ESCOLA DE GUERRA NAVAL

CC RAFAEL BRIÃO

O PLANEJAMENTO DA GUERRA CIBERNÉTICA:
Riscos e oportunidades da computação quântica

Rio de Janeiro

2025

CC RAFAEL BRIÃO

O PLANEJAMENTO DA GUERRA CIBERNÉTICA:
Riscos e oportunidades da computação quântica

Dissertação apresentada à Escola de Guerra Naval como requisito parcial para a conclusão do Curso de Estado-Maior para Oficiais Superiores.

Orientador: CF (FN) Alexandre Quintanilha Sanctos

Rio de Janeiro
Escola de Guerra Naval
2025

DECLARAÇÃO DA NÃO EXISTÊNCIA DE APROPRIAÇÃO INTELECTUAL IRREGULAR

Declaro que este trabalho acadêmico: a) corresponde ao resultado de investigação por mim desenvolvida, enquanto discente da Escola de Guerra Naval (EGN); b) é um trabalho original, ou seja, que não foi por mim anteriormente utilizado para fins acadêmicos ou quaisquer outros; c) é inédito, isto é, não foi ainda objeto de publicação; e d) é de minha integral e exclusiva autoria.

Declaro também que tenho ciência de que a utilização de ideias ou palavras de autoria de outrem, sem a devida identificação da fonte, e o uso de recursos de inteligência artificial no processo de escrita constituem grave falta ética, moral, legal e disciplinar. Ademais, assumo o compromisso de que este trabalho possa, a qualquer tempo, ser analisado para verificação de sua originalidade e ineditismo, por meio de ferramentas de detecção de similaridades ou por profissionais qualificados.

Os conceitos e ideias expressas neste trabalho acadêmico são de responsabilidade do Autor e não retratam qualquer orientação institucional da EGN ou da Marinha do Brasil.

Documento assinado digitalmente
gov.br
RAFAEL BRIAO
Data: 28/11/2025 12:24:30-0300
Verifique em https://validar.iti.gov.br

AGRADECIMENTOS

A Deus, por me conceder a saúde, a perseverança necessária para concluir mais esta etapa de minha vida profissional e acadêmica.

À minha esposa, Mônica, e à minha filha, Maria Tereza, pelo amor, compreensão e apoio incondicional ao longo de todo este processo. Aos meus pais, Lourival e Ana, por todos os ensinamentos, incentivos e valores transmitidos desde a infância, que serviram de base sólida para cada conquista ao longo da jornada.

Ao Capitão de Fragata (Fuzileiro Naval) Sanctos, meu orientador, pelas valiosas orientações, pela disponibilidade e pelo profissionalismo demonstrado durante todas as fases de elaboração deste trabalho.

À Escola de Guerra Naval, pelo ambiente de excelência acadêmica e pelo corpo docente comprometido com a formação dos Oficiais-Alunos. À Marinha do Brasil, instituição à qual sirvo com orgulho, pelo contínuo investimento na capacitação de seu pessoal e pela oportunidade de participar do Curso de Estado-Maior para Oficiais Superiores.

“Vivemos numa sociedade profundamente dependente da ciência e da tecnologia, em que quase ninguém sabe nada sobre ciência e tecnologia”.

Carl Sagan

RESUMO

A presente dissertação analisa o planejamento da guerra cibernética no contexto das doutrinas do Ministério da Defesa, com ênfase na integração do domínio cibernético aos níveis estratégico, operacional e tático do emprego militar. Parte-se da constatação de que a crescente digitalização das operações militares e a ampliação da superfície de ataque tornam indispensável a adoção de medidas robustas de defesa no domínio cibernético. Nesse cenário, examinam-se os fundamentos doutrinários que orientam o planejamento conjunto, as estruturas organizacionais e as atribuições específicas relacionadas ao ambiente cibernético, bem como a incorporação de capacidades de comando e controle e de inteligência em operações nesse domínio. O estudo avança para a análise da computação quântica como fator disruptivo, destacando seu potencial para comprometer os sistemas criptográficos vigentes e alterar a dinâmica da segurança da informação. A investigação adota abordagem qualitativa, fundamentada em documentos normativos e doutrinários, nacionais e internacionais, além de literatura técnico-científica. Conclui-se que, embora a doutrina militar brasileira reconheça o espaço cibernético como domínio estratégico, ainda é necessário ampliar o detalhamento sobre ameaças quânticas e acelerar a adoção de contramedidas, como a criptografia pós-quântica. Recomenda-se, portanto, a incorporação das ameaças quânticas às diretrizes de planejamento e a intensificação de exercícios conjuntos que contemplem cenários desse tipo, com o objetivo de reforçar a capacidade de resposta e aprimorar a resiliência das infraestruturas críticas de defesa.

Palavras-chave: Guerra Cibernética. Planejamento Militar. Doutrina Militar. Computação Quântica. Criptografia Pós-Quântica.

ABSTRACT

Cyber warfare planning: risks and opportunities of quantum computing

This dissertation analyzes cyber warfare planning within the context of the doctrines of the Brazilian Ministry of Defense, with emphasis on the integration of the cyber domain into the strategic, operational, and tactical levels of military employment. It starts from the observation that the increasing digitalization of military operations and the expansion of the attack surface make it essential to adopt robust defense measures in the cyber domain. In this context, it examines the doctrinal foundations guiding joint planning, the organizational structures, and the specific responsibilities related to the cyber environment, as well as the incorporation of command and control and intelligence capabilities into operations in this domain. The study advances to the analysis of quantum computing as a disruptive factor, highlighting its potential to compromise current cryptographic systems and alter the dynamics of information security. The research adopts a qualitative approach, based on national and international normative and doctrinal documents, as well as technical and scientific literature. The findings indicate that, although Brazilian military doctrine recognizes cyberspace as a strategic domain, there is still a need to expand the level of detail regarding quantum threats and to accelerate the adoption of countermeasures, such as post-quantum cryptography. It is therefore recommended to incorporate quantum threats into planning guidelines and to intensify joint exercises that address such scenarios, with the aim of strengthening response capabilities and enhancing the resilience of critical defense infrastructures.

Keywords: Cyber Warfare. Military Planning. Military Doctrine. Quantum Computing. Post-Quantum Cryptography.

LISTA DE ABREVIATURAS E SIGLAS

BIKE	-	Mecanismo Bit Flipping Key Encapsulation
CASNAV	-	Centro de Análise de Sistemas Navais
ComDCiber	-	Comando de Defesa Cibernética
ECDSA	-	Algoritmo de Assinatura Digital de Curva Elíptica
EMCFA	-	Estado-Maior Conjunto das Forças Armadas
HQC	-	Mecanismo Hamming Quasi-Cyclic
IC	-	Infraestruturas Críticas
MB	-	Marinha do Brasil
MD	-	Ministério da Defesa
NIST	-	National Institute of Standards and Technology
NOSDCiber	-	Normas Operacionais do Sistema Militar de Defesa Cibernética
PEECFA	-	Plano Estratégico de Emprego Conjunto das Forças Armadas
PKP	-	Mecanismo Public Key Protocol
PPC	-	Processo de Planejamento Conjunto
QKD	-	Distribuição Quântica de Chaves
RSA	-	Algoritmo Rivest-Shamir-Adleman
SCCN	-	Sistema Criptográfico para Comunicações Navais
SIDH	-	Supersingular Isogeny Diffie-Hellman
SisPECFA	-	Sistemática de Planejamento do Emprego Conjunto das Forças Armadas
SMDC	-	Sistema Militar de Defesa Cibernética
SPEM	-	Sistemática de Planejamento Estratégico-Militar

SUMÁRIO

1 INTRODUÇÃO

No cenário atual dos conflitos, a evolução tecnológica desempenha um importante papel na transformação das estratégias e dos domínios da guerra. Nas últimas décadas, o espaço cibernético[1] consolidou-se como um ambiente de confronto a ser explorado, ao lado dos domínios tradicionais (terrestre, marítimo, aéreo e espacial), obrigando os países a adaptar suas doutrinas e capacidades de defesa. Em paralelo, surge no horizonte a computação quântica[2], uma fronteira científica com potencial para alterar as bases da segurança da informação e, por consequência, as dinâmicas da guerra cibernética[3], promovendo tanto oportunidades quanto ameaças, especialmente no âmbito da defesa de Infraestruturas Críticas[4] (IC).

Incluída entre os novos domínios de conflito, a guerra cibernética caracteriza-se pelo uso ofensivo e defensivo de recursos computacionais e redes de informação para alcançar objetivos militares, com ações marcadas pela potencial assimetria de capacidades, dificuldade de atribuição de ataques e pela possibilidade de sua utilização desde o estado de paz. Na doutrina militar, esse tipo de ação exige uma abordagem multidisciplinar e atuação conjunta integrada para proteger as IC e, se necessário, explorar vulnerabilidades do adversário. Assim, a dimensão cibernética tornou-se parte integrante do planejamento de defesa, demandando estruturas organizacionais e conceitos específicos para seu tratamento.

Diante desse panorama, com a consolidação da guerra cibernética como componente essencial da defesa e do surgimento de uma tecnologia disruptiva para

---

1 O espaço cibernético consiste em um ambiente formado por dispositivos computacionais onde informações digitais são armazenadas, processadas e transmitidas (Brasil, 2015). Como será visto no capítulo dois, configura um domínio operacional que demanda estratégias específicas.

2 A computação quântica é um modelo de processamento de informações baseado em princípios da mecânica quântica que permite a realização de operações de forma exponencialmente mais rápida do que os sistemas clássicos. Como será visto no capítulo três, possui potencial disruptivo, o que impõe desafios inéditos ao planejamento da guerra cibernética (National Academies of Sciences, Engineering and Medicine, 2019).

3 A guerra cibernética refere-se ao emprego coordenado de ações ofensivas e defensivas sobre informações e sistemas digitais, com o objetivo de comprometer as capacidades de comando e controle do adversário em operações militares, envolvendo o uso de tecnologias da informação e comunicações para explorar, degradar ou destruir infraestruturas críticas inimigas, ao mesmo tempo em que se busca proteger os próprios sistemas (Brasil, 2015).

4 Infraestruturas críticas são instalações, serviços, bens ou sistemas cujo mau funcionamento, interrupção ou destruição pode causar efeitos severos sobre a segurança nacional, a estabilidade social, a economia, o ambiente político ou as relações internacionais (Brasil, 2015). No contexto da guerra cibernética, essas infraestruturas se tornam alvos estratégicos, pois sua vulnerabilidade digital pode comprometer a resiliência do Estado frente a ataques assimétricos.

a segurança digital, este trabalho busca investigar de que maneira a evolução da computação quântica atualmente se relaciona com o planejamento da guerra cibernética. Estaria a atual forma de planejamento da guerra cibernética preparada para a era da computação quântica? E de que modo essa nova tecnologia pode ser integrada ao planejamento da guerra cibernética? Em termos concretos, coloca-se a seguinte questão de pesquisa: até que ponto e de que forma a computação quântica pode ser incorporada ao planejamento da guerra cibernética? Por se tratar de uma pesquisa exploratória, não foram formuladas hipóteses iniciais.

Em consonância com as questões de pesquisa formuladas, definiu-se como objetivo geral deste trabalho avaliar a aderência da computação quântica ao planejamento da guerra cibernética, ou seja, examinar de que forma e em que grau as capacidades proporcionadas pela computação quântica podem integrar-se às ações cibernéticas, considerando tanto os riscos quanto as oportunidades envolvidas. Para alcançar esse objetivo geral, foram estabelecidos alguns objetivos específicos complementares: compreender o panorama atual da guerra cibernética na perspectiva da doutrina militar brasileira, analisando seus conceitos, documentos normativos e a estrutura do sistema de defesa cibernética; investigar os potenciais impactos disruptivos da computação quântica sobre as tecnologias de segurança da informação; analisar as implicações desses avanços tecnológicos para o planejamento da guerra cibernética, identificando desafios e possibilidades de emprego da computação quântica no âmbito militar; e, por fim, refletir sobre as adequações necessárias nas diretrizes de defesa cibernética para incorporar as transformações advindas da era quântica.

Metodologicamente, a pesquisa caracteriza-se como qualitativa e exploratória, baseada em análise documental. Foi adotado um delineamento que confronta a teoria com a realidade. Inicialmente, foi realizada uma revisão bibliográfica e documental cobrindo os dois eixos centrais do tema. De um lado, examinar-se-á a doutrina brasileira de guerra cibernética, abrangendo as publicações do Ministério da Defesa (MD) e estudos acadêmicos sobre o assunto, de forma a delinear o panorama conceitual e normativo vigente. De outro lado, investigar-se-á os fundamentos da computação quântica, bem como os avanços dessa tecnologia no âmbito da segurança da informação, conforme retratados na literatura científica, buscando compreender as capacidades projetadas dessa tecnologia e seus possíveis efeitos. Não se trata, portanto, de uma pesquisa empírica, mas sim de

uma reflexão teórico-analítica fundamentada em fontes documentais e bibliográficas. Dessa forma, a metodologia adotada permite articular os conceitos e evidências disponíveis, identificando possíveis caminhos para a integração dessa nova tecnologia ao planejamento da guerra cibernética.

A aplicação da metodologia qualitativa seguiu um processo de análise documental estruturado em etapas. Inicialmente, foram identificados e selecionados os documentos doutrinários oficiais do Ministério da Defesa e da Marinha do Brasil que tratam do tema da guerra cibernética, observando-se critérios de relevância, atualidade e aplicabilidade. Em seguida, esses documentos foram examinados à luz dos referenciais teóricos sobre computação quântica e segurança da informação, permitindo estabelecer um confronto entre as orientações normativas e os avanços tecnológicos projetados. Essa comparação foi conduzida com o objetivo de observar aderência, identificar convergências, lacunas e potenciais impactos sobre o planejamento da guerra cibernética.

