ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP INF ANDRÉ FELIPE DRUMMOND SALVADOR

A COMPUTAÇÃO QUÂNTICA APLICADA À DEFESA CIBERNÉTICA: ANÁLISE SOBRE SUAS CAPACIDADES DE EXPLORAÇÃO NO ESPAÇO CIBERNÉTICO

Rio de Janeiro
2019

ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP INF ANDRÉ FELIPE DRUMMOND SALVADOR

A COMPUTAÇÃO QUÂNTICA APLICADA À DEFESA CIBERNÉTICA:
UMA ANÁLIE DE SUAS CAPACIDADES DE EXPLORAÇÃO NO ESPAÇO CIBERNÉTICO

Trabalho acadêmico apresentado à Escola de Aperfeiçoamento de Oficiais, como requisito para a especialização em Ciências Militares com ênfase em Gestão Operacional.

Rio de Janeiro
2019

A COMPUTAÇÃO QUÂNTICA APLICADA À DEFESA CIBERNÉTICA: UMA ANÁSILE SOBRE SUAS CAPACIDADES DE EXPLORAÇÃO NO ESPAÇO CIBERNÉTICO

André Felipe Drummond Salvador[*]
Samuel Schilling da Silveira[**]

RESUMO
No presente trabalho, buscou-se apresentar uma visão sobre o impacto da computação quântica quando aplicada a atividades ligadas a defesa cibernética, mais especificamente na criptografia. Sua finalidade é alertar quanto à necessidade da Força Terrestre se antever a possíveis vulnerabilidades em relação a essa nova tecnologia. Para tanto, esse artigo foi desenvolvido, de fevereiro a setembro de 2019, por meio de uma pesquisa bibliográfica e qualitativa, utilizando-se, também, os recursos pesquisa e entrevista. A fim de ampliar a sua compreensão, este trabalho apresenta comentários sobre princípios de computação e criptografia. São abordados aspectos teóricos da segurança das informações, particularmente, a forma como as informações são mantidas seguras no ambiente cibernético. Discorre-se sobre a possibilidade da computação quântica configurar-se como uma ameaça e a necessidade de adoção de novas formas de manter a segurança das informações no espaço cibernético no futuro, contribuindo para a capacidade da Força Terrestre de defesa cibernética. A preocupação de buscar identificar ameaças potenciais reside no fato de que, no cenário atual, essas ameaças são caracterizadas por sua incerteza, mutabilidade e volatilidade e pela importância da atividade cibernética como meio de exercício do Comando e Controle (C^2) em todos os escalões, em especial os escalões mais altos, pois normalmente encontram-se a grandes distâncias de seus escalões subordinados. Na conclusão, as ideias expressas ao longo deste trabalho são ratificadas, enfatizando-se a importância da adoção de medidas de proteção cibernética.

Palavras-chave: Defesa cibernética. Identificação de ameaças. Computação quântica. Espaço cibernético.

ABSTRACT
An attempt to present a vision on the impact of quantum computing applied to activities related to cyber defense, more specifically in cryptography, was made in the present work. It's purpose is to alert of the Land Force's need to anticipate possible vulnerabilities in relation to this new technology. For that, this article was developed, from February to September of 2019, through a bibliographical and qualitative research, also using the research and interview resources. In order to broaden their understanding, this paper presents comments on principles of computation and encryption. It addresses theoretical aspects of information security, particularly on how information is kept secure in the cyber environment. It is argued the possibility of quantum computing be set as a threat and the need to adopt new ways of maintaining information security in cyberspace in the future, contributing to the ability of the cyber defense Land Force. The concern to identify potential threats lies in the fact that, in the current scenario, these threats are characterized by their uncertainty, mutability and volatility and by the importance of cybernetic activity as a means of exercising Command and Control (C^2) at all levels, especially the upper echelons, since they are usually at great distances from their subordinate echelons. In conclusion, the ideas expressed throughout this work are ratified, emphasizing the importance of adopting cybernetic protection measures.
Keywords: Cyber defense. Threat identification. Quantum computing. Cyber space.

[*] Capitão da Arma de Infantaria. Bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN) em 2009. Mestre em Ciências Militares pela Escola de Aperfeiçoamento de Oficiais (AMAN) em 2019.
[**] Capitão da Arma de Infantaria. Bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN) em 2006. Mestre em Ciências Militares pela Escola de Aperfeiçoamento de Oficiais (AMAN) em 2015.

1 INTRODUÇÃO

Ao redor de todo o globo, são criados, por dia, 2,5 exabytes (o equivalente a 2,5 bilhões de gigabytes) de dados, permeando e tornando cada vez maior o espaço cibernético (IBM, 2016, p. 3). Com base nessa quantidade de dados criados diariamente, é estimado que 90% de todos os dados foram gerados nos últimos 2 anos (IBM, 2016, p. 3).

Conforme SILVA (2014, p. 200) “o objetivo básico, seja no nível estratégico, tático ou operacional, em uma guerra cibernética, é a informação.”. Portanto, esse crescimento no aumento da produção de dados, sejam estes militares ou não, torna as ações no ambiente cibernético propícias para a atividade de inteligência.

