HOPLOS
VOL. 07 Nº 12/2023

Nilton Lopes da Silva Gomes

Graduado em Humanidades (2017) e Relações Internacionais (2020) pela Universidade da Integração Internacional da Lusofonia Afro-Brasileira (UNILAB) e Mestrando no Programa de Pós-Graduação em Segurança Internacional e Defesa na Escola Superior de Guerra (ESG).

PLANEJAMENTO BASEADO EM CAPACIDADES NOS DOCUMENTOS DE SEGURANÇA E DEFESA CIBERNÉTICA

CAPABILITY BASED PLANNING IN BRAZILIAN CYBER SECURITY AND DEFENSE DOCUMENTS

RESUMO: Existe variedade de modelo de Planejamento Baseado em Capacidade (PBC) implementado no sistema da defesa em diferentes países. O PBC é definido como ferramenta metodológica para identificar e avaliar as lacunas ou excesso de capacidade militar a partir da criação de cenário prospectivo. Assim, reduzindo despesas dos recursos. Este estudo tem como objetivo compreender as contribuições do método PBC na segurança e defesa cibernética brasileira, a partir da análise descritiva nos seguintes documentos oficiais do Estado: Doutrina Militar de Defesa Cibernética e Estratégia Nacional de Segurança Cibernética (E-Ciber). Ademais, aborda termos conceituais e contextuais relativamente à temática. Diante do estudo realizado entende-se que o PBC contribui para identificação das capacidades de SegCiber e Defesa Cibernética no nível político, ao passo que no nível tático e operacional apresentaram-se *gaps* na operação conjunta provocados pelo cenário volátil. Finalmente, concluiu-se que são necessários exercícios constantes para sanar os desafios contemporâneos que ameaçam a soberania nacional.
Palavras-chave: Brasil; Defesa Cibernética; Militar; Segurança Cibernética; PBC.

ABSTRACT: There are variety of Capability-Based Planning (CBP) models implemented in the defense system in different countries. CBP is defined as a methodological tool to identify and assess military capability gaps or surplus by creating a forward-looking scenario. Thus, reducing resource expenditures. This study aims to understand the contributions of the PBC method in Brazilian cyber security and defense, from the descriptive analysis in the following official state documents: Military Doctrine for Cyber Defense and National Strategy for Cyber Security (E-Ciber). Furthermore, it addresses conceptual and contextual terms regarding the theme. Given the study carried out, it is understood that the CBP contributes to the identification of Cybersecurity and Cyber Defense capabilities at the political level, while at the tactical and operational level gaps were presented in the joint operation caused by the volatile scenario. Finally, it was concluded that constant exercises are needed to remedy the contemporary challenges that threaten national sovereignty.
Keywords: Brazil; Cyber Defense; Military; Cybersecurity; CBP.

1 Introdução

O cenário mundial apresenta grandes desafios ao longo dos tempos, face à segurança e defesa no âmbito local, regional e/ou internacional. Nessa linha cronológica, verificam-se diferentes estratégias adquiridas pelos Estados desde a Primeira Grande Guerra mundial até os dias de hoje. Nesse percurso, as mudanças em termos político, econômico e industrial surgem como alavanca para desencadear as inovações das ferramentas que podem auxiliar na melhoria das técnicas de conter possíveis riscos e ameaças existentes. Nesse sentido, vale discorrer alguns marcos históricos dessas transformações a nível global. Após a Segunda Guerra Mundial, no meado da década de quarenta, ou seja, durante a Guerra Fria, o foco das ameaças se limitava no desenvolvimento estratégico entre as duas grandes potências internacionais (Estados Unidos e União Soviética) que se contrapunham na expansão do poder e domínio mundial (DA SILVA, 2019; BARROS, 2022). Nesta disputa ideológica, a queda do Muro de Berlim nos finais dos anos oitenta simbolizou o fracasso da União das Repúblicas Socialistas Soviéticas (URSS). Desse modo, os Estados Unidos buscam desenvolver novas técnicas que garantam a segurança e defesa nacional e ao redor do mundo. No entanto, foi criado o Programa de Cooperação Técnica conhecida por *The Technical Cooperation Program (TTCP)* nos anos de 1957, com intuito de estreitar laços cooperativos entre os países aliados (Canadá, Reino Unido, Austrália e Nova Zelândia) na área de ciência e tecnologia centralizado em matéria de Defesa, apoiando outros países no aprimoramento e aplicação da metodologia (BRASIL, 2022). Nos anos 2000 ocorre avanço sistemático, tendo em vista surgimento das mudanças imprevisíveis no cenário internacional.

Desse modo, o principal eixo da transformação no planejamento da defesa estadunidense, foi marcado pelo evento de 11 de setembro de 2001, com ataques às torres gêmeas na cidade de Nova York, onde o terrorismo surge como nova ameaça não premeditada e, abrindo grandes debates a respeito de segurança internacional. Além disso, os múltiplos desafios tais como: desastre naturais, crimes transnacionais, narcotráfico, pirataria, ataque cibernético, guerra híbrida e entre outros, se configuram como ameaças reais. Labbé, et al (2006), mostram duas características que diferenciam o domínio da defesa das demais experiências em termo de capacidades. A primeira caraterística está relacionada à análise dos fenômenos físicos, enquanto a segunda, encontra-se associada as experiências no domínio da defesa que examinam operações militares envolvendo seres humanos e os seus equipamentos de combate. Para os autores, as novas tecnologias militares são desenvolvidas a partir das

experiências da defesa básicas e aplicadas, ou seja, por meio do desenvolvimento da indústria e pesquisa no meio académico. Nesse contexto, diversos países buscam incorporar uso do *Capability Based Planning (CBP)* ou Planejamento Baseado em Capacidade (PBC) como ferramenta que permite identificar os *gaps* ou excessos de capacidades voltadas a vários setores, tanto nos meios corporativos, industriais, quanto na arena militar. É importante mencionar exemplos de países que adotaram as metodologias do PBC para analisar seus sistemas de defesa nacional.

De acordo com Despont (2022), as Forças Armadas suíças continuam a depender fortemente de sistemas da Guerra Fria, tais como veículos blindados pesados. O Autor afirma que,

> Está atrasada em termos de novas capacidades trazidas pela mais recente Revolução nos Assuntos Militares (RMA), incluindo tecnologias como a Inteligência Artificial (IA) e os Veículos Não Tripulados (UV). Estas tecnologias estão a mudar a forma como os conflitos futuros são abordados e, acima de tudo, a forma como são combatidos (DESPONT, 2022, p. 1).[1]

Por outro lado, para atualizar o sistema de defesa suíço e preencher os *gaps* identificados, o exército necessitou de consultar as experiências inovadoras de outros países (DESPONT, 2022). Esse modo, iniciou uma fase de transição para se distanciar dos métodos de planejamento anteriores e decidir implementar PBC como método mais moderno de desenvolvimento das Forças.