Esta dissertação está estruturada em cinco capítulos, sendo o capítulo um correspondente a esta Introdução. No capítulo dois, apresenta-se o contexto e os fundamentos do planejamento da guerra cibernética segundo a doutrina militar brasileira. São explorados conceitos relativos ao tema e revisados os seus principais documentos normativos. O capítulo três dedica-se à computação quântica e suas implicações para a segurança da informação. Nesse capítulo, expõem-se os princípios básicos da tecnologia de computação quântica e discutem-se os impactos potenciais sobre as tecnologias de segurança vigentes, com destaque para as vulnerabilidades das tecnologias de segurança atuais e as novas possibilidades propiciadas pela computação quântica. Em seguida, o capítulo quatro realiza a análise integradora proposta: examina-se a aderência da computação quântica ao planejamento da guerra cibernética, avaliando de que maneira as capacidades quânticas poderiam ser incorporadas às ações cibernéticas das Forças Armadas. Esse capítulo confronta as perspectivas tecnológicas com as diretrizes doutrinárias vigentes, identificando possibilidades de emprego da tecnologia no âmbito militar. Por fim, no capítulo cinco, são apresentadas as considerações finais da pesquisa, com a síntese dos resultados obtidos e sugestões de desdobramentos futuros, visando contribuir para o aperfeiçoamento do planejamento da guerra cibernética diante dos desafios e oportunidades da era da computação quântica.

2 O PLANEJAMENTO DA GUERRA CIBERNÉTICA

O presente capítulo busca analisar como o planejamento da guerra cibernética é contemplado nas publicações do âmbito do MD. A abordagem adotada fundamenta-se na identificação das estruturas, normas e processos que orientam a integração do espaço cibernético ao planejamento militar, destacando suas particularidades. Esse exame fornecerá as bases para a compreensão dos desafios associados às ameaças cibernéticas, conectando o referencial doutrinário ao cenário tecnológico em constante evolução.

2.1 FUNDAMENTOS DOUTRINÁRIOS DO PLANEJAMENTO MILITAR

O planejamento, em sua acepção mais ampla, pode ser compreendido como uma atividade contínua e sistemática voltada à idealização e organização de ações coordenadas, com distintos níveis de detalhamento, destinadas à solução de problemas e ao alcance de objetivos previamente estabelecidos, definindo responsabilidades, prazos, métodos e finalidades, sendo conduzido de modo racional e orientado por critérios técnicos e decisórios. Já em um contexto mais específico, o planejamento militar diz respeito à concepção de emprego do Poder Militar por parte das Forças Armadas, ou de uma de suas frações, com vistas à consecução dos Objetivos Nacionais. Essa abordagem abrange tanto a dimensão estratégica do emprego conjunto quanto a sistematização dos processos decisórios aplicáveis à resolução de problemas de natureza militar (Brasil, 2015, 2020a).

Na perspectiva doutrinária, o planejamento é subdividido em três níveis interdependentes: estratégico, operacional e tático. O nível estratégico corresponde à formulação de diretrizes amplas e políticas de defesa, no âmbito do MD, com fundamento em documentos como a Estratégia Nacional de Defesa. O nível operacional refere-se à elaboração de planos e à condução de operações em teatros de operações[5] específicos. Já o nível tático concentra-se na execução das ações

5 Teatros de operações são áreas geográficas delimitadas onde se desenvolvem operações militares, sob responsabilidade de um comando operacional, com vistas ao cumprimento de missões estabelecidas (Brasil, 2015).

militares pelas Forças Componentes[6], mediante ordens e planos voltados à concretização das missões atribuídas pelo nível operacional (Brasil, 2020a).

O planejamento do emprego das Forças Armadas é conduzido segundo uma lógica escalonada em níveis, de modo a assegurar a articulação coerente entre as orientações políticas e a execução das ações militares. No nível estratégico, aplica-se a Sistemática de Planejamento Estratégico-Militar (SPEM), a qual se desenvolve em três fases sucessivas: concepção estratégica e configuração de forças; planejamento e preparo; e planejamento do emprego operacional. Esta última fase é desdobrada por meio da Sistemática de Planejamento de Emprego Conjunto das Forças Armadas (SisPECFA). Já no nível operacional, os planejamentos são realizados por intermédio do Processo de Planejamento Conjunto (PPC), conduzido pelos Comandos Operacionais ativados, com base nas diretrizes e nos documentos elaborados no nível estratégico. Cabe a esses comandos articular as forças disponíveis, visando ao alcance dos estados finais estabelecidos para a operação conjunta (Brasil, 2020a).

Dessa forma, observa-se que o planejamento no contexto militar configura-se como uma prática estruturada e hierarquizada, cujo propósito é garantir a integração coerente entre os diferentes níveis de decisão e execução. O encadeamento dessa atividade permite que diretrizes estabelecidas em instâncias superiores sejam desdobradas em ações concretas por meio de metodologias específicas, ajustadas às exigências de cada nível. No âmbito estratégico, a racionalidade do processo reside na capacidade de transformar orientações políticas e diretrizes de defesa nacional em planos de emprego do poder militar de maneira eficiente. Já no nível operacional, a ênfase recai sobre a coordenação entre meios e modos de atuação, assegurando que as ações sejam conduzidas em consonância com os objetivos delineados estrategicamente. Essa lógica sequencial e articulada reforça a importância da sistematização doutrinária como instrumento de coerência e efetividade na aplicação do Poder Militar.

A seguir, o foco recai sobre a maneira como o componente cibernético é incorporado ao processo de planejamento militar, delineando suas especificidades e implicações para o emprego conjunto das Forças Armadas.

---

6 Forças Componentes são os agrupamentos de meios e efetivos, organizados sob um comando específico, com a finalidade de cumprir missões táticas (Brasil, 2015).

2.2 A INSERÇÃO DO COMPONENTE CIBERNÉTICO NO PLANEJAMENTO

O espaço cibernético foi progressivamente incorporado ao planejamento de defesa em razão de sua identificação como setor estratégico nacional, o que impulsionou sua integração aos esforços de capacitação, interoperabilidade e mobilização do poder militar, com a formulação de capacidades específicas para atuação nesse ambiente, abrangendo aspectos organizacionais, doutrinários e decisórios (Brasil, 2020b, 2020c).

A Doutrina Militar de Defesa Cibernética estabelece os fundamentos que orientam a atuação no setor cibernético no âmbito da Defesa Nacional, em razão da crescente importância do espaço cibernético como ambiente operacional. Essa doutrina delimita o planejamento das ações de Defesa Cibernética com base em fundamentos próprios, em consonância com os demais documentos normativos do MD (Brasil, 2023).

Do ponto de vista metodológico, o planejamento cibernético demanda uma abordagem preditiva e resiliente, na qual a antecipação de cenários adversos e a mitigação de vulnerabilidades, por meio de protocolos técnicos e de planos estruturados, são compatíveis com a volatilidade e a velocidade das ameaças digitais. O reconhecimento do espaço cibernético como ambiente de operações e a formulação de diretrizes específicas permitiram que o planejamento passasse a ser orientado por princípios voltados ao exercício do comando e controle, à proteção dos ativos informacionais e à negação desses recursos ao adversário, no contexto das operações conjuntas (Brasil, 2023).

As ações cibernéticas são organizadas conforme os níveis da estrutura de planejamento militar: no nível estratégico, concentram-se as diretrizes e mecanismos de coordenação conduzidos pelo Comando de Defesa Cibernética (ComDCiber)[7] em articulação com o Estado-Maior Conjunto; no nível operacional, são planejadas e controladas as ações de defesa, exploração e ataque; no nível tático, executam-se ações específicas, alinhadas aos objetivos superiores (Brasil, 2023).

---

7 O Comando de Defesa Cibernética (ComDCiber) é a organização militar de nível estratégico responsável por planejar, orientar, coordenar e controlar as operações de defesa cibernética no âmbito das Forças Armadas. Atua como órgão central do Sistema Militar de Defesa Cibernética (SMDC), podendo, quando previsto no planejamento de operações conjuntas, ser designado como Força Componente de Guerra Cibernética, subordinando-se ao Comando Operacional do Teatro de Operações ou Área de Operações (Brasil, 2020).

Ao ComDCiber cabe coordenar ações ofensivas e defensivas, propor normas e doutrina, e participar da elaboração das Normas Operacionais do Sistema Militar de Defesa Cibernética (NOSDCiber), que regulamentam as ações cibernéticas no âmbito militar. O componente cibernético é incorporado às operações conjuntas por meio de documentos elaborados pela Seção de Guerra Cibernética dos comandos ativados e por destacamentos especializados, em conformidade com os parâmetros das NOSDCiber. A elaboração desses documentos requer a compatibilização entre os meios disponíveis, os objetivos definidos e a natureza das ameaças, de modo a viabilizar respostas coordenadas e alinhadas ao emprego conjunto (Brasil, 2023).

Pesquisas recentes indicam que a consolidação do componente cibernético nas estruturas de defesa pressupõe reconfigurações institucionais e adaptações estratégicas que desafiam paradigmas tradicionais. Em determinados contextos, o domínio cibernético pode adquirir primazia operacional em relação aos demais, sobretudo em cenários assimétricos e de guerra híbrida, nos quais sua capacidade de produzir efeitos estratégicos independe do emprego direto de força convencional (Fakhouri, 2022; Cavadas, 2022). Essa centralidade crescente reforça a necessidade de incorporar seu preparo e emprego de forma abrangente aos processos de planejamento e condução das operações.

Nesse sentido, a salvaguarda das infraestruturas críticas de interesse da Defesa[8] deve ser tratada como um elemento estruturante desse esforço, contemplada desde períodos de normalidade. Essa proteção demanda ações coordenadas de planejamento, exploração e resposta, apoiadas na identificação de vulnerabilidades e na integração de diversas fontes de inteligência, assegurando que esses ativos mantenham sua resiliência e capacidade de sustentar as operações conjuntas diante das ameaças cibernéticas (Brasil, 2023).

A inserção do espaço cibernético no planejamento de defesa, respaldada por doutrinas e publicações, evidencia que esse domínio passou de elemento complementar a componente estratégico. A organização de suas ações segundo os níveis de planejamento militar e a centralidade do ComDCiber na coordenação, normatização e integração às operações conjuntas refletem um amadurecimento institucional que busca compatibilizar meios, objetivos e ameaças em um ambiente caracterizado pela volatilidade e pela necessidade de resposta imediata.

8 Infraestruturas críticas de interesse da Defesa são aquelas instalações, serviços, bens ou sistemas cuja interrupção, degradação ou destruição possa comprometer de forma significativa a capacidade operacional das Forças Armadas e a segurança nacional (Brasil, 2015, 2023).

Esse avanço, contudo, implica repensar estruturas e estratégias, sobretudo diante de cenários assimétricos e de guerra híbrida, nos quais o componente cibernético pode alcançar primazia operacional. Nesse contexto, a proteção de infraestruturas críticas de interesse da Defesa deixa de ser uma medida reativa para se tornar pilar preventivo do planejamento, sustentada por ações coordenadas e integradas de inteligência. Tal abordagem reforça a coerência do emprego conjunto e amplia a resiliência das operações frente às ameaças digitais emergentes.

Assim, a efetividade do planejamento da guerra cibernética requer não apenas a articulação harmoniosa entre diretrizes e execução, mas também a implementação de medidas capazes de resguardar a integridade e a disponibilidade das informações estratégicas. A proteção desses ativos informacionais, por meio de soluções técnicas e procedimentos específicos, torna-se importante elemento para sustentar a vantagem operacional no espaço cibernético. Com base nessa premissa, o próximo subcapítulo examinará os mecanismos de proteção e integração cibernética no planejamento militar.

2.3 PROTEÇÃO E INTEGRAÇÃO NO PLANEJAMENTO CIBERNÉTICO

No contexto da estrutura de planejamento militar, o espaço cibernético consolidou-se como um domínio operacional que deve estar plenamente alinhado às diretrizes superiores e integrado aos demais componentes da força. Essa integração demanda a adaptação de procedimentos, a definição clara de responsabilidades e a organização dos fluxos de comando, de forma que as ações cibernéticas, em qualquer nível, contribuam efetivamente para o alcance dos objetivos estabelecidos na condução das operações conjuntas (Brasil, 2023).

Para que esse alinhamento se concretize, o exercício do comando e controle no setor cibernético requer estruturas especializadas, aptas a conduzir, coordenar e integrar ações ofensivas, defensivas e de exploração. Nesse papel, o ComDCiber é responsável pela elaboração das NOSDCiber, compatíveis com a natureza dinâmica e transnacional das ameaças digitais, regulamentando o planejamento, a coordenação e o emprego dos meios disponíveis. Tais normas contemplam a uniformidade de atuação entre as Forças e comandos, permitindo que, mesmo em ambientes complexos e de rápida evolução, as operações mantenham

interoperabilidade e coerência, alinhadas aos objetivos estratégicos definidos (Brasil, 2023).

A manutenção dessa coerência depende, em grande medida, da proteção do fluxo de informações entre os diferentes níveis de comando. Garantir que esse fluxo permaneça seguro, contínuo e imune a interferências externas é condição essencial para preservar a capacidade decisória e coordenar o emprego das forças. Por isso, a preservação da integridade, autenticidade e disponibilidade das comunicações deve ser considerada desde as fases iniciais do planejamento (Brasil, 2020a).

Contudo, a eficácia das ações de defesa cibernética não se limita à execução das operações. Ela depende também da constante atualização das normas e dos procedimentos, de forma a acompanhar a evolução tecnológica e as mudanças no perfil das ameaças. A dinâmica do ambiente cibernético impõe ajustes frequentes na doutrina e na capacitação dos meios, sob pena de surgirem lacunas que comprometam a capacidade de resposta e a integração com os demais componentes do esforço conjunto (Brasil, 2023).

Nesse sentido, a proteção dos ativos informacionais de interesse da Defesa demanda a adoção de medidas técnicas e organizacionais que assegurem a confidencialidade, a integridade e a disponibilidade das informações críticas. Tais medidas devem estar previstas desde períodos de normalidade e incluir ações de monitoramento, identificação de vulnerabilidades e implementação de salvaguardas compatíveis com a sensibilidade dos dados e com as exigências das operações conjuntas (Brasil, 2023).

A padronização e a integração das soluções de segurança da informação constituem, assim, requisitos estratégicos para ampliar a interoperabilidade entre os sistemas das Forças Armadas. A harmonização de procedimentos e tecnologias facilita a troca segura de informações e reduz a exposição a vulnerabilidades, criando um arcabouço coerente para a aplicação de mecanismos de proteção especializados (Brasil, 2023).

Entre esses mecanismos, a criptografia ocupa lugar de destaque, pois oferece meios técnicos para resguardar informações sensíveis contra acesso não autorizado, manipulação ou interceptação. Sua aplicação, integrada a outras medidas de segurança, reforça a capacidade de comando e controle e a proteção dos fluxos informacionais estratégicos no âmbito das operações conjuntas (Brasil, 2023).