O ambiente cibernético só é um ambiente seguro graças à utilização de métodos criptográficos, garantindo que as informações que lhe perpassam estejam protegidas. Os sistemas criptográficos atuais garantem a proteção dos dados pelo uso de algoritmos (conjunto de regras e procedimentos matemáticos) que necessitam de pouco tempo para criptografar, porém, sem a posse da chave correta para desfazer a operação, requer uma quantidade de tempo que em alguns casos superam até mesmo a idade do universo (KIRSCH, 2015, p. 3).

O espaço cibernético tem se apresentado como um ambiente operacional que ultrapassa as três dimensões físicas, acrescentando uma quarta dimensão ao ambiente operacional no combate moderno, onde são travadas batalhas por informações e liberdade de utilização (BRASIL, 2017, Prefácio). Vendo a importância desse novo campo de batalha, a Estratégia Nacional de Defesa (END), em dezembro de 2008, estabeleceu o Setor Cibernético como prioridade para a Defesa Nacional (BRASIL, 2014, p. 14).

A fim de assegurar a capacidade de utilizar seus dispositivos computacionais em segurança, o Exército Brasileiro (EB), busca, de forma permanente, analisar conjunturas e cenários possíveis (BRASIL, 2015, p. 19). Portanto, deve-se sempre buscar a identificação de potenciais ameaças procurando possíveis métodos de proteção ante estas potenciais ameaças.

1.1 PROBLEMA

No momento presente, os computadores não possuem uma capacidade computacional suficientemente grande para permitir a quebra de um sistema criptográfico atual (KIRSCH, 2015, p. 4). Sem uma máquina que seja capaz de

quebrar tais sistemas, estes são capazes de manter seguras as informações que circulam no espaço cibernético.

Porém, um modelo de computador, proposto em 1982 por Richard P. Feynman, baseado em princípios da mecânica quântica, possui características que fazem com que a sua capacidade computacional cresça de maneira exponencial (HAYWARD, 1999, p. 12). Sendo capaz de crescer dessa maneira, um computador desse modelo pode ser capaz de quebrar determinados modelos criptográficos, tão logo atinja níveis de desenvolvimento necessários.

A fim de manter a capacidade de proteção do espaço cibernético, foi formulado o seguinte problema:

Com o desenvolvimento tecnológico da computação quântica, qual é a atual capacidade da mesma para a realização de ações de exploração cibernética no espaço cibernético?

1.2 OBJETIVOS

A fim de estudar o impacto do desenvolvimento da computação quântica nos sistemas de segurança criptográficos, o presente estudo pretende analisar a atual capacidade da computação quântica como um meio para a condução de ações de exploração no espaço cibernético.

Para viabilizar a consecução do objetivo geral de estudo, foram formulados os objetivos específicos, abaixo relacionados, que permitiram o encadeamento lógico do raciocínio descritivo apresentado neste estudo:

a. Descrever o modo de funcionamento dos computadores clássicos e dos quânticos;

b. Descrever o funcionamento da criptografia no espaço cibernético;

c. Apresentar a capacidade de um computador quântico aplicado à guerra cibernética;

d. Analisar as possibilidades da computação quântica quando usada para ações de exploração cibernética; e

e. Citar medidas que aumentem a capacidade defensiva a ataques que utilizem a tecnologia da computação quântica.

1.3 JUSTIFICATIVAS E CONTRIBUIÇÕES

A Defesa Cibernética deve manter-se constantemente preparada para

proteger o espaço cibernético de ameaças atuais e futuras. Para tanto, é fundamental o estudo de potenciais ameaças, mesmo que não representem riscos significativos nos dias atuais.

A existência de vulnerabilidades em sistemas computacionais constitui uma das limitações da Defesa Cibernética. Portanto, a identificação de possíveis vulnerabilidades deve ser feita para que se busquem meios e/ou técnicas a fim de minimizar o risco de um possível ataque no espaço cibernético.

Nesse sentido, o presente estudo se justifica por promover uma pesquisa a respeito de um tema atual e de suma importância para a evolução do poderio bélico das pequenas frações do EB até o escalão SU, do qual se espera um importante papel no cenário dos conflitos urbanos.

O trabalho pretende, ainda, abastecer os gestores dos projetos de modernização, independente da nomenclatura atribuída, de conhecimento acerca das necessidades dos combatentes para operar no cenário urbano, servindo de pressuposto teórico para outros estudos que sigam nesta mesma linha de pesquisa.

2 METODOLOGIA

Para colher subsídios que permitissem formular uma possível solução para o problema, o delineamento desta pesquisa contemplou leitura analítica e fichamento das fontes, entrevistas com especialistas, questionários, argumentação e discussão de resultados.

Quanto à forma de abordagem do problema, utilizaram-se, principalmente, os conceitos de pesquisa **qualitativa**, devido ao publico alvo restrito, pois trata-se de um tema técnico e especifico, não sendo possível quantificar dados através de pesquisa.