Outro caso relevante sobre a temática se refere às Forças Armadas do Canadá, um país que em termos geopolítico e geoestratégico possui, parcialmente, semelhança com os Estados Unidos em relação à questão da defesa. Por essa razão, o Estado canadense, também se apropria do método PBC para atender às suas necessidades. Em agosto de 2017, Taylor desenvolveu um trabalho científico para auxiliar o *Director General Capability and Structure Integration* (DGCSI) com atividade das Forças Armadas canadenses para potencializar a identificação dos riscos futuros e explorar as capacidades de solucionar eventuais incidentes. A Pesquisa e Desenvolvimento da Defesa apoiou a implementação do projeto do Vice-Ministro Assistente (Ciência e Tecnologia), utilizando plano de preparação para ciclos do PBC nos próximos anos. Segundo o Autor, "A abordagem proposta para o CBP visa efetuar análises de capacidade e de aptidão em paralelo para poupar tempo" (TAYLOR, 2017, p. 2). Posto isto, identifica ainda na

[1] *It lags in terms of new capabilities brought by the latest Revolution in Military Affairs (RMA), including technologies like Artificial Intelligence (AI) and Unmanned Vehicles (UV). These technologies are changing the way future conflicts are approached and, above all, the way they are fought (DESPONT, 2022, p. 1).*

proposta, cinco etapas do processo, sendo: (I) validar o conjunto de cenários; (II) Estimativa da Força; (III e IV) análise da capacidade e; (V) integração dos resultados.

É importante realçar o interesse da Austrália na adoção do PBC. Assim sendo, o país australiano tem se aprofundado no planejamento e desenvolvimento da capacidade militar desde a década de 1970 (CHIM; NUNES-VAZ; PRANDOLINI, 2010). Ainda na perspectiva dos autores,

> Uma vez que não existe uma ameaça dominante ou um perigo primordial para a segurança do país, o planejamento militar estratégico considera uma vasta gama de contingências e ameaças. A natureza da resposta exigida à Força de Defesa Australiana é especificada num conjunto de tarefas estratégicas. As tarefas identificadas a partir desta abordagem são consistentes com a perspectiva estratégica da Austrália e ajudam a identificar opções de capacidade credíveis e versáteis. Só numa fase posterior do processo CBP é que são identificadas as opções de capacidades específicas para realizar uma tarefa e é nomeado um serviço (ou serviços) de Defesa como gestor de capacidades. Quando são implementados, espera-se que as soluções de capacidades trabalhem em conjunto para alcançar a unidade de esforço, de acordo com a doutrina das operações conjuntas (CHIM; NUNES-VAZ; PRANDOLINI, 2010, p. 84, 85).[2]

A Austrália continua aumentando a capacidade das Forças Armadas, aplicando as metodologias do PBC em diversas áreas. Com larga experiência no melhoramento do setor militar para a segurança e defesa, em setembro de 2021, o governo australiano assinou acordo com Reino Unido e Estados Unidos que permite ao país receber a tecnologia para submarinos com propulsão nuclear capaz de enfrentar crescente ameaças em seu entorno. Principalmente, proveniente da República Popular da China no Oceano Pacífico (CHAPMAN, 2022). A literatura aponta diversas estratégias políticas e econômicas relacionadas ao uso do método PBC adotado pela Austrália para efetivar redução dos gastos militares e proporcionar capacidade de atuar perante riscos e ameaças futuras.

Além dos países acima mencionados como exemplo, encontra-se ao redor do mundo vários outros em buscas de planejamento das forças baseado em capacidades (INKSTER, 2015). Todavia, este trabalho centraliza na compreensão da aplicação do PBC nas Forças Armadas (FA) do Brasil, especificamente no setor cibernético vinculado ao exército brasileiro. Nesse contexto, o estudo tem por finalidade analisar as contribuições do PBC nas estratégias

[2] *As there is no dominating threat or overriding hazard to the country's security, strategic military planning considers a broad range of contingencies and threats. The nature of the response required from the Australian Defence Force is specified in a set of strategic tasks. The tasks identified from this approach are consistent with Australia's strategic outlook and help identify credible and versatile capability options. It is only at a later stage of the CBP process that specific capability options to conduct a task are identified and a Defence service is (or services are) nominated as the capability manager. When deployed, the capability solutions are expected to work together to achieve unity of effort in accordance with the doctrine of joint operations (CHIM; NUNES-VAZ, PRANDOLINI, 2010, P. 84, 85).*

de Segurança cibernética (Seg Ciber) e defesa cibernética brasileira. Ou seja, como as ferramentas do PBC contribuem para com as FA brasileira no fortalecimento da capacidade de defesa cibernética do país?

Em termos metodológicos, buscou-se um enfoque qualitativo a partir de levantamento dos dados descritivos caracterizados nos documentos oficiais referente a temática (Doutrina Militar de Defesa Cibernética e Estratégia Nacional de Segurança Cibernética - E-Ciber).

No que tange a estrutura organizacional da pesquisa, contando com a introdução, o trabalho possui cinco seções. A segunda seção, apresenta-se discussão sobre o conceito do PBC em diferentes pontos de vista abarcando o contexto brasileiro que inclui planejamento no âmbito político e estratégico da nação a partir do modelo adequado. Em seguida, a terceira seção, demonstra uma abordagem teórica da Seg Ciber e defesa cibernética. A quarta seção, aponta a estrutura das capacidades do país implementadas no setor de segurança e defesa cibernética por meio da utilização da abordagem metodológica do PBC. Por fim e, não menos importante, na quinta seção apresentam-se os resultados e a considerações finais do estudo.

2 Planejamento Baseado em Capacidade (PBC): contexto e conceito

O PBC tem sido utilizado como ferramenta estratégica no sector militar para organizar táticas de operações em eventuais ameaças e/ou ataques e amenizar gastos orçamentários com produtos industriais de defesa, treinamento operacional, assim como descrito na primeira seção. No sistema internacional é suficientemente perceptível as capacidades de diferentes forças militares tanto a nível tático quanto a nível operacional (SAN MARTIN, 2022). No entanto, quando se trata da atuação no campo de combate percebe-se diversos elementos como fatores-chave que influenciam o processo de planejamento. Nessa perspectiva, destaca-se o cenário, no qual se baseia a aplicação do PBC. Para da Silva (2019), o planejamento em cenários prospectivos define o atual estágio da instituição, transitando para um estágio futuro. Portanto, observa-se a dependência probabilística quando se trata de planejamento em cenário, uma vez que, em poucos casos, aumentam os riscos, desafios e/ou ameaças associada ao seu contexto.

