JCSPP JOURNAL OF CYBERSECURITY AND PUBLIC POLICIES

Vol. 1, N. 2 (Jan - Abr 2026)
www.cybersecuritypolicies.com.br

O Crescimento da Importância da Cibersegurança para a Defesa Nacional[1]

DOI: *10.29327/2864546.1.2-5*

Gregor G. A. A. de Rooy[1]

Resumo

A importância da cibersegurança como elemento da Defesa Nacional cresceu no Brasil e no mundo nas últimas décadas. Esse artigo trata de como a cibersegurança ganhou relevância de acordo com as edições (da primeira edição à mais recente) dos dois principais documentos da Defesa Nacional, ou seja, a Política Nacional de Defesa (PND) e a Estratégia Nacional de Defesa (END). A verificação deste crescimento sugere que o campo tem se consolidado como elemento chave da Defesa, apontando para a pertinência de novos estudos como a relação entre a cibersegurança e suas implicâncias para as telecomunicações e geopolítica.

Palavras-Chave: Cibersegurança; Defesa; Estratégia.

Abstract

The importance of cybersecurity as a component of national defence has grown in Brazil and worldwide in recent decades. This article examines how cybersecurity has gained prominence across the various editions (from the first to the most recent) of the two main national defence documents: the National Defence Policy (Política Nacional de Defesa - PND) and the National Defence Strategy (Estratégia Nacional de Defesa- END). This growth suggests that the field has established itself as a key element of defence. It also highlights the relevance of further studies, such as those on the relationship between cybersecurity and its implications for telecommunications and geopolitics.

Keywords: Cybersecurity; Defence; Strategy.

1 Gregor G. A. A. de Rooy é Doutor em Ciências Militares pela Escola de Comando e Estado-Maior do Exército e realiza pós-doutorado por esta Escola. Contato: gregorooy@gmail.com

Introdução

A internet, oriunda da ARPANET, criada em 1969 pelo Departamento de Defesa dos Estados Unidos da América (EUA) para garantir a comunicação entre instituições de pesquisa, popularizou-se no mundo a partir de 1989 com o primeiro *browser* da rede mundial de computadores e a criação do *World Wide Web* (WWW) pelo britânico Tim Berners-Lee quando trabalhava no *Conseil Européen pour la Recherche Nucléaire* (CERN). Segundo o CERN, o WWW é: "a wide-area hypermedia information retrieval initiative aiming to give universal access to a large universe of documents" (CERN, 2026). A partir da criação dessa estrutura, tem-se a internet como se conhece hoje.

Com o advento da internet e da enorme quantidade de serviços ou funções, tanto para fins civis como militares, que ocorrem a partir desta plataforma ou de sistemas de intranet, surgiu uma série de desafios que exigem o empenho do Estado. Na próxima seção, sugere-se um conjunto de conceitos do campo dos estudos de Defesa que contribuem para a compreensão da dimensão cibernética como um elemento que suscita ações de Defesa e Segurança. Consecutivamente, compreende-se a cibersegurança a partir do nível estratégico. Por fim, analisa-se como o Estado Brasileiro, mediante as diferentes edições de seus principais documentos de Defesa, tem se adequado a esta nova e dinâmica realidade.

Sobre esta análise explica-se que a Política de Defesa Nacional (PDN), chamada de Política Nacional de Defesa (PND) a partir de 2012, tem seis edições (1996, 2005, 2012, 2016, 2020 e 2025) e a Estratégia Nacional de Defesa conta com cinco edições (2008, 2012, 2016, 2020 e 2025). O estudo de todas as edições permitiu que se verificasse o crescimento da importância da dimensão ciber para a Defesa. Isto foi feito por meio da busca pelas menções ao termo "ciber" e a compreensão deste termo nos documentos a partir dos seguintes aspectos: frequência de menções, associações com outros setores estratégicos (nuclear e aeroespacial), recomendações institucionais e atribuições por Força. Daí se verificou continuidades e descontinuidades em relação à cibersegurança entre as edições, bem como seu crescimento em relevância para a Defesa Nacional. Esta pesquisa nos documentos, de cunho qualitativo, é também respaldada pela revisão bibliográfica sobre o assunto que se sucede nas próximas duas seções.

1 Cibersegurança sob perspectiva

O primeiro vírus que ganhou notoriedade com o surgimento do WWW foi o *Love Letter*. Com este vírus marca-se um momento em que estes programas[2] já não eram injetados em redes de computadores a partir de disquetes, mas a partir da própria internet (Karspersky Lab, 2026). Com o avanço desta tecnologia, no que diz respeito à segurança dos Estados, Kaplan escreve que:

> Uma vez que o funcionamento de quase tudo na vida era controlado por ou através de computadores – os sistemas de orientação de bombas inteligentes, as centrífugas em um laboratório de enriquecimento de urânio, as válvulas de controle de uma represa, as transações financeiras dos bancos, até mesmo a mecânica interna dos carros, termostatos, alarmes contra roubo, torradeiras – invadir uma rede dava a um espião ou guerreiro cibernético o poder de controlar essas centrífugas, represas e transações: mudar suas configurações, desacelerá-las, acelerá-las ou desativá-las, até mesmo destruí-las (Kaplan, 2016, p. 9).