Quanto ao objetivo geral, foi empregada a modalidade **exploratória**, tendo em vista o pouco conhecimento disponível, notadamente escrito, acerca do tema, o que exigiu uma familiarização inicial, materializada pelas entrevistas exploratórias

2.1 REVISÃO DE LITERATURA

Iniciamos o delineamento da pesquisa com a definição de termos e conceitos, a fim de viabilizar a solução do problema de pesquisa, sendo baseada

em uma revisão de literatura no período de jan/1982 a abr/2013. Essa delimitação baseou-se na necessidade de atualização do tema, visto que as tecnologias se encontram em constante evolução e uma grande preocupação com o tema iniciou-se na década passada.

2.1.1 Doutrina Militar de Defesa Cibernética – Conceituação e Princípios

O Manual de Guerra Cibernética (EB 70-MC-102.32) define o espaço cibernético como sendo:

> Um domínio global dentro da dimensão informacional do ambiente operacional que consiste em uma rede interdependente de infraestruturas de Tecnologia da Informação e Comunicações (TIC) e de dados, incluindo a internet, redes de telecomunicações, sistemas de computador, processadores embarcados e controladores (BRASIL, 2017, prefácio).

Portanto o espaço cibernético compreende não somente os dados, mas também todo o sistema físico que processa, transmite e armazena os dados informatizados.

Conforme o EB 70-MC-102.302, a segurança da informação e comunicações (SIC) tem por finalidade garantir quatro propriedades para os dados e informações: disponibilidade, integridade, confidencialidade e autenticidade (BRASIL, 2017, p. 2-3). A primeira visa garantir a acessibilidade da informação, sob demanda, por um determinado agente. A integridade objetiva impedir a modificação da informação de forma não autorizada. A confidencialidade nega o acesso por parte de agentes não autorizados à informação. Por fim, a autenticidade garante a identificação do agente que realizou qualquer alteração na informação (BRASIL, 2017, p. 2-3).

Apesar de compartilhar com os princípios de guerra já estabelecidos pelo Exército Brasileiro, a guerra cibernética possui 04 (quatro) princípios de emprego que lhe são peculiares: efeito, dissimulação, rastreabilidade e adaptabilidade (BRASIL, 2017, p. 2-3).

Sobre o princípio do efeito o EB 70-MC-102.302 diz que “as ações cibernéticas devem produzir efeitos que se traduzam em vantagem estratégica,

operacional ou tática que afetem o mundo real, mesmo que os efeitos não sejam cinéticos (BRASIL, 2017, p. 2-4)".

Silva exemplifica alguns objetivos de ações cibernéticas que podem trazer tais vantagens. No nível estratégico: sistemas de energia, financeiros e infraestrutura social; no nível operacional: sistemas de C2; e no nível tático: sistemas de apoio à decisão e logística (SILVA, 2014, p. 200).

O princípio da dissimulação é o conjunto de medidas que buscam dificultar o rastreamento das ações realizadas contra oponentes, mascarando o ponto de origem e a autoria da ação (BRASIL, 2017, p. 2-4). De forma antagônica, o princípio da rastreabilidade constitui-se das medidas adotadas para rastrear e detectar as ações cibernéticas realizadas contra um sistema de informação amigo (BRASIL, 2014, p. 2-4).

O princípio da adaptabilidade consiste na habilidade de adaptar-se às mudanças do espaço cibernético, a fim de manter suas capacidades mesmo com mudanças rápidas e imprevisíveis (BRASIL, 2017, p. 2-4).

A guerra cibernética, devido à sua atividade especializada, possui características que lhe são peculiares. O MD 31-M-07 (Doutrina Militar de Defesa Cibernética) apresenta 10 (dez): insegurança latente, alcance global, vulnerabilidade das fronteiras geográficas, mutabilidade, incerteza, dualidade, paradoxo tecnológico, dilema do atacante, função assessoria e assimetria (BRASIL, 2014. p. 20/36).

A característica de insegurança latente diz respeito ao fato da inexistência de um sistema computacional completamente seguro, visto que a busca e a exploração dessas vulnerabilidades nestes tipos de sistemas serão sempre alvos de ameaças cibernéticas (BRASIL, 2014, p. 21/36).

Quanto o alcance global, os limites físicos de distância não afetam a capacidade da atividade cibernética de conduzir ações com alcance em todo o globo, de maneira simultânea, e a partir de diferentes frentes (BRASIL, 2014, p. 21/36).

A vulnerabilidade das fronteiras geográficas diz respeito ao fato de que os agentes podem atuar em qualquer local para produzir efeitos em outro lugar qualquer, fazendo com que as ações de Defesa Cibernética não se restrinjam a fronteiras geograficamente definidas (BRASIL, 2014, p. 21/36).

A doutrina atual atribui 03 (três) capacidades operativas à capacidade militar terrestre cibernética, elas são: proteção, ataque e exploração cibernética (BRASIL, 2017 p. 3-4).

A capacidade operativa de proteção cibernética é a capacidade de realizar ações para neutralizar os ataques e explorações cibernéticas feitas contra os nossos ativos da informação, devendo ser uma atividade de caráter permanente (BRASIL, 2017, p. 3-4).

