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

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

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

Resumo

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

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

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

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

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

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

Introdução

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

O ciberespaço e os documentos de defesa do Brasil

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Considerações finais

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

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

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

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

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

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

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

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

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

Referências

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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