Dessa forma, a segurança da informação, ao integrar procedimentos, sistemas e tecnologias voltados à proteção dos dados estratégicos e operacionais, assume papel estruturante no planejamento cibernético. A salvaguarda desse patrimônio informacional requer a adoção de medidas que impeçam acessos indevidos, mitiguem vulnerabilidades e garantam a confiabilidade das comunicações, especialmente em cenários de alta contestação, nos quais o domínio cibernético é explorado de forma ofensiva por atores hostis (Brasil, 2023). Nesse quadro, a capacidade de sustentar a disponibilidade e a veracidade dos dados mesmo sob ataque revela-se condição indispensável ao exercício do comando e controle. Ao reconhecer a centralidade de mecanismos estruturados de proteção e padronização, evidencia-se que a criptografia não é apenas uma ferramenta técnica, mas um elemento basilar do planejamento da guerra cibernética, premissa que orientará a análise do próximo subcapítulo.

2.4 A CRIPTOGRAFIA NO PLANEJAMENTO DA GUERRA CIBERNÉTICA

A proteção da informação constitui um dos pilares do planejamento da guerra cibernética, e a criptografia representa, nesse contexto, um recurso técnico essencial para garantir a confidencialidade, a integridade e a autenticidade dos dados estratégicos. Essa função é reconhecida pelas Forças Armadas como um componente indispensável à preservação dos ativos informacionais e à eficácia do comando e controle nas operações conjuntas. Os ativos informacionais devem ser considerados recursos estratégicos, cuja proteção deve estar prevista desde a fase de planejamento, com emprego de medidas técnicas de segurança, entre as quais se inclui a criptografia, como meio de garantir o sigilo das comunicações e o acesso autorizado aos dados (Brasil, 2023).

A criptografia historicamente desempenha um papel relevante no contexto militar, permitindo comunicações sigilosas desde épocas remotas e ao longo dos grandes conflitos mundiais. O emprego de cifras assegurou que informações estratégicas permanecessem confidenciais, muitas vezes influenciando os rumos dos conflitos (Khan, 2024). Essa importância se amplificou no cenário contemporâneo, com as Forças Armadas utilizando algoritmos criptográficos como o

Advanced Encryption Standard (AES)[9] e o Rivest-Shamir-Adleman (RSA)[10], entre outros, para resguardar dados sensíveis em redes de comando e controle e em sistemas de armas, garantindo que ordens e informações vitais não sejam interceptadas ou alteradas por adversários, provendo confidencialidade e integridade às informações (Criptografia, 2024). A criptografia moderna, portanto, está inserida nas estruturas militares, das comunicações táticas às estratégicas, provendo confidencialidade, autenticidade e integridade das informações. Reconhecendo essa relevância, a doutrina de defesa cibernética brasileira prevê a definição de padrões interoperáveis de criptografia no âmbito da Defesa, complementando os das Forças Singulares, de modo a unificar e fortalecer a proteção das comunicações militares sigilosas (Brasil, 2012).

No nível estratégico, a proteção criptográfica é tratada como parte da capacidade cibernética projetada nas diretrizes de planejamento emitidas pelo Estado-Maior Conjunto das Forças Armadas (EMCFA). Os documentos de planejamento estratégico, como o Plano Estratégico de Emprego Conjunto das Forças Armadas (PEECFA), orientam a previsão de medidas de proteção e negação de informações, compatíveis com os princípios da guerra cibernética e da segurança da informação. A criptografia, nesse contexto, é aplicada à preservação da confidencialidade dos dados estratégicos, à proteção das comunicações entre os escalões decisórios e à salvaguarda de sistemas de comando e controle (Brasil, 2023). Essa previsão é feita de modo transversal, integrando os recursos criptográficos ao sistema de defesa como um todo, por meio da interoperabilidade dos protocolos de segurança, do controle de acesso lógico e da autenticação de usuários em ambientes digitais sensíveis.

No nível operacional, o uso da criptografia está diretamente associado à integridade dos fluxos de dados que sustentam o comando e controle e a coordenação das forças. A Doutrina de Defesa Cibernética destaca que, no planejamento das operações conjuntas, os documentos elaborados pelas Seções de

9 O AES é um algoritmo de criptografia simétrica amplamente adotado para proteger informações sensíveis em ambientes civis e militares. Baseia-se na utilização da mesma chave para cifrar e decifrar dados e é empregado na proteção de comunicações e na salvaguarda de dados de comando e controle (NIST, 2001).

10 O algoritmo RSA é um sistema de criptografia assimétrica que utiliza um par de chaves matematicamente relacionadas, uma pública e uma privada, para cifrar e decifrar dados ou assinar digitalmente informações. Sua segurança está baseada na dificuldade de fatoração de grandes números primos. É amplamente empregado na troca de chaves e na autenticação em sistemas militares e governamentais (Rivest; Shamir; Adleman, 1978).

Guerra Cibernética devem prever a adoção de medidas técnicas de proteção da informação. Entre essas medidas, inclui-se a criptografia para a transmissão de dados e para seu armazenamento, a utilização de protocolos seguros de comunicação e a adoção de padrões interoperáveis entre os diversos sistemas empregados pelas Forças Singulares (Brasil, 2023). Esses mecanismos permitem a continuidade das operações mesmo sob ataques cibernéticos, assegurando que as ordens, os dados táticos e os sistemas de monitoramento não sejam interceptados, adulterados ou inutilizados pelo adversário.

No nível tático, a criptografia é empregada como medida de proteção ativa durante a execução das operações cibernéticas, sendo essencial para garantir a segurança das comunicações entre os elementos de combate e para evitar que informações críticas sejam comprometidas em situações de confronto direto ou de exploração adversária. Os Planos Táticos de Guerra Cibernética, elaborados pelas Forças Componentes, devem prever a utilização de algoritmos criptográficos robustos e atualizados, a definição de políticas de chaves criptográficas e a integração desses mecanismos aos sistemas de comando e controle em tempo real (Brasil, 2023).

Além disso, as NOSDCiber definem critérios técnicos e procedimentos de interoperabilidade que asseguram a padronização dos mecanismos criptográficos entre os diversos entes envolvidos, ampliando a resiliência do sistema diante tentativas de interceptação, sabotagem ou negação de serviço (Brasil, 2023).

As diretrizes da Marinha do Brasil (MB) no campo da tecnologia da informação contemplam a atividade de criptoanálise[11] como parte integrante das ações de segurança da informação no contexto institucional. Essa atuação divide-se em dois campos principais: a criptoanálise certificacional, que envolve a verificação da robustez das cifras utilizadas, além de serviços de certificação e homologação dos sistemas criptográficos; e a criptoanálise operacional, voltada para tarefas de inteligência, como a interceptação e a decifração de mensagens criptografadas. Tal

11 A criptoanálise é o conjunto de métodos e técnicas voltados à quebra ou enfraquecimento de sistemas criptográficos, visando obter informações protegidas sem o conhecimento ou a posse legítima das chaves. Envolve desde abordagens matemáticas e estatísticas até ataques por força bruta ou exploração de vulnerabilidades na implementação dos algoritmos. É uma capacidade estratégica tanto para operações ofensivas, ao permitir a interceptação e decifração de comunicações inimigas, quanto para a proteção, ao orientar a evolução e o fortalecimento dos próprios sistemas de proteção (Stallings, 2017).

estrutura reflete uma orientação doutrinária voltada à constante avaliação da eficácia dos recursos criptográficos empregados nos sistemas da Força (Abi-Abib, 2020).

No ambiente militar, a segurança da informação é estruturada por meio de um conjunto de medidas técnicas destinadas a assegurar a confidencialidade, integridade e disponibilidade de dados e sistemas críticos. Entre essas medidas, a criptografia é reconhecida como um mecanismo essencial, aplicada em conjunto com controles de acesso, autenticação e estratégias de redundância (Cristo Junior, 2020). No contexto da guerra cibernética, essas camadas de proteção contribuem para preservar a resiliência dos ativos informacionais frente a ameaças digitais e garantir a continuidade das operações em ambiente hostil.

A centralidade da criptografia no planejamento cibernético das Forças Armadas se justifica não apenas por seu papel técnico de proteção de dados, mas por sua natureza estratégica, atuando como elemento estruturante da segurança da informação em todos os níveis de planejamento. A atuação eficaz em ambientes hostis exige a garantia de confidencialidade, integridade e autenticidade das comunicações e dos sistemas críticos, o que torna a criptografia um recurso valioso à conquista da superioridade informacional. Ao integrar soluções criptográficas robustas desde as fases iniciais do planejamento, as instituições militares ampliam sua capacidade de dissuasão, mitigam riscos de exploração de vulnerabilidades e asseguram a continuidade operacional em cenários de conflito digital com elevado grau de complexidade e volatilidade.

A análise das diretrizes normativas, das práticas institucionais e das orientações doutrinárias evidencia que a criptografia não é um recurso acessório, mas sim uma condição para a viabilidade do planejamento da guerra cibernética no âmbito das Forças Armadas. Ao permitir a proteção de comunicações sensíveis, a defesa dos sistemas de comando e controle e a integridade dos dados estratégicos, os mecanismos criptográficos asseguram as condições mínimas para que as operações militares sejam conduzidas com segurança e eficácia. Essa constatação reforça a necessidade de se manter a criptografia como eixo estruturante das capacidades cibernéticas, articulando-a de forma coerente com os processos decisórios e com as fases de execução nos níveis estratégico, operacional e tático. A seguir, serão examinados os principais desafios que esse planejamento enfrenta, à luz das transformações tecnológicas e institucionais do ambiente digital contemporâneo.

2.5 CARACTERÍSTICAS E DESAFIOS DA GUERRA CIBERNÉTICA

A Guerra Cibernética é caracterizada pelo emprego coordenado com outras capacidades no âmbito das operações de informação, incluindo inteligência, guerra eletrônica e operações psicológicas. Ela pode ser conduzida de forma integrada em diferentes níveis de planejamento, abrangendo ações de proteção, exploração e ataque. Quando articulada a outros domínios operacionais, a guerra cibernética amplia o leque de possibilidades estratégicas disponíveis ao comandante. Essa integração permite a geração de efeitos combinados que potencializam os resultados desejados e oferecem maior adaptabilidade frente à natureza assimétrica dos conflitos contemporâneos (Brasil, 2023; MB, 2021).

Ainda, ela apresenta características assimétricas marcantes, como a possibilidade de atores estatais ou não estatais com recursos limitados provocarem efeitos significativos sobre potências estatais estabelecidas, desde que disponham de conhecimento técnico e acesso a vulnerabilidades de sistemas (Clarke e Knake, 2011). Essa assimetria operacional reforça a necessidade de abordagens doutrinárias e estruturais que incorporem flexibilidade e resposta distribuída. Ao mesmo tempo, a execução de ações exploratórias ofensivas somente pode ser conduzida com base em regras de engajamento previamente definidas e mediante autorização superior, garantindo o controle institucional do uso da força no domínio cibernético, com limites operacionais para a execução autônoma de ofensivas digitais em tempo real (Brasil, 2020a).

Nesse contexto, simulações e treinamentos em larga escala são fundamentais. Tais exercícios valorizam a sistematização das lições aprendidas, incentivam a integração entre agências e promovem a colaboração em diversos níveis decisórios. Em cenários de crise cibernética simulada, esses exercícios fortalecem a coordenação entre as Forças Armadas, o setor público, o setor privado e a academia, funcionando como instrumentos de evolução de processos e protocolos (ComDCiber, 2024; CyberTech, 2022).

Apesar dos avanços normativos e institucionais, o Brasil ainda carece de uma governança cibernética voltada especificamente à proteção das infraestruturas críticas marítimas, especialmente no contexto de uma estratégia marítima de segurança cibernética. Em contraste, o Reino Unido já implementa códigos de boas

práticas para navios e portos, diretrizes para resiliência digital e instrumentos de certificação de segurança, consolidando uma abordagem integrada e multissetorial. Oliveira (2022) defende a criação de uma Estratégia de Segurança Marítima Cibernética com diretrizes claras para a proteção digital de portos, navios e instalações logísticas. O autor também propõe a adoção de medidas como códigos de boas práticas, sistemas de avaliação de resiliência e regulamentos específicos, que contribuiriam para o fortalecimento da doutrina cibernética aplicada ao ambiente marítimo.

Paralelamente, a crescente sofisticação dos ataques cibernéticos, conforme discutido por Fakhouri (2022), evidencia que a guerra cibernética não deve ser compreendida apenas como um vetor técnico, mas também como um componente estrategicamente versátil. Suas aplicações ultrapassam o escopo tradicional da segurança da informação e passam a integrar operações de influência e atividades táticas de reconhecimento. Articulada a tecnologias emergentes, como a inteligência artificial, a guerra cibernética amplia sua capacidade de produzir efeitos combinados. Ela pode inclusive operar de forma autônoma na identificação de alvos ou na execução de tarefas de neutralização de ameaças, alcançando desempenho superior ao de um humano em certos contextos operacionais (Fakhouri, 2022).

No contexto nacional, o planejamento da guerra cibernética nas doutrinas do MD e da MB já revela avanços normativos e estruturais importantes. Entretanto, persistem desafios que demandam contínua adaptação e atualização frente às transformações do ambiente digital. Entre esses desafios, destacam-se a dificuldade de sincronização entre ações cibernéticas e operações cinéticas; a complexidade de ameaças assimétricas e de difícil atribuição; a necessidade de integração com estruturas civis e interagências; bem como a ausência de uma governança cibernética consolidada para a proteção das infraestruturas críticas marítimas (MB, 2021; Oliveira, 2022).

Em resposta a esses desafios, observa-se que o planejamento da Guerra Cibernética nas Forças Armadas vem evoluindo tanto no âmbito normativo quanto no institucional, evidenciado pela produção de documentos doutrinários e pela realização de exercícios interagências voltados à proteção do espaço cibernético nacional. No entanto, esse processo ainda enfrenta entraves, exigindo maior amadurecimento técnico, doutrinário e organizacional para o pleno desenvolvimento da capacidade de planejamento no setor. Ademais, a articulação estratégica

pressupõe não apenas a elaboração de normativas e a condução de exercícios, mas também a consolidação de competências, o fortalecimento da doutrina e o avanço da interoperabilidade entre os diferentes atores envolvidos. Esses elementos são importantes para assegurar respostas coordenadas e eficazes diante dos desafios emergentes do ambiente digital contemporâneo.