A capacidade operativa de exploração cibernética refere-se à capacidade de realizar ações de busca e/ou coleta de dados em sistemas de interesse, objetivando a obtenção de dados (BRASIL, 2017, p. 3-4).

2.1.2 O Bit e o Qubit

O Dígito Binário (Bit) é o bloco fundamental de construção das informações em um computador clássico (HAYWARD, 1999, p. 8). Um bit é a representação de uma peça de informação, a qual pode assumir o valor de 0 ou 1, que é gravado em um chip de silício ou em um disco de metal de um disco rígido, formando uma sequência de bits que codificam as informações (HAYWARD, 1999, p. 8).

Já o computador quântico utiliza bits quânticos (qubits) como bloco fundamental para a construção das informações (LI et al, 2001). O qubit opera utilizando um princípio da mecânica quântica chamada superposição, permitindo que ele exista simultaneamente no estado de 1 e 0, permitindo que seu cálculos sejam realizados de forma paralela (KIRSCH, 2015, p. 5.).

Dessa maneira, um computador quântico composto por dois qubits é capaz de representar quatro estados (00, 01, 10 e 11) ao mesmo tempo, efetivamente realizando quatro operações simultâneas (KIRSCH, 2015, p. 5.). Aumentando o computador para N qubits, este será capaz de realizar 2^n operações simultâneas, portanto, um computador quântico com um processador de 1000 qubits tem a capacidade de realizar $2^{1000} \approx 10^{301}$ operações simultâneas (KIRSCH, 2015, p. 5.).

Tabela 1 - Tabela de equivalência entre qubits e bits

Qubits	Bits	Qubits	Bits
1 qubit	2 bits	13 qubits	8.192 bits (1 kibibyte)
2 qubits	4 bits	23 qubits	8.388.608 bits(1 mebibyte)
3 qubits	8 bits (1 byte)	33 qubits	8.589.934.592 bits (1 gibibyte)
5 qubits	32 bits	43 qubits	8.796.093.022.208 bits (1 tebibyte)
10 qubits	1.024 bits	*N* qubits	2^n bits

Fonte: O Autor

2.1.2 A CRIPTOGRAFIA NO ESPAÇO CIBERNÉTICO

Conforme Guimarães (2001, p. 16), a segurança de um processo criptográfico é determinada por sua chave, e não pela técnica empregada. Guimarães (2001, p. 18) ainda diz que os algoritmos de criptografia dependem de uma variável, a chave, a qual funciona como uma senha, visto que somente com ela será possível reverter o processo criptográfico, e que possuem 02 (duas) classificações: simétrica (ou secreta) e assimétrica (ou pública).

Por muito tempo a criptografia foi baseada em um emissor e um receptor que possuíam e utilizavam uma mesma chave, tanto para criptografar quanto para decriptografar uma mensagem, este método ficou conhecido como criptografia de chave secreta (FANH, 1993, p.2). Este modelo criptográfico possui uma grande deficiência no tocante à segurança da chave, a qual corria o risco de ser interceptada, comprometendo a segurança da criptografia das mensagens (GUIMMARÃES, 2001, p. 19).

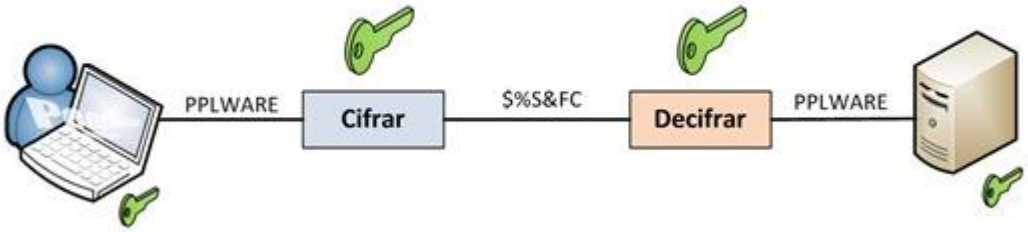

IMAGEM 1 – Criptografia de chave secreta

Fonte: https://pplware.sapo.pt/tutoriais/networking/criptografia-simetrica-e-assimetrica-sabe-a-diferenca/

A segurança de uma chave cresce de forma exponencial em relação ao seu tamanho em bits, portanto uma chave com 10 bits possui 1.024 combinações distintas, com 20 bits serão 1.048.576 possibilidades e com 40 bits as combinações chegam a 1.099.511.627.776 chaves distintas (GUIMARÃES, 2001, p. 17).

Como solução a esta deficiência, Whitfield Diffie e Martin Hellman criaram, no ano de 1976, a criptografia de chave pública (GUIMARÃES, 2001, p. 21). Neste novo sistema existem dois tipos de chaves: as chaves públicas e as chaves privadas. As chaves públicas são divulgadas, podendo qualquer pessoa conhece-la, e utilizadas para codificar as mensagens, ao passo que as chaves privadas são mantidas em segredo e são utilizadas para decriptografar as mensagens (FANH, 1993, p. 2).