2 Os vírus de computador podem ser definidos como "programs that self-replicate and spread from one computer to another with disruptive and damaging intentions, such as stealing, altering, or deleting data" (Arinze & Agwu, 2024, p. 12).

A versatilidade das ciber ameaças suscitou diferentes esforços de classificação e categorização. Lehto (2022) as divide em seis: o ciber vandalismo; a ciber espionagem; o ciber crime; o ciber terrorismo; a ciber sabotagem e a ciber guerra. As categorias que mais podem comprometer a soberania do Estado são a ciber espionagem, sabotagem e guerra (Lehto, 2022). Especificamente sobre ações de ciber guerra ou ciber ataques, Raza (2013) elabora uma diferenciação entre as capacidades cinéticas (meios dissuasórios convencionais) e as capacidades cibernéticas.

Na capacidade cinética, tem-se três aspectos chave: a potencialidade, a intencionalidade e a plausibilidade. Por potencialidade entende-se que a "geração, por um potencial atacante, da percepção no adversário de que seu arsenal é superior ao seu" (Raza, 2013, p. 14). A plausibilidade significa a "percepção, da parte que detém a ofensiva, de que os riscos previstos compensam os ganhos prováveis na defesa dos interesses disputados entre as partes" (Raza, 2013, p. 15). Por fim, no que diz respeito à intencionalidade: "a percepção, pelo adversário, de que há a intenção política da outra parte de efetivamente usar força cinética letal após esgotado seu arsenal defensivo de táticas diplomáticas" (Raza, 2013, p. 15).

Já a dissuasão cibernética, explica Raza, não funciona sob essa tríade. Segundo o autor:

> A geopolítica dos espaços de conflitos cibernéticos é diferente: a potencialidade da ameaça é neutralizada pela sempre possível superioridade defensiva cibernética de adversários claramente menos dotados de arsenal cinético. Com isso, a relação defesa-ataque na guerra cibernética é muito mais difícil de estabelecer do que na guerra cinética, tornando a distinção entre dissuasor e dissuadido muito mais complicada. Com relação à plausibilidade, na guerra cinética, uma vez empregada determinada tática (seja com sucesso ou não), ela praticamente estará alijada do arsenal disponível para emprego, já que imediatamente o adversário irá desenvolver uma contramedida. Essa é a razão do enorme "secretismo" da guerra cibernética (Raza, 2013, p. 15).

Dentre os ataques que podem ser compreendidos a partir do espectro cibernético, em vez do cinético, é possível citar o bloqueio de serviços eletrônicos na Estônia, em 2007, e na Geórgia em 2008 — provavelmente, orquestrados por Moscou (Cardoso, 2013). Outro exemplo foi o uso do vírus Stuxnet a partir de um ataque coordenado entre os EUA e Israel contra centrífugas de enriquecimento de urânio do Irã em 2007.

Na literatura também se encontram operações que combinam meios convencionais ou cinéticos e ciberataques, como a israelense, em 2007, que permitiu o bombardeio de instalações de enriquecimento de urânio na Síria. Raza explica que "os Sírios viam em seus radares o que os israelenses queriam e necessitavam que eles vissem nada — permitindo que os F-15 Eagle e F-16 Falcon 'fizessem o trabalho'" (Raza, 2013, p. 9)[3].

Desta forma, tem-se que quão mais o Estado depende dos meios cibernéticos, mais grave pode ser o dano infringido a sua segurança. Esta realidade suscita duas perguntas: Como

3 O que chama atenção neste ataque em específico é que, apesar da internet ser o principal meio a partir do qual um ciber ataque pode ser realizado, ela não é o único. Redes ou sistemas de computadores, ainda que não estejam ligados à internet, podem ser atacados de outras formas. Neste caso, a invasão dos sistemas de computadores sírios se deu a partir de Vants (Veículos Aéreos Não Tripulados) dotados de recursos que atingiram o sistema sírio de detecção de radar (Raza, 2013).

compreender a dimensão ciber a partir de uma perspectiva da Defesa Nacional? De que maneira o Estado Brasileiro tem tratado essa realidade, ao longo dos anos, de acordo com seus principais documentos de Defesa?

2 A cibersegurança compreendida a partir do nível estratégico

A guerra, como principal objeto de estudos das Ciências Militares, é compreendida em três principais dimensões ou níveis: o estratégico, o operacional e o nível tático (Maxwell, 1997; Harvey, 2022). Para Harvey (2022), o nível estratégico engloba a dimensão política e a estratégia do teatro de operações; o operacional seria aquele referente às campanhas e grandes operações e o nível tático o relativo aos combates, engajamentos e ações de frações e guarnições (Harvey, 2022).

Maxwell define a dimensão estratégica como o nível centrado no apoio à política nacional e que está diretamente relacionado com o resultado de uma guerra ou de outro conflito no seu conjunto. Comumente, as guerras e os conflitos modernos são vencidos ou perdidos neste nível e não nos operacional ou tático.