Com o surgimento constante de novas ameaças e demandas operacionais no cenário cibernético global, existe espaço para a expansão conceitual, a integração tecnológica e o refinamento normativo. Observa-se também um esforço contínuo de aproximação entre a Defesa, agências governamentais, órgãos reguladores civis e a iniciativa privada. Esse engajamento conjunto ocorre especialmente por meio de simulações que testam processos decisórios compartilhados e promovem uma cultura de cooperação no enfrentamento de ameaças cibernéticas.

2.6 CONCLUSÕES PARCIAIS

A análise desenvolvida ao longo deste capítulo evidenciou que o planejamento da guerra cibernética, conforme delineado nas publicações do MD, consolidou-se como um processo estruturado em múltiplos níveis de decisão e execução, agora enriquecido pelo componente cibernético. Observou-se que a lógica escalonada de planejamento militar, abrangendo os níveis estratégico, operacional e tático, permanece como alicerce para articular diretrizes amplas à condução efetiva de operações. Nesse contexto, o espaço cibernético foi progressivamente integrado a essa estrutura, deixando de ser um elemento meramente complementar para se tornar um domínio operacional estratégico.

Documentos doutrinários, a exemplo da Doutrina Militar de Defesa Cibernética, formalizaram princípios e fundamentos específicos para a atuação no ambiente digital, enquanto órgãos especializados como o ComDCiber assumiram papel central na coordenação de ações ofensivas, defensivas e de exploração no espaço cibernético. Essa integração doutrinária e institucional assegura que as operações cibernéticas, em qualquer nível, estejam alinhadas aos objetivos definidos para as operações conjuntas, ao mesmo tempo em que padroniza normas e procedimentos entre as Forças Singulares, condição para manter a interoperabilidade e a coerência do esforço militar em um ambiente dinâmico.

Outra constatação fundamental foi a ênfase na proteção da informação como pilar do planejamento cibernético. Diante da volatilidade e da velocidade das ameaças digitais, o capítulo destacou que a garantia da segurança dos fluxos de informação entre os diferentes escalões de comando é tão crítica quanto o movimento cinético. Medidas de segurança da informação foram incorporadas desde as fases iniciais do planejamento, abrangendo controles de acesso, autenticação robusta e, notadamente, a criptografia como recurso técnico indispensável.

Conforme discutido, a criptografia provê confidencialidade, integridade e autenticidade aos dados estratégicos e comunicações militares, sustentando a eficácia do comando e controle mesmo sob ameaça adversária. Seu emprego abrange todos os níveis: no estratégico, protege comunicações de alto nível e dados sigilosos previstos em documentos e diretrizes; no operacional, resguarda os fluxos de informação que coordenam as forças em combate; e no tático, assegura sigilo e confiabilidade nas comunicações entre unidades.

Historicamente crucial em conflitos passados, a criptografia moderna, com algoritmos como AES e RSA, permanece no centro da resiliência cibernética militar, e a doutrina brasileira prevê a adoção de padrões interoperáveis de criptografia em toda a Defesa. Inclusive, sublinhou-se que as Forças Armadas incorporam práticas de criptoanálise tanto para verificar a robustez de seus próprios sistemas (certificação e homologação) quanto para fins de inteligência, ampliando sua capacidade de dissuadir, detectar e eventualmente decifrar comunicações adversárias (Abi-Abib, 2020; Cristo Junior, 2020). Esse conjunto de medidas técnicas e organizacionais reforça a disponibilidade, integridade e confidencialidade dos ativos informacionais, elementos sem os quais não se concebe a condução segura de operações no espaço cibernético.

O capítulo também permitiu consolidar características e desafios que singularizam a guerra cibernética no contexto contemporâneo. Diferentemente dos domínios tradicionais, o espaço cibernético confere assimetria ao confronto: atores com recursos limitados podem infligir danos significativos a potências estabelecidas, explorando vulnerabilidades tecnológicas (Clarke e Knake, 2011). Tal realidade impõe uma postura doutrinária flexível e descentralizada, apta a enfrentar ameaças difusas e de difícil atribuição.

Por outro lado, ficou claro que a atuação cibernética eficaz não se dá de forma isolada, ela é integrada a outras capacidades no âmbito das chamadas

operações de informação. Inteligência, guerra eletrônica e operações psicológicas compõem, junto com a guerra cibernética, um leque de ferramentas que podem ser orquestradas para efeitos estratégicos combinados (Brasil, 2023; MB, 2021). Essa integração amplia as opções do comandante e aumenta a complexidade para o adversário, mas demanda também regras de engajamento claras e controle institucional rigoroso.

O uso da “força digital” segue subordinado às diretrizes político-estratégicas, o que requer autorização superior para ações ofensivas exploratórias, prevenindo escaladas não intencionais (Brasil, 2020a). Adicionalmente, a preparação para esse tipo de conflito revelou a importância de simulações e exercícios interagências em larga escala. Tais treinamentos, envolvendo Forças Armadas, órgãos governamentais, setor privado e academia, vêm se mostrando instrumentos valiosos para aperfeiçoar protocolos de crise, fortalecer a cooperação e sedimentar uma cultura de resposta coordenada às incidentes cibernéticos (ComDCiber, 2024; CyberTech, 2022).

No âmbito nacional, iniciativas doutrinárias e estruturais já alcançaram progressos notáveis (como a publicação de normativas específicas e a ativação de unidades cibernéticas permanentes), porém alguns desafios persistem. Dentre eles, destacam-se lacunas de governança cibernética em setores críticos, como por exemplo, a proteção de infraestruturas críticas marítimas ainda carece de uma estratégia dedicada, diferentemente de países como o Reino Unido, que adotam códigos de boas práticas e certificações específicas para portos e navios (Oliveira, 2022).

Também foram mencionadas dificuldades em sincronizar plenamente as ações cibernéticas com operações militares convencionais e em acompanhar a sofisticação crescente dos ataques, que já envolvem automação por inteligência artificial e outras tecnologias emergentes (Fakhouri, 2022). Esses pontos de atenção indicam que, apesar do avanço normativo e institucional, o amadurecimento contínuo do planejamento cibernético é necessário para enfrentar a natureza evolutiva do domínio digital.

Concluindo este capítulo, fica evidente que o planejamento da guerra cibernética no Brasil atingiu um patamar de maior maturidade e integração: há hoje uma compreensão clara de seus fundamentos doutrinários, uma incorporação estruturada do componente cibernético nos processos de planejamento militar e uma

preocupação transversal com a segurança da informação. A articulação harmoniosa entre as esferas estratégica, operacional e tática, incluindo plenamente o espaço cibernético, assegura coerência desde as diretrizes nacionais de Defesa até a execução das ações no terreno digital. Além disso, a valorização de mecanismos de proteção como a criptografia, aliada a protocolos padronizados e à interoperabilidade entre as Forças, fortalece a capacidade de comando e controle diante de interferências adversárias.

No entanto, ficou igualmente claro que essa arquitetura planejada deve manter-se dinâmica e adaptável. O ambiente cibernético é marcado por rápidas transformações tecnológicas e pela aparição constante de ameaças inéditas, o que exige uma postura proativa de atualização doutrinária, aperfeiçoamento técnico e coordenação interinstitucional. Somente assim será possível preservar a superioridade informacional e a efetividade das operações conjuntas frente aos desafios emergentes. Consequentemente, a manutenção da eficácia do planejamento cibernético demanda vigilância contínua e capacidade de adaptação diante de novas ameaças e avanços tecnológicos no horizonte, aspectos que começam a delinear desafios disruptivos para os quais as estruturas atuais de defesa cibernética deverão se preparar.

Entre essas novas ameaças, desponta no horizonte tecnológico um desafio associado à computação quântica. Apesar da eficácia dos algoritmos criptográficos atuais, essa tecnologia emergente poderá suplantar os sistemas criptográficos hoje em uso, tornando obsoletos os algoritmos empregados na proteção de dados sigilosos (Brasil, 2024; Parker, 2025). Estima-se que, por volta de meados da década de 2030, um computador quântico seja capaz de decifrar grande parte das comunicações militares criptografadas por métodos tradicionais, caso contramedidas não sejam adotadas (Parker, 2025). Adversários estatais já estariam, inclusive, interceptando e armazenando comunicações cifradas atualmente, na expectativa de decifrá-las futuramente com tecnologia quântica (Brasil, 2024).

A transição para esse novo cenário tecnológico será explorada no próximo capítulo, que aprofundará os efeitos da computação quântica, em particular sobre a criptografia militar e a segurança da informação, e oferecerá uma perspectiva instigante e fundamental para o entendimento das futuras dinâmicas da guerra cibernética.

3 COMPUTAÇÃO QUÂNTICA E SEUS IMPACTOS

Este capítulo busca explorar os impactos da computação quântica sobre o planejamento militar da guerra cibernética, analisando seus riscos, desafios e oportunidades no contexto da defesa nacional. A abordagem adotada parte dos fundamentos técnicos da computação quântica e avança para a discussão de suas implicações estratégicas, doutrinárias e operacionais para as Forças Armadas, com vistas a subsidiar reflexões prospectivas sobre o tema.

A proteção da informação é um componente central em todas as fases do planejamento da Guerra Cibernética, seja em sua formulação e disseminação nos níveis estratégico, operacional e tático, na definição de regras de engajamento no nível operacional ou na execução tática de ações digitais. A confidencialidade, a integridade e a autenticidade dos dados são sustentadas por mecanismos criptográficos, desde as comunicações seguras até a proteção de bancos de dados e sistemas embarcados. Assim, avanços tecnológicos que comprometam a eficácia desses mecanismos apresentam riscos diretos à operacionalidade, à resiliência e à superioridade informacional das Forças. Nesse sentido, compreender os fundamentos e os impactos da computação quântica torna-se importante para antecipar vulnerabilidades e reestruturar o planejamento cibernético à luz desse novo paradigma.

3.1 OS FUNDAMENTOS DA COMPUTAÇÃO QUÂNTICA

A computação quântica configura-se como um campo transformador, com potencial para introduzir avanços em áreas como a criptografia e o processamento de informações. Ela baseia-se em sistemas quânticos, que são entidades físicas microscópicas, como átomos, elétrons ou fótons, regidas pelas leis da mecânica quântica, que exibem comportamentos distintos dos sistemas clássicos, como a capacidade de existir em múltiplos estados simultaneamente. Isso se deve à exploração de fenômenos quânticos, como a superposição de estados e o entrelaçamento, que possibilitam capacidades inéditas, como a geração de números pseudoaleatórios e o desenvolvimento de novos métodos de criptografia e representação de dados (Santa Cruz, 2024).

Na computação quântica, a menor unidade de informação é o qubit (abreviação de quantum bit), que se diferencia do bit clássico por poder representar simultaneamente os estados “zero” e “um”. Essa característica é possível graças ao fenômeno da superposição. No contexto da computação quântica, a superposição de estados refere-se à capacidade de um qubit assumir, ao mesmo tempo, múltiplas configurações possíveis (zero e um), enquanto o entrelaçamento descreve o fenômeno em que qubits se tornam interdependentes, de modo que o estado de um influencia diretamente o do outro, mesmo a grandes distâncias. Esses fenômenos demonstram a eficiência que os computadores quânticos podem assumir em tarefas específicas e, também, ajudam a entender por que a evolução dessa tecnologia apresenta novos desafios ao planejamento da defesa cibernética.

A exploração da superposição de estados permite que todos os caminhos possíveis de um cálculo sejam percorridos simultaneamente. Essa propriedade confere aos computadores quânticos um potencial de processamento substancialmente superior ao dos sistemas clássicos, pois as amplitudes associadas aos diferentes caminhos se combinam para determinar a probabilidade de cada resultado possível (Rocha, 2023).

Em síntese, a principal distinção entre a computação quântica e a computação clássica reside na capacidade do computador quântico explorar, de forma simultânea, múltiplos estados durante a execução de operações. Isso significa que, graças ao fenômeno da superposição, cada unidade de informação do computador quântico (o qubit) pode representar, ao mesmo tempo, os valores “zero” e “um”, permitindo que diversas possibilidades sejam consideradas em paralelo em um único ciclo de processamento. Esse paralelismo intrínseco amplia significativamente o espaço de busca e análise em operações matemáticas complexas. Assim, os computadores quânticos têm a possibilidade de superar os limites do processamento sequencial dos sistemas tradicionais, resolvendo problemas até então considerados intratáveis, incluindo aqueles que fundamentam os sistemas de criptografia assimétrica utilizados na proteção da informação.

Apoiando-se em propriedades subatômicas para realizar cálculos, a computação quântica introduz um modelo computacional distinto daquele usado pelos computadores tradicionais. Sua aplicação tornou-se particularmente relevante no contexto da criptografia. Algoritmos amplamente utilizados, como o RSA e o

Algoritmo de Assinatura Digital de Curva Elíptica (ECDSA)[12], baseiam-se em na dificuldade computacional de determinados problemas, como a fatoração de inteiros e o cálculo de logaritmos discretos, que exigem enorme poder de processamento para serem solucionados pelos computadores clássicos (Vilas Bôas Araújo, 2019).

Os algoritmos RSA e ECDSA são amplamente utilizados na proteção de dados e comunicações seguras. O RSA baseia-se na dificuldade de fatorar números inteiros grandes, enquanto o ECDSA explora a complexidade dos cálculos envolvendo logaritmos discretos em curvas elípticas. Essas operações são consideradas computacionalmente onerosas para máquinas clássicas, o que na prática inviabiliza a decodificação de informações protegidas por esses algoritmos sem a chave adequada.

Entretanto, a evolução da computação quântica passou a ameaçar essas estruturas, sobretudo com o surgimento do Algoritmo de Shor[13]. Esse algoritmo permite a um computador quântico resolver, em tempo polinomial, problemas matemáticos como a fatoração de números inteiros e o cálculo de logaritmos discretos, funções que formam a base de algoritmos de segurança assimétrica como RSA e ECDSA. Essa realidade compromete a integridade desses mecanismos e torna recomendável a transição para abordagens criptográficas resilientes ao poder computacional quântico, de forma a preservar a confidencialidade e a autenticidade das informações estratégicas (Vilas Bôas Araújo, 2019; Vásquez, 2018). Tais desafios impulsionaram esforços de pesquisa em criptografia pós-quântica, com o objetivo de criar mecanismos de segurança compatíveis com o advento da computação quântica (Vásquez, 2018). Vale notar que o termo “tempo polinomial” significa que o tempo necessário para resolver um problema cresce de forma muito mais lenta do que nos métodos tradicionais, tornando viável, na prática, a resolução prática de cálculos antes considerados proibitivos.

