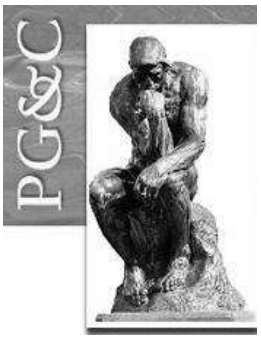


NECESSIDADES INFORMACIONAIS PARA FORMAÇÃO DA CONSCIÊNCIA SITUACIONAL EM OPERAÇÕES DE DEFESA CIBERNÉTICA NO BRASIL

José Ricardo Souza Camelo
Doutorando em Ciências da Informação pela Universidade de Brasília, Brasil.
E-mail: profcamelo@gmail.com

Lillian Maria Araújo de Rezende Alvares
Doutora em Ciências da Informação pela Universidade de Brasília, Brasil. Professora da Universidade de Brasília, Brasil.
E-mail: lillianalvares@unb.br

Resumo
Esta pesquisa tem por objetivo estabelecer os elementos norteadores essenciais para identificação de necessidades informacionais para o processo de formação da consciência situacional de defesa cibernética em operações militares. A metodologia do trabalho foi baseada em uma pesquisa de características descritiva, documental, bibliográfica, de observação participante e lidou com dados de natureza qualitativa. O resultado da pesquisa foi gerado a partir da correlação entre dois conjuntos de informações. O primeiro abrangeu os elementos teóricos oriundos da literatura científica e as referências advindas da literatura técnica e doutrinária pesquisada, enquanto o segundo foi composto da documentação sobre os fatos relevantes observados e das lições aprendidas nas operações militares de defesa cibernética. Como resultado, foram reconhecidos 35 elementos norteadores primordiais para identificação das necessidades informacionais. A conclusão do trabalho foi a concretização da possibilidade de se construir um conjunto de informações para subsidiar o conhecimento necessário à de consciência situacional de futuros comandantes de operações de defesa cibernética.

Palavras-chave: necessidades informacionais; gestão da informação; consciência situacional; Ciclo OODA; Defesa cibernética.

INFORMATIONAL NEEDS FOR SITUATIONAL AWARENESS PROCESS IN CYBER DEFENSE OPERATIONS

Abstract
This research aims to establish the essential guiding elements for identifying informational needs for situational awareness process in cyber defense operations. The methodology employed was based on a descriptive, documentary, bibliographic, and participant observation research, dealing with qualitative data. The research outcome resulted from the correlation between two sets of information. The first set encompassed theoretical elements from scientific literature and references from the researched technical and doctrinal literature, while the second set consisted of documentation on relevant observed events and lessons learned from military cyber defense operations. As a result, 35 essential guiding elements for identifying informational needs were recognized. The conclusion of the study confirms the feasibility of constructing a set of information to support the knowledge necessary for situational awareness in future commanders of cyber defense operations.

Keywords*: Informational needs; information management; situational awareness; OODA; cyber defense.*

1 INTRODUÇÃO

Em 2008, a publicação da Estratégia Nacional de Defesa – END (Brasil, 2008) estabeleceu as três maiores prioridades da Defesa Nacional para o país: o Setor Espacial, o Setor Nuclear e o Setor Cibernético. A escolha deste último, que é considerado um ramo do combate moderno, seguiu uma tendência mundial de que uma nação deve defender seus sistemas de informação no espaço cibernético para manter a sua soberania. Há mais de 20 anos o espaço cibernético vem sendo utilizado por criminosos, terroristas e até para a guerra.

Nesse sentido, especial atenção é dada às "infraestruturas críticas" (Brasil, 2009), tais como as estruturas telecomunicações, fornecimento de energia elétrica, energia nuclear, além de outras. Por meio de ataques cibernéticos contra essas infraestruturas, é possível comprometer os sistemas de informação que as sustentam e causar impactos muito severos a um país, comprometendo a sua capacidade de defesa.

O Setor Cibernético, como pode ser depreendido da END, é um conjunto de elementos heterogêneos abrangendo sistemas computacionais e suas redes, os processos, as tecnologias, as metodologias gerenciais, o pessoal, as normas técnicas, a legislação e os desenvolvimentos científicos envolvidos para processar, armazenar e transmitir os dados digitais críticos ao país. Esse setor estratégico foi priorizado pela END para que fossem desenvolvidos sistemas digitais de defesa da soberania nacional complementares aos mecanismos tradicionais de defesa da Nação.

As lições aprendidas no âmbito internacional dos confrontos militares demonstram a relevância desse setor na defesa nacional de qualquer país. Um exemplo de aplicação da cibernética como parte da estratégia de guerra se deu no conflito Rússia e Geórgia, em 2008, quando a capacidade de reação da Geórgia à invasão russa foi prejudicada devido a um ataque cibernético aos sistemas digitais do país (Clarke; Knake, 2010, p. 19).

No Brasil, desde 2011, uma série de operações militares reais e de treinamento ocorreram com emprego da cibernética. Destaque especial tiveram as operações de defesa e segurança cibernética nos chamados grandes eventos: a Conferência das Nações Unidas sobre o Desenvolvimento Sustentável (Rio + 20) (Vianna 2013, p. 127), a Copa das Confederações FIFA 2013 (Camelo; Carneiro, 2014, p. 149), a Jornada Mundial da Juventude 2013, a Copa do Mundo FIFA 2014 e os Jogos Olímpicos e Paralímpicos 2016. Em cada uma dessas operações, uma unidade temporária de combate, denominada Destacamento de Defesa e Segurança Cibernética, foi organizada pelo Exército Brasileiro e, em conjunto com as demais Forças Armadas, realizou uma ação coordenada com diversas agências de segurança da informação, inteligência e policiais para proteger os sistemas de informações digitais que suportavam esses eventos.

Em qualquer operação militar, o número de dados a serem processados é muito elevado e difícil de abranger e consolidar em termos da percepção humana. No contexto da defesa cibernética, o problema se eleva em magnitude de várias ordens de grandeza, uma vez que os sistemas de informação processam dados em quantidades e taxas inviáveis para o ser humano lidar diretamente. Nesse sentido, as operações de defesa cibernética, tais como as realizadas nos grandes eventos, demandam acompanhamento e integração de grande massa de dados a serem monitorados, de tal modo que seja viável ao comandante da operação ter consciência situacional sobre o que ocorre no espaço cibernético de interesse da missão.

Ao mesmo tempo, a consciência situacional só é alcançada de modo efetivo se a atenção do comandante for despertada conforme necessidade informacionais bem mapeadas previamente à missão. Neste artigo, o conceito de necessidades informacionais é empregado conforme a abordagem que Choo (1998, p. 26) utiliza, na qual se busca responder sobre o que

o indivíduo que possui a necessidade informacional precisa saber, além de mais seis desdobramentos desse questionamento. Apenas como exemplo de uma das definições existentes e que guarda uma forte compatibilidade com seu emprego neste artigo, pode-se citar o estabelecido no glossário da norma ISO/IEC/IEEE 15939, no qual se tem que necessidade informacional é um "entendimento necessário para gerir objetivos, metas, riscos e problemas (ISO/IEC/IEEE, 2007, p.3.12).

Desse modo, escolher adequadamente como mapear as necessidades informacionais de um comandante de uma operação de defesa cibernética, as quais definirão o que deve ser apreendido para a formação de sua consciência situacional, é um importante objeto de atenção e de difícil delimitação.

Em consequência, este artigo apresenta uma possível abordagem de como lidar com o problema da identificação das necessidades informacionais para a formação da consciência situacional de um comandante de uma operação de defesa cibernética. Assim, formulou-se o seguinte questionamento a ser respondido: como construir um conjunto de elementos essenciais para identificação das necessidades informacionais na formação da consciência situacional de um comandante de uma operação de defesa cibernética em nível estratégico para a Defesa Nacional brasileira?

Em consequência, o objetivo da pesquisa foi propor um conjunto de elementos essenciais para identificação das necessidades informacionais na formação da consciência situacional de um comandante de uma operação de defesa cibernética em nível estratégico para a Defesa Nacional brasileira.

A justificativa da escolha da temática que constitui o núcleo deste artigo se baseou na necessidade originada na área militar, não só brasileira, mas em âmbito internacional, de desenvolver conhecimentos para lidar com um recente campo na área de combate, ou seja, a cibernética. Especificamente, este trabalho enfocou as necessidades informacionais exigidas à formação da consciência situacional em operações de defesa cibernética e, assim, agregar valor às instâncias superiores de tomada de decisão do processo da Defesa Nacional. Para tal, a abordagem deste artigo tomou a área do conhecimento da Ciência da Informação como perspectiva de análise do problema, partindo de um dos seus campos de estudo: a gestão da informação, tal qual conceituado por Choo (1998, p.24), conforme descrito em detalhes na seção 2.1.

A temática escolhida congrega três aspectos distintos, quais sejam, necessidades informacionais, consciência situacional e defesa cibernética, todos articuláveis com a Ciência da Informação. As necessidades informacionais estão intrinsecamente ligadas ao estudo da gestão da informação (Choo, 1998, p. 23-50). A consciência situacional está inserida no campo das ciências cognitivas, também relacionado à Ciência da Informação (Robredo, 2003, p. 148).

Por fim, a defesa cibernética, que, embora seja um aspecto das ciências militares, tem por objeto central de preocupação os dados digitais, seja na sua preservação quando próprios, seja na sua degradação se pertencente a um agressor da nação. Assim, a defesa cibernética está voltada para; (i) a gestão da informação (que no meio militar essa gestão é, em geral, retratada como ciclo de comando e controle) na sua forma de dados digitais; (ii) para a segurança da informação, campo este relacionado à Ciência da Informação (Robredo, p. 150), tomando especificamente o aspecto de tecnologia da informação, ou seja, a cibernética, aspecto esse também ligada à Ciência da Informação (Robredo, 2003, p. 148).

De modo a corroborar a pertinência da pesquisa, ressalta-se que o primeiro autor deste artigo foi, por três vezes, comandante de destacamentos de defesa cibernética (unidades militares temporárias com caráter de comando ou coordenação de várias outras unidades militares ou civis), duas vezes em grandes eventos (Copa das Confederações, 2013 e

Jogos Olímpicos 2016) e uma vez em exercício conjunto de treinamento militar do Ministério da Defesa (Operação Atlântico 2012), além de ter participado em diversas funções em operações militares, projetos do Setor Cibernético brasileiro e comissões internacionais que interagiram com representantes de defesa e segurança cibernética de todos os continentes entre os anos de 2008 e 2016.