Na mesma linha argumentativa, Gomes, Belderrain e Marchi (2021) mostram que “o conceito de PBC reconhece a interdependência de sistemas (incluindo material e Pessoas), doutrina, organização e suporte no fornecimento de capacidade de defesa e a necessidade de poder examinar opções e compensações entre esses componentes [...]”. Em termos conceituais,

PBC se define pela adaptação de sistema já existente, ou seja, a partir dos fundamentos do TTCP que já possuía uma estrutura padrão de análise.

O Guia de TTCP basicamente constrói orientação de alto nível do poder seguido por diretrizes, busca ajustar a doutrina militar com outras formas de combate das forças. Logo após, cria categorias de capacidades agrupadas, assim, permite a facilitação do processo. Finalmente, adequa as capacidades aos recursos acessíveis (DAVIS, 2012; TTCP, 2012; LABBÉ et al, 2006). Interessa notar que esse modelo segue a lógica *top-dow,* significa que, dessa forma, a formulação e o passo a passo são decididos no nível político. De outro modo, o mesmo modelo oferece uma análise *bottom-up*, porém numa perspectiva de envolvimento dos órgãos da defesa, subordinados a participar no processo decisório da política de defesa (CORRÊA, 2020).

Vale destacar que o modelo *top-down e bottom-up* são os métodos do PBC mais aplicados na análise de capacidades das instituições, ainda que esse ciclo seja considerado fundamental, o PBC possui outros meios de aplicação em contextos diferentes. Além disso, não há uma "receita de bolo" para sua definição (BARROS, 2022).

A concepção do PBC na perspectiva brasileira é entendida por Conjunto de procedimentos voltados ao preparo das FA, mediante a aquisição de capacidades adequadas ao atendimento dos interesses e necessidades militares de defesa do Estado, em um horizonte temporal definido, observados cenários prospectivos e limites orçamentários e tecnológicos. O PBC foi superficialmente mencionado na Política Nacional de Defesa (PND) e a Estratégia Nacional de Defesa (END) a princípio em 2012, com propósito de estruturar e desenvolver as FA para monitorar e controlar todo território nacional (terrestre, aéreo e marítimo), afora apoiando na gestão de pessoal e material coadunável com os planejamentos estratégicos e operacionais (GOMES; BELDERRAIN; MARCHI, 2021; NOGUEIRA NEVES et al., 2021).

Ao longo do tempo, o PBC teve interpelação mais aprofundada nos documentos oficiais nacionais. Desde 2016 o MD tem empenhado na execução de trabalhos entre as FA. Como resultado, em 2020 foi aprovado pelo MD a Diretriz para a Implantação e Execução do Planejamento Baseado em Capacidades (PBC) (EB20-D-03.041)[3] no Comando do Exército por meio da Portaria nº 081-EME, de 29 de abril de 2020 para força tarefa entre as FA (BRASIL, 2020). Mormente, foi criado o Grupo de Trabalho-PBC (GT-PBC) em fevereiro de 2021

[3] Diretriz para a implantação e execução do Planejamento Baseado em Capacidades (PBC) com objetivo de regular as medidas necessárias, discriminar as principais atribuições e responsabilidades dos diferentes Órgãos e Comandos envolvidos, que darão efetividade à presente Diretriz e estabelecer parâmetros para a execução e a condução dos trabalhos do PBC.

instituído pela Portaria Nº 646/GM-MD com intuito de aprovar o Guia PBC do Brasil, no qual a 1ª edição encontra-se em desenvolvimento (BRASIL, 2022).

Segundo Stephan (2011, p. 20) [4], "atualmente, o PBC apresenta-se em três vertentes principais. A abordagem anglo-saxónica, mais bem exemplificada no trabalho do Programa de Cooperação Técnica, continua a atribuir aos cenários um papel central no processo do PBC. Dado que o PBC pode ser aplicado nos setores administrativo, cenário prospectivo, capacitação de pessoal etc. A próxima seção, tem por finalidade, criar um fio condutor da relação do referido método e/ou ferramenta com a questão da Segurança e Defesa Cibernética, visto que essas abordagens são diferentes em vários países que o tenham implementado

3 SegCiber e Defesa Cibernética

Dada a incerteza e variabilidade de potenciais ameaças em ambientes virtuais que afetam ambientes reais, bem como a intervenção de novos ambientes não virtuais, segurança e defesa cibernética tornaram-se um tema de destaque em debates acadêmicos e fóruns internacionais. Nesse sentido, os atores estatais atuam diretamente em cenários de conflito. Para exemplificar, certamente no mundo atual, o novo cenário de conflitos conhecido por conflito híbrido ou complexamente por guerra híbrida influencia mudança de atuação no campo de combate. Um dos casos mais recentes verifica-se no leste da Europa, onde a hostilidade entre a Rússia e a Ucrânia apresenta intensamente novas estratégias empregadas em combate (BARGUÉS e PIÑERA, 2022). Por outro lado, nota-se (des)informação sem precedentes em torno dos fatos, isso descreve ainda mais a incerteza das ameaças. Observando por essa lente, o Estado brasileiro tem demonstrado tais preocupações ao longo dos tempos, em novembro de 2014, publicou no Diário Oficial da União (D.O.U) a Doutrina Militar de Defesa Cibernética, com intuito de proporcionar fundamentos que contribuem para atuação conjunta das FA na defesa do país no espaço cibernético (BRASIL, 2014). Não obstante, em fevereiro de 2020, foi publicado a E-Ciber, com o propósito de orientar a sociedade brasileira acerca das principais ações do governo federal a níveis nacionais e internacionais, sobretudo na área da segurança cibernética dentro do limite temporal compreendido a partir da sua publicação até 2023 (BRASIL, 2020).

[4] *CBP today comes in three major strands. The Anglo-Saxon approach, as best exemplified in the work of The Technical Cooperation Program, still gives scenarios a central role within the CBP process* (STEPHAN, 2011, p. 20).

O exército brasileiro possui o Programa Estratégico para Defesa Cibernética do país desde 2008, com cerca de seis estruturas de projetos que visam potencializar a criação da capacidade cibernética nas forças armadas. Dessa forma, os projetos são guiados pelas Organizações Militares conectadas ao setor, como o Instituto Militar de Engenharia, o Comando de Comunicações e Guerra Eletrônica do Exército, o Centro de Desenvolvimento de Sistemas do Exército, o Centro integrado de Telemática, o Centro de Inteligência, e Centro de Defesa Cibernética (BRASIL, 2022). Nesse sentido, esta seção busca discorrer sobre a compreensão da estrutura institucional preparada para assegurar e defender das ameaças interna e externa.