Nesse sentido, Baseri et al. (2024) propuseram um modelo abrangente de avaliação de riscos de segurança voltado à migração para algoritmos criptográficos

12 O Elliptic Curve Digital Signature Algorithm (ECDSA) é um método de criptografia assimétrica utilizado para gerar e verificar assinaturas digitais, baseado nas propriedades matemáticas das curvas elípticas sobre corpos finitos. Comparado a outros esquemas, como o RSA, oferece nível equivalente de segurança com chaves menores, resultando em maior eficiência computacional e menor consumo de recursos (NIST, 2013).

13 Shor é um algoritmo quântico que permite a fatoração eficiente de grandes números inteiros e o cálculo de logaritmos discretos, tarefas consideradas computacionalmente inviáveis para computadores clássicos em tempo hábil. Sua relevância estratégica decorre do fato de que tais operações são a base da segurança de algoritmos de criptografia amplamente utilizados, como o RSA e o ECDSA (Shor, 1994).

resistentes à computação quântica. O modelo examina vulnerabilidades em três camadas distintas: algorítmica, certificação e protocolos, e abrange todas as etapas da transição: antes, durante e após a adoção dos novos algoritmos. Essa abordagem em múltiplas etapas fornece um referencial robusto para antecipar riscos e definir prioridades na substituição progressiva de mecanismos criptográficos legados, sendo especialmente útil para o planejamento da defesa cibernética no nível estratégico. Ao cobrir todas as camadas críticas do processo de segurança da informação, o modelo contribui para estruturar decisões que garantam continuidade operacional e resiliência diante das mudanças tecnológicas.

Os avanços da computação quântica evidenciaram a possibilidade de ruptura dos padrões vigentes na criptografia de chave pública, historicamente fundamentada na dificuldade de resolver problemas como a fatoração de números inteiros e o cálculo de logaritmos discretos, tarefas complexas para computadores tradicionais. Esse cenário impulsionou a busca por novos problemas matemáticos capazes de sustentar sistemas criptográficos resistentes tanto aos ataques tradicionais (criptoanálise clássica) quanto aos realizados por computadores quânticos. Dessa busca surgiu o campo da criptografia pós-quântica (Matsumine, 2024).

Com o reconhecimento desses riscos, intensificaram-se os esforços para formular novos sistemas criptográficos. O objetivo passou a ser criar mecanismos capazes de oferecer proteção tanto contra ataques convencionais quanto contra ataques viabilizados por computadores quânticos. Essa busca por soluções seguras consolidou a criptografia pós-quântica como um dos foco de pesquisa da comunidade científica, reunindo abordagens baseadas em problemas matemáticos para os quais não se conhecem algoritmos quânticos eficientes. O resultado esperado é que os sistemas de segurança permaneçam robustos frente às ameaças atuais e aos avanços tecnológicos futuros, como os computadores quânticos. Em suma, a criptografia pós-quântica busca proteger a informação em um cenário de transição tecnológica.

Diversos candidatos a novos sistemas criptográficos estão em avaliação. Destacam-se, por exemplo, os mecanismos Hamming Quasi-Cyclic (HQC)[14] e Bit

14 O mecanismo HQC é um esquema de criptografia pós-quântica baseado em códigos, projetado para resistir a ataques viabilizados por computadores quânticos, incluindo o algoritmo de Shor. Fundamenta-se no problema da síndrome de decodificação em códigos quase cíclicos binários, considerado computacionalmente intratável mesmo em cenários quânticos (NIST, 2025).

Flipping Key Encapsulation (BIKE)[15], que utilizam códigos capazes de corrigir erros nas mensagens (Paiva, 2023). Esses mecanismos vêm sendo avaliados por órgãos como o National Institute of Standards and Technology (NIST)[16] no processo de definição de novos padrões internacionais de segurança. Alinhar-se a esses padrões é interessante para manter a resiliência das infraestruturas críticas nacionais frente às ameaças quânticas que se avizinham.

Estudos indicam que algoritmos quânticos poderiam explorar problemas relacionados ao cálculo de isogenias[17] em curvas elípticas ordinárias com complexidade subexponencial, o que aumentou a vulnerabilidade de determinados esquemas criptográficos a ataques quânticos. Em resposta, propostas como o protocolo Supersingular Isogeny Diffie-Hellman (SIDH)[18] foram desenvolvidas para utilizar curvas supersingulares, cujo anel de endomorfismos não é comutativo, buscando mitigar tais riscos e prover resistência a ataques quânticos. Esse esquema destaca-se como uma alternativa promissora na criptografia pós-quântica, e o NIST e outras organizações passaram a considerar algoritmos baseados em isogenias no processo de padronização de soluções para a era pós-quântica (Zanon, 2021).

A evolução da computação quântica inaugura uma nova era na segurança da informação, marcada pela iminência de uma ruptura nos paradigmas criptográficos vigentes. Sua capacidade de processamento exponencial representa um risco potencial a algoritmos até então considerados invioláveis, podendo comprometer comunicações protegidas por chaves tidas como inquebráveis (Rocha, 2020).

A adoção das alternativas criptográficas mencionadas não representa apenas um avanço técnico, mas também uma necessidade estratégica para o planejamento da defesa cibernética, a fim de perseguir a continuidade da segurança das

15 O mecanismo BIKE é um mecanismo de encapsulamento de chaves pós-quântico baseado em códigos quase cíclicos binários e no problema da síndrome de decodificação. Utiliza técnicas de correção de erros e um processo iterativo de inversão de bits (bit flipping) para derivar chaves secretas de forma segura contra ataques quânticos (NIST, 2025).

16 O NIST é uma agência federal norte-americana vinculada ao Departamento de Comércio dos Estados Unidos, responsável por desenvolver padrões, diretrizes e boas práticas em ciência, tecnologia e inovação. Atua em áreas como metrologia, tecnologia da informação e segurança cibernética (NIST, 2022).

17 Isogenias são funções matemáticas que relacionam duas curvas elípticas, enquanto a complexidade subexponencial indica que o tempo necessário para resolver determinados problemas cresce mais rapidamente do que nos algoritmos polinomiais, mas ainda mais lentamente do que nos algoritmos exponenciais, o que pode tornar alguns sistemas atuais vulneráveis diante de avanços quânticos (Zanon, 2021).

18 O SIDH é um protocolo criptográfico de troca de chaves baseado em isogenias entre curvas elípticas supersingulares. Desenvolvido como candidato a esquema de criptografia pós-quântica, o SIDH busca oferecer segurança contra ataques de computadores quânticos explorando a dificuldade computacional de encontrar isogenias entre curvas elípticas específicas (Zanon, 2021).

informações diante do potencial disruptivo da computação quântica. Tais avanços demandam ao planejamento militar a necessidade de atualização constante das estratégias de proteção da informação, e modo a antecipar cenários em que a supremacia quântica, situação em que computadores quânticos superam amplamente os sistemas tradicionais em tarefas críticas, torne-se realidade. Tais demandas estratégicas ressaltam a importância de incorporar, desde já, soluções compatíveis no planejamento da guerra cibernética.

A seguir, serão analisados os principais desafios que a computação quântica impõe ao planejamento da guerra cibernética, com ênfase nas vulnerabilidades dos sistemas de segurança atuais e em suas consequências para o ambiente militar.

3.2 OS DESAFIOS PARA O PLANEJAMENTO DA GUERRA CIBERNÉTICA

A rápida evolução da computação quântica representa um desafio considerável para a criptografia tradicional, ao colocar em risco os fundamentos matemáticos que sustentam a segurança das comunicações digitais (Alves, 2024). Esses fundamentos referem-se a problemas extremamente complexos de serem resolvidos por computadores convencionais, como a fatoração de números inteiros ou o cálculo de logaritmos discretos, base dos sistemas criptográficos atuais.

Os algoritmos criptográficos clássicos se fundamentam em problemas matemáticos como a fatoração de inteiros, o logaritmo discreto e sua variante em curvas elípticas. Contudo, esses fundamentos tornam-se frágeis diante da computação quântica, que, explorando o paralelismo quântico, poderá resolvê-los de maneira eficiente e simultânea, desestruturando a base matemática da segurança digital (Rocha, 2020).

Sistemas de criptografia amplamente utilizados para troca de chaves e assinaturas digitais, como RSA e SIDH, tornam-se potencialmente vulneráveis diante do advento dos computadores quânticos, que, por meio de algoritmos como o de Shor, podem comprometer os alicerces da criptografia assimétrica clássica. Isso colocaria em risco as propriedades de sigilo e autenticidade dos sistemas em uso, recomendando a adoção de soluções compatíveis com a nova realidade tecnológica (Giron, 2023; Rocha, 2023). Para as Forças Armadas, essa possibilidade significa que comunicações hoje consideradas seguras poderiam ser interceptadas e decifradas por adversários detentores de tecnologia quântica.

De acordo com Baseri et al. (2025), os algoritmos de chave pública, como RSA e ECC, serão diretamente vulneráveis a ataques de computadores quânticos por meio do algoritmo de Shor, capaz de resolver problemas matemáticos antes intratáveis. Por sua vez, a criptografia simétrica, embora mais resistente, também exigirá adaptações, como a duplicação do tamanho das chaves, para manter níveis equivalentes de segurança. Essa assimetria de impacto demanda estabelecer prioridades na substituição de algoritmos durante o planejamento de defesa cibernética. Enquanto os mecanismos de chave pública requerem migração urgente para alternativas pós-quânticas, os sistemas simétricos podem ser fortalecidos com medidas menos disruptivas, o que influencia diretamente decisões de investimento e cronogramas de atualização de sistemas em infraestruturas críticas.

A criptografia pós-quântica surge, então, como resposta estratégica, baseada em problemas matemáticos para os quais não se conhecem soluções eficientes em computadores clássicos ou quânticos. A adoção prática recomendada passa por um modo híbrido, que combina algoritmos clássicos e pós-quânticos, demandando análise cuidadosa dos impactos no desempenho e decisões criteriosas de projeto (Giron, 2023). Em termos simples, o modo híbrido consiste em empregar, simultaneamente, algoritmos tradicionais e novos algoritmos resistentes a ataques quânticos, criando camadas de proteção complementares durante o período de transição tecnológica.

Essa vulnerabilidade dos esquemas atuais torna-se ainda mais crítica em ambientes militares, nos quais a integridade, autenticidade e confidencialidade das informações são pilares da superioridade estratégica. A confiabilidade de infraestruturas críticas depende, portanto, da substituição programada das técnicas criptográficas hoje vulneráveis. O planejamento estratégico da guerra cibernética precisa antecipar esse ponto de ruptura, incorporando soluções pós-quânticas em seus processos normativos e operacionais. Em outras palavras, já nas etapas iniciais do planejamento deve-se prever a substituição de tecnologias de segurança suscetíveis e a incorporação de novos padrões de proteção.

Como os computadores quânticos apresentam capacidade de processamento matemático inatingível por máquinas clássicas, isso coloca os sistemas criptográficos tradicionais em risco, pois muitos desses sistemas não foram projetados para resistir ao poder computacional quântico, tornando-os suscetíveis a quebras de chaves por meio de cálculos avançados ou buscas exaustivas

aceleradas (Rocha, 2024). Isso representa um desafio adicional ao planejamento militar, que é a previsão e implementação da substituição de mecanismos criptográficos antes que se tornem obsoletos frente a adversários tecnologicamente mais avançados.

Adicionalmente, estudos demonstram que a aplicação de algoritmos quânticos, como o de Shor, poderá comprometer a integridade de sistemas criptográficos usados em infraestruturas críticas baseadas em blockchain[19], como aqueles que empregam curvas elípticas e funções de hash. A viabilidade de calcular chaves privadas a partir de chaves públicas torna-se tecnicamente possível com a computação quântica, o que implicaria em colapsos sistêmicos de segurança em mecanismos como o de Prova de Trabalho (Chicarino, 2019). O blockchain, amplamente empregado para assegurar a integridade de informações em sistemas descentralizados, perderia sua confiabilidade, podendo levar à interrupção de serviços essenciais no contexto militar.

Esse panorama representa riscos significativos para planejamentos militares que utilizem arquiteturas descentralizadas ou que dependam da robustez desses sistemas para assegurar o sigilo e a disponibilidade de informações. Na sequência, serão discutidas as oportunidades decorrentes da evolução da computação quântica, com foco em suas aplicações potenciais para o fortalecimento das capacidades de defesa cibernética.

3.3 OPORTUNIDADES PARA O PLANEJAMENTO DA GUERRA CIBERNÉTICA

A perspectiva de ameaças quânticas impulsionou a formulação de novos padrões criptográficos, dando origem a uma vertente focada especificamente na resistência a adversários com capacidade quântica (Alves, 2024). Tais padrões consistem em regras e algoritmos desenvolvidos para proteger informações contra ataques executados por computadores quânticos. A evolução desses padrões visa assegurar a segurança de comunicações e o armazenamento de dados sensíveis no futuro cenário tecnológico. No âmbito militar, isso significa proteger comunicações

19 Infraestruturas críticas baseadas em blockchain correspondem a sistemas, serviços ou ativos essenciais para o funcionamento de setores estratégicos, como energia, transporte, comunicações e finanças, cuja segurança e disponibilidade são reforçadas pelo uso de tecnologias de registro distribuído. A aplicação do blockchain nesses contextos permite descentralizar a gestão de dados, garantir a imutabilidade das transações e aumentar a resiliência contra falhas ou ataques cibernéticos (Yaga et al., 2018).

estratégicas, redes de comando e controle e sistemas embarcados críticos contra adversários tecnologicamente avançados.

Essa nova abordagem, denominada criptografia pós-quântica, configura-se como um campo estratégico emergente cujos avanços devem ser acompanhados de perto pelos setores de Defesa. É recomendável incorporar esses algoritmos em ambientes militares como resposta institucional ao risco de colapso da segurança da informação, como a interceptação de ordens e planos, a violação de redes de comando e controle ou o comprometimento de bancos de dados estratégicos.