Essa vivência nos eventos ocorridos possibilitou uma observação participativa em amplo espectro de fatos que basearam a pesquisa, que, de outro modo, seriam difíceis de reunir dada a variedade das situações, locais, funções e pessoas envolvidas. Nas oportunidades de comando, mesmo contando com uma seleta equipe de técnicos, especialistas em doutrina militar, especialistas em segurança advindos de organizações parceiras, colaboradores internacionais e aparato tecnológico moderno, o primeiro autor se deparou com severas dificuldades em mapear sistematicamente as necessidades informacionais para consolidar sua consciência situacional e consequente tomada de decisões. Tais referências sugerem a pertinência da necessidade da realização da pesquisa e de sua vinculação à Ciência da Informação.

Os objetivos específicos correspondentes ao objetivo da pesquisa foram os seguintes: (i) elaboração de um conjunto básico de questionamentos para identificação de necessidades informacionais; (ii) modificação do conjunto básico de perguntas em questionamentos personalizados para o contexto de operações cibernéticas brasileiras em nível estratégico; (iii) o estabelecimento de critérios para reconhecer e enunciar as necessidades de informação demandadas pela consciência situacional de um comandante de operação de defesa e cibernética em nível estratégico; (iv) reconhecimento e registro de um conjunto de elementos essenciais para identificação das necessidades informacionais para formação da consciência situacional de um comandante de operações defesa cibernética.

O artigo foi estruturado em: introdução, seção 1, no qual são descritos o contexto da pesquisa, os fatores que a justificam, a metodologia adotada; desenvolvimento composto pelas seções 2 a 6, sendo as seções 2 a 5 abrangendo a revisão de literatura e a seção 6 os resultados; uma conclusão contendo as considerações finais consta da seção 7.

2 GESTÃO DA INFORMAÇÃO E NECESSIDADES INFORMACIONAIS

Nesta seção são abordados os conceitos de gestão da informação e necessidades informacionais, assim como estão estabelecidas as referências para seu uso na pesquisa.

2.1 Gestão da Informação

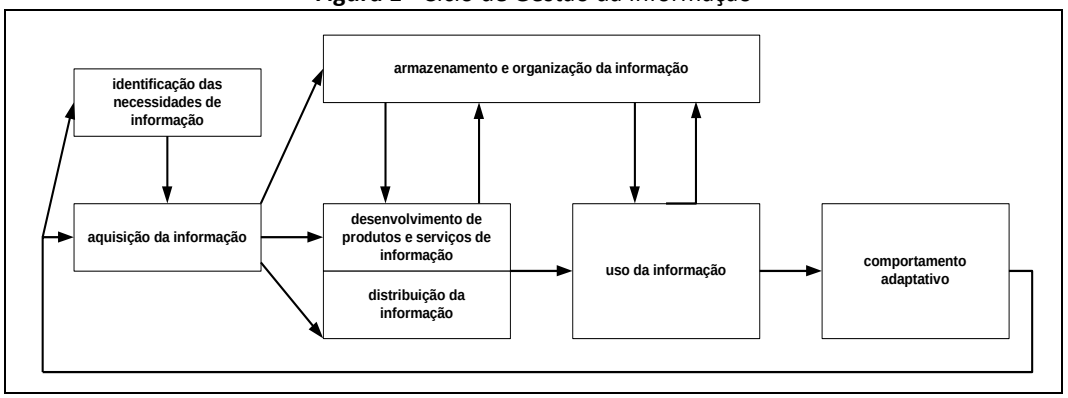
O gerenciamento da informação é considerado como uma das funções responsáveis pelo sucesso ou não das organizações e até da sua sobrevivência. Apesar de tamanha relevância, existe uma deficiência de metodologias para orientar e apoiar o processo de gerenciamento da informação (Beuren, 2000, p.64), assim como a ausência de um gestor da informação e o descompasso entre ele e o gestor de tecnologia da informação estão entre os motivos que contribuem para o insucesso da gerência da informação em uma organização Beuren (2000, p.67).

Jorge e Valentim (2021, p.6), em uma pesquisa conjunta, consideram “a gestão da informação como uma ferramenta estratégica capaz de conceder inúmeras oportunidades e gerar inovações para a organização, aumentando assim a sua competitividade”.

Tais fatos permitem concluir que a empresa que conseguir parametrizar suas alternativas de decisões, mensurar as consequências da decisão tomada e divulgar os seus resultados estabelecerá vantagens competitivas.

No intuito de lidar com a questão de modo sistemático, pesquisadores da área delinearam modelos básicos que representam o processo gerenciamento da informação. A Figura 1 representa um desses modelos, proposto por Choo (1998, p. 24), onde se pode observar seis etapas bem definidas nas quais a informação em um ciclo que vai desde a percepção das necessidades informacionais até o uso da informação, contendo ainda um laço de retroalimentação para promover comportamentos adaptativos.

Figura 1 - Ciclo de Gestão da informação



Fonte: Choo (1998, p.24), tradução nossa

As etapas do modelo de Choo (1998, p. 23-50) são identificadas como segue:

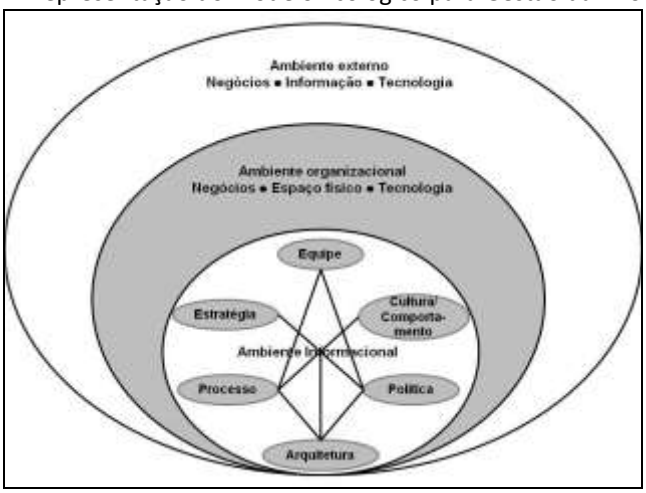
a) **identificação de necessidades informacionais**: fase do processo que busca reconhecer as informações necessárias para resolver problemas e tomar decisões;
b) **aquisição**: fase da obtenção da informação, conforme os critérios apontados pelas necessidades informacionais descobertas;
c) **organização e armazenagem**: fase do processo em que as informações devem ser organizadas segundo critérios que facilitem sua utilização, representação e recuperação;
d) **desenvolvimento de produtos e serviços**: fase do processo na qual os produtos e serviços informacionais são elaborados para agregar valor à informação de modo a potencializar o seu uso por meio da facilitação de sua interpretação, redução do ruído, aumento da qualidade, maior adaptabilidade, além de outras;
e) **distribuição**: disseminação da informação com objetivo de aumentar seu compartilhamento;
f) **uso efetivo**: é o fecho do processo no qual a informação recebe a sua efetiva significação por parte do usuário ou é tomada uma decisão.

Davenport (1997, p.28) considera que, além do ciclo de gestão da informação, é necessário levar em consideração outros elementos para gerir a informação em uma organização de modo adequado. Esses elementos, organizados em três tipos de ambientes, definem o que Davenport designou metaforicamente de “ecologia da informação” (Davenport, 1997, p.10). Esses ambientes são classificados como: ambiente informacional, ambiente organizacional e ambiente externo à organização (DAVENPORT, 1997, p. 33). O ambiente informacional é o mais destacado pelo autor e é subdividido em seis elementos, enquanto, tanto o ambiente organizacional quanto o externo são divididos em três elementos.

Os elementos constituintes do ambiente informacional são os seguintes: estratégia da informação, política da informação, comportamento e cultura informacional, equipe de informação, processos de informação e arquitetura da informação (Davenport, 1997, p.34 - 37).

Os elementos constituintes do ambiente organizacional são: (i) situação de negócios, onde são de destaque a estratégia e os processos de negócio, a estrutura e cultura organizacional e condução dos recursos humanos; (ii) o investimento em tecnologia, onde a ênfase é o acesso simples à informação, fazendo uso da tecnologia que for a mais adequada ao negócio e não necessariamente a última novidade de mercado; (iii) disposição do espaço físico das instalações internas da organização de modo que isso venha a facilitar as interações entre o pessoal interno (Davenport, 1997, p.37-38). Os elementos constituintes do ambiente externo (Davenport, 1997, p. 38-39) que devem ser monitorados são: os mercados da informação (produtos informacionais comercializados), da tecnologia (básicas, de uso corrente e inovadoras) e de negócios (comportamento de competidores, clientes, substitutos e fornecedores). A Figura 2 representa ecologia da informação, composta pelos ambientes informacional, organizacional e externo.

Figura 2 - Representação do Modelo Ecológico para Gestão da Informação



Fonte: Davenport (1997, p.31)

2.2 Necessidades Informacionais

Considerando o foco da pesquisa, que realça a identificação de necessidades informacionais, é preciso fazer destaques específicos de alguns elementos do subtítulo 2.1, muito embora não se possa deixar de frisar que todas as partes estão inter-relacionadas. O principal elemento de destaque é a fase de identificação das necessidades informacionais apontadas no ciclo de gestão da informação de Choo (19989, p.24). Dos elementos ecológicos de Davenport, destacam-se de modo especial, como fatores causais das necessidades da informação, a estratégia da informação, a cultura e comportamento informacional, as escolhas de negócio internas e as variações do ambiente externo onde a organização atua, enquanto os demais elementos estão majoritariamente envolvidos no processamento das informações já determinadas.

Segundo Choo (1998, p. 26), a determinação das necessidades informacionais passa não só pela questão "o que você quer saber?", mas deve passar por questões básicas tais como:

a) Por que você precisa saber disso?
b) Com o que o seu problema se parece?
c) O que você já sabe?
d) O que você pode antecipar?
e) Como isso pode ajudar você?
f) Em que forma você precisa saber disso?

Sobre a articulação entre identificação de necessidades informacionais e o ambiente informacional definido por Davenport (1997, p.34), é relevante destacar a Estratégia da Informação. A Estratégia da Informação, como estabelecida por Davenport (1997, p.35), é constituída a partir da resposta à seguinte pergunta: o que a administração da organização pretende fazer com a informação? A Estratégia aborda os aspectos sobre tipos ou categorias de informação adotadas, as terminologias de aplicação comuns no âmbito da organização, os processos de informação que devem ser usados, o intercâmbio externo de informações e que princípios relativos à informação são estabelecidos na organização (Davenport, 1997, p 69-84). Desse modo, esses aspectos agem como balizadores para as necessidades informacionais, pois são estabelecidos no ambiente de negócios, condicionando o ambiente informacional.

Concluindo os destaques dos demais elementos da ecologia informacional em relação à identificação das necessidades informacionais, tem-se os ambientes organizacional e externo (1997, p.37-39). Dos componentes do ambiente organizacional, a estratégia de negócios é por si, evidentemente, um condicionador para direcionar as necessidades informacionais. Considerando que a estratégia de informação deriva da estratégia de negócios e sua composição sofre influência direta da cultura organizacional, é possível considerar, de modo simplificado, a estratégia informacional como ente cuja formação absorve os requisitos de necessidades informacionais gerados no nível do ambiente organizacional.

