liderar. Além disso, os militares foram bem-sucedidos na resistência às decisões desses ministros, quando contrárias a seus interesses. O objetivo desta seção é aprofundar a análise sobre os avanços no controle civil naqueles anos a partir do exame do perfil dos agentes que atuaram no Ministério.

Os dados utilizados são provenientes de duas fontes:

a) Os seis decretos, já mencionados acima, que trataram das reformas estruturais do Ministério no período[9] e possibilitaram identificar o número total de cargos militares e o nível desses cargos.
b) Consulta ao Ministério da Defesa, por meio do Sistema Eletrônico do Serviço de Informações do Cidadão (e-SIC), realizada em 19 de agosto de 2016 e autuada sob o n. 60502.001569/2016-39.[10]

Como ponto de partida, é importante reafirmar que o Partido dos Trabalhadores promoveu um aumento de 60% no número de posições no Ministério da Defesa (de 818 para 1309) de 2003 a 2016. Esse aumento, porém, não se deu de modo igual para militares e civis. Waldir Pires assumiu um ministério com igualdade de cargos de civis e militares. Ao

entregar a gestão, Aldo Rebelo deixou um órgão bastante dominado pelos militares, que possuíam 730 cargos exclusivos, enquanto o total de cargos que poderiam ser ocupados por civis era de apenas 530. O aumento no número de cargos civis foi de 42,1%, enquanto a elevação dos cargos militares foi de 77,5%.

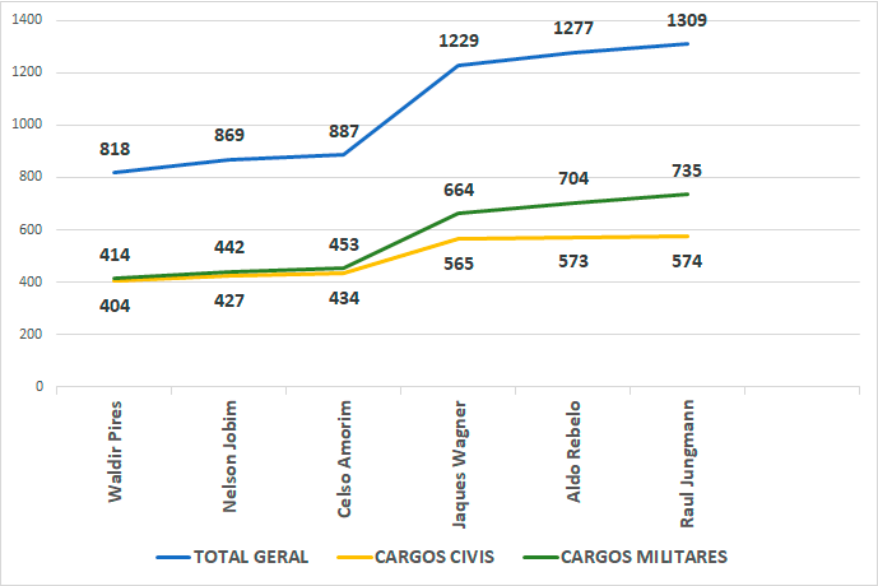


Gráfico 1 — Total de cargos militares e civis no Ministério da Defesa entre 2006 e 2016
Fonte: elaborado pelos autores, com base em dados obtidos pelo e-SIC.

Observe-se que o descolamento entre o número de cargos civis e militares ocorreu na gestão de Celso Amorim, que assumiu o MD com 51,1% de cargos militares (453) e 48,9% de cargos civis (434) e entregou a gestão para Wagner com 54% de cargos militares (664) e 46% de civis (565). Trata-se do período com maior aumento proporcional de posições militares.

Apesar de parecerem preocupantes, os números acima ainda estão distantes de retratar corretamente a realidade da composição do Ministério da Defesa. Para tanto, é preciso destacar que parte das posições que podem ser ocupadas por civis costumam ser destinadas a militares (da ativa ou da reserva), o que passou, nos governos do PT, a ser uma prática cada vez mais comum.

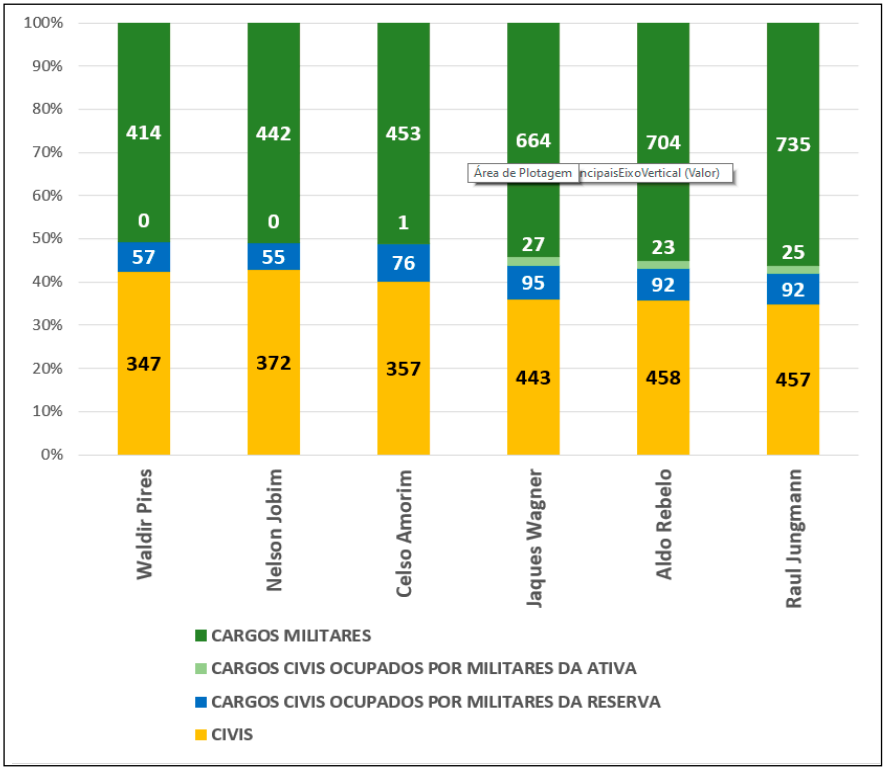


Gráfico 2 — Total de civis e militares ocupando cargos no MD entre 2006 e 2016
Fonte: elaborado pelos autores, com base em dados obtidos pelo e-SIC.

Os dados acima aumentam a percepção de que a gestão Amorim foi um marco no aumento da presença de militares no Ministério da Defesa. O diplomata assumiu o MD com apenas 1 militar da ativa ocupando cargo civil e ampliou esse número para 27. Além disso, e de ter ampliado o percentual de cargos militares em relação aos civis, permitiu que 95 militares da reserva ocupassem cargos civis. Em 04 de agosto de 2011, dia de sua posse, o Ministério da Defesa possuía 40,3% de seus cargos ocupados por civis. Quando deixou o ministério, esse número chegava a apenas 36,1%. Nas duas gestões seguintes, o número continuou caindo, mas em ritmo menor. Quando Rebelo deixou o MD, havia apenas 34,9% do total de cargos ocupados por civis. Se observado o período total analisado por este artigo, a queda é bastante contundente: Waldir Pires assumiu o Ministério da Defesa, em 31 de março de 2006, com 42,4% dos cargos do MD ocupados por civis, número expressivamente maior do que os 34,9% de 2016.

Uma forma de aprofundar essa análise é examinar somente a ocupação de cargos civis ao longo do período analisado:

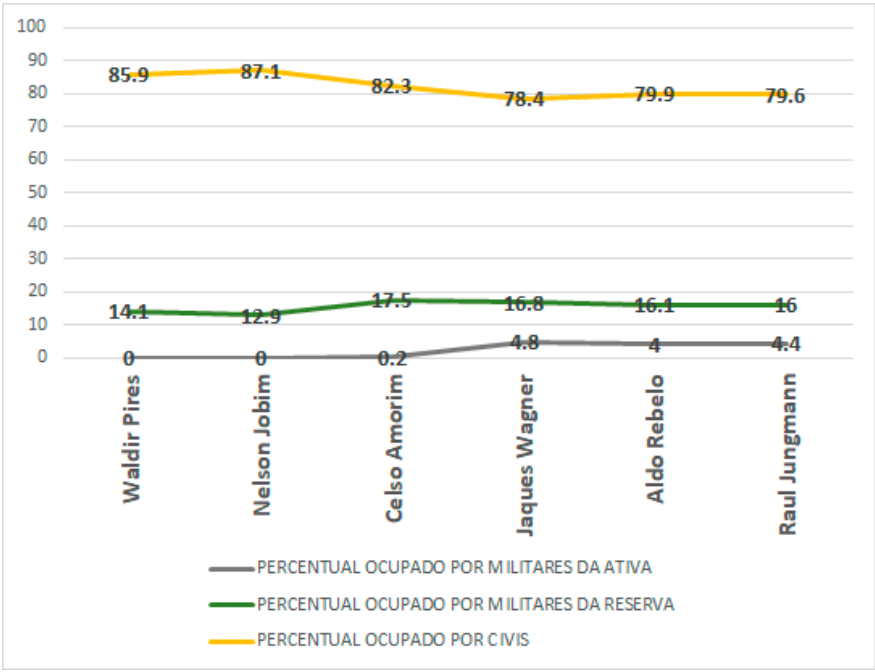


Gráfico 3 — Ocupação dos cargos civis do Ministério da Defesa entre 2006 e 2016
Fonte: elaborado pelos autores, com base em dados obtidos pelo e-SIC.

Como se pode observar, no início da gestão Pires, somente 85,9% dos cargos civis eram efetivamente ocupados civis, percentual que foi levemente ampliado em sua gestão. Durante as duas gestões seguintes, porém, esse percentual passou de 87,1% para 78,4%. A partir de então, Jaques Wagner elevou a taxa e Rebelo a manteve estável. Ressalta-se, ainda, a inexplicável opção por colocar militares da ativa em cargos civis.[11]

Nota-se, claramente, que o PT não foi capaz de diminuir a presença de militares no MD, ocorrendo, de fato, o contrário. Tão importante quanto quantificar os dados desse processo, porém, é qualificá-los. Serão adotados, para tanto, dois critérios básicos: a) os cargos que serão comparados serão divididos em três níveis: superior, intermediário e inferior; b) somente serão contabilizados os cargos mais relevantes nos processos decisórios do ministério, tanto para militares quanto para civis.[12]

As gratificações de exercício em cargo de confiança são divididas em cinco grupos: grupo 0001 (letra A), grupo 0002 (letra B), grupo 0003 (letra C), grupo 0004 (D) e grupo 0005 (E). Enquanto a letra A se refere às gratificações de Oficiais-Generais, as letras B e C são gratificações de Oficiais-Superiores e as letras D e E são destinadas a Oficiais-Intermediários e Subalternos. Com o intuito de facilitar a comparação com o percentual de civis nos níveis hierárquicos do MD, o gráfico abaixo simplifica a divisão em três grupos ao unir as letras B e C na categoria "superior" e as letras D e E como "intermediário e subalterno".[13]

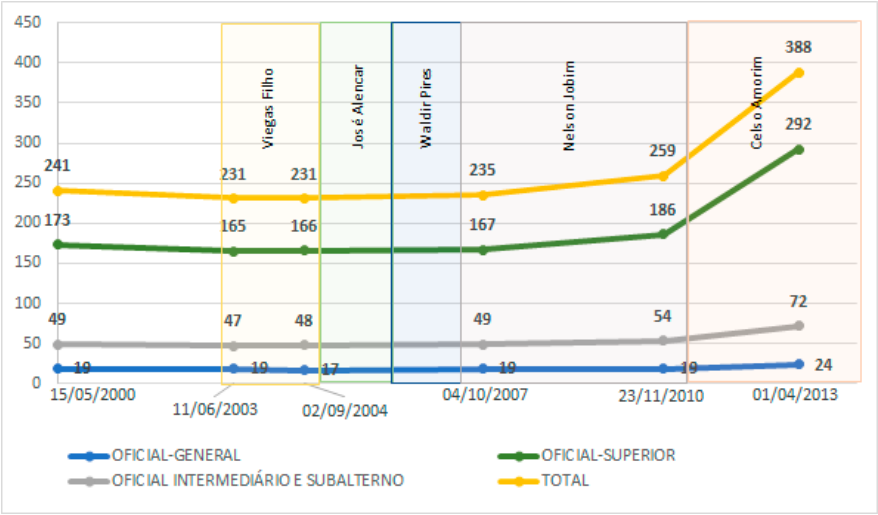


Gráfico 4 — Gratificações de exercício em cargo de confiança privativas de militares nos governos do PT.
Fonte: elaborado pelos autores, com base nos Decretos 3.466/2000, 4.735/2003, 5.201/2004, 6.223/2007, 7.364/2010 e 7.974/2013.

Após um período inicial de estabilidade nos números, a gestão de Jobim aumentou em 12,1% o número de gratificações, em especial de oficiais superiores, nas duas alterações estruturais do MD que promoveu. Houve elevação ainda maior na gestão Amorim, quando o número total passou de 259 para 388, uma elevação de 49,8%. Importante mencionar que esse aumento se deu no mesmo período em que houve também uma elevação da ocupação de DAS por militares, indicando um claro processo de militarização do ministério na gestão do diplomata.

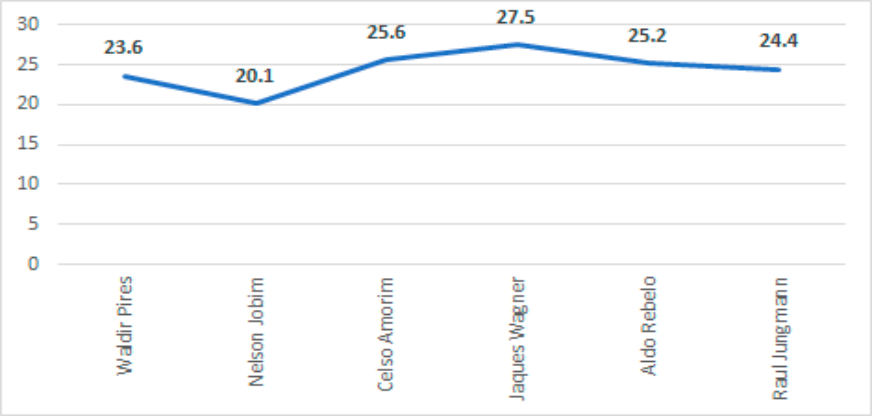


Gráfico 5 — Percentual de militares ocupando das no Ministério da Defesa entre 2006 e 2016
Fonte: elaborado pelos autores, com base em dados obtidos pelo e-SIC.