Essa transição, no entanto, requer não apenas soluções técnica, mas também previsibilidade doutrinária e normatização adaptativa, sob pena de se gerar lacunas sensíveis entre inovação e proteção. Sem doutrinas e normas atualizadas, a introdução de novas tecnologias pode gerar lacunas na integração com sistemas existentes e criar brechas exploráveis por adversários. Nesse cenário, destacam-se os esforços internacionais de padronização, que buscam enfrentar esse desafio de forma coordenada.

No âmbito global, o NIST identificou quatro algoritmos baseados em estruturas matemáticas de reticulados[20] como candidatos robustos à padronização pós-quântica: Frodo, Crystals Kyber e NTRU. Esses mecanismos foram projetados para conciliar resistência a ataques quânticos com eficiência de execução, sendo compatíveis com requisitos operacionais de dispositivos militares, incluindo sistemas embarcados ou autônomos. Suas características indicam um alto potencial de adoção em arquiteturas de defesa, fornecendo segurança aprimorada sem sacrificar o desempenho necessário nas aplicações militares (Rocha, 2023).

A análise prossegue com a discussão das implicações práticas e estratégicas da computação quântica no planejamento militar, destacando os desdobramentos para as decisões institucionais e operacionais.

20 Estruturas matemáticas de reticulados são arranjos geométricos infinitos e periódicos de pontos em um espaço vetorial, definidos como o conjunto de todas as combinações lineares inteiras de um conjunto de vetores linearmente independentes. Essas estruturas apresentam propriedades algébricas e geométricas que as tornam adequadas para aplicações em criptografia pós-quântica, sobretudo na construção de problemas computacionalmente difíceis (Rocha, 2023).

3.4 IMPLICAÇÕES PARA O PLANEJAMENTO MILITAR

No processo de padronização internacional conduzido pelo NIST, os algoritmos Kyber e Dilithium[21] foram selecionados como referências para encapsulamento de chaves e para assinaturas digitais, respectivamente (Alves, 2024). A adoção desses padrões por organizações militares pode representar um diferencial de proteção antecipada, especialmente se forem aplicados em soluções desenvolvidas especificamente para as arquiteturas computacionais já utilizadas pelas Forças. Essa perspectiva reforça a necessidade de alinhar decisões estratégicas de longo prazo aos avanços da engenharia criptográfica, incorporando-os ao planejamento militar desde as fases iniciais.

Esse alinhamento implica, por exemplo, definir requisitos criptográficos atualizados nos documentos orientadores de capacidades militares, atualizar diretrizes operacionais que envolvam proteção da informação e planejar, do ponto de vista logístico e técnico, a substituição de algoritmos legados por soluções pós-quânticas nas infraestruturas críticas de defesa.

Deve-se considerar, no entanto, que mesmo algoritmos tidos como robustos, como o Kyber, podem apresentar comportamentos imprevisíveis em função dos componentes aleatórios que integram suas saídas. Em experimentos conduzidos com classificadores baseados em aprendizado de máquina, observaram-se erros na identificação correta de amostras criptográficas, o que levanta pontos de atenção quanto à previsibilidade e auditabilidade desses esquemas em contextos de segurança crítica (Rocha, 2023).

Os componentes aleatórios introduzem variações imprevisíveis nos cálculos criptográficos, sendo utilizados para dificultar ataques, mas também podem gerar resultados inesperados que comprometam a confiabilidade do sistema. Esse aspecto não pode ser negligenciado: as soluções de segurança precisam ser avaliadas não apenas quanto à sua robustez matemática, mas também quanto à consistência operacional em cenários reais.

---

21 O Kyber é um esquema de encapsulamento de chaves (KEM) baseado em reticulados módulo-LWE, projetado para oferecer alta eficiência e segurança frente à criptoanálise quântica. Já o Dilithium é um esquema de assinatura digital também baseado em reticulados, voltado a garantir autenticidade e integridade de dados em um cenário pós-quântico (Alves, 2024).

Por fim, serão apresentadas reflexões sobre o estado atual da preparação brasileira diante dos desafios e oportunidades oferecidos pela computação quântica no contexto da guerra cibernética.

3.5 CONSIDERAÇÕES SOBRE O ESTADO ATUAL

A evolução da computação quântica representa um dos desafios mais relevantes do cenário atual de segurança da informação e, por consequência, do planejamento militar no domínio cibernético. Diferentemente de tecnologias anteriores, que visavam aprimorar ou complementar sistemas existentes, a computação quântica desafia diretamente as bases matemáticas que sustentam a segurança digital. Embora ainda em estágio experimental, seus potenciais desdobramentos, especialmente no que tange à capacidade de processamento massivo e à quebra de algoritmos criptográficos assimétricos, configuram riscos à durabilidade de paradigmas técnicos amplamente consolidados na defesa digital.

Nesse cenário, a MB estabeleceu como prioridade estratégica a pesquisa e o desenvolvimento de novos algoritmos criptográficos, orientados por modelos matemáticos e computacionais compatíveis com o ambiente operacional militar (Brasil, 2021). Essa diretriz revela uma percepção institucional consolidada sobre o risco de obsolescência precoce das soluções de segurança atualmente adotadas, sobretudo diante da perspectiva de ruptura tecnológica imposta pela computação quântica.

Em continuidade a esses esforços, de acordo com um Analista da Divisão de Criptologia e Segurança Cibernética do Centro de Análise de Sistemas Navais (CASNAV)[22], destacam-se os projetos Sistema Criptográfico para Comunicações Navais (SCCN) e Sistema de Criptografia Pós-Quântica para a Defesa (SISCPQDef), iniciativas estratégicas da MB que visam preparar a instituição para os desafios da computação quântica. Por meio do SCCN, buscam-se algoritmos criptográficos unificados capazes de proteger as transmissões tático-estratégicas em todos esses meios, assegurando que informações sensíveis circulem com confidencialidade e autenticidade entre unidades navais e terrestres sem perda de sinergia.

22 Entrevista de pesquisa concedido em 06 de agosto de 2025.

Por sua vez, o projeto SISCPQDef tem por objetivo manter o sigilo e a integridade de dados sensíveis frente à ameaça futura de computadores quânticos capazes de quebrar os cifradores atuais. Para tanto, são pesquisados e implementados algoritmos pós-quânticos concebidos para permanecerem seguros mesmo diante do poder de processamento quântico.

No plano doutrinário, os documentos de planejamento conjunto ressaltam que a identificação de preponderâncias científicas e tecnológicas por parte de potenciais adversários deve ser incorporada desde as fases iniciais do processo decisório. Tal diretriz visa minimizar desvantagens e potencializar capacidades próprias frente a cenários de assimetria tecnológica (Brasil, 2020), implicando a necessidade de antecipar os riscos associados à introdução de tecnologias disruptivas e promover ajustes estruturais contínuos nos processos doutrinários, logísticos e operacionais da guerra cibernética.

Essa articulação entre pesquisa tecnológica e doutrina operacional configura-se, portanto, como um importante componente para a resiliência cibernética da Defesa Nacional. A computação quântica, nesse sentido, atua não apenas como um risco latente, mas também como um indutor de transformações profundas na forma como se concebe, planeja e executa a defesa cibernética em ambiente militar. Na prática, isso significa alinhar o desenvolvimento de novos algoritmos e ferramentas com as estratégias e procedimentos empregados em operações reais das Forças Armadas.

A antecipação de rupturas tecnológicas recomenda, ainda, o uso de estudos prospectivos como instrumento indispensável para reduzir as incertezas associadas ao avanço da computação quântica no domínio cibernético. Esses estudos iluminam as decisões presentes com base em projeções de futuros plausíveis, oferecendo suporte para o delineamento de estratégias resilientes frente a eventos sem precedentes históricos (Nichols, 2019). No contexto militar, essa abordagem prospectiva fortalece a capacidade de antever rupturas tecnológicas, como as decorrentes da computação quântica.

3.6 CONCLUSÕES PARCIAIS

A computação quântica apresenta-se como uma inovação de destaque na história da tecnologia, com potencial para impactar profundamente os fundamentos

da segurança da informação e, por consequência, o planejamento militar no domínio cibernético. Seu modelo de processamento, baseado em qubits, superposição de estados e entrelaçamento, confere-lhe a capacidade de resolver problemas que desafiam os computadores clássicos, como os algoritmos de criptografia baseados na fatoração de inteiros e no cálculo de logaritmos discretos. Isso representa um risco relevante aos algoritmos criptográficos atualmente utilizados para proteger dados e comunicações estratégicas.

Nesse cenário, os desafios impostos ao planejamento da guerra cibernética requerem ações proativas, como a adoção de criptografia pós-quântica, a atualização das arquiteturas de segurança, a substituição de sistemas vulneráveis e o desenvolvimento de novas doutrinas e normatizações para preservar a resiliência das infraestruturas críticas diante da evolução tecnológica de adversários.

Por outro lado, a computação quântica também oferece oportunidades, como o desenvolvimento de novos mecanismos de proteção e o aprimoramento da capacidade de processamento em aplicações militares. Entre essas aplicações, pode-se citar o uso de algoritmos quânticos, o planejamento de rotas e o processamento de grandes volumes de dados de inteligência. Para que essas oportunidades sejam aproveitadas de forma segura, é salutar que o planejamento cibernético incorpore métodos prospectivos e cenários hipotéticos, antecipando rupturas tecnológicas e ajustando continuamente os processos doutrinários e operacionais.

Portanto, a computação quântica não deve ser vista apenas como um risco latente, mas como um indutor de transformações que demanda um novo olhar sobre o planejamento e a execução da defesa cibernética no contexto militar, apontando para a necessidade de uma postura proativa das instituições militares, baseada em estudos prospectivos e na atualização contínua de suas capacidades tecnológicas e doutrinárias, como forma de fortalecer sua posição estratégica em um cenário global cada vez mais marcado por transformações tecnológicas.

Dessa forma, as análises realizadas neste capítulo oferecem importantes subsídios para os desdobramentos do trabalho, permitindo articular os desafios tecnológicos emergentes abordados ao planejamento cibernético que serão aprofundadas no próximo capítulo.

4 ANÁLISE DA ADERÊNCIA DA COMPUTAÇÃO QUÂNTICA AO PLANEJAMENTO DA GUERRA CIBERNÉTICA

Nos capítulos anteriores foram apresentados os fundamentos da guerra cibernética e as bases de seu planejamento, delineando etapas, ameaças e capacidades envolvidas na preparação de operações nesse domínio. Com esse embasamento, o presente capítulo dedica-se a examinar criticamente como a computação quântica, uma tecnologia emergente de potencial disruptivo, se insere nesse contexto de planejamento da guerra cibernética.

Considerando que:

> A tecnologia só é relevante em termos de seus efeitos nas considerações táticas e estratégicas. Estas são as únicas considerações pertinentes: o que a tecnologia pode ou não pode, exige ou impede no enfrentamento e na campanha (Duarte, 2012, p. 30).

Desse modo, a questão central aqui é determinar se e em que medida as capacidades da computação quântica afetam ou podem vir a afetar o planejamento de operações de guerra cibernética, seja potencializando ações ofensivas, exigindo novas posturas defensivas ou alterando o equilíbrio estratégico entre os atores. A seguir, são analisadas as possíveis ameaças quânticas ao cenário cibernético e as oportunidades de emprego dessa tecnologia em favor da defesa, avaliando-se, por fim, como tudo isso se adere (ou não) às práticas atuais de planejamento.

4.1 AMEAÇAS POTENCIAIS NO CONTEXTO CIBERNÉTICO

Conforme já abordado no capítulo anterior, a computação quântica desponta simultaneamente como promessa tecnológica e como ameaça no campo da segurança cibernética. De um lado, prevê-se que computadores quânticos poderão resolver problemas computacionais hoje intratáveis, abrindo caminho para novas aplicações, por outro, esses mesmos avanços podem comprometer gravemente os alicerces da criptografia atual, tornando obsoletos os algoritmos de proteção de dados usados em redes e comunicações (Schneider, 2024). Em termos práticos, isso significa que informações que hoje trafegam protegidas por criptografia robusta poderão se tornar acessíveis a um adversário equipado com um computador

quântico. Um ataque quântico bem-sucedido poderia quebrar facilmente cifras como RSA ou ECC, algo que, em computadores tradicionais, exigiria um tempo desproporcional, expondo comunicações antes consideradas confidenciais.

As implicações dessa capacidade para a guerra cibernética são profundas. Um ator com poder quântico poderia decifrar comunicações sigilosas do inimigo, caso interceptasse dados criptografados, e neutralizar sistemas considerados seguros em tempo real, revolucionando as operações de espionagem e coleta de inteligência (Schneider, 2024). Operações cibernéticas ofensivas que antes demandariam longos períodos de infiltração e monitoramento poderiam, com computação quântica, colher informações críticas de forma muito rápida, superando defesas convencionais. Além disso, algoritmos quânticos têm potencial para processar volumes massivos de dados em velocidades muito superiores às dos computadores clássicos, viabilizando a identificação célere de vulnerabilidades em sistemas complexos ou a antecipação das respostas defensivas do adversário com precisão inédita. Em outras palavras, uma nova geração de ataques cibernéticos poderia emergir, capaz de contornar até mesmo protocolos de segurança avançados por meio da análise rápida e contínua das contramedidas do oponente.

Um cenário particularmente crítico envolve a ameaça quântica contra infraestruturas estratégicas. Redes de energia, sistemas de telecomunicações, transportes e outras infraestruturas críticas já vêm sendo alvo de intrusão por nações e grupos hostis no contexto cibernético tradicional. Com capacidades quânticas, esses ataques poderiam atingir efeitos disruptivos em larga escala, como cortes de energia em regiões inteiras, colapso de redes de comunicação ou paralisação de sistemas de transporte (Schneider, 2024). A mera possibilidade de realizar ofensivas dessa magnitude conferiria a atores detentores de computação quântica uma poderosa vantagem coercitiva. Na diplomacia internacional, países equipados com essas capacidades poderiam exercer pressão sobre adversários menos avançados, configurando uma forma de dissuasão travada no *front* digital (Ernst & Young, 2023).