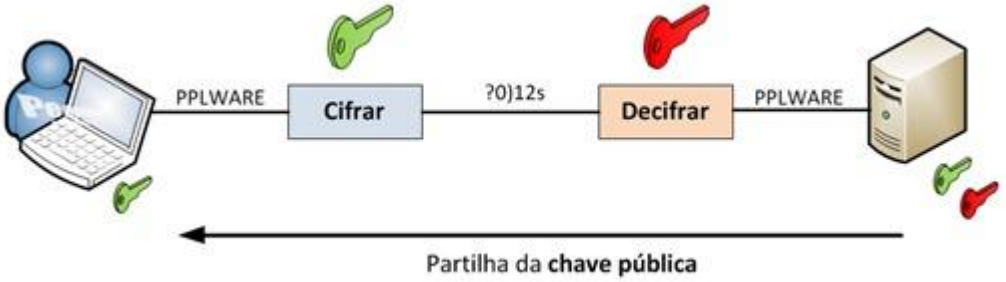

Imagem 2 – Criptografia de chave pública

Fonte: https://pplware.sapo.pt/tutoriais/networking/criptografia-simetrica-e-assimetrica-sabe-a-diferenca/

No ano de 1977, o trio composto por Ron Rivest, Adi Shamir e Leonard Adleman criou um modelo de criptografia de chave pública que ainda hoje é amplamente utilizado e foi batizado em homenagem aos três, o modelo RSA (GUIMARÃES, 2001, p. 21).

Conforme Fanh (1993, p. 5), o modelo RSA funciona seguindo-se algumas etapas: multiplicar dois números primos grandes, *p* e *q*, encontrando o seu produto *n* (modulo); escolher um número, *e* (expoente publico), menor do que n e seu respectivo inverso, *d* (expoente privado), sendo que (*n*, *e)* compõe a chave publica, *d* é a chave privada e os fatores (*p*, *q*) devem ser guardados ou destruídos.

Como disse Silva (2005, p. 4), a segurança do sistema RSA está no fato de que a fatoração de um número muito grande em números primos é um problema difícil de ser resolvido. A maneira mais trivial de se obter a chave privada, *d*, é fatorar o módulo *n* em seus fatores primos *p* e *q*, a partir dos quais, juntamente com o expoente público, é possível calcular de maneira fácil a chave privada (FANH, 1993, p. 7).

TABELA 2 – Tempo de multiplicação x fatoração

Bits no input (Qtd)	Tempo necessário para fatorar	Tempo necessário para multiplicar
25	0,00081 segundos	0,00801 segundos
50	0,15767 segundos	0,03204 segundos
75	6,34809 segundos	0,07208 segundos

100	2 minutos 0,30708 segundos	0,12815 segundos
512	49.093 anos 3 meses 2 dias 16 horas 14 minutos 36 segundos	3,35936 segundos
1024	89.236.889.743 anos 10 meses 19 dias 2 horas 47 minutos 16 segundos	13,43744 segundos
2048	6.871.455.104.760.850.000 anos 1 mês 20 dias 16 horas 52 minutos 48 segundos	53,74975 segundos

Fonte: Khan Academy

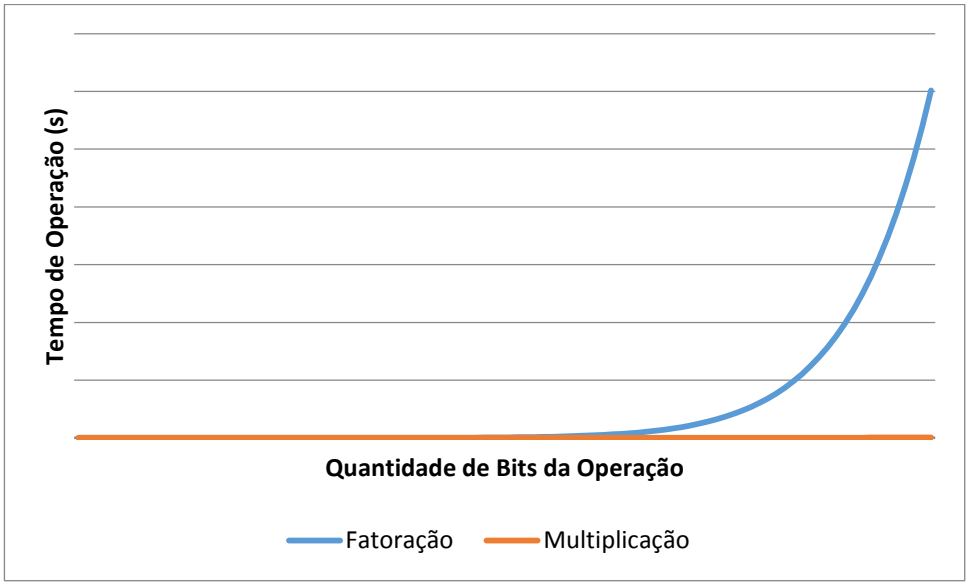

GRÁFICO 1 – Tempo de multiplicação x fatoração

Fonte: Khan Academy

Como é possível ser observado tanto na Tabela 2 quanto no Gráfico 1, a fatoração torna-se um problema exponencialmente complexo à medida que aumenta-se o tamanho da chave. Portanto, criar uma chave através de um processo de multiplicação é uma tarefa fácil de ser computada, ao passo que fatorar essa chave é um processo praticamente impossível de ser computado com os *hardwares* e algoritmos existentes atualmente.