Para iniciar a discussão dos temas, vale ressaltar que o entendimento, tanto da Segurança Cibernética, quanto da Defesa Cibernética é difuso pelo fato de cada organização governamental ou não governamental definir esta temática de acordo com sua realidade ou contexto, ou seja, não há acordo padrão internacional. A palavra "Ciber" tem sido utilizada para conceituar diferentes áreas relacionadas à tecnologia, principalmente, no uso de computadores e rede internet. No caso do Brasil, o Gabinete de Segurança Institucional (GSI) criou um glossário, no qual consta o conceito de Segurança e Defesa Cibernética da seguinte maneira:

> SEGURANÇA CIBERNÉTICA - ações voltadas para a segurança de operações, visando garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético, capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis (BRASIL, 2022).
> DEFESA CIBERNÉTICA - ações 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 ativos de informação de interesse da defesa nacional, obter dados para a produção de conhecimento de inteligência e buscar superioridade sobre os sistemas de informação do oponente (BRASIL, 2022).

É importante perceber que a sigla SegCiber foi definida em 2010 pelo Grupo Técnico para se designar a Segurança Cibernética no livro Verde, visando contribuir com debates críticos à construção a nível nacional. Nessa perspectiva, a SegCiber se configura como "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 (BRASIL, 2010)". Essa definição complementa um pouco a percepção colocada acima pelo GSI. Torna-se interessante observar que no E-ciber, a SegCiber é apresentada como área crítica e necessita de desenvolvimento político, econômico e estratégico envolvendo mais de quarenta órgãos e entidades do governo, sem contar com diversas instituições privadas e do nível acadêmico. Apesar do entendimento que se tem relativamente

à área de SegCiber, é relevante a aplicação do método PBC como ferramenta das ações estratégicas para atuação no contexto doméstico, de modo que a sociedade brasileira compreende os pontos considerados importantes para o país na referida área, ela se baseia nas análises realizadas para diagnosticar a Segurança Cibernética global, inclusive por meio de metodologia *bottom up*, isto é, mediante avaliação de *benchmarking* (BRASIL, 2020).

Em termos de Defesa Cibernética, encontra-se a conceituação em consonância, tanto no Livro Verde quanto na Doutrina Militar. Sem embargo, para contemplar a Defesa Cibernética, a E-Ciber estabelece um modelo centralizado de governança no âmbito nacional, conforme citado no item 2.3.2.[5] do documento. Sendo assim, foram divididas as tarefas para viabilizar a implementação, no qual o Gabinete de Segurança Institucional da Presidência da República (GSIPR) coordena a SegCiber no ambiente doméstico alinhado com atuação de outros órgãos no sentido mais amplo, isto é, preparo contra as ameaças externas. Nesse segmento, se destacam as ações da Defesa Cibernética a cargo do Ministério da Defesa (MD) (BRASIL, 2020).

Especificamente, o setor da Defesa Cibernética localiza-se sob responsabilidade do Exército brasileiro, subordinado ao MD, por entender que as ameaças originárias de ataques cibernéticos transcendem o cenário doméstico. De acordo com Pinto (2016), as principais características do domínio cibernético são ausência de limitações físicas de distância e espaço, fronteiras geograficamente (in)definidas; o ambiente virtual é mutável e depende das condições ambientais e da criatividade humana, assim colocando em risco o seu controle, facilidade de acesso, emprego de diferentes ferramentas e usuários da Tecnologia de Informação (TI); e finalmente, os sistemas de computadores não possuem segurança 100% garantida, ou seja estão suscetíveis a difundir *gaps*. Por essa e outras razões, os Estados atribuíram alto grau de relevância nesse setor que coloca em debate a soberania nacional.

[5] Estabelecer um modelo centralizado de governança no âmbito nacional Estabelecer um modelo centralizado de governança para o País, por meio da criação de um sistema nacional de segurança cibernética, com as seguintes atribuições:
- promover a coordenação dos diversos atores relacionados com a segurança cibernética, além da esfera federal;
- promover a análise conjunta dos desafios enfrentados no combate aos crimes cibernéticos; - auxiliar na formulação de políticas públicas;
- criar um conselho nacional de segurança cibernética;
- criar grupos de debate sobre segurança cibernética, em diferentes setores, sob coordenação do Gabinete de Segurança Institucional da Presidência da República, para fomentar discussões sobre o tema, por meio de mecanismos informais de participação;
- estabelecer rotina de verificações de conformidade em segurança cibernética, internamente, nos órgãos públicos e nas entidades privadas; e
- permitir a convergência dos esforços e de iniciativas, e atuar de forma complementar para receber denúncias, apurar incidentes e promover a conscientização e a educação da sociedade quanto ao tema (BRASIL, 2020).

É notório, profunda e constante mudanças nos ambientes externo e interno aos Estados-Nação. Certamente, tornam o ambiente estratégico mais complexo e incerto. Isso ocorre por diversos motivos, no qual cita-se como exemplo, mudanças climáticas, atos terroristas, ataques cibernéticos dentre outros (NORI KATAGIRI, 2022). Nesse sentido, Poli (2013), mostra distinção de conceito de sistema complicado e sistema complexo, precisamente para auxiliar os analistas dessas mudanças citadas e/ou os decisores na escolha de métodos eficazes para solucionar problemas. De acordo com o autor,

> Os problemas complicados têm origem em causas que podem ser distinguidas individualmente; podem ser abordados peça a peça; para cada entrada no sistema há uma saída proporcional; os sistemas relevantes podem ser controlados e os problemas que apresentam admitem soluções permanentes. Por outro lado, os problemas e sistemas complexos resultam de redes de múltiplas causas interativas que não podem ser distinguidas individualmente; devem ser abordados como sistemas completos, ou seja não podem ser abordados de forma fragmentada; são tais que pequenos contributos podem resultar em efeitos desproporcionais; os problemas que eles apresentam não podem ser resolvidos de uma vez por todas, mas exigem uma gestão sistemática e, normalmente, qualquer intervenção gera novos problemas em resultado das intervenções que os tratam; e os sistemas relevantes não podem ser controlados e os sistemas relevantes não podem ser controlados – o melhor que se pode fazer é influenciá-los, aprender a "dançar com eles", como Donella Meadows disse muito bem (POLI, 2013, p. 142)[6].

