Consciência situacional como ferramenta estratégica da defesa cibernética

André Lucas Alcântara da Silva | *Gills Vilar-Lopes*[1]

INTRODUÇÃO

A segurança cibernética é fundamental no mundo atual, exigindo estratégias inovadoras para lidar com ameaças digitais em constante evolução. A consciência situacional (CS) emerge como uma ferramenta estratégica para proteger ativos digitais. Este artigo explora a teoria da CS, sua interseção com conceitos de estratégia em conflitos modernos e sua versão virtual, a consciência situacional cibernética (CSC), além de sua integração na defesa nacional.

O texto está dividido em quatro seções. A primeira explora a teoria da CS, inicialmente concebida em ambientes operacionais, mas aplicável ao domínio cibernético. São discutidos modelos conceituais e suas aplicações práticas, destacando sua importância na tomada de decisões. A segunda seção estabelece um paralelo entre CS e conceitos tradicionais de estratégia militar e aeroespacial, utilizando obras de Sun Tzu, Carl von Clausewitz e Giulio Douhet como referência. A terceira seção destaca a vertente cibernética da CS, a CSC. Nesse contexto, Singer e Friedman enfatizam que a CSC «se refere à habilidade de entender, prever e reagir eficientemente aos eventos cibernéticos»[2]. A evolução dessa teoria, desde suas bases conceituais até às aplicações práticas na esfera digital,

RESUMO

O crescimento tecnológico nas últimas décadas transformou diversas áreas da sociedade e do Estado, incluindo a defesa, devido à sua natureza tecnológica. Isso levantou discussões sobre o «espaço cibernético», o «poder cibernético» e o «domínio cibernético». O ciberespaço influencia os domínios operacionais tradicionais, tornando crucial o conhecimento do espaço cibernético, tanto próprio quanto dos adversários, como vantagem competitiva em conflitos entre Estados. Isso é conhecido como «consciência situacional», concebida por Mica Endsley nos anos 1980, definida como a capacidade de perceber, compreender e prever atividades em um espaço e tempo específicos. Esse conceito se desdobra no âmbito cibernético, criando a consciência situacional cibernética, o conhecimento das ações no espaço cibernético. Este artigo explora o papel estratégico da consciência situacional cibernética, identificando teorias e modelos de consciência situacional e seus desdobramentos na estratégia militar.

Palavras-chave: consciência situacional cibernética, defesa nacional, estratégia.

→

 https://doi.org/10.23906/ri2024.82a08

ABSTRACT

Situational awareness as a strategic tool for cyber defense

The technological growth of the last decades has changed the way many sectors of society and the state carry out their respective activities. The defense sector is part of this framework due to its essentially technological nature. With these changes, discussions began about phenomena known as 'cyberspace', 'cyber power', and 'cyber domain'. Because cyberspace permeates and can even influence the other operational domains (sea, land, air, and space), having the right knowledge of cyberspace – both one's own and that of one's adversaries – has become a competitive advantage in interstate conflicts. This knowledge is called situational awareness, a concept conceived in the 1980's by Mica Endsley, then Chief Scientist of the United States Air Force, and which can be defined as the ability to perceive and understand activities in a given time and space and to predict the future evolution of the situation. This concept can be unfolded in the cyber domain, giving rise to the so-called cyber situational awareness, which generally means the full knowledge of the actions occurring in the cyber space of interest. Thus, this article aims to elucidate the strategic role of cyber situational awareness, identifying the theories and models of its emerging concept and, subsequently, its developments in military strategy.

Keywords: cyber situational awareness, national defense, strategy.

é abordada aqui. A quarta seção explora a relação entre CSC e defesa nacional, integrando-as na proteção dos interesses nacionais e fortalecendo as capacidades de defesa cibernética e inteligência militar contra ameaças digitais.

Em suma, o artigo estabelece bases teóricas para a relevância da CS e CSC no domínio cibernético, visando proteger ativos digitais e defender contra ameaças cibernéticas contemporâneas.

CONSCIÊNCIA SITUACIONAL: CONCEITO, MODELOS E APLICABILIDADE

O conceito de CS pode ser definido como a consciência apropriada de uma situação específica[3]. De acordo com Stanton[4], o tema ganhou notoriedade na década de 1980, inicialmente na indústria da aviação, com o objetivo de melhorar a capacidade de decisão de pilotos e controladores de tráfego aéreo. Em situações de estresse, o responsável pela decisão deve identificar e interpretar as informações disponíveis para escolher a melhor ação.