2.1.3 A APLICAÇÃO DA COMPUTAÇÃO QUÂNTICA NA DEFESA CIBERNÉTICA

Como dito por Valadares (2009, p.1), a computação quântica destaca-se por sua capacidade de processar, simultaneamente, todas as permutações de *n* bits usando seu circuito lógico, tornando triviais problemas de tentativa e erro para os

computadores clássicos. De acordo com Hayward (1999, p. 15), o trabalho do cientista Peter Shor, no ano de 1994, resultou em um algoritmo para fatorar números grandes em computadores quânticos, atraindo a atenção esse campo.

Hayward (1999, p. 54), em seu trabalho, mostra passo a passo o funcionamento do algoritmo de Shor, inclusive com uma simulação em um computador clássico da fatoração do número 17. Porém Proos (2008, p. 26) apresenta que são necessários um total de aproximadamente 2*n* qubits para quebrar uma chave RSA de *n* bits, como apresentado na tabela 2 abaixo:

Tabela 2 - Tabela de equivalência entre qubits e bits

Algoritmo de Fatoração (RSA)	
N	Número de qubits (Aprox)
	2n
512	1024
1024	2048
2048	4096

Fonte: Proos (2004, p. 26)

Outro trabalho com aplicação em criptografia é o algoritmo de Grover. GRASSL et al (2015, p. 1) afirmam que este algoritmo possui a capacidade de encontrar uma chave simétrica em um tempo equivalente à raiz quadrada do tempo de um computador clássico levaria para cumprir essa mesma tarefa.

Nesse mesmo trabalho, GRASSL et al (2015, p. 11), oferecem uma estimativa de recursos necessários para realizar um ataque a um sistema criptográfico de chave simétrica AES, conforme a tabela abaixo:

Tabela 2 - Tabela de estimativas de recursos para o Algoritmo de Grover atacar AES-*k*

Tamanho da chave (k)	Quantidade de qubits necessários
128	2.953
192	4.449
256	6.681

Fonte: GRASSL et al (2015, p. 11)

a. Critério de inclusão:

- Estudos publicados em português ou inglês, relacionados à guerra cibernética, computação quântica, segurança da informação e programas de modernização militar;

- Estudos, matérias jornalísticas e portfólios de empresas que retratam inovações tecnológicas com reflexos na defesa cibernética; e

- Estudos qualitativos sobre as características do espaço cibernético.

b. Critério de exclusão:

- Estudos que abordam o emprego da computação quântica para atividades de defesa e de ataque cibernético; e

- Estudos cujo foco central seja relacionado estritamente à descrição tecnológica e/ou aos equipamentos militares com finalidade distinta do presente estudo.

2.2 COLETA DE DADOS

Na sequência do aprofundamento teórico a respeito do assunto, o delineamento da pesquisa contemplou a coleta de dados por meio de entrevista exploratória.

2.2.1 Entrevistas

Com a finalidade de ampliar o conhecimento teórico e identificar experiências relevantes, foram realizadas entrevistas exploratórias com os seguintes especialistas, em ordem cronológica de execução:

Nome	Justificativa
BRUNO RODRIGUES BARBOSA CÔRTES – Cap EB	Especialista em defesa cibernética e instrutor do curso de defesa cibernética
BRUNO AGOSTINHO OLIVEIRA SANTOS – Cap EB	Especialista em defesa cibernética

QUADRO 1 – Quadro de Especialistas entrevistados

Fonte: O autor

3 RESULTADOS E DISCUSSÃO

Após relacionar os recursos necessários para tornar os principais modelos criptográficos atuais obsoletos, é necessário saber a quantidade de recursos disponíveis atualmente para determinar se a computação quântica possui a capacidade de quebrar uma chave criptográfica.

Ao ser feito o levantamento por meio de fontes abertas, é possível verificar alguns computadores quânticos que já foram anunciados, destacando-se o computador da empresa IonQ, com o capacidade de processar 79 qubits, seguindo-se o processador quântico do Google, com 72 qubits. Tendo em vista que o requerimento para quebrar uma chave assimétrica é equivalente a 2*n*, os computadores quânticos atuais seriam capazes de quebrar apenas chaves inferiores a 40 bits. As chaves assimétricas empregadas de forma mais ampla atualmente normalmente possuem 512, 1024 ou até 2048 bits, por consequência, é possível afirmar que os computadores quânticos atuais não possuem a capacidade de quebrar uma chave assimétrica nos dias de hoje.

Apesar de não ter sido estabelecida uma relação matemática entre o tamanho de uma chave simétrica e a quantidade de qubits necessários para quebrar tal chave, é facilmente observável que, mesmo para a menor chave simétrica apresentada (128 bits), há uma defasagem muito grande entre a quantidade de qubits para quebra-la (2.953 qubits) e a existente nos computadores quânticos atuais. Com base nesses dados, conclui-se que a computação quântica não é capaz de quebrar as chaves simétricas existentes atualmente.