Sobre o ambiente externo, todos os seus componentes serão considerados, ainda que com adaptações, uma vez que o estudo foi desenvolvido num contexto de operações militares. Assim, tanto o acompanhamento dos mercados de negócio de informações, produtos informacionais e de tecnologias foram absorvidos no estudo.

No caso dos componentes do ambiente externo citados por Davenport (1997, p. 39), a correspondência é feita recorrendo-se a seguinte adaptação: “competidores” e “substitutos”, correspondendo aos adversários no combate; “clientes”, correspondendo às organizações nacionais e infraestruturas críticas do país que receberem apoio na sua proteção durante a operação; “fornecedores”, correspondendo às organizações parceiras que realizam ações cibernéticas de apoio à operação.

3 COMANDO E CONTROLE E CICLO PARA SUPORTE À TOMADA DE DECISÃO EM OPERAÇÕES MILITARES

No âmbito militar, em termos operacionais, ou seja, no que se refere ao aspecto central e fim do emprego das Forças Armadas, a gestão da informação ocorre por meio do processo de comando e controle (C2). Considerando que a expressão possui diversas interpretações, este estudo adotou a definição doutrinária que guia a Defesa brasileira, o qual consta no Glossário das Forças Armadas (Brasil, 2015, p. 65; p. 254):

> COMANDO E CONTROLE - 1. Ciência e arte que trata do funcionamento de uma cadeia de comando. Nesta concepção, envolve, basicamente, três componentes: a autoridade legitimamente investida, apoiada por uma organização, da qual emanam as decisões que materializam o exercício do

> comando e para onde fluem as informações necessárias ao exercício do controle; a sistemática de um processo decisório que permite a formulação de ordens, estabelece o fluxo de informações e assegura mecanismos destinados à garantia do cumprimento pleno das ordens; e a estrutura, incluindo pessoal, equipamento, doutrina e tecnologia necessários para a autoridade acompanhar o desenvolvimento das operações. 2. Constitui-se no exercício da autoridade e da direção que um comandante tem sobre as forças sob o próprio comando, para o cumprimento da missão designada. Viabiliza a coordenação entre a emissão de ordens e diretrizes e a obtenção de informações sobre a evolução da situação e das ações desencadeadas. 3. Ver SISTEMA DE COMANDO E CONTROLE.
> [...]
> SISTEMA DE COMANDO E CONTROLE - Conjunto de instalações, equipamentos, comunicações, doutrina, procedimentos e pessoal essenciais para o comandante planejar, dirigir e controlar as ações de sua organização para que se atinja uma determinada finalidade. Ver COMANDO E CONTROLE.

O exercício das funções de comando e controle na guerra requer metodologia própria que garanta aos tomadores de decisão (comandantes) e seus assessores (estado-maior) o entendimento e a identificação de todos os processos necessários para realizar o ciclo decisório e superar as incertezas e pressões decorrentes das informações incompletas e do tempo.

Em um teatro de operações (zona em que ocorre um conflito), a quantidade de eventos que ocorre é expressiva, tornando complexo o seu gerenciamento, exigindo de um comandante habilidades individuais específicas, experiência e conhecimento da metodologia apropriada. A utilização da metodologia traz como vantagens a melhoria da gerência dos meios, dos recursos humanos e dos processos, implicando numa realização mais efetiva do ciclo de comando e controle.

Os manuais militares de C2 brasileiros vigentes à época da pesquisa adotavam o modelo tradicional OODA (Boyd, 2018, p. 383) para descrição do ciclo de comando e controle. As fases do ciclo de C2 OODA são: observar, orientar, decidir e agir. O ciclo OODA está representado na Figura 3, destacando-se que a consciência situacional se dá nas duas primeiras fases do ciclo.

3.1 Observar

Observar consiste em buscar ou coletar dados por meio de diversas fontes. Basicamente, essa coleta é composta pelo levantamento de informações, tais como: o inimigo; o estado das forças amigas; da meteorologia e geografia da área de operações. O Manual EB20-MC10.205 (Brasil, 2015, p. 2-6) sobre Comando e Controle do Exército Brasileiro, estabelece que:

> A fase observar caracteriza-se por perceber o cenário no qual se deseja atuar e se está inserido. Nessa fase, capta-se o maior número possível de estímulos que influenciam o ambiente operacional, provenientes, por exemplo, de sensores dos escalões superiores, dos subordinados, do escalão considerado, ou ainda, oriundos de sensores civis. Nessa observação, devem-se considerar os aspectos concernentes a todos as dimensões do ambiente operacional.

3.2 Orientar

Orientar é o desenvolvimento de opções das quais, após a aplicação de processos decisórios, será escolhida aquela que resultará em uma ação. A orientação será baseada na análise das informações disponíveis. O Manual EB20-MC10.205 (Brasil, 2015, p. 2-7) define essa fase como:

> Na fase orientar-se, as percepções coletadas na fase anterior são consolidadas, interpretadas e analisadas em um contexto global, a fim de delinear um cenário atualizado da situação, com base no qual serão identificadas ameaças prováveis ou reais, os riscos e suas consequências. A partir dessa análise, serão formuladas as linhas de ação a serem apresentadas ao decisor.

3.3 Decidir

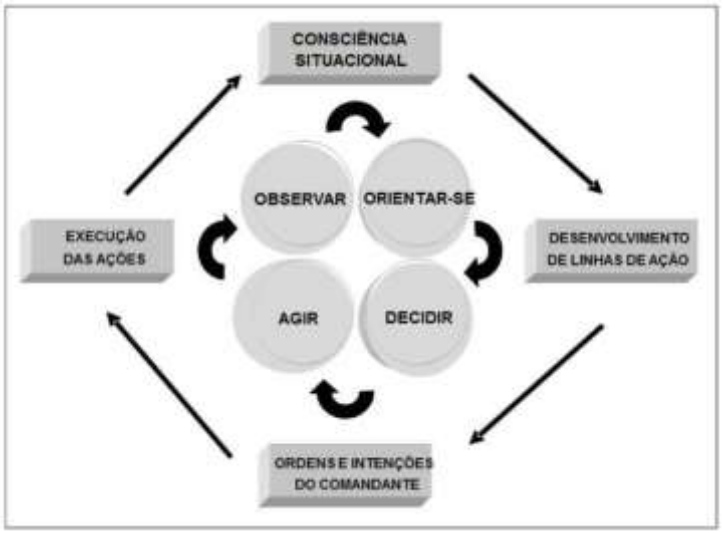
Decidir é selecionar a opção, ou opções, desenvolvidas na fase anterior. Dessa forma, é decidido o curso das ações, e, em consequência, é preparada a distribuição de ordens.

3.4 Agir

Finalmente, o ciclo da metodologia de comando e controle é concluído com a fase de agir, a qual consiste em executar e avaliar as ações, promovendo a realimentação do ciclo.

A Figura 3 representa o ciclo OODA de comando e controle, cujas fases estão explicadas nos itens 3.1 a 3.4. Especial ênfase foi dada às fases observar e orientar, pois, conforme se pode constatar da Figura 3, a consciência situacional ocorre nessas duas primeiras fases.

Figura 3 - Ciclo de C2 OODA – Observar, Orientar, Decidir e Agir



Fonte: Brasil (2015f, p.2-7)

O ciclo OODA de C2 permite que sejam entendidos com clareza os processos relativos às funções gerenciais de comando e controle e identificá-los. Dessa forma, torna-se mais fácil definir o que é necessário fazer.

A forma de aplicação do ciclo de C2 está ligada ao nível de decisão envolvido. Logo, para uma mesma questão a ser submetida ao ciclo, aplicando-a em níveis decisórios distintos, a pertinência ou não de certas informações será diferente. Como exemplo, seja considerado a seguinte questão: o emprego militar em uma situação de conflito é necessário? Se o nível decisório for o do comandante supremo, ou seja, no caso brasileiro, do Presidente da República, uma informação meteorológica não será relevante, no entanto, pode ser essencial para o comandante da tropa a ser empregada.

Em suma, quando a metodologia é corretamente empregada ela possibilita a eliminação de processos que causam trabalhos desnecessários, tornando o ciclo de C2 mais rápido e otimizando a gestão da informação e, por conseguinte, tornando mais precisa a identificação das necessidades informacionais.

4 CONSCIÊNCIA SITUACIONAL EM AMBIENTES DINÂMICOS

De especial importância para entendimento do campo da consciência situacional para ambientes dinâmicos e complexos são os trabalhos da pesquisadora Mica Endsley, em particular um artigo seminal usado em diversas pesquisas na área (Endsley, 1995, p. 32-64), no qual a cientista provê uma valiosa série de conhecimentos sobre o tema, além de propor um modelo sobre o assunto. Como definição sobre o que é a consciência situacional, Endsley (1995, p.36) enuncia o seguinte:

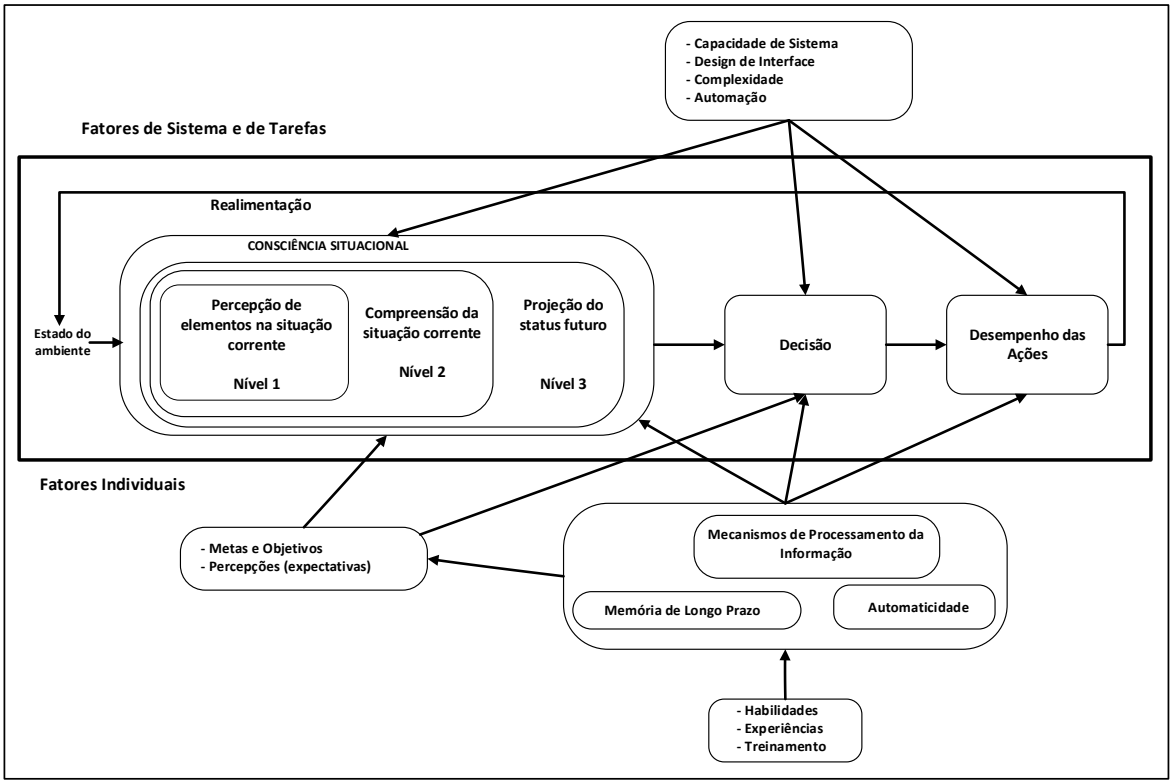
> Consciência situacional é a percepção dos elementos do ambiente dentro de um período de tempo e espaço, a compreensão do seu significado e a projeção do seu estado no futuro próximo. (Endsley, 1995, p.36, tradução nossa).