O gráfico demonstra que o percentual de militares ocupando especificamente DAS foi maior que os números referentes ao total de cargos civis. Além disso, percebe-se, novamente, que a tendência se acelerou nas gestões Jobim e Amorim, tendo sido reduzida, em especial, na gestão de Wagner e, em menor peso, na de Rebelo[14].

Qualificando os dados acima, percebe-se que a situação é agravada pelo fato de que os percentuais de ocupação por militares dos DAS de níveis superiores são maiores. Como os DAS são divididos em seis níveis e as letras militares foram divididas em três níveis nesta análise, os autores optaram por também dividir os DAS em três níveis. Desse modo, foi possível identificar como estão distribuídos civis e militares nos níveis superior, intermediário e inferior do MD. No cômputo do primeiro nível, foram incluídos os DAS 6 e 5 e as gratificações A. No nível intermediário, os DAS 4 e 3 e as gratificações B e C. No nível inferior, os DAS 2 e 1 e as gratificações D e E.

É possível observar no gráfico abaixo que os militares, tanto pelo aumento do número de cargos específicos quanto pela maior ocupação de DAS, mantiveram grande prevalência nos níveis superior e intermediário, dominando os processos decisórios no ministério, ao tempo em que "permitiram" presença maior de civis no nível inferior.

A partir da divisão das principais posições do MD em níveis, fica claro que os militares privilegiaram a ocupação de postos de liderança. Mais de 2/3 dos cargos mais importantes do MD foram, durante todo o período, dominados por militares. O ápice desse domínio ocorreu ao final da gestão

Amorim, quando os militares ocupavam 75% dos cargos superiores e quase o mesmo montante dos intermediários.

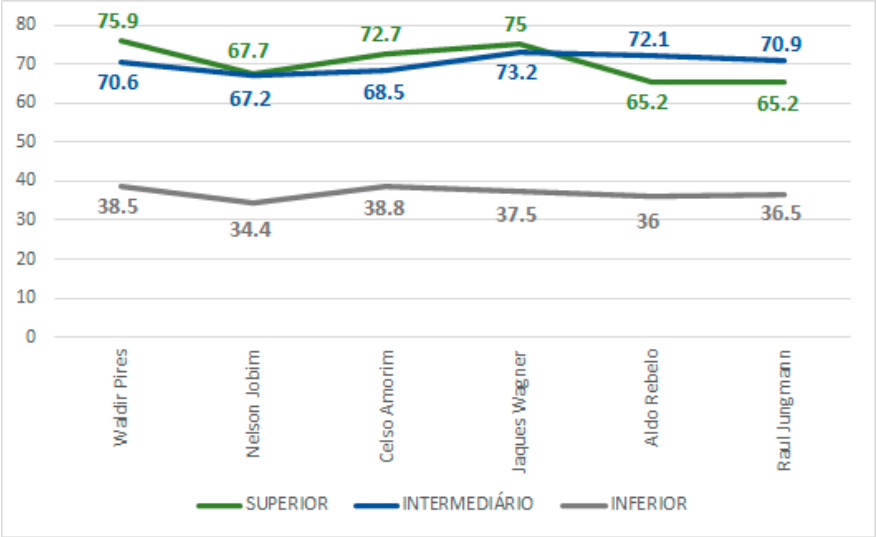


Gráfico 6 — Percentual de militares nos níveis superior, intermediário e inferior do Ministério da Defesa de 2006 a 2016
Fonte: elaborado pelos autores, com base em dados do e-SIC e nos Decretos 3.466/2000, 4.735/2003, 5.201/2004, 6.223/2007, 7.364/2010 e 7.974/2013

O conjunto de dados acima deixa claro que as gestões do PT conseguiram (ou não buscaram) alterar o equilíbrio de forças entre civis e militares no ministério da Defesa, o que impossibilitou que houvesse o estabelecimento do controle civil sobre as forças armadas. A falta de tal controle, além de prejudicar a qualidade da democracia brasileira, pode explicar a ausência de uma definição política clara sobre o papel dos militares no Brasil, a falta de racionalização do orçamento de defesa e a baixa interoperabilidade entre as forças, entre outros problemas do setor.

CONCLUSÃO

A eleição de Lula, em 2002, deu-se a partir do argumento de que era necessária uma mudança nas relações de poder na sociedade brasileira. No âmbito das relações civis-militares, porém, tal mudança não foi realizada. Em mais de 13 anos, o PT não foi capaz de avançar, ao contrário do que

afirmam alguns estudiosos, na imposição do controle civil sobre as forças armadas, um dos pilares fundamentais dos Estados democráticos.

Há indicadores positivos durante o período, como a manutenção de ministros civis e a criação de órgãos como o EMCFA e a SG. Três problemas fundamentais, porém, comprometeram o otimismo que poderia ser decorrente dessas reformas. Primeiramente, não foi criado um nível adicional entre as forças e o ministro para reduzir o poder militar na cadeia de comando da estrutura do Ministério da Defesa. Segundo, o EMCFA continuou sendo considerado hierarquicamente inferior aos comandos das forças, não sendo capaz de impor a interoperabilidade e o racionamento dos gastos, ambos necessários para aprimorar o sistema de defesa e para a efetiva supremacia do MD sobre as forças. Terceiro, e mais grave, a SG, órgão principal de administração do Ministério, passou, ainda nos governos do PT, a ser ocupada por um militar, retirando qualquer chance de que pudesse contribuir para ampliar o controle civil. Ao contrário, passou a ser um meio de centralizar informações e decisões para consolidar o controle militar sobre o MD.

Apesar de a análise desses problemas ter sido importante, as contribuições mais relevantes do artigo foram as críticas ontológicas e epistemológicas realizadas a modelos tradicionais sobre o tema, que permitiram construir uma análise específica do caso brasileiro que examinasse o perfil dos agentes do MD. Os dados descritos demonstram que houve, naqueles anos, aumento da presença de militares na pasta, tanto pela ampliação das gratificações exclusivamente destinadas a eles quanto pela ocupação de cargos que deveriam ser prioritariamente destinados aos civis.

Esse dado indica, em primeiro lugar, que não basta nomear civis para o cargo máximo do ministério da Defesa. Para que haja aumento do controle civil sobre os militares, os ministros precisam conhecer profundamente o tema e possuir apoio do chefe de Estado. Na primeira crise de sua gestão, por exemplo, teria sido fundamental que Lula tivesse tomado decisão favorável ao ministro Viegas, de modo a demonstrar que a relação entre civis e militares seria reposicionada em favor do controle civil. A presidenta Dilma também não deu condições para que seus ministros da Defesa impusessem o controle civil ou não nomeou ministros decisivamente comprometidos com tal objetivo.

Apesar de o objetivo desse artigo não ter sido examinar as razões pela manutenção da preponderância de militares no Ministério da Defesa, foi possível perceber que a presença de representantes das forças armadas no principal órgão de condução política sobre o tema aumentou de modo mais visível durante as gestões de Jobim e Amorim, podendo indicar que a permanência de ministros por longo prazo possa torná-los mais suscetíveis à pressão dos militares, hipótese a ser testada futuramente.

Para além da falta de vontade política de presidentes e ministros, a ausência de carreira civil no ministério, prevista desde a END 2008, parece estar entre os fatores que mais contribuíram para que os militares ocupassem, ao final da gestão do PT, 65,2% das posições superiores e 70,9% das posições intermediárias do MD, tendo total prevalência sobre os civis. Sem uma carreira civil no ministério, nunca estarão garantidas as condições para a consolidação plena de nossa democracia. É essencial, para tanto, que os militares estejam totalmente afastados da política nacional, o que somente ocorrerá quando as decisões sobre o papel das forças armadas, sobre o tamanho do contingente e sobre as prioridades orçamentárias, entre outras, estiverem totalmente sob controle civil, tendo os militares somente a função de assessores técnicos nessas questões.

A partir dos dados examinados, percebe-se que os governos do PT representaram uma grande oportunidade perdida para o estabelecimento do controle civil sobre os militares no Brasil, o que pode ter contribuído decisivamente para que seja possível o forte intervencionismo militar na política brasileira que se observa na atualidade. Se governos de tendências mais progressistas foram incapazes de fazer as necessárias reformas no ministério, a tendência atual é de total destruição dos poucos avanços alcançados ao longo dos governos do PT. Como o controle civil sobre as forças armadas nunca foi estabelecido plenamente no país, a democracia brasileira nunca deixou de estar sob grande risco.

REFERÊNCIAS

Amorim Neto, Octávio. 2010. "O Papel do Congresso nas questões de defesa: entre a abdicação e o comprometimento". In *Segurança Internacional: Perspectivas Brasileiras*, edited by João Paulo Soares Alsina Júnior, Nelson A. Jobim, and Sérgio W. Etchegoyen: 436–48. Rio de Janeiro: FGV Editora.

Bruneau, Thomas C. 2005. "Civil-Military Relations in Latin America: The Hedgehog and the Fox Revisited". *Revista Fuerzas Armadas y Sociedad* 19, no. 1–2: 111–31.

Bruneau, Thomas C., Scott D. Tollefson. 2014. "Civil-Military Relations in Brazil: a reassessment". *Journal of Politics in Latin America* 6, no. 2: 107–38.

Cantanhêde, Eliane, Simone Iglesias. 2009. "Contra 'Comissão Da Verdade', Comandantes Ameaçam Sair". *Folha de S. Paulo* (Dezembro. https://www1.folha.uol.com.br/fsp/brasil/fc3012200907.htm.

Carlsnaes, Walter. 1992. "The Agency-Structure Problem in Foreign Policy Analysis". *International Studies Quarterly* 36, no. 3: 245–70.

Cortinhas, Juliano S., and Giovanni Hideki Chinaglia Okado. 2015. "Transformação de Defesa? Exame do Primeiro Ciclo de Atualização dos Principais Documentos da Defesa Nacional". *Revista Brasileira de Estudos Estratégicos* 7, no. 13, 67–102.

Costa, Octávio. 2011. "Relações militares. Ex-chanceler do governo Lula, Celso Amorim assume a pasta da Defesa no lugar de Nelson Jobim — mas a escolha já provoca insatisfação na caserna." *IstoÉ* (Agosto). https://istoe.com.br/150322_RELACOES+MILITARES/.

Desch, Michael C. 2001. *Civilian Control of the Military: the changing security environment.* Baltimore: Johns Hopkins University Press.

Dessler, David. 1989. "What's at Stake in the Agent-Structure Debate?" *International Organization* 43, no. 3, 441–73.

Fuccille, Alexandre. 2006. "Democracia e questão militar: a criação do Ministério da Defesa no Brasil." Tese de Doutorado, Unicamp.

Gedes. 2011. Informe Brasil nº 22/2011. Observatório Sul-Americano de Defesa e Forças Armadas.

https://gedes-unesp.org/wp-content/uploads/2018/06/Informe-Semanal-Brasil-Sul-Americano-22-2011.pdf

Gedes. 2015. Informe Brasil nº 32/2015. Observatório Sul-Americano de Defesa e Forças Armadas.

https://gedes-unesp.org/wp-content/uploads/2018/06/Informe-Semanal-Brasil-Sul-Americano-32-2015.pdf

Madruga, Florian Augusto de Abreu Coutinho. 2015. "O Congresso Nacional, as relações civis-militares e a política de defesa no Brasil (1999-2014)". Dissertação de Mestrado, FGV.

Marques, Adriana. 2004. "El Ministerio de Defensa en Brasil. Limitaciones y perspectivas". *Revista Fuerzas Armadas y Sociedad* 18, no. 3–4: 27–51.

Martins Filho, Joao Roberto. 2010. "Tensões militares no governo Lula (2003-2009): a pré-história do acordo com a França". *Revista Brasileira de Ciência Política*, no. 4: 283–306.

Monteiro, Tania, and Ana Paula Scinocca. 2007. "Comandante contraria ministro e defende controle aéreo militar". *O Estado de S. Paulo* (Abril).

Moraes, Marcelo de. 2010. "Jobim admite falha e garante que FAB não omitiu documentos secretos"" *O Estado de S. Paulo* (Março).

Moreira, William de Sousa. 2011. "A Obtenção de Produtos de Defesa no Brasil: O Desafio da Transferência de Tecnologia". *Revista da Escola de Guerra Naval* 17, no. 1: 127–50.

Pion-Berlin, David. 2005. "Political Management of the Military in Latin America". *Military Review* 85, no. 1: 19–31.

_____. 2009. "Defense Organization and Civil-Military Relations in Latin America". *Armed Forces & Society* 35, no. 3: 562–86.

Pion-Berlin, David, and Rafael Martínez. 2017. *Soldiers, Politicians, and Civilians: Reforming Civil-Military Relations in Democratic Latin America.* Cambridge University Press.

Redação NSC. 2011. "Diário Oficial traz nomeação de Amorim. Escolha do ex-chanceler para substituir Jobim no Ministério desagradou os militares." *NSC Total* (Agosto). https://www.nsctotal.com.br/noticias/diario-oficial-traz-nomeacao-de-amorim.

Rocha, Fernando, Hector Luis Saint-Pierre, and Sérgio Paulo da Silva. 2004. "Parlamento e Defesa: o caso Brasileiro." In *Parlamento y Defensa en América Latina: el papel de las comisiones*, edited by Gilda Follietti and Luis Tibiletti. Buenos Aires: SER en el 2000.

Saint-Pierre, Héctor Luis. 2009. "La defensa en la política exterior del Brasil: el Consejo Suramericano y La Estrategia Nacional de Defensa." Documento de trabajo 50. Real Instituto Elcano.

Stepan, Alfred. 1988. *Rethinking Military Politics: Brazil and the Southern Cone.* New Jersey: Princeton University Press.

Wendt, Alexander. 1987. "The Agent-Structure Problem in International Relations Theory". *International Organization* 41, no. 3: 335–70.