Consoante Woods[5], para manter um nível aceitável de CS, é necessário acompanhar os acontecimentos e sua evolução ao longo do tempo, identificando «gatilhos» que indicam a necessidade de uma reação adequada. A CS é obtida de forma gradual, à medida que o cenário é compreendido pelo tomador de decisão. Com a evolução dos estudos relativos à CS, o conceito foi expandido para áreas distintas da aviação, mas que, igualmente, exigiam dos envolvidos um amplo conhecimento sobre determinado ambiente. Kaber e Endsley[6] entendem que a CS também pode ser utilizada em outros ambientes industriais devido a similaridades como: múltiplos objetivos simultâneos, tarefas concorrentes pela atenção e ambientes de alto estresse. Essas características comuns permitem extrapolar a aplicação da CS a cenários como a defesa, incluindo a defesa cibernética.

Os estudos sobre CS evoluíram, resultando em quatro teorias principais, cada uma com idiossincrasias específicas. A primeira, de Mica Endsley, define CS como «a percepção de elementos do ambiente dentro de um volume de tempo e espaço, a compreensão do seu significado e uma projeção do seu estatuto no futuro próximo»[7]. A segunda teoria, de Bedny e Meister[8], incorpora a dimensão temporal, enfatizando a adaptabilidade da

CS às mudanças nas condições operacionais. Em terceiro lugar, o modelo de Stanton[9] destaca a CS como uma habilidade distribuída, influenciada por fatores sociais, tecnológicos e organizacionais. Por último, o quarto modelo, de Smith e Hancock[10], conhecido como «ciclo perceptivo», evidencia o processo contínuo de percepção e interação humana no ambiente operacional, alcançando a CS através da repetição do processo de percepção e da postura proativa do elemento humano.

Essas teorias possuem pontos fortes e fracos, podendo ser aplicadas de forma isolada ou conjunta em diferentes cenários. A seguir, são detalhados aspectos particulares de cada uma delas.

MODELO DE ENDSLEY

O modelo de CS proposto por Endsley[11] oferece uma estrutura conceitual que delineia a percepção humana em ambientes complexos e dinâmicos. Constituído por três componentes interrelacionados – percepção da situação, compreensão da situação e projeção da situação – esse *framework* é conhecido como «modelo de três níveis». Esses níveis são progressivos: o nível 3, «projeção», é alcançado após o nível 2, «compreensão», que depende do nível 1, «percepção».

A fase inicial concentra-se na percepção dos elementos no ambiente, envolvendo a assimilação de informações sensoriais, como dados visuais e auditivos. Endsley destaca que a percepção é uma compreensão ativa do ambiente, fornecendo as entradas para o processo cognitivo subsequente.

No estágio seguinte, a compreensão da situação, as informações percebidas são interpretadas, permitindo um entendimento mais profundo do contexto. A compreensão evolui com novas informações, representando a transição crucial da percepção para a interpretação, fornecendo uma base sólida para a tomada de decisões.

A terceira componente, projeção da situação, envolve a capacidade de antecipar mudanças futuras no ambiente. A projeção permite prever eventos potenciais, proporcionando uma visão abrangente e preparando os tomadores de decisão para eventos futuros.

Essas três componentes formam um ciclo contínuo, constituindo a base do entendimento humano em ambientes complexos. O modelo de Endsley oferece uma estrutura robusta para a interação entre percepção, compreensão e projeção, aplicável a diversos contextos, incluindo o militar e o cibernético.

MODELO DE BEDNY E MEISTER

O modelo de Bedny e Meister[12] oferece uma perspectiva orientada às atividades individuais, integrando a dimensão temporal na construção da CS. Este modelo reconhece que a consciência da situação é dinâmica e evolui em resposta às mudanças operacionais. Bedny e Meister argumentam que a CS não pode ser compreendida sem considerar seu desenvolvimento ao longo do tempo. Assim, a adaptação e atualização constante da compreensão da situação tornam-se centrais na construção da CS.

O modelo destaca a necessidade de uma CS adaptativa, implicando que os indivíduos devem ajustar continuamente sua compreensão da situação para refletir as condições em evolução.
Em operações militares/cibernéticas, em que a dinâmica do campo de batalha pode mudar abruptamente, a capacidade de antecipar e reagir a alterações na situação é vital.