Endsley (1995) propõe o modelo representado na Figura 4 para consciência situacional em ambientes dinâmicos. O primeiro estágio da consciência situacional, segundo Endsley (1995, p. 36), é a **percepção**. Neste contexto, o estágio de percepção é o ato de notar o estado, os atributos e a dinâmica dos elementos relevantes do ambiente. A capacidade de perceber o que é relevante no ambiente pode ser influenciada por vários fatores.

A **compreensão** da situação corrente está baseada numa síntese formada na mente do operador a partir dos elementos desconexos captados no nível 1, ou seja, na **percepção** (ENDSLEY, 1995, p. 37). A compreensão desses elementos se processa sempre à luz dos objetivos da observação.

O nível 3 da consciência situacional é constituído pela habilidade de projetar as ações dos elementos do ambiente, no mínimo, no curto prazo, e é referido como **projeção**. Esse estágio da Consciência Situacional é atingido como consequência direta do conhecimento do estado e da dinâmica dos elementos do ambiente e da compreensão da situação corrente (Endsley, 1995, p.37).

Figura 4 - Modelo de Consciência Situacional para tomada de decisão dinâmica



Fonte**:** Endsley (1995, p. 35, tradução nossa)

De especial importância para esta pesquisa são os fatores individuais, ou seja, centrados no indivíduo e não na tecnologia, conforme representados na parte inferior da Figura 4. Assim, as habilidades, as experiências e o treinamento proveem conteúdo tanto para o grupo formado pelos mecanismos mentais de processamento de informação, memória de longo prazo e reações automatizadas quanto para o grupo formado pelas metas e objetivos da missão e pelas expectativas prévias existentes. Por sua vez, esses grupos influenciam diretamente em todas as fases da tomada da consciência situacional.

5 CONSCIÊNCIA SITUACIONAL EM OPERAÇÕES DE DEFESA CIBERNÉTICA

Segundo Barford e*t al*. (2010, p. 3-5), a consciência situacional em defesa cibernética está associada a sete aspectos: (i) consciência do que ocorre, ou seja a percepção da ocorrência de um ataque, seu tipo, fonte, alvo etc.; (ii) consciência do nível atual e possível desdobramento do impacto do ataque; (iii) consciência da evolução da situação; (iv) ciência do comportamento do adversário; (v) ciência do porquê e como a situação corrente foi causada; (vi) ciência da qualidade (confiabilidade) das informações coletadas e das decisões de inteligência que foram derivadas dessas informações; (vii) avaliação dos futuros plausíveis da situação corrente. Barford, Dacier et al. (2010, p. 3-5) ainda distribuem esses aspectos pelos níveis de consciência situacional definidos por Endsley (1995) do seguinte modo:

a) percepção dos elementos do ambiente: aspectos (i) e (vi).

b) compreensão da situação corrente: aspectos (ii), (iv) e (v).

c) projeção de estados futuros: aspectos (iii) e (vii).

A consciência situacional de defesa cibernética do comandante é continuamente formada e atualizada por aspectos associados às fases **observar** e **orientar** do ciclo OODA,

sendo a fase da **percepção** relacionada à fase **observar**, enquanto as fases de **compreensão** e **projeção** à fase de **orientar**, conforme a Figura 3.

No contexto da Defesa brasileira, o emprego da cibernética nas operações militares realizadas no período da pesquisa, mostrou que a consciência situacional de defesa cibernética pode ser consolidada a partir do acompanhamento pelo comandante sobre os efeitos dos três tipos de ações cibernéticas descritas nas documentações doutrinárias: ações de proteção cibernética; ações de exploração cibernética; ações de ataque cibernético. (Brasil, 2014, p. 23).

As ações de proteção cibernética preservam a segurança dos dados digitais, os respectivos sistemas que os processam e as redes por onde trafegam no espaço cibernético de interesse da defesa nacional. As ações de exploração cibernética buscam no espaço cibernético obter informações que provejam apoio à decisão nos vários níveis de comando e controle da operação. Por fim, as ações de ataque cibernético têm por alvo os sistemas informacionais digitais localizados no espaço cibernético, cujo comprometimento pode neutralizar ou degradar a capacidade ofensiva de um agente ameaçador à soberania nacional.

Os efeitos das ações cibernéticas (Carneiro, 2012, p.120) são desencadeados de duas formas distintas. A primeira diz respeito à proteção dos ativos digitais críticos para a Defesa Nacional, a qual se dá pela contenção na quantidade e na gravidade das violações da segurança cibernética ocorridas nesses ativos. Em grande parte dos casos, esses efeitos não podem ser percebidos diretamente, sendo capturados por dispositivos que mensuram os estados dos parâmetros de confidencialidade, disponibilidade e integridade da informação processada nos ativos informacionais críticos no espaço cibernético (ABNT, 2015, p.15).

A segunda forma de desencadear efeitos cibernéticos diz respeito aos impactos causados em sistemas de informações pertencentes ou utilizados por adversários, causando a sua degradação ou neutralização direta ou de estruturas por eles suportadas. Por “adversário”, neste contexto, entende-se uma entidade hostil ao país, cujas ações impliquem na necessidade de uma resposta dos entes que integram a Defesa Nacional para proteger a soberania nacional. Essas entidades hostis, no contexto da cibernética, podem ser pessoas, grupos, organizações ou até forças armadas de outras nações.

6 PROCEDIMENTOS METODOLÓGICOS

O presente trabalho tem por características ser um estudo aplicado descritivo e fez uso de técnicas de pesquisa bibliográfica, documental e de observação participante do tipo natural, ou seja, o pesquisador pertence à mesma comunidade analisada (Marconi; Lakatos, 2003, p. 194). Outra característica deste estudo é que ele constitui uma abordagem preliminar do tema, pois as possibilidades existentes, complexidade dos campos de conhecimento envolvidos e demais fatores relacionados sugerem que o exame da matéria pode evoluir significativamente.

O objetivo geral da pesquisa foi: propor um conjunto de elementos essenciais para identificação das necessidades informacionais na formação da consciência situacional de um comandante de uma operação de defesa cibernética em nível estratégico no contexto da Defesa Nacional brasileira.

Como procedimentos de pesquisa, foram executadas as seguintes tarefas: (A) para o objetivo específico (i), lançou-se mão da leitura e seleção dos elementos bibliográficos necessários, a partir das perspectivas de Choo (1998), Davenport (1997), Boyd (2018), Endsley (1995) e Barford *et al*. (2010), resultando no registro dos questionamentos buscados; (B) para o objetivo específico (ii), procedeu-se a leitura e seleção dos elementos documentais vigentes à época das observações, ou seja, a Política Cibernética de Defesa (Brasil, 2012), Doutrina Militar

de Defesa Cibernética (Brasil, 2014), os documentos de planejamento das operações de defesa cibernética ocorridas no período da pesquisa e o conjunto formado pelos registros de Lições Aprendidas (LA) e elementos de análise pós-ação (APA – registros que reúnem pontos fortes e oportunidade de melhoria para eventos observados durante a operação) à luz da experiência vivida pelo primeiro autor como comandante de operações de defesa cibernética para a personalização dos questionamentos levantados no objetivo (i); (C) para o objetivo específico (iii), foram utilizadas as referências de Endsley (1995, p. 35) sobre fatores individuais que influenciam na consciência situacional, a documentação de planejamento, doutrina e o conjunto formado pelos registros de LA e APA para se estabelecer critérios que viabilizassem o reconhecimento de fatores favoráveis à formação da consciência situacional; (D) para o objetivo específico (iv), realizou-se a enunciação dos elementos essenciais de necessidades informacionais buscadas na pesquisa, conforme os critérios estabelecidos no objetivo (iii), montando-se um quadro de referência para ajudar futuros comandantes de operações de defesa cibernética a responderem as perguntas personalizadas que guiam o levantamento das necessidades informacionais para subsidiar a tomada de consciência situacional em operações.

6 RESULTADOS

Nesta seção são descritos os resultados alcançados com a execução de cada objetivo específico, e assim demonstrando o alcance do objetivo geral pela proposição das necessidades informacionais pesquisadas.

6.1 Análise da Literatura de Referência e Documentação das Operações para Personalização dos Questionamentos

Da análise da bibliografia que compôs o referencial teórico, foi possível alcançar o resultado almejado para o objetivo específico (i), o qual buscava estabelecer um rol de questionamentos gerais para levantamento de necessidade informacionais. Esse resultado foi representado nas colunas identificadas como **Questionamento**, nos Quadros 1, 2, 3 e 4, acompanhado pela citação da fonte de referência nas colunas sob o título Ref. Teórico.

Do estudo do texto de Choo (1998, p.26), constatou-se que o autor propõe um rol de perguntas básicas voltadas para as necessidades informacionais já consolidado e este foi aproveitado na íntegra no Quadro 1. Da análise do texto de Davenport (1998), depreendeu-se que a estratégia da informação, pertencente ao ambiente informacional, e todos os elementos que compõem o ambiente externo são suficientes para identificar necessidades informacionais, conforme demandado nesta pesquisa.

Por processarem majoritariamente informações já determinadas, os demais elementos dos ambientes informacional e organizacional não foram considerados como indutores de necessidades informacionais primordiais. Em consequência, os questionamentos elaborados para essas partes do texto de Davenport (1998) foram inferidos com base no que o autor chamou de focos para constituir a estratégia da informação, Davenport (1998, p. 49-56), e das caraterísticas do ambiente externo, Davenport (1998, p. 195-205), dando origem aos Quadros 2 e 3. Dos textos de Boyd (2018), Endsley (1995) e Barford *et al*. (2010), adotou-se, para a composição do Quadro 4, a síntese dessas três fontes já direcionadas para a defesa cibernética, conforme proposta por Barford, Dacier *et al*. (2010, p. 3-5).