Outro ponto de preocupação imediata é a estratégia conhecida como “capturar agora, decifrar depois”, adotada por agentes maliciosos frente à ameaça quântica. Ainda que computadores quânticos capazes de quebrar a criptografia hoje vigente não existam comercialmente, especialistas estimam que isso pode se tornar viável em um horizonte de cinco a quinze anos. Cientes desse prazo, adversários já

estariam interceptando e armazenando grandes volumes de comunicações e dados confidenciais na expectativa de descriptografá-los futuramente, quando a tecnologia quântica estiver madura (Schneider, 2024). Esse quadro impõe um senso de urgência: informações sigilosas trocadas no presente podem, em uma década ou menos, perder completamente a proteção caso medidas de segurança resistentes à era quântica não sejam implementadas a tempo.

Diante de todas essas potenciais ameaças: quebra de criptografia, aumento de ataques cibernéticos e obsolescência de mecanismos de segurança, fica claro que a computação quântica tende a elevar os riscos considerados no planejamento da guerra cibernética. A possibilidade de um inimigo acessar comunicações militares classificadas ou paralisar defesas críticas por meio de poder computacional superior representa um fator de desequilíbrio estratégico que não pode ser ignorado pelos planejadores. Na próxima seção, serão abordadas as contrapartidas a esse cenário: de que modo a própria tecnologia quântica pode também oferecer meios para fortalecer a segurança cibernética.

4.2 OPORTUNIDADES PARA A DEFESA CIBERNÉTICA

Apesar do panorama desafiador descrito, a computação quântica não traz apenas ameaças; ela também abre oportunidades para a proteção cibernética e a resiliência das operações. A mesma base física que permite a um computador quântico quebrar cifras pode ser empregada para criar canais de comunicação seguros e praticamente à prova de interceptação. Uma das principais inovações nesse sentido é a Distribuição Quântica de Chaves (QKD)[23], técnica que utiliza propriedades quânticas para distribuir chaves criptográficas de forma absolutamente sigilosa. Na QKD, qualquer tentativa de interceptação da chave altera o estado quântico e denuncia a presença do intruso, tornando a comunicação virtualmente inviolável (Schneider, 2024).

Paralelamente, a comunidade de segurança da informação vem trabalhando intensamente em algoritmos de criptografia pós-quântica (PQC), isto é, novos

23 A QKD é um método criptográfico que utiliza princípios da mecânica quântica para permitir a troca segura de chaves de criptografia entre duas partes. Diferentemente dos métodos clássicos, a QKD explora propriedades como o princípio da incerteza de Heisenberg e o entrelaçamento quântico para detectar qualquer tentativa de interceptação, uma vez que a medição de estados quânticos altera irremediavelmente suas propriedades (Bennett; Brassard, 2014).

esquemas criptográficos projetados para resistir inclusive a ataques de computadores quânticos. Em 2022, por exemplo, os Estados Unidos, por meio de memorando de segurança nacional, determinaram a adoção de criptografia pós-quântica em todos os sistemas críticos do governo, estabelecendo o ano de 2035 como prazo para substituição dos algoritmos atuais (Parker, 2025). Essa iniciativa reflete a dimensão do desafio: migrar infraestruturas inteiras de comunicação e armazenamento de dados para novos padrões de criptografia é um processo complexo e demorado, que precisa ser iniciado com antecedência para surtir efeito antes que a ameaça se concretize.

Diversas nações vêm investindo em capacidades de defesa quântica, tanto na área de comunicações seguras quanto na de criptografia resistente a computadores quânticos. A China, por exemplo, implementou uma infraestrutura integrada de comunicação quântica que combina redes terrestres com 4,6 mil quilômetros de comprimento e enlaces via satélite, permitindo a distribuição de chaves quânticas entre estações terrestres e espaciais (Chen et al., 2021). Em paralelo, países ocidentais têm direcionado esforços para o desenvolvimento de algoritmos de criptografia pós-quântica. Nesse sentido, o NIST anunciou, em 2022, a seleção inicial de quatro algoritmos resistentes a ataques quânticos, resultado de um processo de padronização conduzido em cooperação internacional (NIST, 2022).

Vale notar que há um debate estratégico sobre qual caminho seguir: se apostar em PQC, em QKD, ou em ambos. Cada abordagem possui vantagens específicas. A criptografia pós-quântica pode ser implementada via software e aproveita grande parte da infraestrutura existente, enquanto a QKD oferece segurança baseada em leis físicas (considerada incondicional), porém ao custo de requerer novos equipamentos e enlaces dedicados. A Agência de Segurança Nacional dos EUA (NSA), por exemplo, não apoia o uso de QKD para proteger informações nacionais sigilosas, citando custos e limitações práticas, e foca seus esforços em soluções de criptografia pós-quântica (Parker, 2025). Já governos como o chinês investem fortemente em QKD, sem abdicar de pesquisas em algoritmos pós-quânticos, possivelmente buscando uma abordagem combinada para essas defesas (Ernst & Young, 2023).

4.3 IMPLICAÇÕES PARA O PLANEJAMENTO DA GUERRA CIBERNÉTICA

Considerando os aspectos abordados sobre ameaças e oportunidades quânticas, cabe avaliar em que medida os processos atuais de planejamento da guerra cibernética estão preparados para tais mudanças tecnológicas. No estado atual, pode-se dizer que a aderência da computação quântica ao planejamento ainda é incipiente: os manuais e doutrinas vigentes de ações cibernéticas focam majoritariamente em capacidades existentes e ameaças convencionais (Duarte, 2012), sem referências explícitas a computadores quânticos ou criptografia quântica.

Entretanto, diversos especialistas enfatizam que aguardar a ameaça quântica se concretizar para então reagir seria um erro estratégico grave (Ernst & Young, 2023). Uma vez que a quebra das criptografias vigentes ocorra, a janela de reação será curta e o dano potencial, enorme. Assim, o planejamento da guerra cibernética precisa se antecipar, incorporando desde já hipóteses e medidas relacionadas à computação quântica.

Isso implica algumas ações concretas no âmbito do planejamento (Parker, 2025):

- Revisão das avaliações de ameaças, passando a incluir a possibilidade de adversários desenvolverem ou adquirirem computadores quânticos e as consequências disso para a segurança nacional;
- Coordenação com nações aliadas, buscando o alinhamento de estratégias de proteção contra ataques quânticos e o compartilhamento de informações sobre avanços nessa área;
- Capacitação e desenvolvimento tecnológico interno, inserindo a temática quântica em exercícios militares (inclusive simulados interagências) e promovendo a formação de pessoal especializado em tecnologias quânticas e criptografia avançada; e
- Atualização de protocolos e infraestruturas, com a adoção gradual de algoritmos pós-quânticos nos sistemas críticos e a eventual experimentação de enlaces QKD em ambientes que exijam o mais alto nível de segurança, a título de prova de conceito.

4.4 CONCLUSÕES PARCIAIS

A análise desenvolvida neste capítulo permite concluir que, embora ainda inicial, a incorporação da computação quântica ao planejamento da guerra cibernética tende a se tornar inevitável. As capacidades quânticas prometem transformar aspectos cruciais da guerra cibernética, vulnerabilizando infraestruturas criptográficas atualmente utilizadas pelo oponente, ampliando o espectro e a velocidade dos ataques cibernéticos, e, ao mesmo tempo, oferecendo novos meios para proteger dados e comunicações. Ignorar essa tendência não é uma opção responsável, pois o tempo de reação para mitigar riscos quânticos é contado em anos, exigindo ações no presente para evitar surpresas estratégicas no futuro.

Desse modo, a computação quântica deve gradativamente deixar de ser tratada apenas como um tópico de ciência e tecnologia, passando a figurar nas considerações práticas do planejamento de defesa cibernética. Este capítulo evidenciou pontos frágeis na estrutura atual, como a dependência exclusiva de algoritmos clássicos, e sugeriu caminhos para seu fortalecimento, como a adoção de criptografia pós-quântica, exploração de comunicações quânticas e cooperação internacional em novos padrões de segurança. Em termos de aderência ao planejamento, ainda existe um descompasso: as diretivas de guerra cibernética vigentes não contemplam explicitamente o fator quântico, mas é provável que isso mude à medida que a viabilidade de computadores quânticos se aproxima. A partir das reflexões apresentadas, reforça-se a importância de engajar o meio militar, acadêmico e industrial na construção conjunta de soluções e doutrinas que integrem a computação quântica, garantindo que, quando essa tecnologia atingir maturidade, as Forças Armadas estejam prontas para neutralizar suas ameaças e explorar suas vantagens em prol da segurança nacional.

5 CONCLUSÃO

O presente trabalho permitiu constatar que o planejamento da guerra cibernética nas Forças Armadas brasileiras evoluiu significativamente nos últimos anos, incorporando o domínio cibernético como componente estratégico nos níveis político, estratégico, operacional e tático. As doutrinas do Ministério da Defesa e da Marinha do Brasil já preveem estruturas especializadas, processos decisórios adaptados e medidas de proteção da informação, evidenciadas pela atuação do Comando de Defesa Cibernética, pela elaboração de anexos cibernéticos nos planos conjuntos e pela criação de grupamentos operativos dedicados. Apesar desses avanços, ficou claro que o ambiente digital impõe desafios dinâmicos: ameaças difusas, dificuldade de atribuição de ataques e necessidade de constante atualização tecnológica.

Nesse contexto, a computação quântica emerge como um fator disruptivo, capaz de comprometer os alicerces criptográficos que sustentam a superioridade informacional militar. A análise desenvolvida enfatiza que a resiliência da defesa cibernética dependerá de uma postura proativa e flexível, em que planejamento e tecnologia avancem de mãos dadas. Em síntese, verificou-se que o planejamento cibernético brasileiro está em franco desenvolvimento e alinhado às melhores práticas internacionais, mas enfrenta o imperativo de adaptar-se rapidamente às transformações tecnológicas iminentes para garantir a segurança dos ativos informacionais e a efetividade das operações conjuntas no espaço cibernético.

Em síntese, respondendo às questões centrais deste estudo, observa-se que a forma atual de planejamento da guerra cibernética, embora apresente progressos importantes, ainda não se encontra plenamente preparada para a era quântica, exigindo ajustes ágeis e estratégicos. Da mesma forma, as capacidades da computação quântica podem ser incorporadas gradativamente ao planejamento cibernético por meio de diversas medidas, desde a transição tecnológica, como a adoção de criptografia pós-quântica nas infraestruturas críticas, até o investimento em pesquisa e capacitação especializada em tecnologias quânticas, bem como a atualização das doutrinas e estratégias de defesa para incluir cenários de ameaças quânticas.

Nesse panorama, cabe ao Ministério da Defesa e às Forças Singulares adotarem medidas pragmáticas para consolidar e ampliar a capacidade de guerra

cibernética diante da era quântica. É fundamental, em primeiro lugar, acelerar a transição para algoritmos de criptografia pós-quântica em todas as infraestruturas críticas de comunicação militar, alinhando-se aos padrões internacionais emergentes e antecipando prazos de migração para mitigar o risco de quebras criptográficas futuras. Paralelamente, recomenda-se o fortalecimento da pesquisa e desenvolvimento em segurança quântica, incluindo parcerias com centros acadêmicos e a formação de pessoal especializado em computação quântica e criptografia avançada, de modo a internalizar conhecimento e reduzir dependências externas.

A integração do tema quântico ao planejamento deve ser formalizada: a atualização das doutrinas e normas precisa contemplar cenários de ameaça quântica, e exercícios conjuntos, a exemplo do Guardião Cibernético, podem incorporar simulações de ataques quânticos para calibrar respostas institucionais. Adicionalmente, evidencia-se a necessidade de aprimorar a governança cibernética no setor marítimo, mediante a elaboração de uma estratégia de segurança cibernética dedicada que estabeleça diretrizes específicas para proteger portos, sistemas navais e demais infraestruturas críticas costeiras contra ameaças digitais cada vez mais sofisticadas.

Por fim, manter uma postura de cooperação internacional e interagências será decisivo: compartilhar inteligência sobre ameaças emergentes, acompanhar os esforços globais de padronização pós-quântica e estabelecer protocolos de atuação conjunta com órgãos civis e parceiros estrangeiros contribuirá para elevar o patamar de resiliência cibernética nacional. Essas medidas, tomadas de forma coordenada e gradual, permitirão que as Forças Armadas do Brasil enfrentem com solidez os desafios identificados neste estudo, assegurando que o planejamento da guerra cibernética permaneça eficaz e alinhado aos avanços tecnológicos.

REFERÊNCIAS

ABI-ABIB, Gabriel de Carvalho. **Um estudo de ferramentas de criptoanálise baseadas em técnicas não convencionais**. 2020. Monografia (Curso de Aperfeiçoamento Avançado em Segurança da Informação e Comunicações) – Centro de Instrução Almirante Wandenkolk, Marinha do Brasil, Rio de Janeiro, 2020.

ALVES, Everaldo Antonio Moreira. **Implementação em Software dos Algoritmos Pós-Quânticos Kyber e Dilithium na Plataforma ARMv8**. 2024. Dissertação (Mestrado em Ciência da Computação) – Universidade Estadual de Campinas, Instituto de Computação, Campinas, 2024. Disponível em: https://www.repositorio.mar.mil.br/bitstream/ripcmb/847834/1/Disserta%c3%a7%c3%a3o_Everaldo_Unicamp_VFinal.pdf. Acesso em: 07 jun. 2025.

BASERI, Yaser; CHOUHAN, Vikas; GHORBANI, Ali; CHOW, Aaron. Evaluation framework for quantum security risk assessment: A comprehensive strategy for quantum-safe transition. **Computers & Security**, v. 150, p. 104272, mar. 2025. Disponível em: https://doi.org/10.1016/j.cose.2024.104272. Acesso em: 21 jun. 2025.

BENNETT, Charles H.; BRASSARD, Gilles. Quantum cryptography: Public key distribution and coin tossing. **Elsevier**, 2014. p. 7–11. Disponível em: https://www.sciencedirect.com/science/article/pii/S0304397514004241. Acesso em: 15 jul. 2015.

BRASIL. Ministério da Defesa. **Doutrina de Operações Conjuntas – MD30-M-01**. 2. ed. Brasília: Ministério da Defesa, 2020a. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/ajuste-01/legislacao/emcfa/publicacoes/doutrina/md30-m-01-vol-1-2a-edicao-2020-dou-178-de-15-set.pdf. Acesso em: 13 mar. 2025.

BRASIL. Ministério da Defesa. **Doutrina Militar de Defesa Cibernética – MD31-M-07**. 2. ed. Brasília: Ministério da Defesa, 2023. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/estado-maior-conjunto-das-forcas-armadas/doutrina-militar/publicacoes-1/publicacoes/MD31M07DoutrinaMilitardeDefesaCiberntica2Edio2023.pdf. Acesso em: 13 mar. 2025.

BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa**. Brasília: Ministério da Defesa, 2020b. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_congresso_.pdf. Acesso em: 07 mai. 2025.

BRASIL. Ministério da Defesa. **Glossário das Forças Armadas. MD35-G-01**. 5. ed. mod. Brasília: Ministério da Defesa, 2015. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/ajuste-01/legislacao/emcfa/publicacoes/doutrina/md35-G-01-glossario-das-forcas-armadas-5-ed-2015-com-alteracoes.pdf. Acesso em: 13 mar. 2025.

BRASIL. Ministério da Defesa. **Política Cibernética de Defesa – MD31-P-02**. Brasília: Ministério da Defesa, 1ª ed., 2012. Disponível em:

https://www.gov.br/defesa/pt-br/assuntos/estado-maior-conjunto-das-forcas-armadas/doutrina-militar/publicacoes-1/publicacoes/MD31P02PolticaCibernticadeDefesa1Ed2012.pdf. Acesso em: 13 mar. 2025.

BRASIL. Ministério da Defesa. **Política Nacional de Defesa**. Brasília: Ministério da Defesa, 2020c. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_congresso_.pdf. Acesso em: 07 mai. 2025.

BRASIL. Senado Federal. **Ata da 5ª Reunião da Subcomissão Permanente de Defesa Cibernética – 30/10/2024**. Brasília: Senado Federal, 2024. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento/download/ca8c5e95-e277-41d4-a84f-fdb4ca31be84. Acesso em: 13 mar. 2025.

CAVADAS, Victor Andrês Veloso. **Mensurando Forças no Ciberespaço: Uma Aplicação de Social Network Analysis para Mensurar a Influência de Estados Unidos e China na Rede do Backbone da Internet (2011–2017)**. 2022. Dissertação (Mestrado em Relações Internacionais) – Instituto de Relações Internacionais, Universidade de São Paulo, São Paulo, 2022. Disponível em: https://sucupira-legado.capes.gov.br/sucupira/public/consultas/coleta/trabalhoConclusao/viewTrabalhoConclusao.jsf?popup=true&id_trabalho=11594882. Acesso em: 11 mar. 2025.

CHEN, Yu-Ao et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. **Nature**, v.589, p.214–219, 2021. Disponível em: https://www.nature.com/articles/s41586-020-03093-8. Acesso em: 16 jul. 2025.

CHICARINO, Vanessa Rocha Leandro. **Uma heurística para a detecção de ataques ao mecanismo de consenso por Prova de Trabalho em Blockchain**. 2019. Dissertação (Mestrado em Computação) – Universidade Federal Fluminense, Instituto de Computação, Niterói, 2019. Disponível em: https://www.repositorio.mar.mil.br/bitstream/ripcmb/844280/1/Dissertacao_Vanessa.pdf. Acesso em: 07 jun. 2025.

CLARKE, Richard A.; KNAKE, Robert K. **Guerra Cibernética: a próxima ameaça à segurança e o que fazer a respeito**. Rio de Janeiro: Brasport, 2015.

COMANDO DE DEFESA CIBERNÉTICA (ComDCiber). **Anexo A – Concepção Geral do EGC 6.0**. Brasília: ComDCiber, 2024.

CRIPTOGRAFIA em comunicações militares: dados protegidos. Portal Supervivo, 18 dez. 2024. Disponível em: https://supervivo.pt/criptografia-em-comunicacoes-militares-dados-protegidos. Acesso em: 07 jun. 2025.

CRISTO JUNIOR, Eduardo Vieira. **A influência da guerra cibernética no ambiente militar da Marinha**. 2020. Monografia (Curso de Aperfeiçoamento Avançado em Segurança da Informação e Comunicações) – Centro de Instrução Almirante Wandenkolk, Rio de Janeiro, 2020.

CYBERTECH Report. **Simulação de ataques em cenários realistas**. n. 8, fev. 2022. Disponível em: https://www.cisco.com/c/dam/global/pt_br/solutions/pdfs/report8-distrito.pdf. Acesso em: 13 mar. 2025.

DUARTE, Érico Esteves. **Conduta da Guerra na Era Digital e suas Implicações para o Brasil: Uma Análise de Conceitos, Políticas e Práticas de Defesa**. Brasília: Instituto de Pesquisa Econômica Aplicada, 2012. Disponível em: https://portalantigo.ipea.gov.br/agencia/images/stories/PDFs/TDs/td_1760.pdf. Acesso em: 14 jul. 2025.

ERNST & YOUNG. Por que as organizações devem se preparar para a segurança cibernética da computação quântica agora. **EY Insights**, 14 abr. 2023. Disponível em: https://www.ey.com/pt_br/insights/innovation/why-organizations-should-prepare-for-quantum-computing-cybersecurity-now. Acesso em: 14 jul. 2025.

FAKHOURI, Luis Gustavo Perez. **The new face of power of the 21st century: technology and data**. 2022, Dissertação (Master in International Management) - Escola de Administração de Empresas de São Paulo, Fundação Getulio Vargas, São Paulo, 2022. Disponível em: https://sucupira-legado.capes.gov.br/sucupira/public/consultas/coleta/trabalhoConclusao/viewTrabalhoConclusao.jsf?popup=true&id_trabalho=11499798. Acesso em: 11 mar. 2025.

GIRON, Alexandre Augusto. **Hybrid Post-Quantum Cryptography in Network Protocols**. 2023. Tese (Doutorado em Ciência da Computação) – Universidade Federal de Santa Catarina, Programa de Pós-Graduação em Ciência da Computação, Florianópolis, 2023. Disponível em: https://sucupira-legado.capes.gov.br/sucupira/public/consultas/coleta/trabalhoConclusao/viewTrabalhoConclusao.jsf?popup=true&id_trabalho=6405734. Acesso em: 07 jun. 2025.

KHAN, Shaza. Intercepted communications: Encryption standards for the defense edge. **Mercury Systems Blog**, 18 mar. 2024. Disponível em: https://www.mrcy.com/company/blogs/intercepted-communications-encryption-standards-defense-edge. Acesso em: 21 jun. 2025.

MARINHA DO BRASIL (MB). **Manual de Operações Cibernéticas na Marinha – EMA-419**. Brasília: Marinha do Brasil, 2021.

MATSUMINE, Vitor Satoru Machi. **Avaliação de técnicas de multiplicação modular voltadas a criptossistemas baseados em isogenias em sistemas ARMv8**. 2024. Dissertação (Mestrado em Ciência da Computação) – Universidade Estadual de Campinas, Instituto de Computação, Campinas, 2024. Disponível em: https://sucupira-legado.capes.gov.br/sucupira/public/consultas/coleta/trabalhoConclusao/viewTrabalhoConclusao.jsf?popup=true&id_trabalho=16167371. Acesso em: 07 jun. 2025.

NATIONAL ACADEMIES OF SCIENCES, ENGINEERING AND MEDICINE. **Quantum Computing: Progress and Prospects**. Washington, DC: The National

Academies Press, 2019. Disponível em: https://doi.org/10.17226/25196. Acesso em: 16 jul. 2025.

NICHOLS, Giselli Christina Leal. **Guerra Naval do Futuro: Estudo de Cenários Prospectivos na Era Pós-Humana**. Rio de Janeiro: Escola de Guerra Naval, 2019. Disponível em: https://www.repositorio.mar.mil.br/bitstream/ripcmb/845653/1/NICHOLS.pdf. Acesso em: 07 jun. 2025.

National Institute of Standards and Technology (NIST). **About NIST**. Gaithersburg: NIST, 2022. Disponível em: https://www.nist.gov/about-nist. Acesso em: 12 mai. 2025.

National Institute of Standards and Technology (NIST). **Announcing the Advanced Encryption Standard (AES)**. FIPS PUB 197, 2001. Disponível em: https://doi.org/10.6028/NIST.FIPS.197. Acesso em: 12 mai. 2025.

National Institute of Standards and Technology (NIST). **Digital Signature Standard (DSS)**. FIPS PUB 186-4, 2013. Disponível em: https://doi.org/10.6028/NIST.FIPS.186-4. Acesso em: 12 mai. 2025.

National Institute of Standards and Technology (NIST). **NIST announces first four quantum-resistant cryptographic algorithms**. 5 jul. 2022. Disponível em https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms. Acesso em: 12 jul. 2025.

National Institute of Standards and Technology (NIST). **Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process**. Gaithersburg, MD: NIST, 2025. Disponível em: https://doi.org/10.6028/NIST.IR.8545. Acesso em: 12 mai. 2025.

OLIVEIRA, Márcio Rebello de. **As infraestruturas críticas nacionais ante às ameaças cibernéticas: análise comparativa das governanças cibernéticas do Brasil e do Reino Unido, com foco nas infraestruturas críticas marítimas**. 2022. Tese (Curso de Política e Estratégia Marítimas) – Escola de Guerra Naval, Rio de Janeiro, 2022. Disponível em: https://www.repositorio.mar.mil.br/handle/ripcmb/845968. Acesso em: 08 mar. 2025.

PAIVA, Thales Areco Bandiera. **Attacking and defending post-quantum cryptography candidates**. 2023. Tese (Doutorado em Ciências – Ciência da Computação) – Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo, 2023. Disponível em: https://sucupira-legado.capes.gov.br/sucupira/public/consultas/coleta/trabalhoConclusao/viewTrabalhoConclusao.jsf?popup=true&id_trabalho=12520635. Acesso em: 07 jun. 2025.

PARKER, Edward. U.S.-Allied Militaries Must Prepare for the Quantum Threat to Cryptography. Santa Monica: **RAND Corporation**, 6 jun. 2025. Disponível em: https://www.rand.org/pubs/commentary/2025/06/us-allied-militaries-must-prepare-for-the-quantum-threat.html. Acesso em: 21 jun. 2025.

RIVEST, Ron L.; SHAMIR, Adi; ADLEMAN, Leonard. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. **Communications of the ACM**, v. 21, n. 2, p. 120-126, 1978. Disponível em: https://doi.org/10.1145/359340.359342. Acesso em: 12 mai. 2025.

ROCHA, Bruno dos Santos. **Identificação de Criptossistemas Pós-Quânticos por Meio de Aprendizado de Máquina**. 2023. Dissertação (Mestrado em Ciências em Sistemas e Computação) – Instituto Militar de Engenharia, Rio de Janeiro, 2023. Disponível em: https://www.repositorio.mar.mil.br/bitstream/ripcmb/846593/1/Bruno_Rocha_Dissertacao.pdf. Acesso em: 07 jun. 2025.

ROCHA, Caio Carneiro Silva. **Os efeitos da computação quântica para a Marinha do Brasil**. Rio de Janeiro: Centro de Instrução Almirante Wandenkolk, 2020. Monografia (Curso de Aperfeiçoamento Avançado em Segurança da Informação e Comunicações). Disponível em: https://www.repositorio.mar.mil.br/bitstream/ripcmb/845456/1/1T%20QC-CA%20CAIO%20ROCHA.pdf. Acesso em: 07 jun. 2025.

SANTA CRUZ, Luis José Mantilla. **Multigraphs: Emergence from Hilbert Space Subdivision in Superposed Quantum Systems and their Image Encoding Application**. 2024. Dissertação (Mestrado em Ciência da Computação) – Universidade Federal de Uberlândia, Uberlândia, 2024. Disponível em: https://sucupira-legado.capes.gov.br/sucupira/public/consultas/coleta/trabalhoConclusao/viewTrabalhoConclusao.jsf?popup=true&id_trabalho=15189916. Acesso em: 07 jun. 2025.

SCHNEIDER, Guilherme. Quantum Computing and state-sponsored Cyber Warfare: How quantum will transform Nation-State Cyber Attacks. **Modern Diplomacy**, 07 nov. 2024. Disponível em: https://moderndiplomacy.eu/2024/11/07/quantum-computing-and-state-sponsored-cyber-warfare-how-quantum-will-transform-nation-state-cyber-attacks. Acesso em: 14 jul. 2025.

SHOR, Peter. W. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In: Proceedings 35th Annual Symposium on Foundations of Computer Science. **IEEE Computer Society**, 1994. p. 124-134. DOI: https://doi.org/10.1109/SFCS.1994.365700. Acesso em: 12 mai. 2025.

STALLINGS, William. **Cryptography and Network Security: Principles and Practice**. 7. ed. Boston: Pearson, 2017.

VÁSQUEZ, Juan del Carmen Grados. **Criptografia pós-quântica: uma análise diferencial eficiente e um novo esquema de assinatura de uso único**. 2018. Tese (Doutorado em Ciências) – Laboratório Nacional de Computação Científica, Petrópolis, 2018. Acesso em: 07 jun. 2025.

VILAS BÔAS ARAÚJO, Thales. **Implementação de Paralelismo para Geração de Chaves no Esquema XMSS**. 2019. Dissertação (Mestrado em Engenharia Eletrônica e Computação) – Instituto Tecnológico de Aeronáutica, São José dos

Campos, 2019. Disponível em: https://sucupira-legado.capes.gov.br/sucupira/public/consultas/coleta/trabalhoConclusao/viewTrabalhoConclusao.jsf?popup=true&id_trabalho=8370406. Acesso em: 07 jun. 2025.

WITCHER, Rob. Threat Modeling Methodologies: STRIDE, PASTA, DREAD and More. **Destination Certification**, 27 jan. 2025. Disponível em: https://destcert.com/resources/threat-modeling-methodologies. Acesso em: 07 jun. 2025.

YAGA, Dylan et al. **Blockchain Technology Overview**. Gaithersburg: National Institute of Standards and Technology, 2018. (NISTIR 8202). Disponível em: https://doi.org/10.6028/NIST.IR.8202. Acesso em: 08 jun. 2025.

ZANON, Gustavo Henrique Muriel. **Técnicas de compressão de chaves para criptossistemas baseados em isogenias**. 2021. Dissertação (Mestrado em Ciência da Computação) – Escola Politécnica da Universidade de São Paulo, São Paulo, 2021. Disponível em: https://sucupira-legado.capes.gov.br/sucupira/public/consultas/coleta/trabalhoConclusao/viewTrabalhoConclusao.jsf?popup=true&id_trabalho=10800360. Acesso em: 07 jun. 2025.