CICLO DO CONHECIMENTO ORGANIZACIONAL APLICADO À CONSCIÊNCIA SITUACIONAL DE DEFESA CIBERNÉTICA NACIONAL: UM FRAMEWORK ESTRATÉGICO

E-mail:
ricardo.camelo@gmail.com
lillianalvares@unb.br

José Ricardo Souza Camelo, Lillian Maria Araujo de Rezende Alvares[1]

RESUMO

Busca produzir um *framework* de necessidades informacionais primordiais que oriente a preparação de comandantes ou gestores de operações de defesa cibernética e seu *staff* para acompanhar e lidar com os eventos do espaço cibernético, tomando consciência situacional de defesa cibernética frente a eventos que representem riscos à defesa nacional brasileira. O estudo pretende articular o modelo da teoria do conhecimento organizacional de Choo (1998) com o modelo de consciência situacional de Endsley (1995). Para alcançar esse objetivo, *frameworks* de segurança cibernética e de ataque cibernético foram utilizados. Trata-se de pesquisa aplicada, fazendo uso de métodos hipotético-dedutivos, técnicas de pesquisa bibliográfica e documental e observação participante do tipo natural, sustentada em revisão narrativa de literatura. Para aferir a pertinência do *framework* proposto, serão utilizados os registros de operações de defesa cibernética coordenadas pelo Exército Brasileiro entre 2012 e 2016, quando a instituição teve papel significativo na segurança e logística de grandes eventos no país.

Palavras-chave: conhecimento organizacional, consciência situacional, defesa cibernética, *framework.*

ABSTRACT

This study aims to develop a framework of primary informational needs to guide the preparation of commanders or managers of cyber defense operations and their staff in monitoring and addressing events in the cyber space, fostering situational awareness of cyber defense in response to events posing risks to the Brazilian national defense. The research seeks to integrate Choo's (1998) organizational knowledge theory model with Endsley's (1995) situational awareness model. To achieve this objective, cybersecurity and cyber attack frameworks were employed. The study is of applied nature, utilizing hypothetical-deductive methods, bibliographic and documentary research techniques, and naturalistic participant observation, supported by a narrative literature review. To assess the relevance of the proposed framework, records from cyber defense operations coordinated by the Brazilian Army between 2012 and 2016 will be utilized, a period during which the institution played a significant role in the security and logistics of these events.

Keywords: organizational knowledge, situational awareness, cyber defense, framework.

[1] Pesquisa em andamento no Programa de Pós-Graduação em Ciência da Informação da Universidade de Brasília (PPGCINFO/UnB). Qualificada em 18/12/2023.

1 INTRODUÇÃO

Em 2008, por meio da publicação da Estratégia Nacional de Defesa (END) (BRASIL, 2008), o Brasil estabeleceu três setores de maior prioridade para a Defesa Nacional: o espacial, o nuclear e o cibernético. A escolha do Setor Cibernético, conforme designado na END, seguiu uma tendência mundial de reconhecer que é essencial à soberania de uma nação possuir capacidade de atuar no espaço cibernético para sua defesa.

Os trabalhos desenvolvidos no âmbito do Ministério da Defesa nos últimos 10 anos para a construção do Setor Cibernético envolveram uma série de operações militares. Dentre essas missões, estão as operações de defesa e segurança cibernética dos grandes eventos ocorridos no Brasil entre 2012 e 2016. Operações de defesa e segurança cibernética envolvem grande número de informações a serem acompanhadas, as quais devem ser consolidadas na consciência situacional que o comandante da operação deve formar sobre o que ocorre no espaço cibernético de interesse da missão.

Para tornar viável este processo de tomada de consciência situacional, é imprescindível ter disponíveis as informações adequadas, saber percebê-las como relevantes, ter a capacidade de recuperá-las, processá-las e utilizá-las para a devida apreensão do que ocorre e a gerar os conhecimentos decorrentes. Nesse sentido, apresenta-se como promissor e pertinente tomar as abordagens da Ciência da Informação (CI) pelo viés da gestão do conhecimento como elementos que possam contribuir com o suporte ao processo de tomada de consciência situacional como tema de estudo.