Os resultados do objetivo específico (ii), no qual se trata a personalização dos questionamentos gerais para o contexto da defesa cibernética brasileira no seu nível estratégico, estão representados nos Quadros 1 a 4, na coluna **Personalização**. Para atingir

esse objetivo, foram realizados dois procedimentos de correlação, sendo o primeiro entre os elementos documentais vigentes à época das observações e as perguntas gerais representadas nas colunas **Questionamento** dos Quadros 1 a 4. Esses documentos foram a Política Cibernética de Defesa (Brasil,2012), a Doutrina Militar de Defesa Cibernética (Brasil, 2014) e os documentos de planejamento das operações de defesa cibernética ocorridas no período da pesquisa, qual seja, de junho de 2012 a agosto de 2016.

A segunda correlação foi entre as perguntas gerais e a documentação onde estavam registradas as lições aprendidas e elementos da APA das operações militares de defesa cibernética correspondentes a cada um dos grandes eventos ocorridos no Brasil e aos exercícios militares conjuntos do Ministério da Defesa entre 2012 e 2016.

Para evitar a verificação desnecessária de todos as LA e APA, pois totalizavam mais de 900 registros, foram considerados os que possuíam atributos de planejamento estratégico, mantendo a coerência com as delimitações da pesquisa. A personalização das questões foi facilitada pela experiência do primeiro autor como ex-comandante dessas operações no mesmo período.

Aos dois procedimentos de correlação, foi acrescido um procedimento de classificação dos questionamentos. Esse procedimento se tornou necessário para viabilizar a correspondência entre os questionamentos personalizados e o mapeamento de elementos essenciais das necessidades informacionais de defesa cibernética, conforme o objetivo geral da pesquisa. Para isso, recorreu-se a uma parte dos atributos usados originalmente nos registros das LA e das APA para sua ordenação, que se referiam às fases do processo utilizado nas operações observadas. Esses atributos foram constituídos dos estágios: (i) planejamento e preparo (**PL**, **PR**); (ii) execução (**E**); (iii) desmobilização. O estágio de desmobilização foi desconsiderado, pois suas informações estavam majoritariamente relacionadas à logística e não à cibernética. Esses atributos foram representados nas colunas de categoria (**CAT**) dos Quadros 1 a 4. Uma categoria adicional foi acrescida àquelas coletadas nas LA e APA, denominada como **fundamental** (**F**). Essa categoria foi acrescida devido ao fato percebido na pesquisa de que, como primícias das necessidades informacionais, foi necessário o entendimento prévio do contexto onde as necessidades informacionais sobre defesa cibernética deviam ser majoritariamente buscadas ou ser baseadas antes de qualquer operação. Em consequência, essa categoria apontou para as documentações doutrinárias e de diretrizes gerais.

Por fim, das análises realizadas para personalização das perguntas gerais, constatou-se a necessidade de associar mais de uma categoria para vários dos questionamentos personalizados. Assim, por exemplo, pode-se ter um questionamento associado ao mesmo tempo às categorias fundamental (**F**) e de planejamento (**PL**). Essa caraterística de classificações múltiplas para um mesmo questionamento personalizado se dá pelo fato constatado na pesquisa de que, no contexto da defesa cibernética, a mesma pergunta deve ser aplicada a níveis diferentes desse tipo de operação, apontando para necessidades informacionais distintas.

Quadro 1 - Questionamentos gerais e personalizados a partir dos questionamentos de Choo (1998, p.24) para mapeamento das necessidades informacionais para consciência situacional de defesa cibernética

Nr	Questionamento	Ref. Teórico	Personalização	CAT
1	O que você quer saber?	Choo (1998, p.24).	O que o comandante de uma operação de defesa cibernética precisa estar ciente para ter melhores chances de formar uma consciência situacional adequada durante a operação?	**F PL PR**
2	Por que você precisa saber disso?	Choo (1998, p.24).	Por que o comandante precisa saber dos elementos identificados na pergunta 1?	**F PL PR**
3	Com o que o seu problema se parece?	Choo (1998, p.24).	Com o que tipos e exemplos de operações militares a operação de defesa cibernética se parece?	**PL PR**
4	O que você já sabe?	Choo (1998, p.24).	O que o comandante já sabe genericamente sobre defesa cibernética e sobre uma operação específica ser realizada?	**F PL**
5	O que você pode antecipar?	Choo (1998, p.24).	O que o comandante pode antecipar a partir dos possíveis cenários e riscos existentes no espaço cibernético de interesse da operação de defesa cibernética?	**PL PR**
6	Como isso pode ajudar você?	Choo (1998, p.24).	Como o conhecimento provido pela resposta à pergunta 1 pode ajudar durante a operação de defesa cibernética?	**PL PR**
7	Em que forma você precisa saber disso?	Choo (1998, p.24).	Qual o formato pode representar mais amigavelmente a informação necessária para subsidiar a tomada de consciência situacional durante a operação de defesa cibernética?	**EX**

Fonte: Dados da pesquisa (2023)

Quadro 2 - Questionamentos gerais e personalizados gerados a partir dos elementos para mapeamento da estratégia informacional (DAVENPORT, 1997, p.49-60)

Nr	Questionamento	Ref. Teórico	Personalização	CAT
8	Quais tipos de conteúdos de informação que a estratégia informacional estabelece ou indica?	Davenport (1997, p.49)	Quais tipos de conteúdo de informação críticas para a operação que o planejamento estratégico para a operação de defesa cibernética estabelece ou demanda?	**PL PR**
9	Que terminologias de aplicação comuns no âmbito da organização existem?	Davenport (1997, p.52)	Quais as terminologias de aplicação em comum que existem no âmbito dos times de segurança e defesa cibernética que colaboram?	**PR**
10	Qual ou quais os processos de informação devem ser usados?	Davenport (1997, p.54)	Quais os ciclos de gestão da informação utilizados para realização de ataques, tratamento de incidentes de segurança e defesa cibernética e de Inteligência devem ser usados?	**PL PR**
11	Que intercâmbio externo de	Davenport	Que intercâmbio externo de informações	**EX**

	informações é necessário?	(1997, p.56)	sobre os adversários, incidentes de redes, vulnerabilidades, ameaças, riscos, tipos de ataques cibernéticos, além de outros é necessário?	
12	Que princípios relativos à informação são estabelecidos na organização?	Davenport (1997, p.57)	Que princípios relativos à informação são estabelecidos no planejamento da operação?	**PL**

Fonte: Dados da pesquisa (2023)

Quadro 3 - Questionamentos gerais e personalizados gerados a partir dos elementos para mapeamento do ambiente externo (DAVENPORT,1997, p. 195 -208)

Nr	Questionamento	Ref. Teórico	Personalização	CAT
13	O que é necessário saber sobre consumidores, concorrentes, associados externos e condicionantes governamentais?	Davenport (1997, p.195)	O que é necessário saber sobre órgãos apoiados, adversários, agências parceiras e condicionantes governamentais?	**PL PR**
14	Que tecnologias da informação de infraestrutura, de uso e inovadoras devem ser rastreadas para adoção?	Davenport (1997, p.200)	Que tecnologias da informação de infraestrutura, de uso e inovadoras devem ser rastreadas para possível emprego ou prevenção?	**PL**
15	Que informações do mercado de informação externo devem ser adquiridas? Que informações devem ser distribuídas ou negociadas?	Davenport (1997, p.205)	Que informações sobre o espaço cibernético de interesse para a missão devem ser obtidas ou compartilhadas com organizações parceiras?	**PL PR EX**

Fonte: Dados da pesquisa (2023)

O Quadro 4 possui a particularidade de ter duas classes de perguntas de personalização. A primeira está associada à ação de proteção cibernética (**P**), enquanto a segunda está associada às ações de exploração e ataque cibernético (**E/A**). Essa distinção foi necessária, pois o Quadro 4 contém as perguntas do exercício da tomada de consciência situacional, ou seja, de execução da operação. Durante a operação, é necessário realizar todas as ações cibernéticas e as execuções das ações de proteção são significativamente distintas das ações de exploração e de ataque. Nesse sentido, destaca-se que, em geral, a ação de exploração precede a ação de ataque, estando ambas em profunda ligação, o que fez com que elas fossem consideradas juntas neste estudo. Pelo fato de todas as ações serem da categoria de execução (**E**), a coluna correspondente às categorias foi suprimida de modo a tornar a representação do Quadro 4 mais simples. As perguntas 16 e 17 correspondem ao nível de percepção da consciência situacional e ao estágio observar do ciclo OODA. As perguntas 18 a 20 correspondem ao nível de compreensão da consciência situacional e ao estágio orientar do ciclo OODA. Por fim, as perguntas 21 e 22 correspondem ao nível de projeção da consciência situacional e ao estágio orientar do ciclo OODA.

Quadro 4 - Questionamentos gerais e personalizados nos aspectos de Barford *et al*. (2010, p. 3-5) (continua)

Nr	Questionamento	Ref. Teórico	Personalização	
			Ação de Proteção (P)	**Ações de Exploração e Ataque (E/A)**
16	Qual é a percepção da ocorrência de um ataque, seu tipo, fonte, alvo etc.?	Barford, Dacier et al. (2010, p. 3-5).	Qual a percepção de eventos de segurança no espaço cibernético de interesse da operação que são incidentes?	Qual a percepção dos efeitos desejados sobre os sistemas de informação do adversário no espaço cibernético de interesse da operação?
17	Qual a ciência da qualidade (confiabilidade) das informações coletadas e das decisões de inteligência que foram derivadas dessas informações?	Barford, Dacier et al. (2010, p. 3-5).	Qual o nível de confiabilidade das informações sobre os eventos e incidentes de segurança no espaço cibernético de interesse da operação?	Qual o nível de confiabilidade das informações sobre os efeitos cinéticos ocorridos nos ativos de informação do adversário?
18	Qual a consciência do nível atual e possível desdobramento do impacto do ataque?	Barford, Dacier et al. (2010, p. 3-5).	Quais impactos estão ocorrendo no espaço cibernético de interesse da operação a ser protegido?	Quais impactos estão ocorrendo nos ativos de informação do adversário como resultantes dos ataques realizados?
19	Qual a ciência do comportamento do adversário?	Barford, Dacier et al. (2010, p. 3-5).	Qual a ciência das capacidades, interesses e tipos de ataques cibernéticos o atacante está utilizando?	Qual a provável ciência que o adversário tem sobre as capacidades, interesses e tipos de ataques cibernéticos utilizados contra ele?
20	Qual a ciência do porquê e como a situação corrente foi causada?	Barford, Dacier et al. (2010, p. 3-5).	Qual a ciência sobre o efeito pretendido pelo adversário com o ataque, quais as vulnerabilidades foram exploradas e qual o caminho do C2 de ataque?	Qual a provável ciência que o adversário tem sobre o efeito pretendido por meio do ataque a ele dirigido, as vulnerabilidades exploradas e qual o caminho do C2 de ataque?