O nível estratégico aplica-se a todas as formas de guerra e de conflito, desde as atividades militares fora da guerra até à guerra insurrecional, convencional e nuclear. Envolve um conceito estratégico, planos para preparar todos os instrumentos nacionais de poder para a guerra ou conflito, orientação prática para preparar as Forças Armadas e liderança das Forças Armadas (Maxwell, 1997, p. 1, traduzido pelo autor).

O nível estratégico, portanto, ou faz parte do nível político (Harvey, 2022) ou é aquele que apoia diretamente a política (Maxwell, 1997). Como explica Maxwell (1997), o nível estratégico engloba as atividades militares fora da guerra e envolve "planos para preparar todos os instrumentos nacionais de poder para a guerra ou conflito" (Maxwell, 1997). Neste sentido, o Brasil organizou três principais documentos que versam sobre as suas necessidades de Defesa neste nível. Nas próximas seções, analisar-se-á como a ciberdefesa ou a cibersegurança, que solicitam uma série de recursos materiais e humanos, são contempladas em dois destes documentos nas suas diferentes edições.

3 Os documentos de Defesa

O governo do presidente Fernando Henrique Cardoso (1995-2002) lançou, em 1996, a Política de Defesa Nacional (PDN) que, a partir de sua terceira edição, em 2012, passou a se chamar Política Nacional de Defesa (PND). A PND é o documento condicionante de mais alto nível do planejamento de Defesa. Em 1999, Cardoso também criou o Ministério da Defesa em substituição aos Ministérios do Exército, da Marinha e da Aeronáutica.

Além da PND, no início deste século, mais dois documentos/diretrizes foram lançados: a Estratégia Nacional de Defesa (END) e o Livro Branco de Defesa Nacional (LBDN).

Nesta seção, analisa-se como a cibersegurança e a ciberdefesa, termos explicados adiante, se sobressaem nestes documentos. Para tanto, foi realizada a leitura das diferentes edições da Política Nacional de Defesa (PND) e da Estratégia Nacional de Defesa. As versões da PND foram lançadas em 1996 e 2005 (com o nome de Política de Defesa Nacional — PDN); 2012; 2016; 2020 e 2025, e as da END em 2008; 2012; 2016; 2020 e 2025.

Em poucas linhas, a PND é o documento mais importante do País sobre a Defesa Nacional e seus objetivos são baseados nos princípios constitucionais (Brasil, 2012). Segundo a versão da PND de 2012, da distinção entre a PND e a END tem-se que:

> a PND fixa os objetivos de Defesa Nacional e orienta o Estado sobre o que fazer para poder alcançá-los. A END, por sua vez, estabelece como fazer o que foi estabelecido pela Política. Em comum, os documentos pavimentam o caminho para a construção da Defesa que o Brasil almeja (Brasil, 2012, p. 7).

A PND é um documento mais sucinto do que a END. A análise a seguir se deu pela busca do termo "ciber" ao longo das diferentes versões da PDN/PND. A partir desta busca, observa-se como a cibersegurança e a ciberdefesa crescem em relevância para a Defesa.

3.1 A cibersegurança e a ciberdefesa na PDN/PND

A versão de 1996 não conta com menções à esfera ciber, encontrando-se, somente, alusões à importância do campo científico-tecnológico. Na edição de 2005, há alguns aspectos a se observar. O primeiro diz respeito à definição proposta que deve assim ser assimilada pelas Forças Armadas sobre segurança e defesa (subitem 1.4 do item 1 "O Estado, a Segurança e a Defesa"):

> I – Segurança é a condição que permite ao País a preservação da soberania e da integridade territorial, a realização dos seus interesses nacionais, livre de pressões e ameaças de qualquer natureza, e a garantia aos cidadãos do exercício dos direitos e deveres constitucionais;
>
> II – Defesa Nacional é o conjunto de medidas e ações do Estado, com ênfase na expressão militar, para a defesa do território, da soberania e dos interesses nacionais contra ameaças preponderantemente externas, potenciais ou manifestas (Brasil, 2005, p. 2).

A partir destas definições, pode-se compreender e diferenciar a cibersegurança da ciberdefesa. Verificou-se menção ao termo "ciber" pela primeira vez na versão de 2005. No item 6 "Orientações Estratégicas", subitem 6.19, escreveu-se que para minimizar os danos de possível ataque cibernético "é essencial a busca permanente do aperfeiçoamento dos dispositivos de segurança e a adoção de procedimentos que reduzam a vulnerabilidade dos sistemas e permitam seu pronto restabelecimento" (Brasil, 2005, p. 9).

No item 7 "Diretrizes", subitem XII, tem-se como diretriz de política de Defesa o aperfeiçoamento dos "dispositivos e procedimentos de segurança que reduzam a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra ataques cibernéticos e, se for o caso, permitam seu pronto restabelecimento" (Brasil, 2005, p. 10). As instruções nas Orientações

Estratégicas e nas Diretrizes da PDN de 2005 marcam a primeira vez em que o tema é tratado no nível estratégico da Defesa.