2 CONTEXTO DA PESQUISA

A consciência situacional (CS) é um tema que por força da necessidade sempre mereceu atenção nos estudos relacionados às ciências militares e, mais recentemente, no campo das disciplinas ligadas aos estudos organizacionais. Seu desenvolvimento se dá nos ambientes informacionais do campo de batalha ou de gestão das organizações. No entanto, a dependência atual que os ambientes informacionais têm da tecnologia da informação implica na necessidade de lidar com uma enorme quantidade de dados, processados de modos diversos, complexos e em rede.

Sendo a consciência situacional um processo que ocorre na mente humana, a partir da percepção e compreensão do que se passa e a projeção de futuros possíveis e prováveis para tomada de decisão, a consecução desse processo com base em um ambiente informacional digital requer inúmeras e sucessivas integrações de dados, o que requer métodos para otimizar todos os estágios da tomada de consciência situacional e na diminuição da ambiguidade que a complexidade do ambiente cibernético envolve. Logo, surge a necessidade de realização de pesquisas científicas que abordem o tema da consciência situacional sobre defesa e segurança cibernéticas de modo a esclarecer suas características, como se realiza, possíveis limitações, dentre outras possibilidades.

A respeito da consciência situacional no espaço cibernético, Barford, Dacier et al. (2010) apontam que os conhecimentos desenvolvidos até o momento não estão amadurecidos em três aspectos de relevância: (i) a existência de uma grande lacuna entre a capacidade das ferramentas que propiciam a consciência situacional cibernética e os modelos mentais do analista de cibernética; (ii) a carência no tratamento da incerteza inerente aos dados nas abordagens existentes sobre consciência situacional cibernética; (iii) os modelos existentes não proporcionam capacidades de aprendizado e cognição necessárias à formação de uma consciência situacional de defesa cibernética plena.

Por outro lado, pela perspectiva de gestão, particularmente pelas perspectivas da informação e do conhecimento, Choo (1998) elaborou uma teoria sobre o desenvolvimento de uma organização de conhecimento. Nesse modelo, Choo descreveu processos envolvidos na potencialização da capacidade dos gestores de administrarem a informação e ampliarem o conhecimento pessoal e organizacional, desde sua percepção no ambiente até a tomada de decisão, o que implica na realização do processo de consciência situacional, otimizando seus instrumentos e conteúdos internos.

Ao mesmo tempo, as práticas consagradas pelo mercado de tecnologias de segurança cibernética, sejam produtos tecnológicos ou metodologias para sua gestão, são baseadas em conhecimentos advindos da prática de seu uso e que é conhecido como "melhores práticas". Em geral, essas melhores práticas são consolidadas em normativos ou em recomendações que tomam um aspecto de quadro de referência conhecidos como *frameworks*. Na grande maioria das situações de seu emprego, esses *framework*s são voltados para gerar metodologias de gestão de segurança cibernética nas organizações por meio de políticas e métodos de aplicação de tecnologia personalizados para o negócio da instituição, além de gerar cultura de segurança na organização e servir de substrato para execução de tarefas operacionais. Processo análogo ocorre em organizações voltadas para realização de ataques cibernéticos, os quais devem seguir *framework*s complexos.

Desse modo, tanto no aspecto da segurança cibernética quanto na atividade de ataque cibernético, o emprego de *framework*s se demonstra um instrumento de aplicação tanto da teoria envolvida na definição de uma organização de conhecimento quanto o emprego de elementos-chave nas fases do processo de consciência situacional.

Considerando as possíveis lacunas de conhecimento a serem exploradas nas pesquisas sobre consciência situacional em defesa cibernética, tomando por elemento potencializador da CS as teorias voltadas para organizações do conhecimento, além de fazer uso das ferramentas de *framework* de segurança cibernética e ataque cibernético, esta pesquisa tem como elemento central a seguinte questão: "*Como seria estruturado um framework que, baseado no ciclo de conhecimento organizacional, forneça um conjunto de elementos de referência para a determinação das necessidades informacionais primordiais à formação da consciência situacional em defesa cibernética no contexto da Defesa Nacional Brasileira no seu nível estratégico?*"

A escolha de focar o estudo nas necessidades informacionais primordiais para a consciência situacional na pesquisa se deu pelo fato de que a consciência situacional propriamente dita é formada em cada indivíduo após uma série de processos cognitivos, emocionais e situacionais, cujo mapeamento completo fugiria do escopo desta pesquisa. Por outro lado, ao observar as necessidades informacionais primordiais, torna-se viável mapear elementos essenciais para dar início à formação de consciência situacional de defesa cibernética de modo a direcioná-la com maior probabilidade de sucesso.