A fim de antecipar possíveis ameaças, é preciso analisar os possíveis efeitos advindos do cenário em que um computador quântico, mesmo que não seja capaz hoje em dia, atinja a capacidade de quebrar as chaves empregadas no presente, de forma a ser possível responder oportuna e adequadamente a este tipo de ameaça, conforme diz a Doutrina Militar de Defesa Cibernética (BRASIL, 2014, p. 13/36).

Segundo CÔRTES, as chaves assimétricas são empregadas principalmente para realizar a autenticação entre os ativos da informação e o compartilhamento seguro de chaves simétricas (informação verbal). Como este tipo de chave é usada para autenticação, o seu comprometimento pode acarretar em perda de autenticidade nas informações.

Conforme dito por CÔRTES, as chaves simétricas são utilizadas para realizar a criptografia dos dados transmitidos entre os ativos da informação de forma segura (informação verbal). No caso de comprometimento da chave simétrica, seria possível obter todas as informações que forem transmitidas por um determinado ativo da informação, resultando na perda da confidencialidade dos dados e informações.

Dentro do escopo deste trabalho, não foi possível identificar nenhuma capacidade da computação quântica que possa afetar a disponibilidade e/ou a integridade dos dados no meio cibernético.

No escopo dos princípios de emprego da guerra cibernética, a computação quântica não consegue produzir, nos dias atuais, efeitos que afetem o mundo real, visto que em seu estágio de desenvolvimento atual é incapaz de quebrar qualquer tipo de chave criptográfica empregada.

No tocante aos princípios de dissimulação e rastreabilidade não é possível tirar conclusões devido ao fato de não terem sido encontradas fontes contendo dados pertinentes aos respectivos princípios mencionados.

Como visto anteriormente, um dos fatores que atraiu a atenção para o desenvolvimento da computação quântica foi o algoritmo de Shor, bem como o algoritmo de Grover, ambos com a possibilidade de afetar a segurança dos modelos criptográficos atuais. Mesmo que a computação quântica não possa produzir efeitos reais agora, os algoritmos de Shor e de Grover, combinados com o desenvolvimento deste tipo de tecnologia, compõem uma vulnerabilidade dos ativos da informação atual, podendo aumentar a insegurança latente a medida que o poder computacional desse tipo de máquina for aumentando.

Apesar de ser uma tecnologia que ainda encontra-se em desenvolvimento, já existem computadores quânticos que estão integrados ao espeço cibernético, com destaque para o projeto IBM Q, aonde são disponibilizados máquinas com até 32 qubits através da nuvem para a experimentação de circuitos. Mesmo que seja possível acessar um computador desse tipo a partir de qualquer parte do globo, essa tecnologia ainda não possui alcance global, visto que as suas ações ainda são muito restritas para fins de pesquisa, bem como não haver histórico de ações cibernéticas com essa tecnologia aonde se ultrapassem as fronteiras geográficas.

4 CONSIDERAÇÕES FINAIS

Quanto às questões de estudo e objetivos propostos no início deste trabalho, conclui-se que a presente investigação atendeu ao pretendido, ampliando a compreensão sobre a capacidade de exploração cibernética da computação quântica no espaço cibernético, o qual vem ganhando grande importância no campo de batalha nos últimos anos.

A revisão de literatura possibilitou identificar as principais características do computador quântico e suas aplicações no espaço cibernético, alinhando o que foi apresentado com a doutrina militar de defesa cibernética, possibilitando concluir que no atual estágio de desenvolvimento a computação quântica é incapaz de realizar ações de exploração cibernética, não se constituindo como uma ameaça de forma imediata, mas que constitui uma ameaça potencial à medida que avançar.

Dessa forma, entende-se que é necessário acompanhar o desenvolvimento desta tecnologia a fim de permitir que seja possível responder adequadamente e oportunamente, preservando a capacidades cibernéticas da Força Terrestre frente a esta possível ameaça.

Recomenda-se, assim, que sejam realizados estudos no futuro que permitam identificar soluções para aumentar o nível de segurança das informações no espaço cibernético, permitindo sua proteção mesmo no cenário em que a computação quântica atinja os níveis que a possibilite ameaçar as chaves empregadas atualmente.

Conclui-se, portanto, que o computador quântico é um ativo da informação que ainda não tem possibilidades como meio de realizar ações exploratórias no ambiente cibernético, porém não deve ser ignorada, pois com o seu desenvolvimento ela poderá adquirir tais capacidades, configurando-se como uma potencial ameaça, sendo interessante a busca por novos processos de criptografia que consigam elevar a capacidade de proteção dos dados no ambiente cibernético.

REFERÊNCIAS

BRASIL. Exército. **EB20-C-07.001: Catálogo de Capacidades do Exército**. 1. ed. Brasília, DF, 2015. Disponível em <http://bdex.eb.mil.br/jspui/123456789/433>. Acesso em: 23 mar. 19

_____. _____. **EB70-MC-10.232: Guerra Cibernética**. 1. ed. Brasília, DF, 2017. Disponível em <http://bdex.eb.mil.br/jspui/handle/1/631>. Acesso em: 18 mar. 19

_____. _____. **C 20-1: Glossário de Termos e Expressões para uso no Exército**. 3. ed. Brasília, DF, 2003.

_____. Ministério da Defesa. **MD31-M-M-07: Doutrina Militar de Defesa Cibernética.** 1 ed. Brasília, DF, 2014.

DA SILVA, Fernanda Taline; PAPANI, Fabiana Garcia. **Um Pouco da História da Criptografia.** In: XXII Semana Acadêmica da Matemática.