Quadro 4 - Questionamentos gerais e personalizados nos aspectos de Barford *et al*. (2010, p. 3-5) (conclusão)

Nr	Questionamento	Ref. Teórico	Personalização	
			Ação de Proteção (P)	**Ações de Exploração e Ataque (E/A)**
21	Qual a consciência da evolução da situação?	Barford, Dacier et al. (2010, p. 3-5).	Qual a ciência da progressão atual do ataque no espaço cibernético a ser protegido?	Qual a provável ciência do adversário sobre a progressão atual do ataque contra seus ativos de informação?
22	Qual é a avaliação dos futuros plausíveis da situação corrente?	Barford, Dacier et al. (2010, p. 3-5).	Quais os tipos de desdobramentos dos impactos causados pelos ataques cibernéticos	Quais os tipos de desdobramentos dos impactos causados pelos ataques cibernéticos contra

			sofridos se podem esperar e quais as possibilidades de reação?	o adversário se podem esperar e quais as alternativas em caso de neutralização total ou parcial do ataque?

Fonte: Dados da pesquisa (2023)

6.2 Análise para Mapeamento de Elementos Essenciais

Para satisfazer o objetivo específico (iii), ou seja, o estabelecimento de critérios para reconhecer e enunciar as necessidades de informação demandadas pela consciência situacional de um comandante de operação de defesa cibernética, utilizou-se por base os fatores individuais, conforme a Figura 4. Esses fatores nutrem o processo de formação da consciência situacional, por meio das habilidades, a experiência e o treinamento, que, em conjunto, proveem conteúdo tanto para o grupo formado pelas metas, objetivos e expectativas quanto para o grupo formado pelos mecanismos mentais de processamento de informação, memória de longo prazo e reações automatizadas. Considerando esses fatores individuais, três critérios foram adotados.

O primeiro critério foi a utilização do grupo das metas, objetivos e expectativas prévias como referência para busca de elementos informacionais favoráveis à formação da consciência situacional de defesa cibernética. Isso levou ao estudo da documentação doutrinária e de planejamento das operações militares de defesa cibernética ocorridas no período abrangido pela pesquisa. Esses elementos informacionais ditos favoráveis poderiam ser palavras, expressões ou descrições, desde que já tivessem se demonstrado como elementos-chave nas operações, de acordo com as LA e com a experiência de ex-comandante do primeiro autor.

O segundo critério foi a utilização do grupo formado pela memória de longo prazo, as reações automatizadas e o processamento de informações. Foi dada maior ênfase à memória de longo prazo, pois, no entrelaçamento desses três elementos, é possível reconhecer que a memória de longo prazo supre os demais. Tomou-se o cuidado de restringir a busca por subsídios à memória de longo prazo com base em conhecimentos explícitos, conforme definido por Takeuchi (1995, p.8 *apud* Choo, 1998, p. 120), para que não se extrapolasse as áreas de conhecimento de base da pesquisa. O acervo analisado foi o das lições aprendidas e APA das operações ocorridas no período analisado, filtradas para o nível estratégico, e a busca dos elementos informacionais favoráveis foi definida nos mesmos moldes estabelecidos para o primeiro critério. Em consequência, as perguntas gerais nos Quadros 1 a 4 foram confrontadas com 477 lições aprendidas (LA) e aproximadamente 500 itens de Análise Pós-Ação correspondentes às operações do período estudado. Antes e proceder a correlação, houve uma filtragem desse total de LA e APA para que fossem verificados apenas os de caráter estratégico, conforme o escopo da pesquisa. Assim, aproximadamente 39% foram selecionados e analisados.

O terceiro critério foi a adoção da mesma ordenação provida pela classificação adotada para as perguntas personalizadas, de modo a organizar os achados resultantes da aplicação dos dois primeiros critérios. Assim, foi possível fazer a associação dos elementos de mapeamento das necessidades informacionais buscados na pesquisa com as perguntas personalizadas.

Para alcançar o objetivo (iv), portanto, para se expressar cada elemento essencial de necessidade informacional, tomou-se os registros obtidos pela aplicação dos critérios estabelecidos no objetivo específico (iii) e, a cada um, foi associada uma expressão-chave que

sintetizasse o significado do registro. À medida que os registros foram sendo analisados, as expressões-chave já estabelecidas passaram a se repetir, seja por expressarem a mesma ideia central de algum registro anterior, seja por expressarem um conceito que era abrangido ou abrangia o de registros anteriores de mesma categoria. Neste segundo caso, o significado geral associado à expressão-chave era enriquecido.

Assim, o conjunto dessas expressões-chave e seus significados gerais geraram os elementos essenciais de necessidades informacionais buscados. Esses elementos essenciais de informação para formação da consciência situacional de defesa cibernética de um comandante de operações dessa natureza estão representados nos Quadros 5 a 7.

Esses resultados fornecem um quadro de referência que, ao mesmo tempo, reflete a essência das informações reconhecidas nos documentos doutrinários, nas LA e nos registros das APA analisados, quanto dá margem à formação de modelos mentais (Endsley, 1995, p. 43) que inevitavelmente serão formados e utilizados por cada comandante no exercício de sua tomada de consciência situacional individual.

Nos Quadros 5 a 7, também estão discriminados os números correspondentes às perguntas associadas a cada elemento essencial de informação, conforme procedimento de classificação estabelecido no objetivo (ii). Cabe ressaltar que os elementos de necessidade de informação não respondem integralmente à pergunta associada, mas subsidia as respostas a serem compostas por cada comandante, à luz das suas habilidades, treinamento e experiências pessoais e o contexto da operação específica.

Desse modo, os resultados da pesquisa estão compilados nos Quadros 5 a 7. Foram mapeados 35 elementos essenciais de necessidades informacionais distintos a partir dos quais se pode esperar que um comandante de operações de defesa cibernética possa iniciar o seu preparo para estar em condições de formar sua consciência situacional de defesa cibernética e tomar suas decisões de forma compatível com as necessidades da operação. Fazendo-se uso da ordenação escolhida para a disposição das informações e achados da pesquisa, realizou-se a divisão dos resultados nos quadros, sendo o Quadro 5 correspondente aos elementos de necessidade de informação e respectivas perguntas personalizadas da categoria **fundamental**, o Quadro 6 correspondendo aos resultados das categorias **planejamento** e **preparo**, e por fim o Quadro 7 abrangendo a categoria **execução**. Embora as categorias **planejamento** e **preparo** tenham sido processadas separadas uma da outra, a sua apresentação final foi conjunta pelo fato de os planejamentos estudados considerem essas fases em conjunto, mantendo a compatibilidade com a documentação estudada.

Cabe ressaltar é que quase todos os elementos do Quadro 7, a exceção de um, são repetições do Quadro 6, pois têm funções que se estendem de uma categoria para outra, num *continuum*. Em consequência, a numeração dos Quadros 5 a 7 termina no número 55, e não em 35, em função dessas repetições.

Quadro 5 – Elementos essenciais para identificação de necessidades informacionais fundamentais

ELEMENTOS DE NECESSIDADES INFORMACIONAIS FUNDAMENTAIS			
Nr	**Elem. Nec. Informacionais**	**Significado**	**Quest. Pers.**
1	**Objetivos da defesa cibernética**	Objetivos estratégicos definidos nos documentos específicos de cibernética de mais alta hierarquia.	1,2,4
2	**Ações cibernéticas**	Ações definidas na Doutrina Militar de Defesa Cibernética, por meio das quais as decisões operacionais do comandante de operações de defesa cibernéticas se concretizam.	I1,2,4
3	**Capacidades**	Capacidades referentes às ações cibernéticas disponíveis, para	1,2,4

	Cibernéticas	acionamento imediato, se preciso for, ou possíveis, mesmo as não disponíveis por meios próprios da Defesa, porém, passíveis de serem obtidas por mobilização de entes civis para Defesa Nacional.	
4	**Espaço cibernético de interesse**	Porção do espaço cibernético onde estão os ativos de informação a serem protegidos, os ativos de informação do adversário a serem atingidos e as redes passíveis de servirem de vias para alcançar os objetivos da missão.	1,2,4
5	**Sistema Militar de Defesa Cibernética**	Conjunto de instalações, equipamentos, doutrina, procedimentos, tecnologias, serviços e pessoal essenciais para realizar as atividades de defesa no Espaço Cibernético, assegurando, de forma conjunta, o seu uso efetivo pelas FA, bem como impedindo ou dificultando sua utilização contra interesses da Defesa Nacional. (Brasil, 2014, p.25).	1,2,4
6	**Infraestruturas críticas de Informação**	Infraestruturas de TI que suportam infraestruturas críticas próprias a serem protegidas ou adversárias a serem atingidas.	1,2,4
7	**Monitoração contínua**	Processo de acompanhar continuamente o nível de risco do espaço cibernético de interesse da Defesa brasileira.	1,2,4

Fonte: Dados da pesquisa (2023)

Quadro 6 – Elementos essenciais para identificação de necessidades informacionais de planejamento e preparo em defesa cibernética (continua)

ELEMENTOS DE NECESSIDADES INFORMACIONAIS DE PLANEJAMENTO E PREPARO			
Nr	**Elementos**	**Significado**	**Quest. Pers.**
8	**Ação colaborativa**	Atuação integrada entre organizações, civis ou militares, de modo a agregar valor aos resultados da operação, pelo emprego das competências técnicas ou legais específicas de cada entidade e do compartilhamento de informações, devendo ser exercitada independentemente de operações e aprofundada nessas ocasiões.	1 a 6; 8 a 10; 12 a 15; 18,19
9	**Alinhamento de objetivos**	Os objetivos do planejamento das ações cibernéticas devem estar finamente alinhados e compatíveis com os demais objetivos da operação como um todo, sendo claro a quais instâncias a cibernética serve ou é servida ou colabora.	1 a 6; 8 a 10; 12 a 15; 18,19

Quadro 6 – Elementos essenciais para identificação de necessidades informacionais de planejamento e preparo em defesa cibernética (continua)