A especificidade da adjetivação primordial advém do fato de que a tomada de consciência situacional, além de ser individual, depende de cada operação de defesa cibernética específica ou do contexto particular empresarial em que eventos de defesa cibernética de relevância ocorrem e são acompanhados. Em consequência, esse caráter de primordialidade se torna necessário para indicar um ponto de partida e não chegada.

A restrição do questionamento no nível estratégico se faz necessário nesta pesquisa de modo a torná-la viável no que diz respeito ao cronograma a ser aplicado.

Em decorrência da questão de pesquisa, o objetivo geral é "propor um *framework*, baseado no ciclo de conhecimento organizacional de Choo (1998), que forneça um conjunto de elementos de referência para a determinação das necessidades informacionais primordiais à formação da consciência situacional em defesa cibernética, conforme definida por Endsley (1995), no contexto da Defesa Nacional brasileira no seu nível estratégico". Para alcançá-lo, os

seguintes objetivos específicos foram estabelecidos: a) realizar revisão narrativa de literatura, apresentando os modelos basilares da pesquisa e os respectivos contextos; b) identificar *frameworks* consagrados internacionalmente para segurança cibernética, segurança da informação e de ataque cibernético que serão úteis à pesquisa; c) identificar e aplicar critérios para seleção de elementos presentes nos *frameworks* escolhidos que sejam compatíveis com os aspectos do ciclo de gestão do conhecimento de Choo (1998); d) identificar e aplicar critérios para relacionar os elementos de *framework*s selecionados em relação ao ciclo de gestão do conhecimento de Choo (1998) com os estágios de consciência situacional de Endsley (1995) para primeira consolidação do *framework* a ser produzido na pesquisa; e) aplicar o *framework* consolidado nas documentações regulatórias e doutrinárias do Setor Cibernético da Defesa brasileira, assim como nos planejamentos das operações de defesa cibernética ocorridas no período de 2012 a 2016 para identificar as necessidades informacionais de cada evento ocorrido no período; f) discutir e concluir a pertinência do *framework* proposto por meio do correlacionamento entre as necessidades informacionais primordiais mapeadas para cada operação de defesa cibernética e os respectivos registros das lições aprendidas e análises pós-ação realizadas no período estudado.

Sobre a pertinência da pesquisa no campo da CI, a justificativa na conexão desta proposta de pesquisa tem pelo menos três pontos de articulação. O primeiro se baseia no fato de que a pergunta central da pesquisa aborda diretamente de necessidade informacionais e de gestão do conhecimento, elementos bem determinados no estudo da Ciência da Informação. O segundo se refere à CS, a qual está inserida no campo das ciências cognitivas, também relacionado à CI (ROBREDO, 2003). Por fim, o terceiro ponto, composto pela defesa e pela segurança cibernética, as quais possuem como principal alicerce a segurança da informação, área definitivamente relacionada à CI (ROBREDO, 2003). Além disso, o campo em que se desenrolam os processos de defesa e segurança abordados, ou seja, a cibernética, também é tema de estudo da Ciência da Informação (ROBREDO, 2003).

2.1 CONHECIMENTO ORGANIZACIONAL

Segundo Choo (1998), tendo por base as teorias organizacionais, há três arenas nas quais a organização deve lidar com a informação para se adaptar e crescer. A primeira arena é aquela na qual a organização usa a informação para reconhecer o sentido das mudanças do ambiente externo. Assim, as corporações, ao observar esse ambiente, selecionam o que é relevante, interpretam esses sinais e geram respostas conforme seus objetivos. Em curto prazo, o uso da informação aprimora a consciência dos membros da organização sobre o que é e faz, assim como, a longo prazo, esse uso propicia maiores chances de a instituição prosperar e sobreviver (CHOO, 1998).

A segunda arena está baseada no processo de criação de novos conhecimentos a partir do processamento da informação e por meio do aprendizado (CHOO, 1998). Nessa arena, os membros da organização devem estar sensibilizados para, sistematicamente, localizar, compartilhar, revisar e reintegrar o conhecimento entre si, e, guiados pelos objetivos da organização, promoverem sua evolução.