Com a edição de 2012, a cibersegurança ganha maior destaque. Encontra-se menção no subitem 3.6 do item 3 "O Ambiente Internacional" e menção, duas vezes, no item 7 "Orientações" (subitens 7.10 e 7.17). Tanto o subitem 3.6 como o subitem 7.10 destacam que a dimensão ciber é um setor de importância estratégica para o País; tão relevante quanto os setores espacial e nuclear. No subitem 3.6 há, ainda, a orientação de que se desenvolva tecnologias autóctones nesses três setores, tendo em vista a redução da dependência de tecnologias do exterior (Brasil, 2012).

Especificamente sobre o subitem 7.17, cabe um destaque. Como uma das orientações da PND, lê-se o seguinte:

> Para se opor a possíveis ataques cibernéticos, é essencial aperfeiçoar os dispositivos de segurança e adotar procedimentos que minimizem a vulnerabilidade dos sistemas que possuam suporte de tecnologia da informação e comunicação ou permitam seu pronto restabelecimento (Brasil, 2012, p. 34).

Desde então, a cibersegurança começa a ser pensada em conjunto com outros elementos da Defesa, como a tecnologia de comunicações. As edições de 2016 e 2020 apontam para a importância da cibersegurança de forma bastante semelhante à edição de 2012: ambas recomendam a proteção do espaço cibernético, o qual ganha relevância ao passo que processam e armazenam informações digitais responsáveis pelo funcionamento dos sistemas de informações e comunicações de interesse nacional e de parcela significativa da população (Brasil, 2016; 2020).

Na versão de 2016, houve uma importante mudança: a dimensão ciber foi considerada parte essencial da guerra híbrida, onde ações de combate convencional são combinadas com "operações de natureza irregular, de guerra cibernética e de operações de informação, dentre outras, com atores estatais e não-estatais, no ambiente real e informacional, incluindo as redes sociais" (Brasil, 2016, p. 16).

Na edição de 2025, o ciberespaço ganha realce. Desta vez, além de ser considerado um espaço *per se*, é considerado uma dimensão estratégica tanto para a infraestrutura de comunicações, como para a manutenção da ordem social — algo preambulado na edição de 2016.

Acerca disso, o documento destaca que o ciber espaço deve ser protegido de duas formas. A primeira diz respeito à proteção daquilo que é chamado de "infraestruturas críticas de conectividade do País" (Brasil, 2025), ou seja, aquela infraestrutura que permite a existência do ciber espaço, como cabos submarinos e sistemas satelitais. A segunda é o adequado aporte tecnológico para a sua proteção contra ataques cibernéticos. A proteção garantiria o funcionamento dos sistemas de informações e a manutenção das comunicações de interesse nacional, elementos essenciais à prevenção de um cenário hipotético de inoperância ou "apagão" desses sistemas — o que poderia colocar em risco o funcionamento de sistemas vitais do País

ou, até mesmo, causar um cenário de desordem social (Brasil, 2025). Por fim, embora não se aprofunde sobre o tema, a última versão da PND diz que "a sofisticação e a intensificação desses ataques contribuem para desestabilizar as relações entre Estados e corporações" (Brasil, 2025).

A análise das diferentes edições da PDN/PND entre 1996 e 2025 permitiu a verificação de alguns aspectos essenciais que pautam o documento mais importante da Defesa do País depois da Constituição da República Federativa do Brasil de 1988. A dimensão ciber começa a ser mencionada em 2005 e cresce exponencialmente em três momentos. Em 2012, passa a ser observada como parte de uma infraestrutura maior de comunicações. Em 2016, é compreendida como um elemento da guerra híbrida sendo, dentro desta dimensão, as redes sociais um ponto de vulnerabilidade. Em 2025, além da sua relevância para a infraestrutura de comunicações, também mencionada em 2016 e 2020, o ciberespaço é reconhecido como uma dimensão que pode impactar a ordem social e, consequentemente, a ordem política. A ideia de que deve haver o adequado aporte tecnológico e de que ferramentas de cibersegurança ou ciberdefesa devem ser continuamente aperfeiçoadas é uma constante nas diferentes edições — exceto a edição de 2005.

A partir da versão de 2012, a esfera ciber foi mencionada em passagens que também se referiam ou a "comunicações" ou a "informações", fato que demonstra que os meios de comunicações e o ciberespaço são notadamente compreendidos em conjunto aos olhos da Defesa Nacional. Na próxima seção, analisa-se como a END, em suas diferentes edições, trata da importância da cibersegurança e ciberdefesa.

3.2 A cibersegurança/defesa na END

A Estratégia Nacional de Defesa "estabelece como fazer o que foi estabelecido pela Política" (Brasil, 2012, p. 7). Nesta seção, apresenta-se a forma como as diferentes edições foram organizadas e as principais ideias em relação à cibersegurança e à ciberdefesa ao longo do tempo.