ELEMENTOS DE NECESSIDADES INFORMACIONAIS DE PLANEJAMENTO E PREPARO			
Nr	**Elementos**	**Significado**	**Quest. Person.**
10	**Ameaças**	Indícios ou sinais prováveis de agentes (pessoas, grupos, países, técnicas de ataques, softwares maliciosos etc.) que potencialmente podem violar a segurança cibernética de ativos informacionais a serem protegidos na operação.	1 a 6; 8 a 10; 12 a 15; 18,19
11	**Assimilação de LA**	Aproveitamento total ou parcial da LA na doutrina, nos planejamentos e processos de trabalho.	1 a 6; 8 a 10; 12 a 15; 18,19
12	**Ativos críticos**	Ativos informacionais ou não que sustentam sistemas de informação importantes a serem preservados na operação.	1 a 6; 8 a 10; 12 a 15; 18,19
13	**Capacitação**	Manutenção de um alto grau de treinamento e atualização tecnológicos do pessoal empregado para executar as ações cibernéticas necessárias à operação, assim como capacitação do EM e Comandante em cenários cibernéticos	1 a 6; 8 a 10; 12 a 15; 18,19

ELEMENTOS DE NECESSIDADES INFORMACIONAIS DE PLANEJAMENTO E PREPARO			
Nr	**Elementos**	**Significado**	**Quest. Person.**
		e lições aprendidas.	
14	**Cenários**	Situações hipotéticas prováveis, baseadas do contexto da operação, nas quais são avaliados os efeitos de ataques cibernéticos recebidos ou realizados, possíveis reações, chances de agregar valor a outras ações não cibernéticas do conflito, gestão de crises, além do exame das possibilidades de decisão.	1 a 6; 8 a 10; 12 a 15; 18,19
15	**Compartilha-mento de informações**	Prática de partilhar informações sobre tipos de ataques cibernéticos, vulnerabilidades e suas correções, atuação de adversários, ameaças, além de todas as possibilidades informacionais de interesse da operação. Inclui a escolha adequada dos canais de comunicação, métodos e técnicas envolvidos e graus de sigilo.	1 a 6; 8 a 10; 12 a 15; 18,19
16	**Comunicação efetiva**	Processos de comunicação para disseminar ordens, alertas de toda ordem, solicitações e demais possibilidades de interação em uma operação entre forças militares e agencias civis de forma clara, concisa e precisa, mantendo-se a credibilidade e a oportunidade.	1 a 6; 8 a 10; 12 a 15; 18,19
17	**Conhecimento sobre o inimigo**	Conhecimento das capacidades cibernéticas do adversário, sua atuação, interesses, vulnerabilidades, além de outros específicos.	1 a 6; 8 a 10; 12 a 15; 18,19
18	**Coordenação interagências**	Processo formal de colaboração entre entidades civis e militares em uma operação. Distingue-se da ação colaborativa por ser baseada em processos formais entre entidades, formalizadas em protocolos oficiais e planejamento da operação.	1 a 6; 8 a 10; 12 a 15; 18,19
19	**Credibilidade**	Manutenção de alto grau de confiabilidade e precisão das informações compartilhadas com agências colaboradoras e da manutenção da confidencialidade de dados dessas agências.	1 a 6; 8 a 10; 12 a 15; 18,19
20	**Domínio sobre o espaço cibernético de interesse**	Capacidade de: (i) atuar com sucesso na exploração e ataque aos ativos de informação do adversário; (ii) manter a segurança cibernética dos ativos de informação próprios; (iii) monitorar e perceber violações do espaço cibernético de interesse.	1 a 6; 8 a 10; 12 a 15; 18,19

Quadro 6 – Elementos essenciais para identificação de necessidades informacionais de planejamento e preparo em defesa cibernética (continua)

ELEMENTOS DE NECESSIDADES INFORMACIONAIS DE PLANEJAMENTO E PREPARO			
Nr	**Elementos**	**Significado**	**Quest. Person.**
21	**Elementos de ligação**	Representantes civis ou militares da defesa cibernética que atuam como facilitadores na comunicação entre o comandante da operação e a entidade gestora do local onde o representante está.	1 a 6; 8 a 10; 12 a 15; 18,19
22	**Ferramentas cibernéticas**	Acervo de ferramentas de software para usos das ações cibernéticas, em particular as de exploração e ataque, de modo a se contar com meios para que o seu emprego resulte no efeito desejado. É desejável que esse acervo seja o maior e mais diversificado possível.	1 a 6; 8 a 10; 12 a 15; 18,19
23	**Fonte**	Fonte no espaço cibernético para obtenção de dados	1 a 6; 8 a 10;

ELEMENTOS DE NECESSIDADES INFORMACIONAIS DE PLANEJAMENTO E PREPARO			
Nr	**Elementos**	**Significado**	**Quest. Person.**
	cibernética	relevantes	12 a 15; 18,19
24	**Gestão de crises e continuidade da missão**	Processo de gerenciamento de crises na infraestrutura de TI e recursos digitais, que podem comprometer o sucesso da operação.	1 a 6; 8 a 10; 12 a 15; 18,19
25	**Gestão de riscos**	Processo pelo qual se pode estimar os riscos cibernéticos associados ao espaço cibernético durante uma operação de defesa cibernética e em períodos sem conflito declarado.	1 a 6; 8 a 10; 12 a 15; 18,19
26	**Infraestrutura de TI própria**	Maior número possível de ativos críticos próprios ou sob total governança que estejam na infraestrutura de TI utilizada para as ações cibernéticas, em especial para as de exploração e o ataque.	1 a 6; 8 a 10; 12 a 15; 18,19
27	**Integração de EM**	Oficiais do estado-maior (EM) da operação cientes das possibilidades e limitações da defesa cibernética e capacitados para trabalho integrado com às demais células de EM da operação.	1 a 6; 8 a 10; 12 a 15; 18,19
28	**Monitoração**	Acompanhamento contínuo e preciso do estado de risco do espaço cibernético de interesse durante a operação.	1 a 6; 8 a 10; 12 a 15; 18,19
29	**Níveis de alerta cibernético**	Níveis predeterminados associados ao grau de risco que se encontra o espaço cibernético de interesse da missão.	1 a 6; 8 a 10; 12 a 15; 18,19
30	**Operação remota**	Emprego das ferramentas cibernéticas a partir de uma ou mais localizações físicas diferentes de onde estão as demais unidades militares envolvidas no conflito.	1 a 6; 8 a 10; 12 a 15; 18,19
31	**Regras de Engajamento**	Série de instruções predefinidas que orientam o emprego das unidades que se encontram na área de operações, consentindo ou limitando determinados tipos de comportamento, em particular o uso da força, a fim de permitir atingir os objetivos políticos e militares estabelecidos pelas autoridades responsáveis. Dizem respeito à preparação e à forma de condução tática dos combates e engajamentos, descrevendo ações individuais e coletivas, incluindo as ações defensivas e de pronta resposta (Brasil, 2016).	1 a 6; 8 a 10; 12 a 15; 18,19
32	**Relação de confiança**	Exercício da confiança entre as pessoas envolvidas nas inter locuções entre agências, unidade militares, empresas ou qu alquer tipo de organização envolvida na operação. Deve ser fomentada e exercitada continuamente independente de o perações.	1 a 6; 8 a 10; 12 a 15; 18,19

Quadro 6 – Elementos essenciais para identificação de necessidades informacionais de planejamento e preparo em defesa cibernética (conclusão)

ELEMENTOS DE NECESSIDADES INFORMACIONAIS DE PLANEJAMENTO E PREPARO			
Nr	**Elementos**	**Significado**	**Quest. Person.**
33	**Simulação**	Processo para treinamento da aplicação de ações cibernéti cas em cenários produzidos para imitar uma parte do espaç o cibernético de interesse da operação, de modo a verificar as chances de sucesso dessas ações, possíveis efeitos colat erais não desejados, além de outras consequências. Pode s er apenas teórico, em ambiente virtual similar ao real o u, idealmente, em uma ferramenta para simulação integ	1 a 6; 8 a 10; 12 a 15; 18,19

ELEMENTOS DE NECESSIDADES INFORMACIONAIS DE PLANEJAMENTO E PREPARO			
Nr	**Elementos**	**Significado**	**Quest. Person.**
		ral dos ativos a serem protegidos ou alvos cibernéticos a serem explorados ou atacados.	
34	**Tratamento de incidentes de rede**	Processo de proteção cibernética para gerenciamento do ciclo de vida da violação da segurança cibernética de ativos de um ambiente de redes a ser protegido pertencente ao e spaço cibernético de interesse, tendo total similaridade ao processo aplicado internacionalmente pelos times de respo stas a incidentes de segurança computacional.	1 a 6; 8 a 10; 12 a 15; 18,19

Fonte: Dados da pesquisa (2023)

Quadro 7 – Elementos essenciais para identificação de necessidades informacionais de execução em defesa cibernética (continua)

ELEMENTOS DE NECESSIDADES INFORMACIONAIS DE EXECUÇÃO			
Nr	**Elementos**	**Significado**	**Quest. Person.**
35	**Ação Colaborativa**	Mesma definição do nr 8.	7; 11 e 15 a 22
36	**Alinhamento de objetivos**	Mesma definição do nr 9.	7; 11 e 15 a 22
37	**Alvos**	Ativos críticos ou infraestruturas críticas de informação do adversário.	7; 11 e 15 a 22
38	**Ameaças**	Mesma definição do nr 10.	7; 11 e 15 a 22
39	**Ativos Críticos**	Mesma definição do nr 12.	7; 11 e 15 a 22
40	**Compartilhamento de Informações**	Mesma definição do nr 15.	7; 11 e 15 a 22
41	**Comunicação Efetiva**	Mesma definição do nr 16.	7; 11 e 15 a 22
42	**Conhecimento sobre o inimigo**	Mesma definição do nr 17.	7; 11 e 15 a 22
43	**Credibilidade.**	Mesma definição do nr 19.	7; 11 e 15 a 22
44	**Domínio sobre o espaço cibernético de interesse**	Mesma definição do nr 20.	7; 11 e 15 a 22
45	**Elementos de ligação**	Mesma definição do nr 21.	7; 11 e 15 a 22
46	**Ferramentas Adequadas**	Mesma definição do nr 22.	7; 11 e 15 a 22
47	**Fonte cibernética**	Mesma definição do nr 23.	7; 11 e 15 a 22
48	**Gestão de Riscos**	Mesma definição do nr 25.	7; 11 e 15 a 22
49	**Infraestrutura de TI própria**	Mesma definição do nr 26.	7; 11 e 15 a 22
50	**Integração de EM**	Mesma definição do nr 27.	7; 11 e 15 a 22

Quadro 7 – Elementos essenciais para identificação de necessidades informacionais de execução em defesa cibernética (conclusão)

ELEMENTOS DE NECESSIDADES INFORMACIONAIS DE EXECUÇÃO			
Nr	**Elementos**	**Significado**	**Quest. Person.**
51	**Monitoração**	Mesma definição do nr 28.	7; 11 e 15 a 22
52	**Níveis de Alerta Cibernético**	Mesma definição do nr 29.	7; 11 e 15 a 22
53	**Operação Remota**	Mesma definição do nr 30.	7; 11 e 15 a 22

ELEMENTOS DE NECESSIDADES INFORMACIONAIS DE EXECUÇÃO			
Nr	**Elementos**	**Significado**	**Quest. Person.**
54	**Relação de Confiança**	Mesma definição do nr 32.	7; 11 e 15 a 22
55	**Tratamento de incidentes de rede**	Mesma definição do nr 34.	7; 11 e 15 a 22

Fonte: Dados da pesquisa (2023)

A consciência situacional é um processo que ocorre majoritariamente na execução da operação, no entanto, seu sucesso depende inexoravelmente das fases de planejamento e preparo, assim como dos conhecimentos fundamentais. Assim, as necessidades informacionais propostas devem ser encaradas como pontos de partida e não de chegada.