MODELO DE STANTON

O modelo de CS proposto por Stanton[13] destaca-se por sua abordagem inovadora, fundamentada na teoria da habilidade distribuída. Diferente dos modelos tradicionais, este reconhece que a CS é uma habilidade distribuída entre indivíduos e sistemas, crucial em ambientes complexos e dinâmicos. Stanton argumenta que a CS não reside apenas na mente individual, mas é compartilhada entre elementos sociais, tecnológicos e organizacionais, enfatizando a colaboração e a comunicação como componentes essenciais.
A teoria da habilidade distribuída desafia as concepções tradicionais que limitam a inteligência ao indivíduo, postulando que a realização de tarefas envolve a interação entre pessoas, artefatos tecnológicos e o ambiente. Em seu estudo sobre sistemas colaborativos, Hollan, Hutchins e Kirsh[14] afirmam que «o processo cognitivo estende-se para além dos limites da cabeça humana», mostrando que a inteligência é moldada pela comunicação e interação entre componentes distribuídos.
Ao adaptar essa teoria para ambientes cibernéticos, Stanton destaca a relevância dessa abordagem na defesa cibernética contemporânea[15]. Reconhece-se que a CS em contextos digitais não pode ser concebida apenas como uma função individual, mas como um fenômeno coletivo que abrange analistas, operadores de sistemas de segurança e outros atores relevantes.

MODELO DE SMITH E HANCOCK

A teoria do ciclo perceptivo, desenvolvida por Smith e Hancock[16], oferece uma visão dinâmica da CS, destacando a interação contínua entre ser humano e máquina. A CS é vista como um processo ativo de percepção e interpretação constante das informações do ambiente operacional. A percepção ativa, essencial segundo a teoria, implica na busca proativa por dados relevantes, especialmente em ambientes dinâmicos. A abordagem encontra aplicação em contextos operacionais complexos, como operações militares, onde a capacidade de perceber e reagir rapidamente é crucial. Assim, a teoria ressalta a importância da percepção ativa para manter uma CS eficaz em ambientes desafiadores, enfatizando a necessidade de envolvimento contínuo na obtenção e interpretação das informações.

CONSCIÊNCIA SITUACIONAL E ESTRATÉGIA MILITAR

Apesar de grande parte dos estudos relativos à CS ter sido realizada do final da década de 1980 em diante, a história revela que o conceito já havia sido aplicado

pelo piloto alemão Oswald Boelke durante a Primeira Guerra Mundial. Naquela ocasião, ele percebeu a importância de se obter uma consciência do inimigo antes que este pudesse fazer o mesmo[17]. Boelke apontou como o conhecimento do inimigo pode ser decisivo para o sucesso em um conflito, algo também observado por Sun Tzu em *A Arte da Guerra*, fornecendo uma base rica para entender a CS à luz das teorias modernas.

APESAR DE GRANDE PARTE DOS ESTUDOS RELATIVOS À CS TER SIDO REALIZADA DO FINAL DA DÉCADA DE 1980 EM DIANTE, O CONCEITO JÁ HAVIA SIDO APLICADO PELO PILOTO ALEMÃO OSWALD BOELKE DURANTE A PRIMEIRA GUERRA MUNDIAL.

A CS, em si, se dá a partir de um importante insumo: a informação. De acordo com Endsley[18], o primeiro e mais elementar nível da CS é a «percepção dos elementos de um ambiente». Nele, de fato, ainda não há informação, apenas dados disponíveis. A partir deles, o indivíduo deve ter a capacidade de correlacioná-los, dando-lhes significado e chegando ao segundo nível da CS, que trata da «compreensão da situação atual». Neste ponto, sim, existe informação. A maneira como esta informação será tratada pode levar o indivíduo ao nível mais alto de CS, a «previsão do estado futuro de uma situação». Bem, a forma como este processo cognitivo é desenhado, tendo como principal componente a informação, possibilita que tal conceito seja analisado à luz das principais teorias relativas aos estudos estratégicos e da própria guerra.