Wight, Colin. 2009. *Agents, Structures, and International Relations.* Cambridge: Cambridge University Press.

Winand, Erica, and Héctor Luis Saint-Pierre. 2010. "A fragilidade da condução política da defesa no Brasil." *História*, no. 2: 3–29.

NOTAS

1. Os autores agradecem a Thomas Bruneau pelos profundos comentários realizados em versão prévia deste artigo. Agradecem, ainda, aos pareceristas anônimos da RBED pela leitura cuidadosa e pareceres criteriosos, que contribuíram decisivamente para o artigo.
2. Os autores apresentam uma proposta conceitual holística para avaliar o progresso das relações civis-militares na região, incluindo as pontas de um triângulo: militares, políticos e sociedade. A partir desse arcabouço, avaliam o progresso obtido nas reformas qualificando os avanços como nulos, poucos, moderados ou substanciais, além de dar uma nota numérica para cada país.
3. A média do Brasil nas seis dimensões é 1,4 (avanço moderado). Em nenhuma das seis dimensões o Brasil atinge a nota mínima para qualificar avanço substancial (2 pontos). As dimensões com piores notas são Instituições (1,1), arcabouço legal (1,2) e convergência (1,3). Já o conhecimento (1,4), o poder militar (1,7) e a efetividade têm notas melhores. Em termos das fases, o Brasil tem 11 componentes de dimensões ainda em fase de transição (39,3%), 13 em fase de consolidação (46,4%) e 4 em fase consolidada (14,3%).
4. O instituto, por sua configuração, teve de romper diversas desconfianças no início do seu trabalho. A partir de 2016, porém, houve a inserção de militares em sua composição e a perda de cargos relevantes. A tendência, hoje, é de encerramento de suas atividades.
5. Nas democracias consolidadas, nos casos em que a legislação permite que a pasta seja comandada por um militar, costuma-se especificar que o mesmo tenha passado para a reserva há um determinado tempo.
6. Em novembro de 2004, o comandante do Exército, general Francisco Albuquerque, justificou ao jornal Correio Braziliense a morte de Vladimir Herzog. O ministro Viegas exigiu a retratação, mas o general reiterou a primeira opinião. Avaliando que se tratava de uma nova insubordinação do alto oficial contra seu superior civil — anteriormente tinha ocorrido um embate sobre salários — e sem contar com um posicionamento de apoio do presidente, Viegas pediu demissão.
7. A expressão foi cunhada por David Pion-Berlin (2005) para caracterizar a estratégia de diversos governos latino-americanos com relação às forças armadas. O autor argumentou que as lideranças políticas da região tinham adotado ações bem-sucedidas para evitar ameaças graves das suas forças armadas contra a institucionalidade democrática. No entanto, essa estratégia ficava aquém do objetivo de exercer a liderança civil sobre a política de defesa.
8. Segundo Amorim Neto (2010, 443), o poder do ministro estava embasado no fato de que era um dos líderes de um dos partidos mais importantes da base governista.

9. a) Decreto n. 3.466, de 17/05/2000 (que regulava a composição do MD quando Lula assumiu a presidência); b) Decreto n. 4.735, de 11/06/2003; c) Decreto n. 5.201, de 02/09/2004; d) Decreto n. 6.223, de 04/10/2007; e) Decreto n. 7.364, de 23/11/2010; f) Decreto n. 7.974, de 01/04/2013.
10. Na solicitação, foram feitos questionamentos sobre a ocupação de cargos no MD no período de 1999 a 2016. Em sua resposta, o MD informou que: "cabe esclarecer em relação aos questionamentos 1 a 4 que os dados relativos ao período de 1999 a 2004 não estão consolidados em sistemas informatizados, cuja consulta demanda pesquisas em atos publicados a mais de dez anos" (sic). Como as perguntas tinham como referência a data exata de troca entre os ministros da Defesa, o que objetivava compreender como a gestão de cada um influenciou a composição do MD, algumas das observações a seguir excluem as gestões Viegas e Alencar. Mesmo assim, acredita-se que a obtenção de dados referentes a cinco dos sete ministros da Defesa do PT seja suficiente para o teste da hipótese deste estudo.
11. A prática começou na gestão Jobim, que colocou um militar da ativa em um cargo de Direção e Assessoramento Superiores (DAS) 5. Trata-se de um dos cargos mais elevados entre os disponíveis aos civis no Ministério.
12. Para os militares, serão computadas as *gratificações de exercício em cargo de confiança privativa de militar*, as chamadas "letras". Quanto aos cargos tipicamente civis, somente serão contabilizados os cargos de *Direção e Assessoramento Superior (DAS)*, os mais relevantes cargos comissionados do Governo Federal.
13. Em muitas alterações de sua estrutura, o ministério somente possuía as letras A, B e E em suas composições, o que permitiu lógica semelhante para todas as mudanças estruturais do órgão.
14. Com Aldo Rebelo, muitos militares foram substituídos por indicações políticas, tendo em vista que o MD era o único ministério da Esplanada liderado pelo PCdoB, o que gerou a tendência de distribuição de cargos entre membros do partido.

LIMITAÇÕES DAS REFORMAS PARA O CONTROLE CIVIL SOBRE AS FORÇAS ARMADAS NOS GOVERNOS DO PT (2003-2016)

RESUMO:

O artigo debate a evolução do controle civil sobre as forças armadas nas gestões do Partido dos Trabalhadores (PT). A análise está concentrada nas transformações promovidas no Ministério da Defesa (MD), tanto com relação à sua estrutura quanto no perfil dos agentes que lá atuavam. Enquanto a maioria da literatura destaca positivamente as medidas que foram adotadas naquele período, o artigo defende que o período foi marcado pela permanência da autonomia institucional das forças armadas. A divergência decorre de lacunas ontológicas e metodológicas nos modelos analisados. Ontologicamente, tais modelos privilegiam o estudo da estrutura do MD, em detrimento do exame do perfil dos agentes que a compõem. Metodologicamente, há excessiva preocupação com a comparação, que deixa de considerar peculiaridades de cada país. O primeiro objetivo do artigo é contribuir para a correção dessas lacunas. O segundo é apontar os limites dos avanços no controle civil ao longo dos governos do PT. Três variáveis embasam o argumento: a) a evolução da estrutura organizacional do Ministério da Defesa; b) os perfis dos ministros da Defesa; c) o equilíbrio entre civis e militares na pasta.

Palavras-chave: Ministério da Defesa; Partido dos Trabalhadores; Controle Civil; Relações Civis-Militares.

ABSTRACT:

The article discusses the evolution of civilian control over the Armed Forces during the Workers' Party's (PT) Administrations. The analysis is focused on the transformations in the Ministry of Defense (MoD), both in its structure and in the profile of the agents that were serving there. While most of the literature considers that there were positive changes during the period, we argue that it can be best characterized by the continued institutional autonomy of the armed forces. The divergence arises from ontological and methodological gaps in the theoretical models analyzed. Ontologically, such models favor the study of the structure of the MD to the detriment of examining the profile of the agents that served there. Methodologically, there is excessive concern with comparison, which fails to consider the peculiarities of each case studied. The first objective of the article is to contribute to the correction of these gaps. The second is to clarify the limits of advances in the civilian control during PT's governments. Three variables support the argument: a) the evolution of the structure of the Ministry of Defense; b) the profiles of defense ministers; c) the balance between civilians and military in the MoD.

Keywords: Ministry of Defense; Workers' Party; Civilian Control; Civil-Military Relations.

Recebido em 15/03/2021. Aceito para publicação em 26/04/2021.

Forças armadas e segurança pública na Argentina e no Brasil: reafirmação e ruptura do papel interventor

Armed Forces and public security in Argentina and Brazil: disruption and continuity of the military interventionist role

Rev. Bras. Est. Def. v. 7, nº 2, jul./dez. 2020, p. 217-241
DOI: 10.26792/RBED.v7n2.2020.75218
ISSN 2358-3932

DAVID P. SUCCI JUNIOR
HÉCTOR LUIS SAINT-PIERRE

INTRODUÇÃO

A teorização sobre a violência organizada, os fatores que geram a guerra e os que garantem a paz, assim como os princípios que legitimam o uso da força, seus instrumentos, mecanismos de regulamentação e restrição, estão no cerne da disciplina de Relações Internacionais. No pós-Guerra Fria, o debate sobre a definição das atividades militares e policiais foi marcado pelo emprego das forças armadas em âmbitos convencionalmente considerados policiais, assim como a atuação de forças de segurança pública em esferas tradicionalmente entendidas como militares, o que foi caracterizado como um processo de *blurring*[1] destas delimitações. Acadêmicos sul-americanos classificam, em geral, este processo como a indistinção entre defesa e segurança pública (Saint-Pierre 2011), enquanto a bibliografia europeia e estadunidense frequentemente o apresenta como a confusão entre segurança interna e a internacional (Andreas and Price 2001; Bigo 2001; Eriksson and Rhinard 2009).

Os fenômenos que desbotaram a demarcação entre os instrumentos de força do Estado são de natureza diversa. Na América do Sul, este debate

David Paulo Succi Junior — Doutorando e mestre pelo Programa de Pós-Graduação em Relações Internacionais San Tiago Dantas (Unesp-Unicamp-PUC-SP), membro do Grupo de Estudos de Defesa e Segurança Internacional (Gedes) e bolsista Fapesp (2018/11168-3).
Héctor Luis Saint-Pierre — Instituto de Políticas Públicas e Relações Internacionais. Programa de Pós-graduação em Relações Internacionais "San Tiago Dantas". Professor Titular da Unesp. Pesquisador PQ CNPq. Pesquisador Fapesp (2017/21557-4). Coordenador-Executivo do IPPRI/Unesp.

associou-se majoritariamente ao crime organizado transnacional, em particular ao tráfico de drogas ilícitas e o seu impacto na violência urbana (Mathias, Zague, and Santos 2019; Rodrigues 2016; Sain 2017). Em países europeus a questão aparece recorrentemente associada a políticas de combate ao terrorismo, além da gestão migratória e de refugiados (Clarke 2013; Guittet 2008; Lutterbeck 2010). No leste europeu, questionou-se o uso do instrumento militar para a contenção de protestos e proteção de infraestrutura estratégica (Weiss 2012). Em países africanos encontramos debates centrados em conflitos civis (Ojo 2008) e no uso das forças armadas contra crimes ambientais (Reitano, Lugo, and Jesperson 2017), por vezes denominado de militarização verde (Marijnen and Verweijen 2016).

Para além do direcionamento das forças armadas para o interior das próprias fronteiras nacionais, alguns autores se preocupam com as missões atribuídas aos militares em ações externas, com destaque às operações de paz sob a égide da Organização das Nações Unidas (ONU) (Friesendorf 2012; Geener-Barcham 2007), assim como a relação entre estas operações externas e a atuação doméstica dos militares (Harig 2015; Hoelscher and Norheim-Martinsen 2014).

Nossa análise foca-se no emprego dos meios militares no interior de suas fronteiras nacionais, especificamente, em operações que envolvem o uso da força,[2] por tensionar a compreensão convencional sobre a distribuição dos instrumentos de violência letal — militares — e coerção mínima — polícias. Tanto nas teorias do Estado quanto nos fundamentos das Relações Internacionais distingue-se, como função epistemologicamente demarcatória, o âmbito doméstico e o internacional. No primeiro, caracterizado como normativamente pacífico, descarta-se a eliminação física do adversário. No segundo, considerado anárquico, a força é empregada para garantir a ordem jurídica do âmbito internacional, em que a violência letal é um instrumento para lidar com contenciosos e para, no limite, garantir a própria existência (Aron 2002; Freund 1995; Santillán 1997; Waltz 2002).

Ainda que o fenômeno estudado seja recorrentemente associado às características do sistema internacional pós-Guerra Fria, as forças armadas na América do Sul, assumiram as mais diversas atribuições domésticas desde a fundação de seus Estados. Os militares sul-americanos ocuparam uma gama de atividades que abarcou desde o desenvolvimento nacional até a manutenção da ordem institucional e social, sendo a onda de ditaduras, que se propagou nesta região entre as décadas de 1960 e 1980, um dos momentos de maior penetração dos meios castrenses nas instâncias estatais (Rouquié 1984). Neste sentido, ao contrário do que a divisão teórica tradicional entre interno e externo pode nos fazer pensar, na América do Sul a utilização da violência militar no âmbito doméstico não constitui uma

excepcionalidade. Neste sentido, consideramos este fenômeno pela ótica da continuidade e não da exceção.

Inspiramo-nos nos casos argentino e brasileiro, por serem tratados pela bibliografia como exemplos de padrões opostos de emprego das forças armadas. Desde o fim da ditadura, no final da década de 1980, conformou-se na Argentina um consenso básico em matéria de defesa que, mais do que definir um plano para a organização da defesa nacional, representou a nítida delimitação das funções militares no país (Pereira 2019). Como veremos, esta delimitação começou a ser tensionada pelas operações Fortin e Escudo Norte e pelo Decreto 683, de 2018. No Brasil, por outro lado, a Constituição de 1988, que sucedeu o governo autoritário, manteve a garantia da lei e da ordem como função das forças armadas, recorrentemente mobilizadas para segurança pública durante a década de 1990. Ademais, entre fim da década de 1990 e início dos anos 2000, vivenciou-se um processo de institucionalização das missões militares internas.

Como explicar a divergência doutrinaria tão profunda em países com trajetórias históricas semelhantes? Que condições produziram padrões opostos de emprego militar no Brasil e na Argentina? Há três grandes teses consolidadas na bibliografia sobre o emprego interno das força militar na América do Sul: 1) a resposta pragmática, ou seja, a ideia de que a atuação das forças armadas no âmbito doméstico resulta de uma resposta objetiva a uma realidade concreta; 2) o controle político dos civis sobres os militares, isto é, o argumento de que o fenômeno estudado reflete a debilidade do controle político dos civis sobre a instituição militar; 3) e as pressões externas, representadas por interesses estadunidenses na região.