Na terceira arena, o foco está na tomada de decisão por meio do uso estratégico da informação guiada pelos objetivos institucionais. Essa arena tem por uma das suas características a tensão entre o processo ideal de tomada de decisão, no qual se faz uso da racionalidade e de técnicas de escolha da melhor estratégia, e os diversos elementos subjetivos dos integrantes da instituição, os quais podem envolver interesses particulares ou de grupos, barganhas, lacunas de informações, dentre outros (CHOO, 1998).

Essas três arenas são designadas, respectivamente, por três aspectos de uso da informação, quais sejam, formação de significado (*sensemaking*), criação do conhecimento (*knowledge*

creation) e tomada de decisão (*decision making*). Essas arenas devem ser consideradas como processos que interagem mutuamente (CHOO, 1998).

A partir desses elementos, Choo desenvolve um modelo de busca e uso da informação e, a partir dele, examina cada umas das arenas em um ambiente organizacional. O modelo de busca e uso da informação se alicerça em três categorias fundamentais: necessidades cognitivas, reações emocionais e ambiente de uso da informação. Os dois primeiros são ambientes de processamento de informação interno ao indivíduo, enquanto o terceiro constitui o ambiente externo às pessoas, onde a informação é usada (CHOO, 1998).

2.1.1 Ciclo do conhecimento organizacional

O conhecimento organizacional, segundo Choo (1998), apoia-se nas três arenas de uso da informação, ou seja, formação de significado, criação de conhecimento e tomada de decisão. Ao se observar o trajeto da informação por essas arenas, a teoria permite reconhecer que, em cada uma delas, os comportamentos de necessidade, busca e uso informacional são realizados. Por sua vez, cada um desses comportamentos é realizado sob os aspectos emocionais, cognitivos e situacionais. A Figura 1 apresenta as três arenas, os comportamentos informacionais e os aspectos simultaneamente.

Figura 1 - Formação de significado, criação de conhecimento e tomada de decisão

Modelo	Processo	Modos	Interações / Recursos
Formação de significado	- Mudança no ambiente -> Captação, seleção, retenção -> Interpretações representadas - Olhar para trás: criação de significado retrospectiva	- Processos orientados por crenças - Processos orientados por ações	
Criação do conhecimento	- Lacuna de conhecimento -> Conhecimento tácito, explícito, cultural -> Conversão, construção, conexão do conhecimento -> Novo conhecimento - Observar em muitos níveis: aprender com indivíduos, grupos e organizações de vários níveis	- Conversão do conhecimento - Construção do conhecimento - Conexão do conhecimento	
Tomada de decisões	- Situação de escolha -> Alternativas, resultados, preferências -> Regras, rotinas -> Decisões - Olhar para a frente: visão orientada para o futuro, para os objetivos	- Racional - Processual - Político - Anárquico	

Fonte: Choo (1998), traduzido para o português.

A partir do estabelecimento das arenas aludidas, Choo desenvolve o ciclo do conhecimento organizacional. Esse ciclo deve ser interpretado a partir dos sinais do ambiente externo. A informação percorre as três arenas de comportamento informacional, sendo processada internamente em cada arena e gerando resultados que podem seguir as possibilidades de sequenciamento indicadas na Figura 2. Em cada arena, o processamento ocorrido envolve os comportamentos de necessidades, busca e uso da informação, sob a luz dos aspectos emocionais, cognitivos e situacionais (CHOO, 1998).

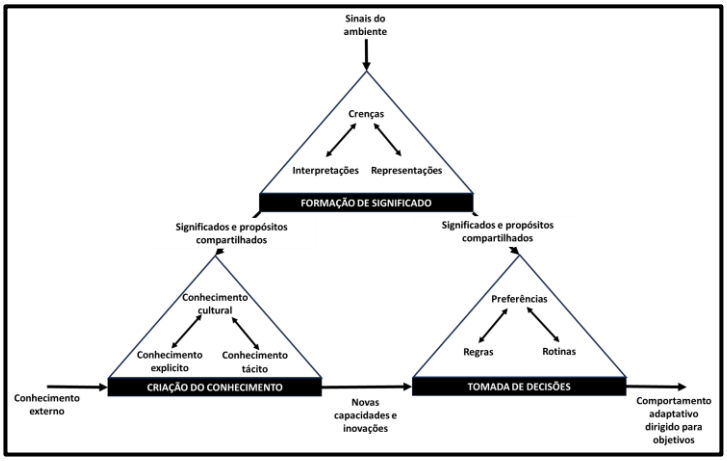
Choo (1998) rearranja os elementos internos de cada arena da Figura 2 de modo a destacar os elementos que constituem uma organização do conhecimento: cultura organizacional, a qual engloba os aspectos emocionais de cada arena; teoria da ação adotada, que abrange os