Sun Tzu, o estrategista chinês do século IV a. C., em sua obra clássica *A Arte da Guerra*[19], fornece uma base rica para entender a CS à luz das teorias modernas. Os princípios filosóficos e estratégicos de Sun Tzu podem ser conectados aos elementos fundamentais das quatro teorias contemporâneas de CS, apresentadas anteriormente:

a) Conhecimento profundo do ambiente: Sun Tzu enfatiza a importância de conhecer o terreno e compreender o ambiente operacional. Em paralelo, o modelo de Endsley destaca a necessidade de uma percepção completa da situação, enfatizando «a percepção do ambiente, incluindo os fatores relevantes no espaço e no tempo»[20]. Essa conexão ressalta a importância do entendimento profundo do ambiente em ambas as perspectivas.

b) Adaptação constante: o estrategista chinês aborda a necessidade de adaptação constante às circunstâncias em mudança. Esse princípio ecoa no modelo de Stanton, que destaca a adaptabilidade como um elemento essencial da CS, incorporando a ideia de «habilidade distribuída» que se ajusta às demandas operacionais.

c) Antecipação e prevenção: Sun Tzu sublinha a importância de antecipar os movimentos do inimigo e evitar conflitos diretos quando possível. Essa abordagem preventiva encontra paralelos na teoria do ciclo de percepção, de Smith e Hancock[21], que destaca a antecipação como um resultado do contínuo processo de «percepção» do ambiente, permitindo a projeção de eventos futuros e, consequentemente, a um estado de CS eficaz.

Por sua vez, Carl von Clausewitz[22], renomado estrategista prussiano do século XIX, também pode ser utilizado para correlacionar a CS e os conceitos de estratégia militar. Em sua obra magistral *Da Guerra*, introduziu o conceito de «névoa da guerra» para descrever a incerteza e a falta de clareza que permeiam os campos de batalha. Ao explorar essa noção, pode-se estabelecer uma ponte com as teorias modernas de CS.

a) «Névoa da guerra» como incerteza: Clausewitz argumenta que a névoa da guerra resulta da incerteza inerente a todas as operações militares, a qual está alinhada com o reconhecimento, no modelo de Endsley[23], de que a CS envolve a percepção e compreensão de eventos em um ambiente dinâmico e incerto.
b) Adaptação à «névoa da guerra»: o general prussiano destaca a necessidade de adaptação constante devido à «névoa da guerra». Essa ideia ressoa com o modelo de Stanton[24], que enfatiza a adaptabilidade como uma característica central da CS, especialmente na teoria da habilidade distribuída.
c) Ciclo de percepção: a «névoa da guerra», de Clausewitz, também pode ser relacionada à teoria do ciclo de percepção, de Smith e Hancock, uma vez que ambos os conceitos reconhecem a limitação da percepção e a necessidade de constantes ciclos de atualização da situação.

Além da «névoa da guerra», outros princípios e conceitos de Carl von Clausewitz em *Da Guerra* podem ser correlacionados com as teorias modernas de CS, oferecendo uma perspectiva mais abrangente. Veja-se:

a) Centro de gravidade e foco estratégico: Clausewitz introduz o conceito de centro de gravidade como o ponto crucial que, se atacado, pode levar à derrota do inimigo. Na CS, a percepção do «centro de gravidade» de uma situação, ou seja, o ponto central que influencia o curso dos eventos, é essencial. O modelo de Endsley, por exemplo, enfatiza a importância de compreender os elementos cruciais no ambiente.
b) Fricção e desafios na percepção: a «fricção» em Clausewitz refere-se às dificuldades e desafios inerentes à guerra. Esse conceito pode ser relacionado à «fricção» na CS, reconhecendo que a percepção e a compreensão de uma situação estão sujeitas a desafios e dificuldades constantes. O modelo de Stanton destaca a necessidade de superar a «fricção cognitiva», uma vez que, em sua perspectiva, o conhecimento necessário para se obter a CS está distribuído e, por vezes, não organizado[25].

Outro conhecido teórico da guerra, o general Giulio Douhet[26], também abordou tópicos e pensamentos considerados nos modelos de CS. Em seu conhecido trabalho *O Domínio do Ar*, no início do século XX, estabeleceu princípios fundamentais sobre o poder aeroespacial. Sua visão revolucionária sobre o papel da aviação nas operações

militares pode ser correlacionada com o conceito de CS, especialmente considerando o contexto aeroespacial:

a) Domínio do ar e percepção global: Douhet defendia a ideia de que o controle do domínio do ar era crucial para o sucesso militar. Essa perspectiva se alinha com a CS no sentido de que a percepção global do ambiente, incluindo elementos no espaço e no tempo, é fundamental. O modelo de Endsley destaca a importância da percepção abrangente.
b) Velocidade e pronta resposta: o general enfatizava a importância da velocidade e da resposta rápida no poder aeroespacial. Essa ênfase encontra paralelo na teoria da habilidade distribuída de Stanton, que destaca a necessidade de uma resposta ágil em ambientes dinâmicos[27].