Consideramos que, apesar de trazerem contribuições muito relevantes para a compreensão das missões militares sul-americanas, estas abordagens são insuficientes para explicar a aceitação e o rechaço do emprego interno das forças armadas na Argentina e no Brasil. Neste sentido, propomos endereçar esta questão com base na perspectiva sociológica de Berger e Luckmann (2009), mais especificamente, através do conceito de papel social. Argumentamos que os processos de rompimento e continuidade do papel das forças armadas nesses países condicionaram a conformação dos padrões divergentes de emprego dos militares. Para mostrar como o conceito de papel, enquanto categoria analítica, revela uma outra dimensão do fenômeno analisado, devemos diferenciá-lo de outros dois termos — função e missão.

A diferenciação é necessária, pois ainda que estes três termos sejam recorrentemente utilizados como sinônimos, carregam semânticas diferentes que, para os fins do nosso argumento, não podem ser intercambiadas. Concordamos com Mathias e Guzzi (2010), que reservam o termo "função" para aquilo que está estabelecido na legislação e "missão" para

se referir a uma tarefa específica que, ao ser atribuída a determinado ator, é tomada pelo mesmo como de sua responsabilidade. O papel, como definido por Berger e Luckmann (2009), indica uma dimensão intersubjetiva. Para os autores, este representa a tipificação de uma forma de ação, o que não se trata somente de "um particular ator que executa uma ação tipo X, mas da ação tipo X como sendo executável por qualquer ator a quem possa ser plausivelmente imputada a estrutura de conveniência em questão" (Berger and Luckmann 2009, p. 101). Desta forma, o papel constitui uma ideia intersubjetivamente compartilhada sobre um tipo de atividade e um modo de executá-la que se perpetua no tempo, gerando a expectativa de que todos aqueles que assumirem este papel particular, independentemente de suas características individuais, o executarão da mesma forma, assim como em uma peça teatral o ator assume um papel previamente existente.

No caso em questão, há um conjunto de atuações que se espera de um militar e da instituição castrense, independentemente dos indivíduos que ocupam esta posição. Neste sentido, a título de exemplo, pode haver a expectativa, socialmente compartilhada, de que a força militar seja direcionada para a segurança pública, por ser considerada uma atividade normal desta instituição, da mesma forma, pode haver a expectativa de que ela se mantenha alheia aos problemas internos, por não fazerem parte de seu espectro de atribuições. O papel tem implicações diretas para a aceitação de determinadas ações e sua naturalização no tempo. Deste modo, revela uma dimensão do fenômeno ignorada pelas três explicações consolidadas nos trabalhos acadêmicos.

Em um primeiro momento, expomos as três principais teses sobre o emprego interno da força militar, apontando suas principais debilidades explicativas. Posteriormente, utilizando o conceito de papel, explicamos a divergência no padrão de emprego das forças armadas brasileira e argentina. Por padrão de emprego entendemos o conjunto de ações efetivamente desempenhadas pelas forças militares no período analisado, o que difere do conceito de papel, enquanto a forma de ação que se espera daquele que assume uma atividade social específica. Ainda que o papel não delimite de forma determinista a ação daquele que o assume, produz restrições e incentivos para seu comportamento. Consideramos que, desde a fundação das forças militares nestes dois países, reconheceu-se um papel interventor, que atribui às forças armadas a responsabilidade e a legitimidade para combater a desordem, cujo significado longe de ser claro, transformou-se ao longo do tempo. A divergência do padrão de emprego dos meios militares nos países estudados estabeleceu-se com a ruptura deste papel, no caso argentino, e sua continuidade no Brasil, como resultado dos diferentes processos de transição da ditadura para o regime democrático.

A TESE DA RESPOSTA PRAGMÁTICA

Do ponto de vista da tese da resposta pragmática, o emprego das forças armadas para a repressão das atividades do crime organizado resultaria de uma decisão racional, tomada em reação a uma avaliação objetiva da conjuntura que se apresenta como fator determinante ao tomador de decisão. Este argumento baseia-se em duas ideias principais: 1) os grupos vinculados a atividades econômicas ilegais, em especial ao narcotráfico, adquiriram armamentos e um elevado grau de organização que superam a capacidade da polícia; e 2) a região sul-americana goza de relativa estabilidade entre Estados, mas, em compensação, sofre de altos índices de violência doméstica. Por estas duas razões, haveria a necessidade de se recorrer ao instrumento estatal de maior poder de fogo para eliminar a violência ilícita (Norden 2016; Pion-Berlin and Trinkunas 2011; Sampó 2019). Neste sentido, Pion-Berlin (2016) caracterizou como pragmática a alocação do instrumento militar para o combater o crime organizado no interior das fronteiras nacionais, opondo-se à delimitação entre interno e externo, que considera ser resultado de uma desconfiança em relação às forças armadas, vinculada às experiências autoritárias protagonizadas pelas instituições militares na região.

Dois argumentos questionam a capacidade explicativa desta perspectiva. Em primeiro lugar, pode-se duvidar da eficácia da resposta militarizada, diante da permanência e intensificação dos altos índices de violência. No Brasil, segundo dados do Ministério da Defesa, de 1992 até junho de 2018 foram desenvolvidas 23 operações de Garantia da Lei e da Ordem (GLO) para combater a violência urbana. Dessas, 10 ocorreram na cidade do Rio de Janeiro, sendo que as mais recentes aumentaram sua duração, como a Operação Arcanjo, que se estendeu de novembro de 2010 a julho de 2012 (Brasil 2020) e a Operação Rio de Janeiro, que teve início em 2017 e foi sobreposta por uma intervenção federal na segurança pública do estado do Rio de Janeiro, estabelecida em fevereiro de 2018 e comandada por um general da ativa (Betim 2018; Martín 2018). Se, sob esta ótica, o emprego do instrumento militar para combater o crime organizado no Rio de Janeiro é em uma ação pragmática que responde a uma realidade objetiva. Esta parece não ter cumprido seu objetivo, uma vez que houve maior recorrência e intensificação das operações militares, o que, por esta lógica, significaria um agravamento da situação.

Por outro lado, o argumento da necessidade objetiva de empregar forças armadas para combater o crime organizado é questionado por um conjunto de autores, para os quais este tipo de resposta corresponde a uma percepção específica da realidade (Saint-Pierre 2007a). Pion-Berlin (2016),

em defesa de uma perspectiva pragmática, argumenta que a escolha de se direcionar a força militar para o âmbito doméstico deve ser baseada em três questões, que considera objetivas, como: urgência do problema; capacidade dos militares de responder ao mesmo de forma efetiva; e a inexistência de solução alternativa. O autor apresenta uma proposta normativa sobre a forma em que os países devem gerir as missões militares, mas não consegue explicar as decisões já tomadas e sem resultados positivos visíveis no caso brasileiro.

Com efeito, a urgência do problema, a capacidade de resposta eficiente dos militares e a inexistência de outras soluções dependem de um processo de definição e interpretação da realidade. Ainda que vários atores observem a mesma realidade material, esta não será necessariamente percebida da mesma forma. Mesmo que o for, a reação à mesma dificilmente será homogênea, de modo que não se pode esperar que haja um único tipo de ação possível para determinada realidade material (Mathias and Soares 2003; Saint-Pierre 2011). Assim, a escolha do instrumento para lidar com o crime organizado e outros problemas de segurança, depende da percepção da realidade e de uma escolha política específica, não de uma resposta meramente técnica.

A TESE DO CONTROLE POLÍTICO SOBRE OS MILITARES

A bibliografia produzida na década de 1990 é caracterizada pela preocupação com o controle político dos militares, cuja questão central é a inserção das forças armadas no ordenamento político democrático posterior às ditaduras militares (D'araujo and Castro 2000; Hunter 1994; 1996; Zaveruccha 2005; 2008). Considerava-se que os países que estabeleceram um controle político mais estrito sobre suas forças armadas conseguiram restringir a atuação interna dos militares, enquanto aqueles que apresentavam debilidades nesse controle tiveram uma atuação militar mais constante no âmbito doméstico (Saint-Pierre 2007b).

Este argumento pressupõe que as forças armadas seriam favoráveis à atuação na segurança pública, como forma de garantir sua influência política, enquanto o governo civil seria contrário a esse emprego devido ao passado ditatorial. Todavia, ao estabelecer uma relação direta entre a subordinação política dos militares e a redução de suas missões domésticas, esse argumento desconsidera as situações em que os próprios governantes civis requerem o emprego da força militar no interior das fronteiras nacionais (Diamint 2015; Head and Scott 2009).

O foco no controle institucional das instituições militares, auxilia-nos a compreender quem decide, mas não o que é decidido. Neste sentido, esta

abordagem é questionada por Levy (2014), que diferencia o controle dos militares — dominação política do governo civil sobre a instituição militar — da militarização — vinculada aos mecanismos de legitimação do uso da força. Com efeito, um governo civil com pleno controle político dos instrumentos militares do Estado pode decidir emprega-los no interior das fronteiras nacionais, assim como militares que gozam de ampla autonomia podem resistir à atuação em questões de segurança pública por inúmeros motivos, como, por exemplo, não se reconhecerem adequados a este tipo de operação ou por considera-la degradante à sua profissão (Pion-Berlin 2012).

O avanço, ainda que lento e deficitário, da institucionalização do controle civil sobre os militares no Brasil não resultou no rompimento com um padrão de emprego interno, pelo contrário, estas operações foram intensificadas. Por outro lado, pode-se considerar a Argentina que, apesar de ser tradicionalmente classificada pela literatura como caso emblemático de consolidação do controle político civil sobre os militares (López 2007; Saint-Pierre 2007b), desde meados do governo de Cristina Kirchner e, principalmente, durante a gestão de Maurício Macri, começou a flexibilizar os impeditivos ao emprego dos instrumento militar no interior de suas fronteiras (Sain 2017).

A TESE DAS PRESSÕES EXTERNAS

As explicações que aludem a pressões externas enquadram a questão das missões militares em um panorama mais amplo, do histórico ímpeto estadunidense por estabelecer a América Latina como zona de influência, ao menos desde o século XIX (Santos 2007). Nesta abordagem argumenta-se que durante a Guerra Fria consolidou-se na região, sob a égide da Doutrina de Segurança Nacional, uma divisão do trabalho militar. Por um lado, um fronte interno, de combate ao inimigo comunista, de responsabilidade das forças armadas latino-americanas. De outro, um fronte internacional, de enfrentamento ao pacto de Varsóvia, de responsabilidade dos Estados Unidos (López 1987). Esta perspectiva defende que o interesse estadunidense de manter as forças armadas latino-americanas voltadas a questões internas perdurou, mesmo com o desaparecimento do inimigo soviético. Assim, o combate ao comunismo teria sido substituído pelo combate às "novas ameaças"[3], especialmente o narcotráfico, que já ganhava espaço na agenda de segurança dos Estados Unidos nos últimos anos da Guerra Fria (Eissa 2014; Rodrigues 2012). Deste modo, as forças armadas da região teriam como foco ameaças não-estatais, deixando a defesa convencional do continente sob a responsabilidade estadunidense (Sanahuja and Verdes-Montenegro 2014; Villa 2014).

Os autores que se atentam a esta dimensão para compreender as missões militares sul-americanas, destacam os arranjos e reuniões regionais referentes à temática, em especial a Organização dos Estados Americanos (OEA), as Conferências de Ministros de Defesa das Américas (CMDAs) e a União das Nações Sul-Americanas (Unasul). No âmbito da OEA destaca-se a consolidação da ideia de multidimensionalidade da segurança e da ameaça, em especial, na Declaração de Bridgetown, de 2002, e na Conferência Especial sobre Segurança, realizada em 2003, no México. A multidimensionalidade flexibiliza a agenda de segurança para abranger elementos das mais diversas naturezas como terrorismo, crime organizado transnacional, tráfico de drogas, armas e pessoas, ataques cibernéticos, corrupção, lavagem de dinheiro, pobreza extrema, exclusão social, deterioração do meio ambiente e riscos à saúde. A multidimensionalidade das ameaças e da segurança torna-se um aspecto particularmente sensível para o nosso objeto de estudo quando abordada nas CMDAs, uma vez que, diferentemente das reuniões da OEA, neste âmbito, as questões são debatidas pelos responsáveis pela pasta de Defesa, ou seja, por aqueles que administram as forças armadas de seus Estados. As mesmas ameaças, não vinculadas a questões convencionais das relações interestatais e da defesa, que foram tratadas na Declaração sobre Segurança nas Américas, de 2003, estiveram presentes em todas as declarações das CMDAs entre 1995 e 2014, tendo o narcotráfico recebido especial atenção. Ainda que a adoção de uma perspectiva multidimensional da ameaça e da segurança não resulte necessariamente na definição dos instrumentos específicos de combate, a ambiguidade com que essas questões são tratadas nas CMDAs favorece a consolidação da agenda estadunidense.

Em contrapartida, em 2008, sob a égide da Unasul, foi aprovada a criação do Conselho de Defesa Sul-Americano (CDS), com a notória ausência dos Estados Unidos. Nesta instituição, as questões referentes ao narcotráfico e à segurança pública foram tratadas em conselhos específicos, distintos daquele destinado à cooperação em defesa — o Conselho sobre o Problema Mundial das Drogas (CSPMD) e Conselho Sul-Americano em Matéria de Segurança Cidadã, Justiça e Coordenação de Ações contra a Delinquência Organizada Transnacional (DOT) (Saint-Pierre 2012).

Neste sentido, pode-se afirmar que em relação às "novas ameaças", a Unasul se opôs à doutrina apregoada pela OEA e pelas instâncias vinculadas à segurança hemisférica. Enquanto no âmbito das CMDAs a defesa e a segurança interna ficaram intimamente vinculadas, no foro sul-americano foram claramente distinguidas. Neste sentido, Martinez e Lyra (2015) defendem que na Unasul houve um processo de dessecuritização do narcotráfico, retirando a excepcionalidade do tema para inclui-lo na lógica da polí-

tica regular dos princípios democráticos. Ademais, os autores consideram que o tratamento dado à questão do narcotráfico nesta organização indicou a pretensão de romper com a lógica estadunidense da guerra às drogas.

Ainda que esta seja uma dimensão relevante para compreender nosso objeto de análise, dificilmente pode ser indicada como uma variável explicativa conclusiva. As pressões externas sofridas por Argentina e Brasil, no que se refere à definição das missões das forças armadas no pós-Guerra Fria, foram similares em sua natureza, o que, porém, não resultou em padrões similares de emprego dos militares nestes países.