elementos cognitivos de cada arena; teoria da ação em uso, que envolve os elementos situacionais de cada arena. A Figura 3 representa esse arranjo.

2.2 CONSCIÊNCIA SITUACIONAL EM DEFESA CIBERNÉTICA

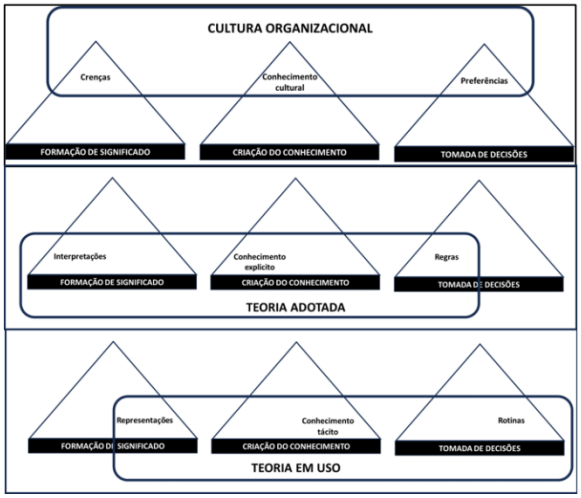
O entendimento do ambiente sempre foi uma necessidade humana, chegando mesmo a ser uma exigência para garantir a sobrevivência. Da consciência adquirida do que era dado da realidade, passa-se à ação, de acordo com a necessidade específica do momento. Desse modo, a consciência do que se passa e o desenvolvimento da capacidade de decidir como reagir conforme as circunstâncias acompanhou o desenvolvimento humano.

Figura 2 - Ciclo do conhecimento organizacional



Fonte: Choo (1998), traduzido para o português

Figura 3 – Elementos emocionais, cognitivos e situacionais



Fonte: Choo (1998), traduzido para o português.

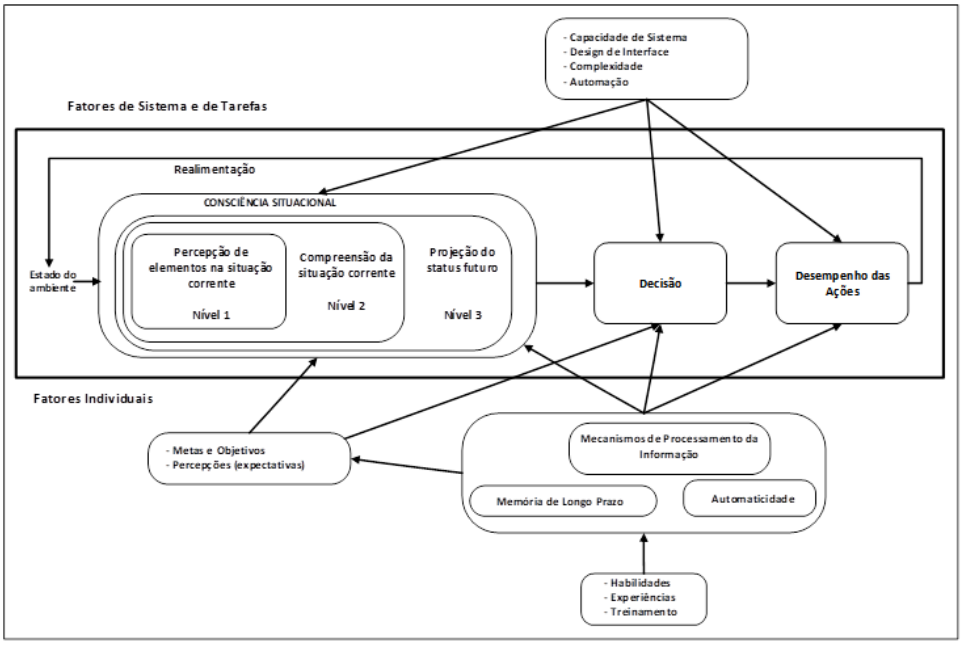
As guerras figuram dentre os eventos que mais requereram uma preparação sistemática para uma plena consciência do estado e da evolução da situação corrente. Numa batalha, os comandantes precisam ter conhecimento, lições aprendidas, experiências pessoais e de outros comandantes, além de virtudes diversas para que, confrontados com os dados advindos da contenda, fossem capazes de perceber o que era relevante, conjugar e interpretar essas percepções, conjecturar evoluções possíveis e decidir.