Por outro lado, Davis (2012) apresenta método desenvolvido pela RAND[7] para análise da incerteza da segurança nacional. Essa metodologia é aplicada por meio do uso de recursos tecnológicos, mais concretamente, computadores e software. Além disso, aplica-se na teoria e na prática em planejamento estratégico e tomada de decisões, bem como nos métodos analíticos e a teoria de sistemas adaptativos complexos. Diante dessa descrição, entende-se que o PBC parte da mesma lógica de análises que representam os riscos ou oportunidades de melhorar as estratégias para uma adaptação mais robusta de capacidades à frente das ameaças volúveis. Ainda que seja para prospecção futura de médio a longo prazo. Dessa maneira, a seção seguinte busca-se descrever as contribuições do PBC no contexto da Seg Ciber e Defesa

[6] *Complicated problems originate from causes that can be individually distinguished; they can be addressed piece by piece; for each input to the system there is a proportionate output; the relevant systems can be controlled and the problems they present admit permanent solutions. On the other hand, complex problems and systems result from networks of multiple interacting causes that cannot be individually distinguished; must be addressed as entire systems, that is they cannot be addressed in a piecemeal way; they are such that small inputs may result in disproportionate effects; the problems they present cannot be solved once and for ever, but require to be systematically managed and typically any intervention merges into new problems as a result of the interventions dealing with them; and the relevant systems cannot be controlled – the best one can do is to influence them, learn to "dance with them", as Donella Meadows aptly said (POLI, 2013, p. 142)* .

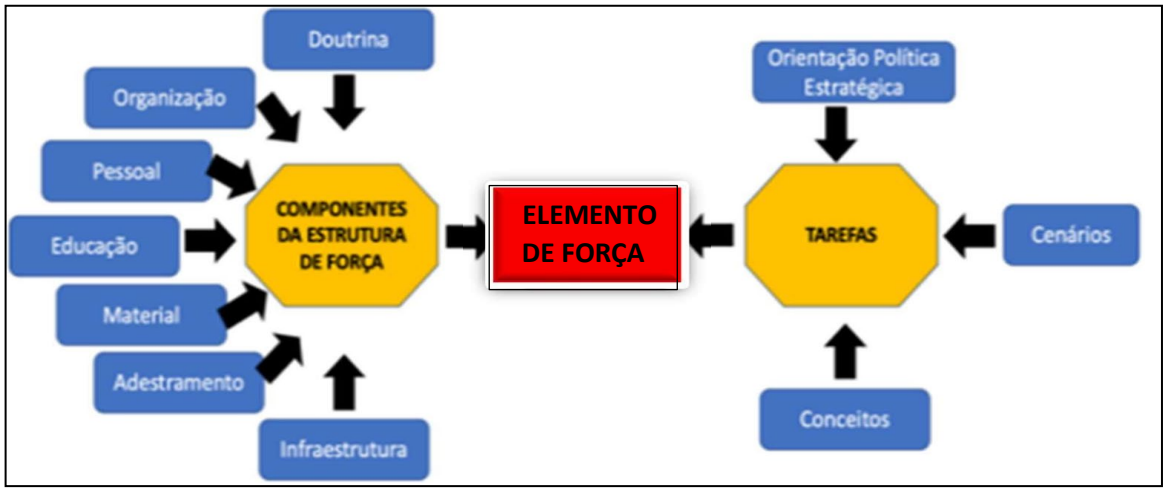
[7] A RAND Corporation é uma organização de pesquisa que desenvolve soluções para desafios de políticas públicas para ajudar a tornar as comunidades em todo o mundo mais seguras, saudáveis e prósperas. A organização é sem fins lucrativos, apartidária e comprometida com o interesse público (RAND, s/a).

Cibernética brasileira, considerando a necessidade de alcançar a capacidade por meio de planejamento de Defesa, estratégia e operações para se opor aos possíveis ataques externos e internos que possam afetar soberania nacional (PINTO, 2016; TAGAREV, 2006).

4 Contribuição do PBC no SegCiber e Defesa Cibernética brasileira

De antemão, o amparo legal do PBC no Brasil ocorre mediante dados contidos nos documentos de alto nível nacional, com o propósito de verificar diretrizes setoriais, a começar pela definição das prioridades, principalmente na área de Defesa, que norteiam o processo decisório relativo à obtenção das capacidades necessárias. Posto isto, nesta seção, inicia-se análise descritiva da 1ª edição da Doutrina Militar de Defesa Cibernética e da E- Ciber. Para tal efeito, faz-se mister uma análise com base no Guia desenvolvido pelo *Institute for Defense Analiyses*[8] (IDA, 2019; NOGUEIRA, 2021) e, paralelamente com Guia do PBC criado no Brasil. Vale realçar que o referido documento brasileiro se encontra em desenvolvimento e, contribui relativamente com este estudo. Com base no modelo PBC e na figura apresentada abaixo, busca-se apontar elementos de forças identificadas ou não. De acordo com Nelson (1993), um país constrói um sistema nacional por meio das capacidades de inovações tecnológicas e essas capacidades contribuem tanto para o desempenho das indústrias quanto para segurança e defesa de uma nação.

Figura 1: Planejamento de Capacidades: Elementos de força



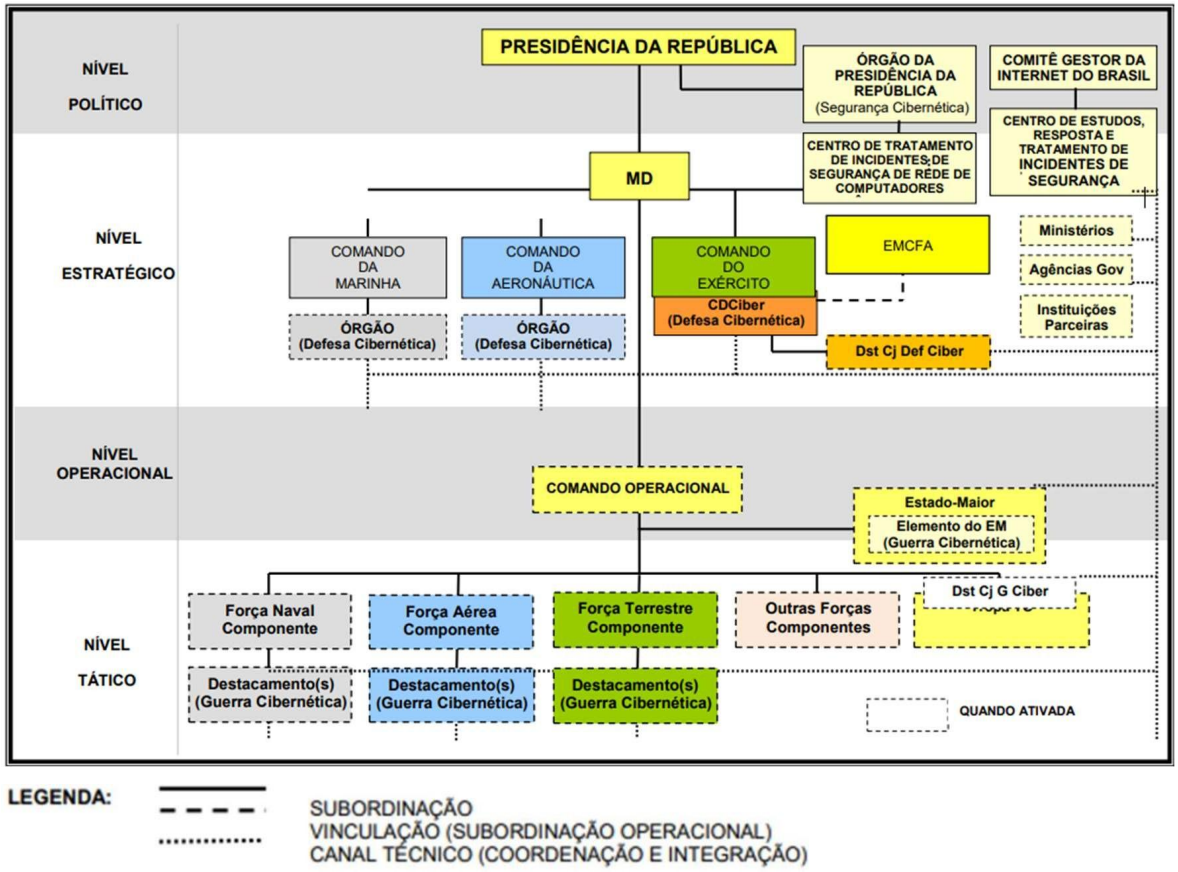
Fonte: adaptado da IDA, (2019).