CONSCIÊNCIA SITUACIONAL CIBERNÉTICA: UMA EXPLORAÇÃO CONCEITUAL

A consciência situacional cibernética (CSC) é uma extensão do conceito de CS para o espaço cibernético, herda as bases conceituais da CS tradicional, mas as adapta ao ambiente digital complexo. Enquanto a CS tradicional lida com elementos físicos, a CSC lida com eventos em redes digitais complexas. Assim como a CS, a CSC é crucial em ambientes críticos que exigem alta atenção e capacidade de decisão. Ela pode ser definida como a percepção de eventos e dados de rede, compreendendo seu significado em termos de missão, recursos, conectividade, ameaças e vulnerabilidades, e projetando seu estado futuro próximo[28].

Ao migrar para a CSC, novas dimensões surgem, como a percepção e a compreensão de eventos em redes digitais. Autores como David D. Woods e Erik Hollnagel[29] destacam a importância de considerar as características únicas do ambiente cibernético.

No entanto, seria equivocado concluir que a CSC é uma mera aplicação da teoria de CS ao contexto cibernético. Na verdade, ela demanda uma abordagem interdisciplinar, incorporando conceitos da teoria de sistemas, da ciência da computação e da engenharia de *software*. Em outras palavras, há de se considerar, além das bases teóricas de CS, os aspectos intrínsecos do ambiente cibernético, o qual é composto não apenas pela componente tecnológica, mas também humana e processual. Ademais, de forma similar ao seu conceito ascendente, a CSC não deve encontrar um fim em si, mas integrar processos mais amplos visando o auxílio na tomada de decisão estratégica. Porém, para compreender a CSC, é essencial contextualizá-no campo mais amplo da CS e explorar as teorias existentes.

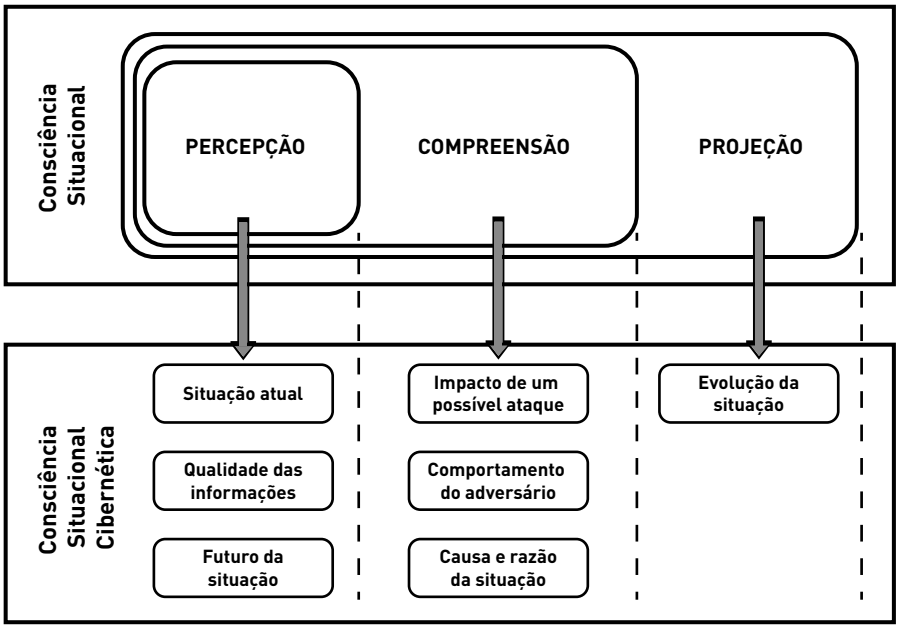
DE FORMA SIMILAR AO SEU CONCEITO ASCENDENTE, A CSC NÃO DEVE ENCONTRAR UM FIM EM SI, MAS INTEGRAR PROCESSOS MAIS AMPLOS VISANDO O AUXÍLIO NA TOMADA DE DECISÃO ESTRATÉGICA.