É ilustrativa a resposta brasileira ao questionário realizado em 2001 pela Secretaria Geral da OEA, como atividade preparatória para a reunião de 2003. Quando questionado sobre as implicações das novas ameaças para a segurança hemisférica, a representação do Brasil posicionou-se explicitamente contrária ao emprego das forças armadas em segurança pública, em contraste com as operações militares observadas no país. Vale recordar que foi também em 2001 que se estabeleceu no país o decreto 3897, que regulamentou as operações de GLO. Por outro lado, a capacidade da Unasul de contrapor a agenda estadunidense pode ser questionada. Em março de 2009, o então presidente brasileiro, Luiz Inácio Lula da Silva, declarou que a América do Sul contaria com uma agência própria para lidar com os problemas do narcotráfico e que os Estados Unidos deveriam atuar não como fiscais, mas como parceiros neste âmbito (Observatório Cone Sul de Defesa e Forças Armadas 2009). No mesmo mês, de acordo com documento disponibilizado pelo portal *Wikileaks*, o então ministro da Defesa, Nelson Jobim, em conversa com o embaixador estadunidense, Clifford M. Sobel, afirmou que Lula da Silva havia prometido a seu homologo estadunidense, Barack Obama, se empenhar em engajar os países da região para trabalhar junto aos Estados Unidos no combate às drogas. Neste contexto, Sobel (2009) reportou que o ministro da Defesa brasileiro considerava o CDS o espaço ideal para levar os Estados da região a empregar seus militares na luta contra o narcotráfico.

REAFIRMAÇÃO E RUPTURA DO PAPEL INTERVENTOR

Ainda que os elementos apresentados influenciem a constituição dos padrões de emprego das forças armadas, consideramos que o papel socialmente atribuído a estas instituições, isto é, a expectativa social em relação a determinada forma de ação considerada própria dos militares, constitui um fator essencial para se compreender a divergência observada nestes países. O papel revela a relação mais profunda de uma sociedade com seus meios de força, que não é capturada pelas perspectivas anteriormente dis-

cutidas, mas que fornece as condições de possiblidade para que um padrão específico de emprego das forças armadas se conforme. Defendemos, assim, que a escolha de um determinado tipo de atuação militar, em detrimento de outra, está vinculada aos processos de reafirmação e ruptura de um tipo específico de papel militar: o papel interventor. Este atribui à instituição militar a responsabilidade e legitimidade de preservar ou recuperar a ordem. A abrangência e consequente maleabilidade da ideia de ordem, porém, permitiu que este papel sustentasse não apenas o uso das forças armadas em segurança pública, mas um amplo conjunto de atividades, de diferentes naturezas, desempenhadas pelos militares ao longo da história argentina e brasileira. Estas compreendem operações que vão desde a ingerência política e destituição de governos, até a atuação direta na garantia da lei e na contenção de movimentos de contestação política.

Não pretendemos aqui identificar a gênese da construção social do papel das forças armadas, mas evidenciar como o envolvimento das instituições militares nas questões internas dos países analisados esteve historicamente associado ao lugar que os militares ocuparam em sua relação com o Estado e a sociedade. Como indicou Rouquié, a priorização de um inimigo interno é uma realidade na região que antecede em muito a Guerra Fria:

> são os problemas internos, os perigos domésticos, sociais ou políticos que solicitam propriamente a ação militar das forças armadas latino-americanas. No Brasil — onde os oficiais desconhecem as guerras desde a do Paraguai, que terminou em 1870 e, sem remontar às 'emoções' regionais que pontuaram o passado imperial, com rebeliões como a da Sabinada na Bahia em 1837, ou as revoltas Praieira e Farroupilha de Pernambuco e do Rio Grande do Sul de 1840 a 1850 — foi o Exército que esmagou, não sem alguma dificuldade, as rebeliões camponesas do Contestado e de Canudos. O Exército argentino nunca teve outros inimigos além dos índios reprimidos no Sul e pacificados no Norte nos anos trinta, dos metalúrgicos de Buenos Aires em 1919, dos trabalhadores temporários agrícolas da Patagônia em 1920 e dos anarquistas vindos da Europa. (Rouquié 1984, 123).

O processo de modernização e profissionalização das forças armadas da região, entre os séculos XIX e XX, foi importante na conformação do papel militar. Segundo Rouquié (1984, 122), em decorrência deste, os militares assumiram atividades que excediam amplamente a tarefa de defesa externa como: a centralização do poder, em oposição a rebeliões indígenas; o controle do território, através das guarnições estabelecidas como representações do Estado; defesa da soberania e integração dos "diferentes componentes étnicos de uma mesma comunidade". Desde então, a ingerência militar na vida política dos países baseou-se em uma suposta neutra-

lidade legitimadora das forças armadas, identificadas como reserva moral e representação da unidade nacional, identificando ameaças domésticas a serem combatidas. Segundo Soprano (2016), a modernização neste período tem um efeito paradoxal, uma vez que o ímpeto de estatização do Exército resultou na conquista do Estado pelo setor castrense.

Na Argentina, o século XX foi marcado por golpes militares e pelo emprego das forças armadas para repressão de mobilizações sociais. Em 1943, um golpe destituiu Ramón Castillo e estabeleceu um governo militar, na esteia do qual Juan Domingo Perón fortaleceu-se como liderança política. Posteriormente, em 1955, Perón foi destituído por uma intervenção militar autodenominada Revolução Libertadora, que prescreveu e combateu o peronismo (O'Donnell 1973). Em 1966, outro golpe militar, autodenominado Revolução Argentina, destituiu o presidente Arturo Illia, da União Cívica Radical, sob o argumento de que apenas um governo autoritário seria capaz de controlar o peronismo. Por fim, em 1976, com um golpe militar chamado de "Processo de Reorganização Nacional", estabeleceu-se uma ditadura militar que perdurou até 1983. Segundo O'Donnell (1973), entre 1955 e 1983 conformou-se um jogo democrático impossível, em que, por um lado, eleições livres resultariam na vitória do peronismo, sobre o qual pesava a desconfiança de que, quando no poder, não respeitaria as regras democráticas; por outro lado, o maior partido de oposição, não apenas não teria condições de ser eleito, sem que houvesse restrições à candidatura peronista, como provavelmente não conseguiria governar. Neste contexto, as elites nacionais aceitavam os militares como árbitros do jogo político — garantes da ordem —, com a atribuição de encerrar a disputa eleitoral se o peronismo saísse vitorioso ou se os partidos antiperonistas não tivessem condição de governar de forma eficaz. Há, portanto, a atribuição de um papel interventor às instituições castrenses, cuja interferência na política era considerada aceitável e legítima. Ademais, mesmo nos momentos em que as forças armadas não estiveram no governo, seu emprego interno, principalmente para a repressão a manifestações e greves, foi constante, como no governo de Arturo Frondizi (1958-1962) (Dellasoppa 1998; Romero 2006).

No Brasil, ainda que a tomada direta do poder pelos militares não tenha sido tão recorrente quanto na Argentina, as forças armadas, em especial o Exército, estiveram presentes em todas as vicissitudes da política nacional (Hayes 1991; Rouquié 1984). Da mesma forma, foram constantemente mobilizadas no interior das fronteiras nacionais. Neste âmbito, chama atenção o termo "pacificação", utilizado para se referir a um série de operações historicamente executadas pelo exército com o objetivo de controlar o território e a população (Souza et al. 2017). O termo foi empregado inicial-

mente na guerra de conquista empreendida pelos portugueses contra os indígenas no contexto da colonização (Moreira 2017), mas se perpetuou na história do país, desde a repressão militar a movimentos contestatórios no século XIX, até as operações de segurança pública desenvolvidas pelas forças militares nos anos 2000 (Souza et al. 2017).

Durante o Império, as forças armadas foram empenhadas na contenção de revoltas internas como: Balaiada (1831-1841); Cabanagem (1835-1840); Farroupilha (1835 e 1845); Sabinada (1837-1838); Revolta de Alagoas (1844); Revolta Praieira (1848-1850). Durante a Primeira República, para além de atividades como o comando de forças policiais e bombeiros, intervenção na política local a mando federal e imposição de ordens legais, destacou-se a atuação interna das forças armadas na repressão a Canudos (McCann 2007). Ademais, a instituição castrense participou diretamente da queda do Império e da República Velha, deu sustentação à ditadura do Estado Novo, em 1937 e destituiu seu líder, Getúlio Vargas, em 1945. Em 1964, um golpe militar instituiu uma ditadura no país que durou até 1985 e representou um dos momentos de maior ingerência das forças armadas no âmbito interno brasileiro. Neste período, enfatiza-se a definição de um inimigo interno sob a lógica da Doutrina de Segurança Nacional, que se baseou na ideia de uma suposta infiltração comunista e teve como resultado a perseguição e repressão política de todos aqueles contrários ao regime (Rouquié 1984).

Tais intervenções estão diretamente vinculadas ao papel de garantidores da ordem, que constitui elemento central da identidade militar brasileira e se cristalizou enquanto função na quase totalidade das constituições nacionais, como salientado por Mathias e Guzzi (2010). É ilustrativo o fato de o militar responsável pela força de "pacificação" que reprimiu a Balaiada, coronel Luiz Alves de Lima da Silva, posteriormente conhecido como Duque de Caxias, ter se tornado modelar no pensamento militar brasileiro (Castro 2002). Ainda que a figura de Caxias tenha se consolidado como exemplo militar entre os anos de 1920 e 1930, os seus principais biógrafos, como o Padre Joaquim Pinto de Campos (1936 [1878]), Affonso Carvalho (1976 [1938]), Paulo Matos Peixoto (1973) e Cláudio Moreira Bento (2003), reproduziram a mesma narrativa sobre Caxias perpetuada no tempo (Souza 2001). Nesta, o patrono do Exército — e, consequentemente, as forças armadas — é apresentado não apenas como garantidor da ordem social e política, mas como a própria representação do Estado e da nação.

A instituição militar historicamente entendeu-se como responsável por garantir a ordem, que consideravam necessária à modernização do país, apresentando-se como superiores à população em geral e às elites políticas. O primeiro editorial da revista militar *A Defeza Nacional*, declarou que "o

Exército — única força verdadeiramente organizada" torna-se "factor decisivo de transformação política e estabilisação social"[4] (A Defeza Nacional 1913). De forma similar, Góis Monteiro, uma das figuras militares mais influentes do século XX, considerava ser dever o Exército garantir a ordem interna, não apenas em termos da existência material, mas do ponto de vista da integridade moral e política (Lima 2011).

As particularidades das transições das ditaduras militares para o regime democrático na década de 1980 são fundamentais para compreender a conformação dos padrões divergentes de emprego interno das forças armadas nestes dois países, uma vez que esse processo levou a uma ruptura do papel interventor na Argentina e uma reafirmação do mesmo no Brasil. No caso argentino, o colapso da ditadura, vinculado ao descontentamento relativo ao desempenho econômico, à repressão violenta aos opositores do governo, assim como à derrota na Guerra das Malvinas, rompeu com o papel dos militares, que deixaram de ser vistos como interventores legítimos (Linz and Stepan 1999; López 1994; Sain 1999). No Brasil, por outro lado, o intenso controle de uma transição lenta, gradual e segura com o qual os militares desenharam sua retirada do centro do poder político, fez com que o papel interventor das forças armadas não fosse questionado e se perpetuasse (Mathias 1995; Oliveira 1994; Soares 2006).

Neste sentido, após o fim da ditadura, estabeleceu-se na Argentina um consenso básico em matéria de defesa, cujo ponto central foi o rechaço à atuação militar no interior das fronteiras nacionais, que se cristalizou em um conjunto de legislações, como a Lei de Defesa Nacional de 1988 e a Lei de Segurança Interna de 1991. Ambas delimitaram a função das forças armadas exclusivamente à defesa em relação a ameaças externas, admitindo seu emprego interno apenas como apoio às forças de segurança, mas proibindo a formulação de doutrina e treinamento específico para este tipo de operação, considerada excepcional. Em 2001, a Lei de Inteligência Nacional estabeleceu a distinção entre Inteligência Criminal e Inteligência Estratégica Militar, restringindo esta última à produção de inteligência operacional e tática necessárias para o planejamento e condução das operações militares. Por fim, em 2006, diante de grupos políticos que pretendiam classificar o crime organizado transnacional e o terrorismo como ameaças externas, a fim de justificar o emprego doméstico das forças armadas, estabeleceu-se o decreto 727, que regulamentou a Lei de Defesa Nacional e definiu como ameaças externas apenas aquelas de caráter militar-estatal, rechaçando enfaticamente a ampliação do uso dos instrumentos militares para combater às denominadas "novas ameaças".

No Brasil, por outro lado, o envolvimento militar em segurança pública, mais especificamente no combate ao narcotráfico, nunca foi controverso,

como o foi na Argentina. Ainda que na década de 1990 houvesse certa desconfiança das forças armadas em relação aos interesses estadunidense no envolvimento dos militares neste tipo de operação (Santos 2004), a função GLO e o papel interventor das forças armadas que legitimava a mobilização militar no âmbito doméstico não foi questionado. Desde a década de 1990, recorreu-se frequentemente ao emprego de militares em operações de segurança pública — entre janeiro de 1992 e junho de 2018, foram realizadas 132 operações de GLO no país (Brasil 2020). Houve um esforço de institucionalizar estas operações através da legislação infraconstitucional. Neste sentido, além da Constituição de 1988, que manteve a garantia da lei e da ordem entre as funções das forças armadas, em 1991, a Lei Complementar 69 limitou a prerrogativa de requisitar a atuação castrense no interior das fronteiras nacionais ao presidente da República. Esta primeira norma foi posteriormente substituída pela Lei Complementar 97 de 1999, a qual determinou que a atuação militar neste tipo de operação deve ocorrer apenas quando os instrumentos destinados à segurança pública forem considerados esgotados. Esta segunda lei foi alterada duas vezes. Em 2004, pela Lei Complementar 117, e em 2010, pela Lei Complementar 136. A primeira estabeleceu que os mecanismos de segurança pública são considerados esgotados quando o chefe do Executivo Federal ou Estadual assim os reconhecerem, enquanto a segunda incluiu ao conjunto de funções militares ações preventivas e repressivas contra crimes transfronteiriços e ambientais.