[8] O *Institute for Defense Analiyses* é uma organização estadunidense sediada em Alexandria, Virgínia que visa assessorar o governo na questão da segurança nacional com base nas exigências do conhecimento científico.

Na figura mostrada, percebe-se duas etapas, nos quais o PBC permite realizar, basicamente, o processo analítico. Em primeiro lugar, são analisados os elementos de força por meio de um conjunto de elementos que compõe uma estrutura de força singular, neste contexto será DOPEMAI[9], considerando diretrizes estabelecidas. Todavia, as capacidades podem ser levantadas, também por meio da análise de orientação de política estratégica, cenários e conceitos. Nesse sentido, os elementos de força são considerados como capacidades quando geram efeitos coletivo, ou seja em harmonia entre si. Por outro lado, caso os elementos de força apresentarem resultados divergentes do grupo, são consideradas *gap*, isto indica a necessidade de melhoria da capacidade. Elemento de força se configura como uma das principais contribuições da análise do PBC. Contudo, a Doutrina da Defesa Cibernética, aponta diversos conceitos e estratégias a serem implementadas, porém, em atenção a esta análise, vale verificar a utilidade do método PBC a partir da figura abaixo, extraído do documento em questão.

Figura 2: Estruturas e Órgãos na Concepção do Sistema Militar de Defesa Cibernética

Cert.Br.



Fonte: Doutrina de Defesa Cibernética **(**Brasil, 2014, p. 35).

[9] Doutrina, Organização, Pessoal, Educação Material e Infraestrutura.

A figura representa a estrutura organizacional da concepção do Sistema Militar de Defesa Cibernética. Observa-se a Doutrina Militar de Defesa Cibernética apresentada sob fundamentos generalizada em quatro níveis de decisão, sendo:

- nível político - Segurança da Informação e Comunicações e Segurança Cibernética - coordenadas pela Presidência da República e abrangendo a Administração Pública Federal direta e indireta, bem como as infraestruturas críticas da Informação Nacionais;
- nível estratégico - Defesa Cibernética - a cargo do Ministério da Defesa, Estado-Maior Conjunto das Forças Armadas e Comandos das Forças Armadas, interagindo com a Presidência da República e a Administração Pública Federal; e
- níveis operacional e tático - Guerra Cibernética - denominação restrita ao âmbito interno das Forças Armadas (Brasil, 2014, p.17).

Esta organização, em termos fundamentais, enquadra-se no modelo PBC *top dow,* demonstrando uma visão mais abrangente sobre o tema, iniciada no PND e END, assim dando sequencias norteadora para outros órgãos responsáveis, de modo que se obtenha definições clara nos documentos e/ou diretrizes com objetivo de priorizar interesse do país e a sua Defesa. Por essa razão, a tomada de decisões que permite a execução das partes específicas, necessariamente ocorrem logo a priori, no nível político e avançando para demais níveis acima mencionados. Portanto, a metodologia do PBC engloba diferentes conjuntos de atividades, tais como: (I) insumos, que auxiliam o planejamento com itens necessários na sua elaboração; (II) Processamento, no qual emprega o uso do método; e por fim, (III) processo decisório, em que as ações devem ser aprovadas ou não (Barros, 2022).

O resultado da criação da Doutrina Militar de Defesa Cibernética originou-se no nível político e demostra coordenação integrada entre os demais órgãos. No nível estratégico, O Comando Cibernética encontra se a cargo do Exército, no qual exige um esforço de operação conjunta com o Comando da Aeronáutica e da Marinha. No nível operacional e tático, se trata da estratégia executada no ciclo real, porém a descrição no item 2.6.1, do documento apresenta uma série de limitações da Defesa Cibernética, tais como:

a) limitada capacidade de identificação da origem de ataques cibernéticos;
b) existência de vulnerabilidades nos sistemas computacionais;
c) dificuldade de identificação de talentos humanos;

d) grande vulnerabilidade a ações de oponentes com poder assimétrico;
e) dificuldade de acompanhamento da evolução tecnológica na área cibernética; e
f) possibilidade de ser surpreendido com base nas vulnerabilidades dos próprios sistemas de informação.

Essas limitações se apresentam como tarefas necessárias para a composição de elemento de força. De mesmo modo, se aplica para análises dos cenários, tendo em vista ambiente cibernético muito volátil. Em relação a observação dos itens no DOPEMAI para formar componentes da estrutura de força, apresenta-se abaixo, o quadro no item 2.7.4 do documento para exemplificar as formas de atuação cibernética (BRASIL, 2014, p. 22).

Quadro 1: As formas de atuação

FORMA DE ATUAÇÃO CIBERNÉTICA / CRITÉRIOS	POLÍTICA / ESTRATÉGICA	OPERACIONAL / TÁTICA
Nível dos Objetivos	Políticos e/ou Estratégicos	Operacionais e/ou Táticos
Foco	Obtenção de Inteligência	Preparação do campo de batalha
Nível de envolvimento nacional	Normalmente interministerial, podendo requerer ações diplomáticas e de vários ministérios e agências (Defesa, Relações Exteriores, Ciência, Tecnologia e Inovação, GSI/PR, Agência Brasileira de Inteligência - ABIN, Agência Nacional de Telecomunicações - ANATEL etc.)	Normalmente no âmbito do Ministério da Defesa, podendo contar com apoio do Ministério das Relações Exteriores
Contexto	Desde o tempo de paz, podendo fazer parte de uma Operação de Informação ou de Inteligência	Em um ambiente de crise ou conflito, apoiando uma ação militar
Nível tecnológico empregado	Normalmente alto ou muito alto	Normalmente médio ou baixo
Sincronização	Dentro do contexto de uma sofisticada Operação de Inteligência, podendo requerer ações diplomáticas anteriores ou posteriores	Dentro do contexto dos sistemas operacionais de uma Operação Militar, sincronizado com a manobra
Tempo de Preparação e Duração	Duração prolongada, com tempo de preparação normalmente mais longo, com desenvolvimento e emprego de técnicas de difícil detecção	Duração limitada, normalmente com moderado ou curto tempo de preparação, utilizando conhecimentos já levantados e técnicas previamente preparadas

Fonte: Estratégia de Segurança Cibernética (Brasil, 2014, p.23).