O termo cibernético/a foi mencionado 17 vezes na END de 2008; 28 vezes na END de 2012; 17 vezes na edição de 2016; 15 vezes em 2020 e 25 vezes na END de 2025. Dentre estas menções, há uma parte relevante de recomendações ou linhas de ação relacionadas à esfera ciber em conjunto com dois outros campos da Defesa: o nuclear e o aeroespacial. Estes são os três setores estratégicos da Defesa Nacional desde a sua primeira versão.

Do total de 17 menções na END de 2008, dez são em conjunto com estes setores. Na versão de 2012, são oito menções do total de 28; três menções de um total de 17 na END de 2016; três de um total de 15 menções na versão de 2020 e três vezes de um total de 25 vezes na END de 2025.

Dito isto, a explanação sobre como a ciberdefesa e a cibersegurança tem espaço na END se dará em três etapas. Na primeira, tratar-se-á de como a esfera ciber é compreendida em conjunto com o setor nuclear e o aeroespacial. Na segunda etapa, analisar-se-á principalmente

a END de 2008 (porque as demais edições repetem importantes menções desta edição no que diz respeito ao campo cibernético). Ao longo da explanação, se apontará para adaptações que ocorreram nas diferentes edições entre 2008 e 2025.

3.2.1 A ciberdefesa compreendida em conjunto com outros setores estratégicos

Na END de 2008, das dez vezes em que o termo cibernético é mencionado em conjunto com os demais setores estratégicos, cinco menções dizem respeito à sua relevância. O campo é compreendido como decisivo, estratégico, essencial e que precisa ser fortalecido (Brasil, 2008). Nas outras menções, são recomendadas a independência tecnológica, a capacitação de recursos humanos nos três setores e a criação de parcerias estratégicas com nações amigas (Brasil, 2008).

Na versão de 2012, as menções são bastante semelhantes à edição de 2008, ou seja, também se recomenda que os setores precisam ser fortalecidos, que são estratégicos, decisivos, essenciais e que se faz necessária uma independência tecnológica a partir da capacitação de recursos humanos. Assim como na versão de 2008, o desenvolvimento destes três campos também poderia ocorrer a partir de parceria com nações amigas. A diferença é que, na de 2008, observa-se uma ênfase reservada ao entorno estratégico brasileiro e à comunidade de países de língua portuguesa (BRASIL, 2008), enquanto na versão de 2012 fala-se acerca de nações da América do Sul e países lindeiros do Atlântico Sul (Brasil, 2012).

Na END de 2016, a menção em conjunto decai significativamente: foram encontradas somente três menções em que estes campos são considerados essenciais e estratégicos e que, portanto, precisavam ser desenvolvidos. Isto repete-se nas versões de 2020 e de 2025, onde os setores nuclear, aeroespacial e cibernético, mencionados em conjunto, precisam ser fortalecidos e são considerados estratégicos.

3.2.2 A ciberdefesa e a cibersegurança na END 2008-2025

A ciberdefesa, na versão de 2008, recebe importantes menções. Dentre estas, consta a necessidade de que o País alcance a independência tecnológica para que o setor cibernético e o setor espacial performem, de forma soberana, a observação e o monitoramento do território nacional (Brasil, 2008).

No que diz respeito às atribuições da Marinha, a autonomia em tecnologias cibernéticas deveria garantir a navegação dos submarinos, orientar seus sistemas de armas e permitir que atuem em rede com outras forças navais e terrestres (Brasil, 2008). Isso também é dito em relação ao exército que necessita dos "instrumentos cibernéticos necessários para assegurar comunicações entre os monitores espaciais e aéreos e a força terrestre" (Brasil, 2008, p. 26).

Além da recomendação de que o País e as Forças Armadas buscassem a independência tecnológica para monitoramento, comunicação inter e intra forças e expansão da força terrestre, o documento também fala da importância de se capacitar recursos humanos em cibersegurança e

ciberdefesa. Por fim, argumenta-se que as capacidades cibernéticas, essenciais para a indústria, educação e forças armadas solicitam a criação de uma organização "encarregada de desenvolver a capacitação cibernética nos campos industrial e militar" (Brasil, 2008, p. 33).

Os pontos apresentados pela END de 2008 são também encontrados na versão de 2012, ou seja, monitoramento do território, navegabilidade de submarino e orientação de seus sistemas de armas, comunicações inter e intra forças armadas e capacitação de recursos humanos no campo, tanto para o setor militar como para o industrial e o educacional.

Naquilo que diz respeito às necessidades operacionais das Forças Armadas, encontra-se menção ao desenvolvimento da "capacitação, preparo e o emprego dos poderes cibernéticos operacional e estratégicos, em prol das operações conjuntas e da proteção das infraestruturas estratégicas" (Brasil, 2012, p. 20). Por fim, o documento reservou ao Departamento de Ciência e Tecnologia do Exército, em ação conjunta com o Ministério da Defesa e Ministério da Ciência, Tecnologia e Inovação, a responsabilidade de promover ações que fomentassem a Base Industrial de Defesa. Estas ações teriam como finalidade a geração de empregos e a proteção de infraestruturas estratégicas. Dentre estas, destacam-se a criação: de um simulador de defesa cibernética; de ferramentas de inteligência artificial; de um sistema integrado de proteção de ambientes computacionais; de um sistema de consciência situacional e algoritmos criptografados e auto autenticáveis (Brasil, 2012).