DOVICCHI, João Cândido Lima. **Alguns Bits de Qubits: Uma Introdução Sobre Bits Quânticos.** Florianópolis – SC, 2015.

FAHN, Paul. **Answers to Frequently Asked Questions About Today's Cryptography.** Redwood City, 1993.

FEYNMAN, Richard P. Simulating Physics with Computers. **International Journal of Theoretical Physics**, Pasadena, v. 21, p. 467-488. 1982.

GRASSL, Markus; LANGENBERG, Brandon; ROETTELER, Martin; STEINWANDT, Rainer. **Applying Grover's algorithm to AES: quantum resources estimates.** 2015.

GUIMARÃES, Carla Rocha. **Criptografia para Segurança de Dados.** Uberlândia. 2001

HAYWARD, Matthew. **Quantum Computing and Shor's Algorithm.** 1999.

KHAN ACADEMY. **Time Complexity (Exploration)**. Disponível em: <https://www.khanacademy.org/computer-programming/time-complexity-exploration/1466763719>

KIRSCH, Z. **Quantum Computing: The Risk to Existing Encryption Methods**. 2015. Disponível em: <http://www.cs.tufts.edu/comp/116/archive/fall2015/zkirsch.pdf>. Acesso em: 18 mar. 19

LI, Shu-Shen et al. Quantum computing. **Proceedings of the National Academy of Sciences**, v. 98, n. 21, p. 11847-11848, 2001.

NICOLIELLO, Heitor. **Introdução à Computação Quântica.** 2009.

PINHEIRO, Alexandre. **O Emprego da Fonte Cibernética para a Produção de Conhecimentos de Inteligência, no Nível Estratégico.** 2018. 28 f. Trabalho de Conclusão de Curso (Especialização em Ciências Militares) – Escola de Aperfeiçoamento de Oficiais, Rio de Janeiro, 2018.

PRESKILL, John. **Quantum Computing: Pro and Con.** Pasadena, 1998.

PROOS, John; ZALKA, Christof. **Shor's Discrete Logarithm Quantum Algorithm for Elliptic Curves**. Department of Combinatorics and Optimization University of Waterloo, Waterloo, 2008

RIGOLIN, Gustavo; RIEZNIK, Andrés Anibal. Introdução à Criptografia Quântica. **Revista Brasileira de Ensino de Física**, Campinas, v. 27, n.4, p. 517-526. 2005

SILVA, Cezar Barreto Leite. Guerra Cibernética: A Guerra do Quinto Domínio, Conceituação e Princípios. **Revista Escola Guerra Naval**, Rio de Janeiro, v. 20, n. 1, p. 193-211, jan/jun 2014.

SILVA, Eduardo Augusto Moraes. **Um estudo do sistema criptográfico RSA**. Disponível em: <http://www.ucb.br/sites/100/103/TCC/12005/EduardoAugustoMoraesSilva.pdf> Acesso em: 23 mar. 2019.

SOUSA, Pedro Henrique de Oliveira. **Análise do Desenvolvimento de Capacidades em Operações Cibernéticas Ofensivas**. 2018. 21 f. Trabalho de Conclusão de Curso (Especialização em Ciências Militares) – Escola de Aperfeiçoamento de Oficiais, Rio de Janeiro, 2018.

STORI, F. T. S.; PAPANI, F. M. G. **Um pouco da história da criptografia**. 2008. Disponível em: <http://projetos.unioeste.br/cursos/cascavel/matematica/xxiisam/artigos/16>. Acesso em: 23 mar. 2019

VALADARES, A. R. S.; BACHMANN, D. E.; JÚNIOR, R. B. **Computação Quântica**. 2009.

ANEXO A: Solução Prática

A presente pesquisa concluiu que “o computador quântico é um ativo da informação que ainda não tem possibilidades como meio de realizar ações exploratórias no ambiente cibernético, porém não deve ser ignorada, pois com o seu desenvolvimento ela poderá adquirir tais capacidades, configurando-se como uma potencial ameaça, sendo interessante a busca por novos processos de criptografia que consigam elevar a capacidade de proteção dos dados no ambiente cibernético.” Desta forma a gestão de risco deve ser o foco, no intuito de aumentar a capacidade das ações de defesa cibernética, em especial a defesa ativa e a pronta resposta a tal ameaça.

Para que a capacidade de defesa cibernética possa se manter atualizada no caso do amadurecimento tecnológico da computação quântica é importante que:

- Seja feito um acompanhamento do desenvolvimento do nível de maturidade desse tipo de tecnologia.

- Realizar estudos para melhorar a segurança oferecida no espaço cibernético, levando em conta o amadurecimento da computação quântica.