Consoante análises dos itens descritos no quadro na perspectiva do DOPEMAI para associar a composição de estrutura de força, entende-se que a ausência de tempo determinado se caracteriza como uma lacuna na infraestrutura. Certamente, provocado pela indefinição do

cenário cibernético incerto. A E-Ciber demostra coordenação entre os órgãos, porém, também se caracteriza como estratégia de curta duração, ou seja, de 2020-2023, tendo em vista que o PBC é uma ferramenta metodológica de análises a meio e longo prazo. Além disso, o método PBC demostrado por TTCP (2012), tem por finalidade avaliar riscos e identificar os desafios futuros, de modo a elaborar planejamento para mitigar riscos de segurança e defesa no campo político. O Estado Maior Conjunto das Forças Armadas (EMCFA) tem utilizado a referida ferramenta para avaliar a capacidades das FA em diferentes cenários, principalmente no que se refere a operações conjuntas. Portanto, a estrutura da Defesa Cibernética ainda apresenta desafios que possibilitam à interoperabilidade dos meios das FA (Marinha, Exército e Aeronáutica).

5 Considerações Finais

Neste estudo, buscou-se aprofundar a compreensão das contribuições do método PBC em matérias de Defesa, principalmente, por meio de análise dos documentos oficiais do Estado brasileiro que tratam da questão da Segurança e Defesa Cibernética, neste caso, referindo-se a Doutrina Militar de Defesa Cibernética e E-ciber. Em primeiro momento, realizou-se uma contextualização história relativamente a origem do PBC, relacionado aos eventos que foram marcados na mudança de estratégia de segurança e defesa dos países a nível global. No decorrer da pesquisa, foi percebido o quão necessária se tornou a discussão sobre os métodos capazes de travar as mais diversas ameaças que colocam em xeque a soberania dos Estados, consequentemente, os riscos à segurança humana. As ameaças cibernéticas, ameaças ambientais e dentre outros, se configuram com frequente atualizações, que apontam enormes desafios. Por essa e outras razões, a literatura tem mostrado o PBC como ferramenta eficaz para apoiar o planejamento em vários setores. As abordagens referentes aos conceitos e contexto do PBC discorreu de forma mais ampla os processos metodológicos do planejamento sob prisma do modelo do PBC. Em seguida, centralizam-se os avanços no nível doméstico por meio dos documentos nacionais (PND, END, Doutrina e E-Ciber) onde foram analisadas as tratativas para implementação do método de maneira conjuntas entre as FA.

Em relação as contribuições do PBC nos documentos oficiais mencionados, teve-se entendimento fundamentado no modelo do PBC que analisa elementos das forças, com intuito de identificar as capacidades geradas em conjuntos ou as lacunas, o que permite melhorar as estratégias. Desta feita, foram identificadas as capacidades no nível político coordenado pelos

decisores. Por outro lado, a análise do DOPEMAI constatou entraves na identificação do cenário no nível tático e operacional. Nesse sentido, considera-se o ambiente virtual mutável, o que dificulta e torna a construção do planejamento estratégico um enorme desafio. É importante realçar, que a metodologia do PBC foi idealizada para análises de médio a longo prazo. A E-Ciber, demostra um período de três anos para o seu efeito, ao passo que a Doutrina Militar de Defesa Cibernética não demostra recorte temporal do planejamento a ser executado. No entanto, a partir das análises realizadas do método PBC, entende-se que os desafios da realidade virtual se configuram como ameaça contemporânea muito complexa. O PBC contribui para a eficiência em ambiente de incerteza, conforme identificado nos documentos de segurança e defesa cibernética brasileira, bem como favorece integração, sinergia, entendimento, economicidade, exequibilidade e a manutenção de fluxo regular de recursos. Por outro lado, entende-se que o PBC é ainda uma ferramenta nova que está sendo analisada nos órgãos estatais, especificamente no MD, para aperfeiçoar planejamento estratégico em diferentes setores. Desse modo, apresenta dificuldade na execução coletiva entre as forças no nível operacional e tática para garantir a Segurança e Defesa Cibernética. Vale realçar que o método foi aplicado inicialmente nos Estados Unidos, em seguida, na Organização do Tratado do Atlântico Norte (OTAN), assim como na Austrália e Nova Zelândia, porém, este processo vem sendo adotado por diversos países, inclusive pelo Brasil.

Destarte, as ferramentas do PBC contribuem com a formulação e análises das estratégias orientadas pelo alto nível do poder, seguindo o modelo *Top-down,* de modo que as FA brasileira identificam as lacunas existente no setor de Defesa Cibernética, as capacidades relacionadas aos recursos orçamentários e a sincronização entre as forças no nível tático e operacional. Sumariamente, observa-se os documentos oficiais em análise como passo inicial para elaboração de estratégias eficientes que fortalecem as capacidades de Segurança e Defesa Cibernética do país. Vale salientar que as ferramentas do PBC contribuem na melhoria dos planos estratégicos pré-existentes, ou seja, a metodologia de planejamento por capacidades descreve os planejamentos estratégicos para complementar operações em cenários prospectivos, averiguando as perspectivas da inteligência, tecnologia e indústria e proporcionando às FA a possibilidade de interagir em sintonia contra riscos e ameaças cibernéticas ao país a meio e longo prazo.

Referências

BARGUÉS, Pol; Piñera Jorge. *Conflicto híbrido, guerra total.* CIDOB opinion. 2022. E-ISSN: 2013-4428. CIDOB - Conflicto híbrido, guerra total.

BRASIL. *Doutrina Militar de Defesa Cibernética.* Ministério da Defesa, Estado- Maior Conjunto das Forças Armadas. MD31-M-08. 2014.
BRASIL. *Glossário de Segurança da Informação.* GSI. Disponível em: Glossário de Segurança da Informação — Português (Brasil) (www.gov.br). Acessado em 20 de jul., 2022.

BRASIL. Estratégia Nacional de Segurança Cibernética. Diário Oficial da União. 2020.