7 CONSIDERAÇÕES FINAIS

A presente pesquisa buscou estabelecer um marco inicial de conhecimento para lidar com as necessidades informacionais necessárias para a formação da consciência situacional do comandante de operações de defesa cibernética. As principais dificuldades do estudo estiveram relacionadas à precisão das inferências resultantes das confrontações entre as referências teóricas, documentação doutrinárias, questionamentos obtidos, LA e APA. Como a pesquisa fez uso da técnica da observação participante, as inferências geradas sempre estavam sob o risco de adquirirem um viés de preferências do primeiro autor.

Dois foram os contrapontos principais a essa vulnerabilidade inerente a técnica. O primeiro veio dos questionamentos de Choo (1998, p.24). Cada inferência gerada pela questão 1, do Quadro 1, era passada pelo crivo das questões de 2 a 7 do mesmo quadro. Embora tais questões fossem simples e diretas, o pesquisador era continuamente forçado a voltar aos fatos em si que observou e realizou, de modo a reiteradamente ser obrigado a testar a pertinência da sua inferência. O segundo fator que provavelmente ajudou a atenuar a questão do viés foi que, durante os 20 anos de acompanhamento de temas profundamente relacionados ao objeto de estudo, o primeiro autor desempenhou papéis variados e críticos em níveis distintos de gestão, variando desde os níveis políticos e estratégicos até os níveis operacional e tático, abordando os temas em termos técnicos, gerenciais ou de chefia e comando. Essas referências, por força da necessidade, propiciaram ao primeiro autor perspectivas variadas, atenuando assim possíveis restrições do horizonte de consciência sobre a questão, como por exemplo, raciocinar a partir e tão somente por um só viés, como técnico ou como gestor.

É fundamental ressaltar que a quantidade de dados e ativos informacionais que se combinam no universo do espaço cibernético onde ocorre uma única operação de defesa cibernética é de magnitude expressiva. Em consequência, o mesmo estudo, aplicado na ampliação para as demais fases de gestão da informação de Choo (1998, p.24) até a formação da consciência situacional no nível estratégico (correspondente à etapa do uso da informação), é recomendável. Da mesma forma, expandir a mesma pesquisa para inclusão das necessidades informacionais nos níveis operacional e tático, provavelmente vai requerer conhecimento capaz de lidar com grandes massas de dados, altas velocidades de processamento e sistematização. Nesse sentido, recomenda-se agregar áreas como a estatística e a computação para essa proposta de pesquisa. Tecnologias e áreas de estudo que amadurecem a passos largos atualmente, por exemplo, aprendizado de máquina, processamento de linguagem natural, ciência de dados, dentre outros, não podem ser ignorados.

Ainda sobre possíveis pesquisas adicionais, sugere-se aprimorar o presente estudo, ainda nas mesmas condições iniciais, porém acrescentando conceitos de dimensões de problema, Choo (1998, p. 26-28), como qualificadores mais precisos das necessidades informacionais e monitoramento ambiental, Choo (1989, p. 72), para lidar com a dinâmica do ambiente externo.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27032**: Tecnologia da Informação - Técnicas de segurança - Diretrizes para segurança cibernética. Rio de Janeiro, 2015.

BARFORD, P.; DACIER, M.; DIETTERICH, T. G.; FREDRIKSON, M.; GIFFIN, J.; JAJODIA, S.; JHA, S.; LI, J.; LIU, P.; NING, P.; OU, X.; SONG, D.; STRATER, L.; SWARUP, V.; TADDA, G.; WANG, C.; YEN, J. Cyber SA: Situational Awareness for Cyber Defense. *In*: JAJODIA S. (Editor), LIU P. (Editor), SWARUP V. (Editor), WANG C. (Editor). **Cyber Situational Awareness**: Issues and Research. Springer, 2010. 249 p.

BEUREN, Ilse Maria. **Gerenciamento Estratégico da Informação**: Um Recurso Estratégico no Processo de Gestão Empresarial. São Paulo: Atlas, 2000.

BOYD, John Richard. A **Discourse on Winning and Losing**. Montgomery: Air University Press, 2018. 392 p.

BRASIL. Exército Brasileiro, Estado-Maior do Exército. Portaria n. 002-EME, de 5 de janeiro de 2015. Aprova o Manual de Campanha Comando e Controle. **Comando e Controle (EB20-MC-10.205)**, Brasília, DF. 2018.

BRASIL. Ministério da Defesa. Portaria Normativa n. 3010, de 13 de janeiro de 2016. Aprova o Glossário das Forças Armadas. **Glossário das Forças Armadas** (**MD35-G-01).** Disponível em: https://www.gov.br/defesa/pt-br/arquivos/legislacao/emcfa/publicacoes/doutrina/md35-g-01-glossario-das-forcas-armadas-5-ed-2015-com-alteracoes.pdf/view. Acesso em: 20 dez. 2023.

BRASIL. Ministério da Defesa. Portaria Normativa n. 3010, de 18 de novembro de 2014. Aprova a Doutrina Militar de Defesa Cibernética. **Doutrina Militar de Defesa Cibernética (MD31-M-07)**. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/legislacao/emcfa/publicacoes/comando_controle/md31a_ma_07a_defesaa_cibernetica_1a_2014.pdf/view. Acesso em: 20 dez. 2023.

BRASIL. Ministério da Defesa. Portaria Normativa n. 3389, de 21 de dezembro de 2012. Dispõe sobre a Política Cibernética de Defesa. **Diário Oficial da União:** seção 1**,** Brasília, DF, n. 249, p. 11, 27 Dez. 2012. Disponível em: https://www.jusbrasil.com.br/diarios/44578940/dou-secao-1-27-12-2012-pg-11. Acesso em: 20 dez. 2023.

BRASIL. Presidência da República, Casa Civil. Decreto n. 6.703, de 18 de dezembro de 2008. Aprova a Estratégia Nacional de Defesa, e dá outras providências. **Diário Oficial da União:** seção 1, Brasília, DF, n. 247, p. 4, 19 dez. 2008. Disponível em:

http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/decreto/d6703.htm. Acesso em: 20 dez.2023.

BRASIL. Presidência da República, Gabinete de Segurança Institucional da Presidência da República. Portaria n. 45, de 8 de setembro de 2009. Institui, no âmbito da Câmara de Relações Exteriores e Defesa Nacional (CREDEN), o Grupo Técnico de Segurança Cibernética e dá outras providências. **Diário Oficial da União:** seção 1**,** Brasília, DF, n. 172, p.2, 09 Set. 2009. Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=09/09/2009&jornal=1&pagina=2&totalArquivos=80. Acesso em: 20 dez.2023.

CAMELO, José Ricardo Souza.; CARNEIRO, João Marinonio Enke. A Atuação do Centro de Defesa Cibernética na Copa das Confederações FIFA/2013. *In*: MEDEIROS FILHO, O. (organizador); FERREIRA NETO, W. B.(organizador); GONZALES, S. L. M. (organizador). **Segurança e Defesa Cibernética**: da fronteira física aos muros virtuais. Recife: Editora UFP, 2014. 196 p.

CARNEIRO, João Marinonio Enke. **A Guerra Cibernética**: uma proposta de elementos para formulação doutrinária no Exército Brasileiro. 2012. Tese (Doutorado em Ciências Militares) – Escola de Estado-Maior do Exército-ECEME, Rio de Janeiro, 2012. p. 203. Disponível em: http://www.eceme.eb.mil.br/images/IMM/producao_cientifica/teses/joao-marinonio-enke-carneiro.pdf. Acesso em: 20 dez. 2023.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA (CERT.br). **CSIRT FAQ**. São Paulo, 2002. Disponível em: https://www.cert.br/certcc/csirts/csirt_faq-br.html. Acesso em: 20 dez. 2023.

CHOO, Chun Wei. **Information Management for the Inteligent Organization**. Medford, NJ: Information Today, 1998. 272 p.

CLARKE, Richard Alan.; KNAKE Robert. **Cyber War: The Next Threat to National Security and What to Do About It**. New York: Harper Collins Publishers, 2010. 290 p.

DAVENPORT, Thomas H. **Information Ecology**. New York: Oxford University Press, 1997. 255p.
ENDSLEY, Mica R. Toward a theory of situation awareness in dynamic systems. *In*: **Human Factors Journal**, Santa Monica, v. 37, n. 1, p. 32–64, 1995.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION/International Electrotechnical Commission, Institute of Electrical and Electronic Engineers. **ISO/IEC/IEEE 15939**: Systems and software engineering - Measurement process. Geneva: ISO/IEC/IEEE,2007.

JORGE, Carlos Francisco Bitencourt; VALENTIM, Marta. L. P. Gestão da informação como estratégia inovadora nas organizações esportivas: um estudo no Marília Atlético Clube. **Encontros Bibli**: Revista Eletrônica de Biblioteconomia e Ciência da Informação. Florianópolis, v.26, p.1-21, 2021. Disponível em: https://www.redalyc.org/journal/147/14768130035/movil/. Acesso em : 21/12/2023.

MARCONI, Marina de Andrade.; LAKATOS, Eva Maria. **Fundamentos de Metodologia Científica**. São Paulo: Editora Atlas S.A. 2003, 311 p.

ROBREDO, Jaime. **Da Ciência da Informação Revisitada aos Sistemas Humanos de Informação**. Brasília: Thesaurus, 2003. 245 p.

VIANNA, Eduardo Wallier. A Segurança Cibernética na Conferência das Nações Unidas para o Desenvolvimento Sustentável – Rio+20. *In*: NAKAYAMA, Keiko Nakayama (org.).; PIMENTEL, Luiz Otávio. (org.).; ZIBETTI, Fabíola Wüst. (org.).; Ziegler, João Alfredo Filho. (org.). **Pontes para a Segurança Pública.** Florianópolis: FUNJAB, 2013. p. 127-156.

Recebido em/Received: 18/04/2023 | Aprovado em/Approved: 23/12/2023