De especial importância para entendimento da consciência situacional para ambientes dinâmicos e complexos são os trabalhos da pesquisadora Mica Endsley, em particular um artigo usado como seminal em diversas pesquisas na área (ENDSLEY, 1995), no qual é proposto e explicado um modelo de CS, conforme a Figura 3. Como definição sobre o que é a consciência situacional, Endsley enuncia o seguinte:

> A consciência situacional é a percepção dos elementos do ambiente dentro de um volume de tempo e espaço, a compreensão de seu significado e a projeção de seu estado no futuro próximo." (ENDSLEY, 1995, p.36).

Embora a pesquisa em andamento aborde todos os elementos aludidos na Figura 3, para fins deste artigo apenas os conceitos fundamentais da pesquisa, quais seja, percepção, compreensão e projeção serão pormenorizados.

Figura 3 - Modelo de Consciência Situacional para tomada de decisão dinâmica



Fonte: Endsley (1995), traduzido para o português.

O primeiro estágio da consciência situacional, segundo Endsley (1995), 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. Endsley (1995) destaca o processamento pré-atenção, a Atenção e as Memórias de Trabalho e de Longo Prazo. Nesta pesquisa em andamento, o elemento de maior relevância para o estágio da percepção é o da pré-atenção.

O processamento de pré-atenção busca notar no ambiente observado características dos elementos que compõem esse ambiente e que chamam a atenção para eles. Exemplos utilizados nos sistemas de monitoração do espaço cibernético das redes de computadores são das cores dos ícones representativos de equipamentos críticos que se tornam amarelos ou vermelhos indicando uma anomalia que merece a atenção.

A Compreensão da situação se baseia numa síntese formada na mente do operador a partir dos elementos desconexos captados na percepção (ENDSLEY). A compreensão desses elementos se processa sempre à luz dos objetivos da operação.

De especial interesse para esta pesquisa em andamento é a memória de longo prazo. Essa memória está presente em todos os estágios representados na Figura 3. A memória de longo prazo, conforme sugere Endsley (1995) age como um repositório de onde a mente pode

recuperar conhecimentos dominados, os quais desempenham papel fundamental no reconhecimento de padrões, estabelecimento de categorizações, aplicação de regras, técnicas e controles, além outras possibilidades de consubstanciar esses conhecimentos à situação corrente. Três elementos são de relevância no contexto da memória de longo prazo: *scripts*, *schematas* e modelos mentais (ENDSLEY).

Schematas são estruturas de representação sob as quais sistemas de informação, mesmo os complexos, podem ser interpretados e representados simplesmente. Na sua descrição desse elemento, Endsley (1995) utiliza termo *framework* na acepção de um modelo esquemático de referência para se avaliar em algum grau uma dada situação ou orientar ações para lidar de modo mais acertado, conforme o conhecimento embutido no *framework*, com algum contexto a ser conduzido ou gerido. O *script* é uma forma simplificada de *schemata*, baseado em sequências de tarefas. *Schematas* e *scripts* facilitam a tomada de consciência situacional, diminuindo o número de inferências sobre as informações advindas do ambiente e sobre as quais se deve ter a CS, decidir e agir.

Os modelos mentais são *schematas* complexos, dos quais se geram descrições da forma e propósito de sistemas, explicações sobre o seu funcionamento e os seus estados observados e, por fim, de predições dos seus estados futuros (ENDSLEY, 1995).

O nível 3 da Consciência Situacional é a habilidade de projetar as ações dos elementos do ambiente, no mínimo, no curto prazo, e é referido como Projeção. Esse estágio da CS é atingido como consequência direta do conhecimento do estado e da dinâmica dos elementos do ambiente e da compreensão da situação corrente (ENDSLEY, 1995).