Em 2016, o documento continua a mencionar a relevância da ciberdefesa para submarinos e seus armamentos, bem como para a comunicação inter e intra forças, além de citar a relevância do aprimoramento da segurança da informação, comunicação e cibernética. Esta orientação acerca do aprimoramento da tecnologia cibernética e independência tecnológica continua nas edições de 2020 e de 2025, as quais mencionam que estes avanços devem se dar por meio de financiamento público, pesquisa, parceria com civis, e/ou a partir de parcerias com outras nações (Brasil, 2016; Brasil, 2020; Brasil, 2024).

Há algumas mudanças importantes na edição de 2016. A principal mudança diz respeito ao argumento de que o ciber espaço deve ser compreendido como uma dimensão espacial que deve ser protegido, assim como outras dimensões espaciais do País. Isto é abordado no item 4 "Estratégias e Ações Estratégicas de Defesa", subitem "Fortalecimento da capacidade de dissuasão", no qual se recomenda o desenvolvimento das "capacidades de monitorar e controlar o espaço aéreo, o espaço cibernético, o território, as águas jurisdiscionais brasileiras e outras áreas de interesse" (Brasil, 2016, p. 59) e o incremento das "capacidades de defender e de explorar o espaço cibernético" (Brasil, 2016, p. 59).

Em 2016, mencionou-se, pela primeira vez, as atribuições da força aérea em relação a este campo[4], a qual continua nas versões de 2020 e de 2025 com poucas alterações no corpo do texto.

4 O trecho da END que trata do assunto diz o seguinte: "Considerando que a Força Aérea se configura como uma organização altamente tecnológica, imprescindível se faz utilizar-se das capacidades de proteção dos Sistemas de Comando e Controle e das Estruturas Estratégicas do País, principalmente daquelas que envolvam o espaço cibernético. Deve, portanto, manter em elevado grau o nível de segurança e de defesa dos seus sistemas computacionais (Brasil, 2016, p. 51). Em 2020, o termo "Estruturas Estratégicas do País" é substituído pelo termo "Estruturas Críticas do País". Em 2025, optou-se por trocar as opções anteriores por "infraestruturas críticas da Força", de modo que a passagem ficou assim: "é imprescindível utilizar as capacidades de proteção dos sistemas de comando e controle e das infraestruturas críticas da Força, principalmente aquelas que envolvam o espaço cibernético de interesse" (Brasil, 2025).

Em relação à Marinha, também se encontrou mudanças nas edições de 2020 e 2025. Em 2020, o foco do documento é que a Marinha tenha capacidades, dentro do campo das capacidades cibernéticas, tanto defensivas como ofensivas (Brasil, 2020). Em 2025, já não se encontrou nenhuma menção ao termo atrelada à Marinha.

Em relação ao Exército, encontrou-se poucas alterações nas versões de 2016, 2020 e 2025. Na edição de 2016, o Sistema de Defesa Cibernética consta como um dos indutores da transformação da força que contribui diretamente para a capacidade de dissuasão (Brasil, 2016). Este sistema, em conjunto com outros sistemas — como o Sistema Integrado de Monitoramento de Fronteira (SISFRON), Sistema de Mísseis e Foguetes, Sistema de Defesa Antiaérea e a Mecanização do Exército — impactam diretamente na "mobilidade, atividade de monitoramento e controle das fronteiras e na capacidade de atuar na negação de acesso indesejado a áreas ou a sistemas estratégicos de interesse nacional" (Brasil, 2016, p. 50). Esta abordagem permanece nas duas edições posteriores com uma alteração na versão de 2025. O termo "Mecanização do Exército" foi substituído por "Programa Aviação" e "Programa Forças Blindadas". Outra alteração na edição de 2025 diz respeito a "sistema de foguetes", que foi removido em favor do termo "programa Astros".

Um aspecto importante na END de 2016 (que será mencionado nas edições futuras) diz respeito à relação entre a cibersegurança e as estruturas estratégicas. O documento destaca que o aprimoramento da segurança da informação, comunicações e cibernética solicita uma ênfase "na proteção das Estruturas Estratégicas relacionadas à Tecnologia da Informação" (Brasil, 2016, p. 56). Em 2020, determinou-se que cabe ao setor cibernético, além de garantir a interoperabilidade dos três ramos das Forças Armadas, "aprimorar a Segurança da Informação e das Comunicações e a Segurança Cibernética em todas as instâncias do Estado, com ênfase na proteção das Estruturas Estratégicas relacionadas à Tecnologia da Informação" (Brasil, 2020).

Em 2025, a menção em relação à proteção da infraestrutura se encontra junto às demais tarefas atribuídas ao setor cibernético, como a consolidação da atuação conjunta interagências, a produção do conhecimento de inteligência ao nível estratégico operacional, a garantia da proteção dos sistemas de comando e controle de defesa (Brasil, 2025).