Soma-se ainda a este conjunto de normas o Decreto 3897, de 2001, que fixou as diretrizes para o planejamento, coordenação e execução das operações de GLO e a Lei 13.491, de 2017, que, por pressões das forças armadas, transferiu para a Justiça Militar a responsabilidade de julgar soldados que cometerem crimes dolosos contra a vida de civis durante operações militares. Destaca-se ainda que, em 2005, foi criado o Centro de Instrução de Operações de Garantia da Lei e da Ordem, destinado ao adestramento e produção de doutrina militar voltada à atuação em operações domésticas. Reafirmando a institucionalização destas funções, em 2013, o Ministério da Defesa publicou um documento que estabeleceu orientações para o planejamento e emprego das forças armadas nas ações de GLO.

Por tanto, pode-se observar que, independentemente das alterações conjunturais de ameaças e dos grupos considerados inimigos internos, manteve-se inalterado o papel interventor das forças armadas no Brasil. Por fim, destacamos que, ao passo que no Brasil há uma constante reafirmação do papel interventor, na Argentina houve mudanças vistas como o tensionamento do papel militar consolidado no consenso básico em matéria de defesa. É representativo, neste sentido, o estabelecimento, em 2011, de dois programas de proteção de fronteira: o Fortín II, do Ministério da

Defesa, e o Escudo Norte, do Ministério da Segurança. O primeiro, assim como seu predecessor, tinha como objetivo intensificar o monitoramento das fronteiras e detectar voos ilícitos vinculados ao narcotráfico, para o qual se previa a cooperação entre forças armadas e policiais. O segundo, por sua vez, visava aumentar a vigilância e controle dos espaços terrestre, fluvial e aéreo na fronteira nordeste e noroeste do país a fim de combater o delito transnacional. Diante desta sobreposição, e com a justificativa de apoio logístico, o Exército aumentou sua participação em operações de segurança pública nas regiões de fronteira. Enquanto a Força Aérea e a Marinha foram reticentes em relação a este tipo de ação, o General César Milani, que havia assumido naquele ano o posto de Chefe do Estado-Maior do Exército, as defendeu (Sain 2017). A possibilidade de flexibilização das funções militares na Argentina ganhou especial destaque durante os debates que precederam as eleições presidenciais em 2016, que resultaram na eleição de Maurício Macri (Anzelini 2017; Soares and Soprano 2016).

Durante a gestão Macri, o decreto 228 de 2016 estabeleceu estado de emergência em segurança pública em todo o território nacional que, segundo Sain (2017), implicou na atuação militar no interior das fronteiras nacionais. Ainda em relação à proteção das fronteiras contra atividades criminosas, foram aprovadas as Regras de Proteção Aeroespacial, autorizando assim, em caso de aeronave não identificada, a realização de uma série de medidas gradativas que podem, no limite, resultar no abate da mesma (Sain 2017). O gesto de ruptura mais profundo empreendido pela gestão Macri foi a promulgação do decreto 683 de 2018, que modificou o 727 de 2006. Em seu preâmbulo, declara-se que as ameaças externas não se restringem àquelas de caráter estatal-militar, em clara contraposição ao decreto de 2006, que rechaçava o uso das forças armadas para lidar com as "novas ameaças", ainda que fossem de origem externa. Ponderamos, porém, que as leis de Defesa Nacional e Segurança Interna não sofreram alterações até o momento e que a designação de forças militares para o âmbito interno se restringiu às áreas de fronteira. Ademais, a reversão das medidas, particularmente do decreto 683, com o fim do governo Macri, sugere a permanência e resistência da ruptura com o papel interventor, que marcou o fim da ditatura militar.

CONCLUSÕES

O emprego da força militar no interior das fronteiras tensiona a concepção tradicional sobre uma clara divisão entre o doméstico e o internacional, que reflete um tipo específico de organização da violência — monopólica no âmbito interno e livre-concorrencial na esfera internacional.

Na América do Sul, porém, a atuação militar no interior das fronteiras nacionais é uma característica que marca a região desde a fundação dos seus Estados, o que ilustramos através dos casos argentino e brasileiro. Ainda assim, a bibliografia tende, implícita ou explicitamente, a tratar este fenômeno como uma ruptura da normalidade, explicada pela necessidade pragmática, pelo controle político deficitário dos civis sobre os militares ou em decorrência de pressões e interesses externos.

O conceito de papel interventor nos possibilita compreender o fenômeno como uma continuidade em oposição à ideia de excepcionalidade. Esta perspectiva revela um processo de normalização e legitimação das missões atribuídas às forças armadas, não considerado pelas outras três perspectivas apresentadas. Ainda que não seja novo o argumento de que as especificidades dos processos de transição das ditaduras para a democracia produziram efeitos divergentes para as forças armadas dos países estudados, consideramos que a interpretação deste processo através da perspectiva proposta, permite aprofundar a compreensão de seu significado e de suas consequências para a definição das missões militares.

Concluímos que a forma na qual se desenvolveu a transição da ditadura militar para o governo civil na Argentina colocou em questão o papel desempenhado pelos militares neste país, o que envolveu a transformação das expectativas sociais em relação às suas forças armadas, assim como a forma em que os militares compreendem sua razão de ser. Este movimento de ruptura afastou os militares não apenas da vida política, mas também das operações de segurança pública. No caso brasileiro, por outro lado, as especificidades da saída controlada da ditadura militar possibilitaram a continuidade do papel interventor dos militares, que nunca foi efetivamente questionado.

REFERÊNCIAS

A Defeza Nacional. 1993. "Editorial". *A Defeza Nacional* 1, no. 1.

Argentina. *Decreto 727, de 12 de junho de 2006*. http://servicios.infoleg.gob.ar/infolegInternet/anexos/115000-119999/116997/norma.htm.

Argentina. *Ley n° 23.554, de 13 de abril de 1988*. http://servicios.infoleg.gob.ar/infolegInternet/anexos/20000-24999/20988/texact.htm.

Argentina. *Ley n° 24.059 de 18 de dezembro de 1991*. http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/458/texact.htm.

Argentina. *Ley n° 24.948 de 18 de março de 1998*. http://servicios.infoleg.gob.ar/infolegInternet/anexos/50000-54999/50229/norma.htm.

Argentina. *Ley n° 25.520 de 27 de novembro de 2001*. http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70496/norma.htm.

Andreas, Peter, and Richard Price. 2001. "From War Fighting to Crime Fighting: Transforming the American National Security State". *International Studies Review* 3, no. 3: 31–52.

Anzelini, Luciano. 2017. *El gobierno de Macri y la (re) militarización de la seguridad pública 2015-2017: algunos apuntes para la discusión*. 1. ed. Buenos Aires: Universidad Metropolitana para la Educación y el Trabajo.

Aron, Raymond. 2002. *Paz e Guerra entre as nações*. Clássicos IPRI. Brasília: Editora Universidade de Brasília.

Bento, Cláudio Moreira. 2003. "Recortes Históricos sobre Caxias". *Defesa Nacional* 796: 42–53.

Berger, Peter L., and Thomas Luckmann. 2009. *Construção social da realidade: tratado de sociologia do conhecimento*. 30. ed. Petrópolis: Vozes.

Betim, Felipe. 2018. Intervenção Federal no Rio decretada por Temer abre inédito e incerto capítulo. *El País* (Fev.). https://brasil.elpais.com/brasil/2018/02/16/politica/1518803598_360807.html

Bigo, Didier. 2001. "The Möbius Ribbon of Internal and External Security(ies)". In *Identities, Borders, Orders: Rethinking International Relations Theory*, edited by Mathias Albert, David Jacobson, and Yosef Lapid: 350. Minneapolis: University of Minnesota Press.

Brasil. 1999. *Lei Complementar n° 97 de junho de 1999*. http://www.planalto.gov.br/ccivil_03/leis/LCP/Lcp97.htm

Brasil. 2004. *Lei Complementar n° 117 de setembro de 2004*. http://www.planalto.gov.br/ccivil_03/leis/LCP/Lcp117.htm

Brasil. 2010. *Lei Complementar n° 136 de agosto de 2010*. http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp136.htm

Brasil. 2011. *Decreto n° 7.496 de junho de 2011*. http://www.planalto.gov.br/ccivil_03/_ato20112014/2011/decreto/d7496.htm

Brasil. 2016. *Decreto n° 8.903 de novembro de 2016.* http://www.planalto.gov.br/ccivil_03/_Ato20152018/2016/Decreto/D8903.htm#art9.

Brasil. Ministério da Defesa. 2013. *Garantia da Lei e da Ordem.* http
Duque de Caxias. Rio de Janeiro: Biblioteca do Exército.

Brasil. Ministério da Defesa. 2020. *Histórico de GLO.* https://www.gov.br/defesa/pt-br/assuntos/exercicios-e-operacoes/garantia-da-lei-e-da-ordem

Carvalho, Affonso de. 1976[1938]. *Caxias.* V. 140. Rio de Janeiro: Biblioteca do Exército.

Castro, Celso. 2002. *A invenção do Exército brasileiro.* São Paulo: Zahar.

Clarke, John L. 2013. "Europe's Armed Forces in Civil Security". *Connections* 12, no. 2: 69–82.

D'araujo, Maria Celina, and Celso Castro (Eds.). 2000. *Democracia e Forças Armadas no Cone Sul.* Rio de Janeiro: Editora FGV.

Dellasoppa, Emilio. 1998. *Ao inimigo, nem a justiça: violência política na Argentina (1943-1983).* São Paulo: Editora Hucitec.

Diamint, Rut. 2015. "A New Militarism in Latin America". *Journal of Democracy* 26, no. 4: 155–68.

Eissa, Sergio Gabriel. 2014. "La política de defensa como política pública: el caso argentino (2005-2010)". *Revista Brasileira de Estudos de Defesa* 1, no. 1: 162–84.

Eriksson, Johan, and Mark Rhinard. 2009. "The Internal–External Security Nexus: Notes on an Emerging Research Agenda". *Cooperation and Conflict* 44, no. 3: 243–67.

Freund, Julien. 1995. *Sociología del conflicto.* Ministerio de Defensa de España, Secretaría General Técnica.

Friesendorf, Cornelius. 2012. "International Intervention and the Use of Force: Military and Police Roles". *DCAF (Geneva Centre for the Democratic Control of Armed Forces)*, 95.

Greener-Barcham, B. K. 2007. "Crossing the Green or Blue Line? Exploring the Military–Police Divide". *Small Wars and Insurgencies* 18, no. 1: 90–112.

Guittet, Emmanuel-Pierre. 2008. "Military activities within national boundaries: the French case". In *Terror, Insecurity and Liberty: Illiberal practices of liberal regi-*

mes after 9/11, edited by Didier Bigo e Anastassia Tsoukala: 121–45. New York: Routledge.

Harig, Christoph. 2015. "Synergy effects between MINUSTAH and public security in Brazil". *BRASILIANA– Journal for Brazilian Studies* 3, no. 2: 142–68.

Hayes, Robert A. 1991. *A Nação Armada: a mística militar brasileira.* V. 278. Rio de Janeiro: Biblioteca do Exército.

Head, Michael, and Mann Scott. 2009. *Domestic Deployment of the Armed Forces: Military Powers, Law and Human Rights.* Farnham: Ashgate Publishing.

Hoelscher, Kristian, and Per Norheim-Martinsen. 2014. "Urban violence and the militarisation of security: Brazilian 'peacekeeping' in Rio de Janeiro and Port-au-Prince". *Small Wars & Insurgencies* 25, no. 5–6: 957–75.

Hunter, Wendy. 1994. "The Brazilian Military after the Cold War: In Search of a Mission". *Studies in Comparative International Development* 28, no. 4: 31–49.

_____. 1996. *State and soldier in Latin America: Redefining the military's role in Argentina, Brazil and Chile.* United States Institute of Peace.

Levy, Yagil. 2014. "What is Controlled by Civilian Control of the Military? Control of the Military vs. Control of Militarization". *Armed Forces and Society* 42, no. 1: 75–98.

Lima, Laura. 2011. "Worlding Brazil: The Theory of Emotional Action and the Development of Thinking about Security in Brazil (1930 -2010)". Doctoral Thesis (International Relations). Aberystwyth: Aberystwyth University.

Linz, Juan, and Alfred Stepan. 1999. *Transição e consolidação da democracia: a experiência do sul da Europa e da América do Sul.* São Paulo: Paz e Terra.

López, Ernesto. 1987. *Seguridad Nacional y Cedición Militar.* Buenos Aires: Legasa.

_____. 1994. *Ni la Ceniza Ni la Gloria: actores, sistema político y cuestión militar en los años de Alfonsín.* Buenos Aires: Universidad Nacional de Quilmes.

_____. 2003. "Nova problemática de segurança e 'novas ameaças'". In *Novas ameaças: dimensões e perspectivas*, edited by Suzeley Kalil Mathias and Samuel Alves Soares. São Paulo: Sicurezza.

_____. 2007. "Argentina: um longo caminho ao controle civil sobre os militares". In *Controle civil sobre os militares e política de defesa na Argentina, no Brasil, no chile e no Uruguai.* São Paulo: Editora Unesp.

Lutterbeck, Derek. 2010. "Wearing the Outside In: Internal Deployment of the Armed Forces in Germany and Italy". *Security and Peace* 28, no. 2: 88–95.

Marijnen, Esther, and Judith Verweijen. 2016. "Selling green militarization: the discursive (re)production of militarized conservation in the Virunga National Park, Democratic Republic of the Congo". *Geoforum* 75: 274–285.

Martín, Maria. 2018. Temer autoriza Forças Armadas no Rio, mas ministro adverte: 'não esperem milagres'". *El País* (Jul.). https://brasil.elpais.com/brasil/2017/07/28/politica/1501264807_474459.html

Martinez, Elias David Morales, and Mariana P. O. de Lyra. 2015. "O Processo de Dessecuritização do Narcotráfico na Unasul". *Contexto Internacional* 37, no. 2: 661–91.

Mathias, Suzeley Kalil. 1995. *Distensão no Brasil: o projeto militar (1973-1979).* Campinas: Papirus.

Mathias, Suzeley Kalil, and André Cavaller Guzzi. 2010. "Autonomia na Lei: as Forças Armadas nas constituições nacionais". *Revista Brasileira de Ciências Sociais* 25, no. 73: 41–57.