2.2.1 Consciência Situacional em Defesa Cibernética

Para aplicação do conceito de CS no contexto da defesa cibernética, Tadda e Salerno (2010) adaptam a definição de Endsley (1995) como segue:

> Consciência situacional é a percepção dos elementos do ambiente dentro de um espaço e tempo específicos, a compreensão do significado desses elementos e a projeção de seu estado em um futuro próximo para possibilitar a superioridade na tomada de decisões. (TADDA E SALERNO, 2010, p.17)

Assim, ao acrescentar o elemento de "superioridade de decisão", os autores apontam para a necessidade de aumentar a probabilidade de que as decisões tomadas sejam mais precisas que a dos eventuais antagonistas no espaço cibernético.

Segundo Barford et al. (2010), a CS em defesa cibernética está associada a pelo menos sete aspectos: (i) 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.

Esses aspectos são observados em operações cibernéticas pelos efeitos das ações cibernéticas sobre os seus alvos informacionais digitais (CARNEIRO, 2012).

Barford et al. (2010) ainda distribuem esses aspectos pelos níveis definidos por Endsley (1995) do seguinte modo: (a) Percepção dos elementos do ambiente (nível1): aspectos (i) e (vi); (b) Compreensão da situação corrente (nível2): aspectos (ii), (iv) e (v); (c) Projeção de estados futuros (nível 3): aspectos (iii) e (vii).

2.2.2 Frameworks e Normas de Segurança da Informação e Cibernética

De um modo geral, os *frameworks* são instrumentos de gestão que funcionam como quadros de referência para as áreas para as quais foram concebidos. Segundo Taherdoost (2022), *framework*s são guias que cobrem uma ampla gama de domínios, com objetivos gerais, mas sem os passos específicos para atingir esses objetivos, além de serem usados como padrão de qualidade para o que deve ser alcançado no contexto de sua aplicação, descrevendo escopo e sumarizando entradas e saídas.

Especificamente sobre *frameworks* de segurança cibernética, Taherdoost (2022) informa que são estruturas que uma organização necessita para se tornar protegida contra ataques cibernéticos, enquanto Syafrizal at al (2020, p. 419) afirma que o principal objetivo *framework*s de segurança cibernética é reduzir riscos, incluindo a prevenção e mitigação de ataques cibernéticos. Syafrizal at al (2020, p. 419) destaca a maior parte dos elementos de um *framework* de segurança cibernética são as melhores práticas do setor.

Nesse sentido, sendo os *framework*s de segurança cibernética reflexos das melhores práticas do setor, observa-se da sua aplicação a abrangência de áreas não só de tecnologia da informação, mas de normatização, gestão de recursos humanos, segurança física, além de outros elementos, o que leva a aplicação desse tipo de *framework* como um instrumento de sensibilização e aculturamento do pessoal em segurança, disciplinamento de ações estratégicas pelos documentos normativos gerados e formação de procedimentos operacionais específicos requeridos pelos ativos onde as ações estratégicas têm reflexos.

3 RESULTADOS PARCIAIS

A primeira delimitação da pesquisa vem do uso dos *frameworks* de segurança cibernética. Por definição, esses *frameworks* são criados para: (i) sensibilizar as pessoas da organização a terem comportamentos favoráveis à segurança, o que atuará sobre as crenças, o conhecimento cultural e as preferências do pessoal, ou seja na **cultura organizacional**; (ii) referenciar a geração de normativos, diretrizes, além de outros instrumentos similares para a segurança da cibernética institucional, o que leva a influenciar as interpretações, os conhecimentos explícitos gerados e as regras para aplicação da segurança, ou seja a **teoria adotada**; (iii) fomentar maneiras operacionais de execução das regras e diretrizes institucionais a respeito da segurança cibernética sejam implementadas na prática alinhadas e agregando valor às regras e diretrizes, refletindo na captação dos elementos informacionais, no conhecimento tácito e nas rotinas empregadas, ou seja, na **teoria em uso**.