Por fim, naquilo que diz respeito à expansão de setores, departamentos ou Comandos dentro das Forças Armadas para gerir as capacidades cibernéticas é importante pontuar que, na edição de 2008, falou-se na criação de uma organização capaz de desenvolver as capacidades cibernéticas no País e na capacitação de recursos humanos. Estas duas ideias são aprimoradas, em 2012, em diferentes sentidos, dentre os quais cita-se o fortalecimento do Centro de Defesa Cibernética (que deverá se tornar o Comando de Defesa Cibernética das Forças Armadas); a criação de uma Escola Nacional de Defesa Cibernética; a necessidade de fomentar a pesquisa e criar laboratórios para o desenvolvimento do setor; o desenvolvimento de sistemas computacionais e de tecnologias que permitam operações a partir do Ministério da Defesa, bem como a organização do conhecimento sobre o campo (Brasil, 2012).

Em 2016, naquilo que diz respeito ao crescimento da defesa cibernética dentro do Exército, o texto limitou-se a informar que o Sistema de Defesa cibernética constava entre um dos indutores da transformação da Força. Em 2020, o tópico é retomado quando se trata da necessidade de "concluir a estrutura do Sistema Militar de Defesa Cibernética (SMDC) com seu marco legal, suas normas afins, bem como desenvolver o seu preparo e o emprego em todos os níveis" (Brasil, 2020, p. 60). Por fim, em 2025, verifica-se que a conclusão desta estrutura continua.

A análise das diferentes edições permite dizer que o Estado Brasileiro, de maneira contínua, reconhece a importância da dimensão ciber e busca por independência tecnológica, capacitação de pessoal e uso desta tecnologia, tanto para a esfera militar, quanto para a esfera civil, especialmente a indústria e a educação. Além destas, existe também o campo das telecomunicações de uso das Forças Armadas e da sociedade civil, mencionado em conjunto com a segurança cibernética, especialmente nas diferentes edições da PDN/PND.

A ciberdefesa foi enquadrada como um campo da responsabilidade do Exército, enquanto os setores nucleares e aeroespaciais foram setores prioritários da Marinha e da Força Aérea. Notou-se, todavia, que o aprimoramento ou a importância desta dimensão, nas diferentes edições, também foi reservado à Marinha e à Força Aérea. Além destes pontos, houve uma contínua preocupação em relação à criação de órgãos ou estruturas, no âmbito do Ministério da Defesa ou do Exército, que fosse capaz de centralizar e/ou gerir as capacidades em ciberdefesa. Neste sentido, menciona-se que o Exército Brasileiro criou, em 2010, o Centro de Defesa Cibernética e, em 2014, o Comando de Defesa Cibernética, o qual abriga a Escola Nacional de Defesa Cibernética criada em 2015.

Considerações Finais

Desde que o WWW foi criado, em 1989, a cibersegurança tem crescido em relevância. Neste artigo, tratou-se brevemente da sua história, de alguns elementos conceituais que caracterizam o seu estudo na guerra e, por fim, das diferentes edições tanto da PDN/PND (1996-2025), como da END (2008-2025), percebendo-se a contínua e crescente atenção do tema por parte do Estado Brasileiro.

A dependência dos sistemas informatizados para o funcionamento de serviços essenciais, como redes elétricas, sistemas bancários, de transportes, serviços de saúde, comércio etc. aponta para o crescimento da importância da cibersegurança. Além disso, com o advento da IA (Inteligência Artificial), mencionada na END de 2012, o setor cibernético é potencializado em suas capacidades defensivas, mas também ofensivas, tornando sistemas digitais mais vulneráveis (Poongodi *et al.* 2025).

Esta realidade suscita possibilidades para pesquisas no campo. Em relação aos documentos de defesa, há os desafios, tanto nas Forças Armadas, como no Ministério da Defesa ou em outros órgãos do governo, na implementação das diretrizes elencadas acima. Especialmente relevante para futuras investigações, além do emergente leque de pesquisas voltado para a IA, é o potencial de estudos multidisciplinares entre cibersegurança, telecomunicações e geopolítica. Conforme verificado nas diferentes edições da PND e da END¸ a importância da cibersegurança para as comunicações do País é uma constante.

O estudo, sob o prisma sugerido, dos cabos submarinos, centros de dados, provisão de energia, sistemas satelitais, ou seja, da infraestrutura que permite a existência do ciberespaço, pode contribuir na compreensão de fragilidades e de vantagens estratégicas do Estado em contexto de crescente instabilidade internacional.

Referências

ARINZE, Echegu D. & AGWU, Chukwuemeka O. (2024). Advancements in Computer Virus Protection: From Origins to Future Trends. **Eurasian Experiment Journal of Scientific and Applied Research**, 6(1):11-16. Disponível em: https://smartie.kiu.ac.ug/public/assets/publications/8daa34f2697be92c06c429e70d09ef9e49876b88.pdf . Acesso em: 12 fev. 2026.