Mathias, Suzeley Kalil, and Samuel Alves Soares (Eds.). 2003. *Novas ameaças: dimensões e perspectivas.* São Paulo: Sicurezza.

Mathias, Suzeley Kalil, José Augusto Zague, and Leandro F. Sampaio Santos. 2019. "A política militar brasileira no governo Dilma Rousseff: o discurso e a ação". *Opinião Pública* 25, no. 1: 136–68.

Mccann, Frank D. 2007. *Soldados da Pátria: História do Exército Brasileiro 1889-1937.* São Paulo: Companhia das Letras.

Moreira, Vânia Maria Losada. 2017. "Guerra, pacificação e sujeição: o nascimento da 'escola severa' de 'civilização dos índios'". In *Pacificar o Brasil: das guerras justas às UPPs*: 126–47. São Paulo: Alameda Casa Editorial.

Norden, Deborah. 2016. "Latin American Militaries in the 21st Century: civili-military relations in the era of disappering bounderies." In *Routledge Handbook of Latin American Security*, edited by David Mares and Arie Kacowicz. New York: Routledge.

O'Donnell, Guillermo. 1973. *Modernization and Bureaucratic-Authoritarianism: Studies in south american politics.* Berkeley: University of California.

Observatório Cone Sul de Defesa e Forças Armadas. 2009. Informe Brasil n° 332 (Maio). http://unesp.br/gedes/produtos/101/observatorio-sudamericano-de-defensa-y-fuerzas-armadas.

Ojo, Emmanuel. 2008. "New missions and roles of the military forces: The blurring of military and police roles in Nigeria". *Journal of Military and Strategic Studies* 11, no. 1: 1–18.

Oliveira, Eliézer Rizzo. 1994. *De Geisel a Collor: Forças Armadas, Transição e Democracia*. Campinas: Papirus Editora.

Peixoto, Paulo Matos. 1973. *Caxias: nume tutelar da nacionalidade*. Rio de Janeiro: Edico.

Pereira, Matheus de Oliveira. 2019. "Controle civil e limites da política de defesa argentina (1983-2001)". *Conjuntura Austral* 10, no. 51.

Pion-Berlin, David. 2012. "Cumprimento de missões militares na América Latina". *Varia História* 28, no. 4: 627–43.

_____. 2016. *Military Missions in Democratic Latin America*. New York: Palgrave Macmillian.

Pion-Berlin, David, e Harold Trinkunas. 2011. "Latin America's growing security gap". *Journal of Democracy* 22, no. 1: 39–53.

Reitano, Tuesday, Lucia Bird Ruiz-Benitez de Lugo, e Sasha Jesperson (Orgs.). 2017. *Militarised Responses to Transnational Organised Crime: the war on crime*. Palgrave Macmillan.

Rodrigues, Thiago. 2012. "Narcotráfico e militarização nas Américas: vício de guerra". *Contexto Internacional* 34, no.1: 9–41.

_____. 2016. "Narcotráfico, Militarização e Pacificações: novas securitizações no Brasil". In *Visões do Sul: crise e transformações do sistema internacional*, edited by Alexandre Fuccille and Rodrigo Duarte Fernandes dos Passos, 2: 55–87. Marília: Cultura Acadêmica.

Rodrigues, Thiago, Mariana Kalil, Roberto Zepeda, and Jonathan Rosen. 2017. "War Zone Acapulco: Urban Drug Trafficking in the Americas". *Contexto Internacional* 39, no. 3: 609–31.

Romero, Luis Alberto. 2006. *História contemporânea da Argentina*. Rio de Janeiro: Jorge Zahar Editor.

Rouquié, Alain. 1984. *O Estado militar na América Latina*. V. 16, no. 1. São Paulo: Alfa-Omega.

Sain, Marcelo Fabián. 1999. "Alfonsín, Menem e as relações cívico-militares: a construção do controle sobre as Forças Armadas na Argentina democrática (1993-1995)". Doutorado em Ciência Política, Campinas: Universidade Estadual de Campinas – Unicamp.

_____. 2017. "Fuerzas Armadas y narcotráfico: la 'lenta' militarización del control del narcotráfico en Argentina (2011-2017)". Apresentado em XIII Congreso Nacional de Ciencia Política de la Sociedad Argentina de Análisis Político (SAAP), Buenos Aires.

Saint-Pierre, Héctor Luis. 2007a. "As 'novas ameaças' às democracias latino-americanas: uma abordagem teórico-coneitual". In *Segurança & Defesa Nacional: da competição à cooperação regional*, edited by Eliézer Rizzo Oliveira, 1. ed.: 59–82. São Paulo: Fundação Memorial.

_____. (Ed.). 2007b. *Controle civil sobre os militares e política de defesa na Argentina, no Brasil e no Uruguai*. São Paulo: Editora Unesp.

_____. 2011. "'Defesa' ou 'Segurança'? Reflexões em torno de conceitos e ideologias". *Contexto Internacional* 33, no. 2: 407–33.

_____. 2012. "El concepto de la seguridad multidemensional: una aproximación crítica". In *El concepto y las relaciones multilaterales de seguridad y defensa en el contexto de la Unasur*, edited by Sonia Mejías and Verónica Ricaurte. Madrid: Instituto Universitario General Gutiérrez Mellado.

Sampó, Carolina. 2019. "¿Entre la tradición y la modernización? El avance del crimen organizado y las fuerzas armadas en Argentina (2008-2018)". In *La transformación de las Fuerzas Armadas en América Latina ante el crimen organizado*, edited by Sonia Alda and Carolina Sampó: 107–28. Lima: Centro de Estudios Estratégicos Ejército del Perú; Real Instituto Elcano.

Sanahuja, José Antonio, and F. J. Verdes-Montenegro. 2014. "Seguridad y defensa en Suramérica: regionalismo, cooperación y autonomía en el marco de UNASUR". In *Anuario de la Integración de América Latina y el Gran Caribe*, edited by A. Serbin, L. Martínez and H. Ramanzini. V. 10.

Santos, Marcelo. 2007. *O poder norte-americano e a América Latina no pós-Guerra Fria*. São Paulo: Annablume.

Santillán, José Fernández. 1997. *Norberto Bobbio: el filósofo y la política: Antologia*. México D.F.: Fondo de Cultura Económica.

Santos, Maria Helena de Castro. 2004. "As novas missões das Forças Armadas latino-americanas no mundo pós-Guerra Fria: o caso do Brasil". *Revista Brasileira de Ciências Sociais* 19, no. 54.

Soares, Samuel Alves. 2006. *Controles e autonomias: as Forças Armadas e sistema político brasileiro (1974-1999)*. 1. ed. São Paulo: Editora Unesp.

Soares, Samuel Alves, and Germán Soprano. 2016. "Políticas de Defesa e Missões das Forças Armadas na Argentina e no Brasil: qual é o presente e o futuro da cooperação e da integração regional?" Apresentado em Latin American Studies Association, New York.

Sobel, Clifford. 2009. *Brazil's defense minister pursuing regional counterdrug cooperation.* Brasília. https://wikileaks.org/plusd/cables/09BRASILIA402_a.html.

Souza Adriana Barreto de. 2001. "Entre o mito e o homem: Caxias e a construção de uma heroicidade moderna". *Locus: revista de história* 7, no. 1.

_____. 2017. "Mito de Estado, Estado é: Duque de Caxias e as práticas pacificadoras do Exército Imperial". In *Pacificar o Brasil: das guerras justas às UPPs*: 175–95. São Paulo: Alameda Casa Editorial.

Souza, Adriana Barreto de, Angela Moreira Domingues da Silva, Luís Edmundo de Souza Moraes, and Maud Chirio (Eds.). 2017. *Pacificar o Brasil: das guerras justas às UPPs*. São Paulo: Alameda Casa Editorial.

Villa, Rafael Duarte. 2014. "O paradoxo da macrossecuritização: quando a guerra ao terror não securitiza outras 'guerras' na América do Sul". *Contexto Internacional* 36, no. 2: 349–83.

Waltz, Kenneth. 2002. *Teoria das Relações Internacionais*. Lisboa: Gradiva.

Weiss, Tomás. 2012. "Fighting Wars or Controlling Crowds? The Case of the Czech Military Forces and the Possible Blurring of Police and Military Functions". *Armed Forces and Society* 39, no. 3: 450–66.

Zaveruccha, Jorge. 2005. *FHC, forças armadas e polícia: entre o autoritarismo e a democracia (1999-2002)*. Rio de Janeiro: Editora Record.

_____. 2008. "La militarización de la seguridad pública en Brasil". *Nueva Sociedad* 213: 128–46.

NOTAS

1. Termo em inglês que se refere a desfocar.
2. Uma série de operações domésticas desenvolvidas pelas forças armadas não envolvem o uso da violência. Neste artigo sempre que mencionarmos operações militares internas nos referimos às ações em que há a possibilidade ou uso efetivo da força.
3. A expressão "novas ameaças" refere-se a questões não necessariamente novas, mas que no contexto do pós-Guerra Fria passaram a ser consideradas ameaças aos Estados e suas sociedades, entre as quais estão: narcotráfico, tráfico de armas, terrorismo, degradação ambiental, migrações e pobreza extrema (López 2003).
4. Mantivemos a ortografia e grafia original, tanto no nome da revista quanto na citação

FORÇAS ARMADAS E SEGURANÇA PÚBLICA NA ARGENTINA E NO BRASIL: REAFIRMAÇÃO E RUPTURA DO PAPEL INTERVENTOR

RESUMO

O presente artigo busca compreender a divergência do padrão de emprego das forças armadas brasileiras e argentinas entre 1990 e 2018. Neste período, os militares argentinos foram treinados e utilizados exclusivamente para defesa contra ameaças externas oriundas de outros Estados, enquanto as Forças Armadas brasileiras foram empregadas essencialmente para lidar com problemas internos, relacionados a atores não-estatais. Questionamos três principais explicações consolidadas na literatura: 1) as missões militares são respostas pragmáticas a uma realidade objetiva; 2) o direcionamento das forças armadas para o interior das fronteiras do Estado corresponde à falência do controle político sobre as instituições militares; 3) operações militares domésticas resultam de pressões externas. Consideramos que estas perspectivas não respondem ao nosso problema de pesquisa e propomos lidar com esta lacuna através do conceito de papel social, definido como o conjunto de expectativas sociais sobre as práticas militares. Argumentamos que a divergência observada na atribuição de missões aos instrumentos de defesa na Argentina e no Brasil pode ser entendida através das dinâmicas históricas de ruptura e continuidade do papel militar nesses países.

Palavras-Chave: Forças Armadas; Brasil; Argentina; Relações Civis-militares; Segurança; Defesa

ABSTRACT

The current paper aims to understand the divergence in the patter of deployment of the Brazilian and Argentine armed forces between 1990 and 2018. During this period, the Argentine military was trained and used exclusively to the defense against external threats from other states, while the Brazilian Armed Forces were mainly deployed to tackle internal issues related to non-state actors. We question three main explanations consolidated in the literature: 1) military missions are pragmatic responses to an objective reality; 2) the armed forces mobilization within the state's borders corresponds to the failure of political control over military institutions; 3) domestic military operations results from external pressure. We consider that these perspectives do not answer our research problem and we propose to tackle this gap through the concept of social role, defined as the set of social expectations about military practices. We argue that the divergence observed in the missions assigned to the defense instruments in Argentina and Brazil can be understood through the historical dynamics of disruption and continuity in the military role.

Keywords: Armed Forces; Brazil; Argentina; Civil-Military Relations; Security; Defense.

Recebido em 27/07/2020. Aceito para publicação em 26/04/2021.

Resenha

Resenha de: Saint-Pierre, Héctor Luis, e Marina Gisela Vitelli (Orgs.). 2018. *Dicionário de Segurança e Defesa*. São Paulo: Editora Unesp; Imprensa Oficial do Estado de São Paulo. 1.038p. ISBN: 978-85-393-0753-1.

TAMIRES APARECIDA FERREIRA SOUZA

O estudo de Defesa e Segurança no Brasil marca-se por sua incipiência e ausência de análises epistêmicas. O cenário de redemocratização dos países sul-americanos proporcionou um aprimoramento das relações civis--militares. Contudo, observa-se que, mesmo com a presença de governos civis democráticos, ainda persiste a interferência de militares e a crença de que os estudos de Defesa e Segurança deveriam estar sob o controle dos membros das forças armadas. Visando questionar e desmistificar tal situação, e promover um aprofundamento da epistemologia na área da Defesa e Segurança, elaborou-se o *Dicionário de Segurança e Defesa.*

O livro se originou do projeto *Rede Nacional de Estudos Estratégicos (ReNEE),* financiado pelos Ministérios da Educação e da Defesa, a partir do Edital Pró-Estratégia. A iniciativa promoveu o diálogo entre Instituições civis e militares sob a coordenação geral do Grupo de Defesa e Segurança Internacional (Gedes) e do Programa de Pós-Graduação em Relações Internacionais San Tiago Dantas (Unesp), reunindo: Universidade de Brasília (UnB), Universidade Federal de São Carlos (UFSCar), Universidade Federal de Rio Grande do Sul (UFRGS), Universidade Federal de Sergipe (UFS), Universidade da Força Aérea (Unifa) e Escola de Comando e Estado-Maior do Exército (Eceme). Com base nos objetivos do projeto, buscou-se uma "univocidade conceitual" entre os pesquisadores envolvidos, culminando na confecção do presente volume. Faz-se importante ressaltar o papel do projeto Pró-Defesa III, que possibilitou a formalização dos textos que compõem o Dicionário.

O volume foi desenvolvido entre 2015 e 2018, estando composto por 97 verbetes relativos aos "conceitos mais significativos empregados na área de defesa e segurança", desvendando os termos utilizados amplamente em periódicos. Os autores são pesquisadores nacionais e internacionais, conhecidos por sua excelência e dedicação acadêmica. Os verbetes estão constituídos

Tamires Aparecida Ferreira Souza — Doutora em Relações Internacionais pelo Programa de Pós-Graduação em Relações Internacionais San Tiago Dantas (Unesp, Unicamp e PUC-SP). Mestre em Estudos Estratégicos Internacionais pela Universidade Federal do Rio Grande do Sul (UFRGS). Pesquisadora do Grupo de Estudos de Defesa e Segurança Internacional (Gedes).

de análises epistêmicas, semânticas e históricas, promovendo uma reflexão e criticidade. Para uma melhor identificação dos termos e de suas abordagens, propõe-se aqui um agrupamento dos verbetes em oito grandes categorias.