Assim, é possível aplicar os *frameworks* de cibernética como instrumentos que levam à formação de significado, a criação de conhecimento e a tomada de decisão. Em termos de estrutura e aplicação, os *frameworks* são majoritariamente correspondentes aos elementos cognitivos no modelo de Choo (1998), pois sua forma é de registro de orientações. Desse modo, a pesquisa limita-se à busca de elementos nos *frameworks* cuja aplicação gere elementos de natureza cognitiva no modelo de Choo (1998). Para viabilizar essa busca, três adaptações serão estabelecidas para os elementos da teoria adotada originais do modelo: (i) **interpretações para defesa cibernética**: Anomalias do espaço cibernético que sejam consideradas como eventos de segurança cibernética que mereçam atenção e análise dos gestores da organização e que se provem úteis para utilização futura, sendo registrados e armazenados para esse fim; (ii) **conhecimentos explícitos para defesa cibernética**: conhecimentos codificados em políticas, planos, relatórios técnicos, processos, lições aprendidas, metodologias, técnicas, categorias e estatísticas de ataque ou outros conhecimentos codificados similares e passíveis de aplicação

para a defesa cibernética; (iii) **regras para defesa cibernética**: regras que especificam o comportamento apropriado, a alocação de atenção, participação nas ocasiões de escolha de decisão para lidar com eventos de segurança cibernética, sendo baseadas em subsídios advindos de gestão de riscos, registros de incidentes, inteligência cibernética e cenários de incidentes cibernéticos.

Outro recorte da pesquisa é em relação ao modelo de consciência situacional de Endsley (1995). Essa personalização foi realizada pela identificação no modelo de Endsley de aspectos articuladores desse modelo com a **teoria adotada de defesa cibernética**. Os aspectos escolhidos pelas suas características majoritariamente ligadas ao domínio cognitivo, conforme primeiro recorte, foram a pré-atenção, para a percepção, e a memória de longo prazo tanto para a compreensão quanto para a projeção. E como elemento de base que permeiam esses aspectos escolhidos foram escolhidos os *schemata*.

Estruturadas essas pontes entre as referências teóricas e os objetivos da pesquisa, espera-se produzir, primariamente e em estágio intermediário da pesquisa, um *framework* para a teoria adotada de defesa cibernética em formato de controles de segurança e, por fim, adaptar a redação desses controles para um *framework* de necessidades informacionais primordiais. Para a sua validação, espera-se confrontar esse *framework* de necessidades primordiais com os registros de operações reais ocorridas entre 2012 e 2016, sob a coordenação do Centro de Defesa Cibernética, organização militar do Exército, responsável por coordenar e integrar as operações de defesa cibernética realizadas no período.

REFERÊNCIAS

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.; LIU P.; SWARUP V. ; WANG C. (org). **Cyber situational awareness:** issues and research. Berlim: Springer, 2010. p. 15-34.

BRASIL, **Decreto n. 6.703**, de 18 de dezembro de 2008. Aprova a Estratégia Nacional de Defesa, e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/Decreto/D6703.htm. Acesso em 16 dez 2023.

CARNEIRO, J. M. E. **A guerra cibernética**: uma proposta de elementos para formulação doutrinária no Exército Brasileiro. 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 16 dez 2023.

CHOO, C. W. **Information management for the inteligent organization**. Medford, NJ: Today, Inc., 1998. 272 p.

ENDSLEY, M. Toward a theory of situation awareness in dynamic systems. In: **Human Factors Journal**, v. 37, n. 1, 1995. p. 32–64.

ROBREDO, J. R. **Da ciência da informação revisitada aos sistemas humanos de informação**. Brasília: Thesaurus, 2003. 245 p.

SYAFRIZAL, M.; SELAMAT, S. R.; ZAKARIA, N. A. Analysis of cybersecurity standard and framework components. **International Journal of Communication Networks and Information Security (IJCNIS),** v. 12, n. 3, 2022. Disponível em https://doi.org/10.17762/ijcnis.v12i3.4817. Acesso em 15 dez 2023.

TADDA, G.; SALERMO, J. Cyber SA: overview of cyber situation awareness. *In*: JAJODIA S.; LIU P.; SWARUP V. ; WANG C. (org). **Cyber situational awareness:** issues and research. Berlim: Springer, 2010. p. 15-34.

TAHERDOOST, H. Understanding cybersecurity frameworks and information security standards: a review and comprehensive overview. **Electronics**. Basel: MDPI, 2022. Disponível em SSRN: https://ssrn.com/abstract=4178718. Acesso em 15 dez 2023.