BATRA, Shefali; GUPTA, Madhu; SINGH, Jessicaa; SRIVASTAVA, Devshri, AGGARWAL, Isha. An Empirical Study of Cybercrime and Its Preventions. 2020 **Sixth International Conference on Parallel, Distributed and Grid Computing** (PDGC). India. Disponível em: https://www.researchgate.net/publication/348539042_An_Empirical_Study_of_Cybercrime_and_Its_Preventions#fullTextFileContent . Acesso em: 3 fev. 2026.

BRASIL. Presidência da República. **Política de Defesa Nacional**. Brasília: Presidência da República. 1996. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/publicacoes-politica-e-estrategia-nacional-de-defesa/politica-de-defesa-nacional-1996.pdf . Acesso em: 10 jan. 2026.

BRASIL. Decreto n. 5.484, de 1º de julho de 2005. **Diário Oficial da União**: seção 1, Brasília, DF, p. 5, 1 de julho de 2005. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2005/decreto/d5484.htm . Acesso em: 25 fev. 2026.

BRASIL. Ministério da Defesa. **Política Nacional de Defesa**. Brasília: MD, 2012. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/ajuste-01/estado_e_defesa/END-PNDa_Optimized.pdf . Acesso em: 15 maio 2025.

BRASIL. Ministério da Defesa. **Política Nacional de Defesa**. Brasília: MD, 2016. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/publicacoes-politica-e-estrategia-nacional-de-defesa/pnd-e-end-2016.pdf . Acesso em: 2 fev. 2026.

BRASIL. Ministério da Defesa. **Política Nacional de Defesa**. Brasília: MD, 2020. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_congressonacional_22_07_2020.pdf Acesso em: 5 fev. 2026.

BRASIL. Ministério da Defesa. **Política Nacional de Defesa**. Brasília: MD, 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/D12725.htm#anexo1 . Acesso em: 10 fev. 2026.

BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa**. Brasília: MD, 2008. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/publicacoes-politica-e-estrategia-nacional-de-defesa/end-2008.pdf . Acesso em: 15 maio. 2017.

BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa**. Brasília: MD, 2012. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/ajuste-01/estado_e_defesa/END-PNDa_Optimized.pdf . Acesso em: 20 dez. 2025.

BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa**. Brasília: MD, 2016. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/publicacoes-politica-e-estrategia-nacional-de-defesa/pnd-e-end-2016.pdf . Acesso em: 12 jan. 2026.

BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa**. Brasília: MD, 2020. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_congressonacional_22_07_2020.pdf . Acesso em: 12 jan. 2026.

BRASIL. Presidência da República. **Decreto n. 12.725, de 18 de novembro de 2025**. Aprova a Política Nacional de Defesa, a Estratégia Nacional de Defesa e o Livro Branco de Defesa Nacional. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/d12725.htm . Acesso em: 10 mar. 2026.

CARDOSO, Alberto. Surpresa: Somos Espionados! **Interesse Nacional**, São Paulo, v. 6, n. 23, p. 18-25, out./dez. 2013.

CONSEIL EUROPÉEN POUR LA RECHERCHE NUCLÉAIRE (CERN). **What is Hyper Text.** Disponível em: https://info.cern.ch/hypertext/WWW/TheProject.html . Acesso em: 5 jan. 2026.

HARVEY, Andrew S. Os Níveis de Guerra como Níveis de Análise. **Military Review**. Primeiro Trimestre 2022.

KAPLAN, Fred. **Dark Territory**: the Secret History of Cyberwar. Nova Iorque: Simon & Schuster. 2016.

KARSPERSKY LAB. **Um breve histórico dos vírus de computador e qual será seu futuro.** Karspersky, 2026. Disponível em: https://www.kaspersky.com.br/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds . Acesso em: 2 fev. 2026.

LEHTO, Martti. (2022). Cyber-Attacks Against Critical Infrastructure. *In* M. Lehto, & P. Neittaanmäki (Eds.), Cyber Security: Critical Infrastructure Protection (p. 3-42). **Springer. Computational Methods in Applied Sciences**, 56. Disponível em: https://jyx.jyu.fi/bitstreams/70a33955-e655-40de-833c-335b699854f2/download . Acesso em: 2 fev. 2026.

MAXWELL, AL AFB. **Three Levels of War**. Air and Space Power Mentoring Guide, v. 1. USAF College of Aerospace Doctrine, Research and Education (CADRE). Air University Press, 1997.

POONGODI, R. K; AROKIYA, Raj. J.; AYATHULLA, N.; BARANITHARAN, V. The AI Paradox: Strengthening Defenses While Empowering Attackers. **International Journal of Scientific Development and Research**, v. 10, n. 2, p. 394-401, 2025. Disponível em: https://ijsdr.org/papers/IJSDR2502146.pdf . Acesso em: 13 abr. 2026.

RAZA, Salvador. Brasil na Contramão da Tecnologia. **Interesse Nacional**, São Paulo, v. 6, n. 23, p. 7-17, out./dez. 2013.