BRASIL. *Portaria nº 081-EME, de 29 de abril de 2020*. Ministério da Defesa. Disponível:http://www.sgex.eb.mil.br/sg8/006_outras_publicacoes/01_diretrizes/04estado-maior_do_exercito/port_n_081_eme_29abr2020.html. Acesso 13 de jul. 2022.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. *Livro verde: segurança cibernética no Brasil.* Brasília: GSIPR/SE/DSIC, 2010, pp.63. Disponível em: http://livroaberto.ibict.br/handle/1/639. Acesso em: 21 de jul. 2022.

BARROS, Araújo Felipe. *A aplicação do planejamento baseado em capacidades no nível tático*. Revista Doutrina Militar. v. 1 n. 29. 2022, pp. 18-27. Disponível em: http://ebrevistas.eb.mil.br/DMT/issue/view/1064. Acesso em: 12 de jul. 2022.

CORRÊA, F. Das G. *Planejamento Baseado em Capacidades e Transformação da Defesa: desafios e oportunidades do Exército brasileiro*. Artigos Estratégicos, v. 8, n. 1. 2020, pp. 27-54. Disponível em: http://www.ebrevistas.eb.mil.br/CEEExArE/article/view/4843. Acesso em 14 de jul. 2022.

CHAPMAN, B. *The Australia, United Kingdom, United States (AUKUS) Nuclear Submarine Agreement: Potential Implications.* Purdue e-Pubs. 2022, pp. 1-54. Disponível em: https://docs.lib.purdue.edu/forces. Acesso em: 13 de jul. 2022.

CHIM, L; NUNES-VAZ, R.; PRANDOLINI, R. *Capability-Based Planning for Australia's National Security*. Security Challenges, 6(3), 2010, pp. 79 - 96. Disponível em: http://www.jstor.org/stable/26459800. Acesso em 13 de jul. 2022.

DA SILVA, C. C. D. *Planejamento Baseado em Capacidades e suas perspectivas para o Exército brasileiro*. Centro De Estudos Estratégicos Do Exército: Artigos Estratégicos, 7(2),

2019, pp. 21-29. Disponível em: http://ebrevistas.eb.mil.br/CEEExArE/article/view/3349. Acesso em: 13 de jul. 2022.

DA SILVEIRA GOMES, Roberto; BELDERRAIN, Mischel; DE MARCHI, Mônica Maria. *Proposta de Modelo para Avaliação de Capacidades no Contexto do PBC.* SIGE, ITA, 28 a 29 Set. 2021. ISSN: 1983 740.

DAVIS, Paul K. *Lessons from RAND's Work on Planning Under Uncertainty for National Security, Santa Monica, Calif.:* RAND Corporation, TR-1249- OSD, 2012. As of July 13, 2022, pp. 1-54. Disponível em: https://www.rand.org/pubs/technical_reports/TR1249.html. Acesso em: 12 de jul. 2022.

DESPONT, C. *Understanding Capability-Based Planning.* CSS Analyses in Security Policy, (298). 2022, pp. 1-4. Disponível em: https://doi.org/10.3929/ethz-b-000526681. Acesso em: 12 de jul. 2022.

IDA. *Guide to Capability-Based Planning.* The Technical Cooperation. Program Joint Systems and Analysis Group Technical Panel3. 2019.

INKSTER, Nigel. *Military Cyber Capabilities*. Adelphi Series, 55:456, 2015. pp. 83-108. DOI: 10.1080/19445571.2015.1181444

LABBÉ, Paul & Bowley. *Guide for Understanding and Implementing Defense Experimentation GUIDEx The Technical Cooperation Program*. Ed. TTCP, 2006. 10.13140/2.1.4937.6648.

NELSON, R. R. *National Innovation Systems: A Comparative Analysis.* New York: ed. Oxford University Press. 1993.

NOGUEIRA NEVES, A. et al. Planejamento Baseado em Capacidades nos documentos de defesa brasileiros. *Revista Hoplos*, v. 5, n. 9, pp. 48-69, 28 dez. Disponível em: https://periodicos.uff.br/hoplos/article/view/513432021. Acesso em 14 de jul. 2022.

NORI KATAGIRI. *Two explanations for the paucity of cyber-military, cross- domain operations,* Journal of Cybersecurity, Volume 8, Issue 1, 2022, pp. 1-10. Disponível em: https://doi.org/10.1093/cybsec/tyac002. Acesso em: 11 de jul. 2022.

SAN MARTIN, Luis & VERA, Jorge. *Modeling and optimization of capabilities for modular organizations under uncertainty.* ORBIT Journal. 17. 2022, pp. 17-22. Disponível em:https://www.researchgate.net/publication/361200771_Modeling_and_optimization_of_ca

pabilities_for_modular_organizations_under_uncertainty/citations#fullTextFileContent. Acesso em: 14 de jul. 2022.

STEPHAN, De Spiegeleire. *Ten Trends in Capability Planning for Defense and Security.* The RUSI Journal, 156:5, 2011. pp. 20-28. DOI: 10.1080/03071847.2011.626270

TAGAREV, Todor. The Art of Shaping Defense Policy: Scope, Components, Relationships (but no Algorithms) Source: **Connections**, Vol. 5, No. 1 Spring-Summer, pp. 15-34, 2006. Disponível em: https://www.researchgate.net/publication/267374585_The_Art_of_Shaping_Defense_Policy_Scope_Components_Relationships_but_no_Algorithms. Acesso em: 11 de jul. 2022.

TAYLOR, B. *Toward an Enhanced Capability Based Planning Approach*. Defence Research and Development Canada. 2017, pp. 1-24. Disponível em: https://cradpdf.drdc-rddc.gc.ca/PDFS/unc282/p805642_A1b.pdf. Acesso em 24 de jul. 2022.

THE TECHNICAL COOPERATION PROGRAM (TTCP). *Guide to Capability-Based Planning* - The Technical Cooperation Program Joint Systems and Analysis Group - Technical Panel 3. Canberra, 2012. Disponível em: https://www.hsdl.org/?view&did=461818#:~:text=Capability%2DBased%20Planning78%0provides%20a,capability%20goals%20to%20strategic%20requirements. Acesso em: 13 ago. 2022.

PINTO, José C. R. *Ciberdefesa e cibersegurança: novas ameaças à segurança nacional*. Rio de Janeiro: ESG. 2016, pp. 1-280.

POLI, Roberto. *A Note on the Difference Between Complicated and Complex Social Systems*. CADMUS Volume 2 - Issue 1, October 2013, pp. 142-147. Disponível em: https://www.cadmusjournal.org/files/pdfreprints/vol2issue1/reprint-cj-v2-i1-complex-vs-complicated-systems-rpoli.pdf. Acesso em 13 de jul. 2022.

RAND, Corporation. *About the RAND Corporation. S/a.* Disponível em: https://www.rand.org/about.html. Acesso em: 23 de jul. 2022.

Recebido em 15 de maio de 2023.
Aceito para publicação em 18 de julho de 2023.