Associa-se, primeiramente, os conceitos clássicos da área, se restringindo a: Ameaça; Defesa; Dissuasão; Estratégia; Geoestratégia; Geopolítica; Grande Estratégia; Guerra; Guerra e Direito; Guerra Preventiva; Guerra Primitiva; História da Guerra; Inteligência; Relações Civis-militares; Segurança Internacional; Tática; e Terrorismo. Os autores dos referidos verbetes se propõem a uma compreensão que perpassa desde as abordagens tradicionais aos estudos críticos, incluindo seus teóricos mais relevantes e os contextos históricos que influenciaram os desdobramentos de tais conceitos. Vale-se destacar o verbete de defesa, em que Ernesto López retoma os estudos clausewitizianos e desenvolve uma visão posteriormente pautada na América Latina, conectando guerra e forças armadas. Como também o conceito de segurança internacional, escrito por Rafael Villa e Camila Braga, em que realizam uma análise pautada nos principais marcos históricos e teóricos das relações internacionais, promovendo questionamentos epistemológicos e normativos.

O segundo bloco refere-se aos verbetes inseridos no nível sistêmico, pautando-se em: Anarquia Internacional; Balança de Poder; Dilema de Segurança; Poder Marítimo e Poder Naval; Potência; Rivalidade; Sociedade Internacional; e Tribunal Penal Internacional. Os presentes conceitos visam a compreensão do sistema internacional e de suas dinâmicas, conectando-se explicitamente ao campo da Defesa e Segurança.

A terceira subdivisão centra-se em Estado e Políticas, incluindo: Autonomia Estratégica; Cultura Estratégica; Diplomacia; Doutrina de Segurança Nacional; Entorno Estratégico; Estado de Exceção e Estado de Sítio; Estado Falido; Estratégia Nacional de Defesa; Garantia da Lei e da Ordem; Golpe de Estado; Militarismo; Ministério da Defesa; Operação Baseada em Efeitos; Parlamento e Defesa; Política de Defesa; Razão do Estado; Regimes Autoritários; Segurança Pública/Interna; Segurança Regional; Sistema de Vigilância da Amazônia; Sistema Integrado de Monitoramento de Fronteiras; e Soberania. Destaca-se aqui a construção das políticas e estratégias nacionais de defesa, bem como o processo de formulação dos Ministérios de Defesa. O ponto comum nas discussões destes verbetes é o fim das ditaduras militares na América Latina e a construção de governos democráticos. Este bloco conecta-se com a quarta categoria, que cerceia o campo das forças armadas, proporcionando uma compreensão de suas características constituintes e históricas, como também questionamentos sobre suas funções, divisões, prerrogativas e restrições. Os conceitos neste campo são: Aeronáutica; Africom; C4ISR; Comando

Sul; Forças Intermediárias; Forward Operating Site; Gênero nas Forças Armadas; História Militar; Interoperabilidade; Justiça Militar; Logística Militar; Marinha; Revolução Militar; e Sociologia Militar. Alinhado às duas categorias anteriores, indicamos o quinto bloco, caracterizado como Indústria de Defesa: Armamento; Base Industrial de Defesa; Economia de Defesa; Empresas Militares Privadas; e Produtos Estratégicos de Defesa. Nesta divisão faz-se presente uma discussão recente sobre a indústria e tecnologia militar, envolvendo desde atores civis como militares e adentrando a centralidade das estratégias de defesa nacionais e os campos cooperativos, propondo uma reflexão sobre a economia, mercado e tecnologia.

As sextas e sétimas categorias destinam-se aos estudos de paz e de cooperação regional e internacional, respectivamente, abrangendo os verbetes de: Construção da Paz; Intervenção Humanitária; Operação de Manutenção da Paz; Paz; Resolução de Conflitos; e Responsabilidade de Proteger; além de Center for Hemispheric Defense Studies; Colégio Interamericano de Defesa; Comunidade de Segurança; Conferência de Ministros de Defesa das Américas; Conselho de Defesa Sul-americano; Conselho de Segurança das Nações Unidas; Cooperação Dissuasória; Escola das Américas; Junta Interamericana de Defesa; Medidas de Confiança Mútua; Otan; Regimes de Não Proliferação Nuclear; Resdal; Segurança cooperativa; Tratado Interamericano de Assistência Recíproca; e Zona de Paz. Verifica-se aqui o elemento quantitativo, visto a expressividade no número de conceitos elaborados nestes dois blocos, como também suas centralidades nas discussões pós-Guerra Fria e pós-2008, com o advento da União de Nações Sul-Americanas e de seu Conselho de Defesa Sul-Americano, demonstrando a essencialidade e atualidade de tais compreensões.

Por fim, elencamos os verbetes circunscritos a temas e discussões contemporâneas, sendo eles: Complexo Regional de Segurança; Crime Organizado; Deslocamento Internos; Espionagem; Narcotráfico; Refugiados; Securitização; Segurança Energética; Segurança Humana; e Segurança Multidimensional. A relevância de tais conceitos é indiscutível, ainda mais com o advento do século XXI e dos Estudos Críticos de Segurança.

Desta forma, um olhar inicial e equivocado classificaria o Dicionário como um glossário, e seus verbetes como simples descrições conceituais. Todavia, uma leitura cuidadosa permite verificar a presença de criticidades e reflexões, promotoras de uma narrativa pioneira e inédita, vinculada a pesquisas científicas e investigadores renomados. Assim, nota-se a busca pela "máxima profundidade nas análises" e a inserção da Defesa e da Segurança como um estudo científico e digno de atenção e reconhecimento, tornando o livro obrigatório a todos os estudiosos.

Recebido em 25/04/2021. Aceito para publicação em 29/04/2021.

Diretrizes para Autores

1. Os artigos e ensaios devem conter aproximadamente 45 mil caracteres (sem espaços) e as resenhas de livros devem conter cerca de 6 mil caracteres (sem espaços) e se referir a obras publicadas há, pelo menos, quatro anos. São aceitas publicações em português, espanhol e inglês. Os artigos e ensaios poderão ser assinados por até três autores, as resenhas por um único autor. Ao menos um dos autores deve ter a titulação mínima de doutor. Nos artigos em coautoria o ordenamento dos autores terá como primeiro critério a titulação e como segundo critério ordem alfabética do nome.

2. Os textos submetidos à RBED devem estar formatados em espaço simples, fonte de 12 pontos, com uso do itálico para ênfases e aspas apenas para citações. As notas de rodapé restringem-se a esclarecimentos adicionais ao texto e devem ser sintéticas. URLs para referências devem ser informadas com as datas de acesso, e sempre ao final do texto, nas referências completas, jamais nas notas de rodapé.

3. A bibliografia deve ser citada de acordo com o sistema Chicago Manual of Style versão de 2017 (Autor ano, página), referenciando a literatura citada ao final do texto; no caso de resenhas de livros, devem ser informados os dados completos e o ISBN da obra analisada. O guia completo pode ser encontrado em: http://www.chicagomanualofstyle.org/tools_citationguide/citation-guide-2.html

Exemplos:

- Livros:

Grazer, Brian, and Charles Fishman. 2015. *A Curious Mind: The Secret to a Bigger Life*. New York: Simon & Schuster.

Smith, Zadie. 2016. *Swing Time*. New York: Penguin Press.

No corpo do texto:

(Grazer and Fishman 2015)

(Smith 2016, 315–16)

- Artigos:

Keng, Shao-Hsun, Chun-Hung Lin, and Peter F. Orazem. 2017. "Expanding College Access in Taiwan, 1978–2014: Effects on Graduate Quality and Income Inequality." *Journal of Human Capital* 11, no. 1 (Spring): 1–34. https://doi.org/10.1086/690235.

LaSalle, Peter. 2017. "Conundrum: A Story about Reading." *New England Review* 38 (1): 95–109. Project MUSE.

Satterfield, Susan. 2016. "Livy and the *Pax Deum*." *Classical Philology* 111, no. 2 (April): 165–76.

No corpo do texto:

(Keng, Lin, and Orazem 2017, 9–10)

(LaSalle 2017)

(Satterfield 2016, 170)

- Capítulos de livros editados:

Bay, Rachael A., Noah Rose, Rowan Barrett, Louis Bernatchez, Cameron K. Ghalambor, Jesse R. Lasky, Rachel B. Brem, Stephen R. Palumbi, and Peter Ralph. 2017. "Predicting Responses to Contemporary Environmental Change Using Evolutionary Response Architectures." *American Naturalist*189, no. 5 (May): 463–73. https://doi.org/10.1086/691233.

No corpo do texto:

(Bay et al. 2017, 465)

- E-books:

Austen, Jane. 2007. *Pride and Prejudice*. New York: Penguin Classics. Kindle.

Borel, Brooke. 2016. *The Chicago Guide to Fact-Checking*. Chicago: University of Chicago Press. ProQuest Ebrary.

No corpo do texto:

(Austen 2007, chap. 3)

(Borel 2016, 92)

4. Os textos submetidos à RBED devem dispor de títulos concisos (máximo de 80 caracteres, com espaço) no idioma em que a submissão for escrita (português, espanhol ou inglês) e em inglês. No caso da submissão ser em inglês, o segundo idioma deverá ser o português.

5. Os textos submetidos à RBED devem vir acompanhados de 4 palavras-chave e de resumo entre 150 e 200 palavras no idioma em que a submissão for escrita (português, espanhol ou inglês) e em inglês. No caso da submissão

ser em inglês, o segundo idioma deverá ser o português.

6. As submissões não devem conter o nome do autor ou quaisquer referências a este, a fim de possibilitar a avaliação cega pelos pares. Atentem para a remoção do autor do arquivo antes da submissão dos originais para avaliação (WORD / Propriedades do Arquivo / Autoria).

7. Os autores que tiverem sua proposição aprovada devem declarar que cedem os direitos autorais à Revista Brasileira de Estudos da Defesa (RBED), podendo esta incluir o trabalho publicado em bases de dados públicas e privadas, no Brasil e no exterior. Devem ainda declarar que são o os únicos responsáveis pelo conteúdo do texto e que o mesmo não contem nada que possa ser considerado ilegal ou difamatório de terceiros.

8. As submissões em desacordo com as Instruções aos Autores não serão admitidas para avaliação e seus propositores serão devidamente comunicados.

CONDIÇÕES PARA SUBMISSÃO

Como parte do processo de submissão, os autores são obrigados a verificar a conformidade da submissão em relação a todos os itens listados a seguir. As submissões que não estiverem de acordo com as normas serão devolvidas aos autores.

1. A contribuição é original e inédita, e não está sendo avaliada para publicação por outra revista; caso contrário, deve-se justificar em "Comentários ao editor".

2. O arquivo da submissão está em formato Microsoft Word, OpenOffice ou RTF que não ultrapassam 2MB.

3. O texto está em espaço simples; usa uma fonte de 12-pontos; emprega itálico em vez de sublinhado (exceto em endereços URL); as figuras e tabelas estão inseridas no texto, não no final do documento na forma de anexos.

4. O texto segue os padrões de estilo e requisitos bibliográficos descritos em Diretrizes para Autores, na página Sobre a Revista.

5. Ao menos um dos autores possui a titulação de doutor.

6. Em caso de submissão a uma seção com avaliação pelos pares (ex.: artigos), as instruções disponíveis em Assegurando a avaliação pelos pares cega foram seguidas.

DECLARAÇÃO DE DIREITO AUTORAL

Autores que publicam nesta revista concordam com os seguintes termos:

1) Autores mantêm os direitos autorais e concedem à revista o direito de primeira publicação, com o trabalho simultaneamente licenciado sob a Licença Creative Commons Attribution que permite o compartilhamento do trabalho com reconhecimento da autoria e publicação inicial nesta revista.

2) Autores têm autorização para assumir contratos adicionais separadamente, para distribuição não-exclusiva da versão do trabalho publicada nesta revista (ex.: publicar em repositório institucional ou como capítulo de livro), com reconhecimento de autoria e publicação inicial nesta revista.

3) Autores têm permissão e são estimulados a publicar e distribuir seu trabalho online (ex.: em repositórios institucionais ou na sua página pessoal) a qualquer ponto antes ou durante o processo editorial, já que isso pode gerar alterações produtivas, bem como aumentar o impacto e a citação do trabalho publicado (Veja O Efeito do Acesso Livre).

POLÍTICA DE PRIVACIDADE

Os nomes e endereços informados nesta revista serão usados exclusivamente para os serviços prestados por esta publicação, não sendo disponibilizados para outras finalidades ou a terceiros.

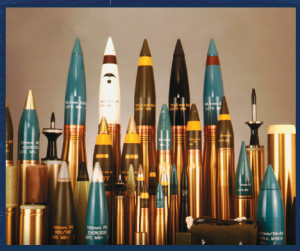
EMGEPRON

EXPANDINDO SEUS HORIZONTES

A Empresa Gerencial de Projetos Navais - EMGEPRON é uma empresa pública criada em 09/06/1982, vinculada ao Ministério da Defesa por intermédio do Comando da Marinha do Brasil. Tendo em vista a necessária adaptação da cultura organizacional vigente às transformações impostas pelas boas práticas de mercado, vem aperfeiçoando para se tornar a empresa mais competitiva no seu âmbito. Nesse escopo, a Empresa delineou seus três focos de negócios, que são:

Gerenciamento de Projetos Estratégicos da Marinha, como os Navios Classe Tamandaré e o Navio de Apoio Antártico.

Economia do Mar, que engloba uma vasta gama de serviços relacionados aos segmentos de negócio do mar.



Plataforma de Exportação de Produtos de Defesa, em especial as Munições fabricadas pela Marinha, e a Interveniência Técnica.

Desta forma, a Empresa se apresenta como uma propícia alternativa para as Forças Armadas e diversas organizações públicas e privadas que buscam solucionar suas demandas específicas, que não fazem parte de seus ambientes de negócios, mas fazem para a EMGEPRON.

www.emgepron.gov.br

facebook.com/EMGEPRON

marketing@emgepron.gov.br

(21) 3907-1800

ISO 9001