Dessa forma, existem facetas que precisam ser consideradas para a obtenção de uma CSC efetiva, a saber: (i) avaliação do atual estado da rede de computadores; (ii) com-

preensão do impacto de um ataque cibernético; (*iii*) compreensão do comportamento do atacante; (*iv*) compreensão das causas do ataque sofrido; (*v*) compreensão da confiabilidade de qualquer consciência obtida; e (*vi*) conhecimento das posições de ataque e defesa, para identificar ações futuras.

De maneira sintética, o conceito de CSC, comparado à CS, pode ser evidenciado pelo diagrama da figura 1.

Figura 1 > Consciência situacional cibernética a partir dos níveis de consciência situacional



Fonte: Elaboração própria.

A avaliação dos parâmetros teóricos da CSC pode ser conduzida considerando a aderência das principais teorias de CS. Cada uma delas oferece perspectivas distintas, e a seleção apropriada deve ponderar os elementos específicos enfatizados no estudo. Por exemplo, o modelo de Endsley destaca-se pela sua aplicabilidade em ambientes cibernéticos, enfatizando a compreensão rápida da situação e a tomada de decisões eficazes diante de ameaças. Suas fases oferecem uma estrutura robusta para investigações no domínio cibernético.

Por sua vez, a teoria da habilidade distribuída de Stanton revela-se pertinente ao considerar a distribuição de tarefas e funções nesses ambientes. Sua ênfase na distribuição da cognição entre diferentes elementos do sistema oferece uma abordagem valiosa para analisar a interação complexa.

Já a teoria do ciclo perceptivo de Smith e Hancock concentra-se nos processos perceptivos dos operadores, sendo relevante para compreender como informações são percebidas e interpretadas em cenários cibernéticos.
Por fim, o modelo de Bedny e Meister destaca a interação entre elementos do sistema, sendo especialmente pertinente na consideração da interdependência entre atores humanos e sistemas tecnológicos em ambientes cibernéticos. Embora a ampla compreensão da CSC passe, necessariamente, pelos conceitos e teorias estabelecidos no âmbito da CS, uma aplicação eficaz no ambiente cibernético pode extrapolar tais referências. Portanto, torna-se latente uma abordagem interdisciplinar sobre o tema, considerando, também, as especificidades inerentes a um ambiente tecnológico cada vez mais complexo, aliado aos objetivos desejados ao se aplicar a CSC. Tal abordagem, de acordo com Jajodia e Albanese[30], passa pela definição do «espaço cibernético de interesse», ou seja, de uma fração do espaço cibernético ao qual o tomador de decisão deseja obter a CS necessária.

CONSCIÊNCIA SITUACIONAL CIBERNÉTICA E A DEFESA NACIONAL

De acordo com a Política Nacional de Defesa (PND) brasileira, a defesa nacional pode ser compreendida como:

> «o conjunto de atitudes, medidas e ações do Estado, com ênfase na expressão militar, para a defesa do Território Nacional, da soberania e dos interesses nacionais contra ameaças preponderantemente externas, potenciais ou manifestas»[31].

Por sua vez, o *Livro Branco de Defesa Nacional* (LBDN) brasileiro reforça que este conceito de defesa nacional:

> «além de ser importante vetor para a preservação da Soberania Nacional, também possibilita a manutenção da integridade territorial, a consecução dos objetivos nacionais, a proteção ao povo e a garantia de não ingerência externa no território nacional»[32].

Ambos os documentos, em conjunto com a Estratégia Nacional de Defesa (END), formam o principal arcabouço teórico/estratégico do Brasil, o qual direciona, principalmente, sua componente militar.
A partir dessas referências, o Brasil descreve e delimita áreas que podem afetar ou comprometer a integridade do território brasileiro, a soberania e os objetivos nacionais. É neste viés que o setor cibernético ganha notoriedade. O LBDN aponta como o referido setor pode influenciar a própria defesa nacional quando assume que:

> «a possibilidade de o País sofrer um ataque cibernético de origens das mais diversas e de difícil identificação, que poderão causar danos consideráveis a estruturas estratégicas

> ou mesmo a outros setores de importâncias vitais para a nação brasileira, faz com que a Defesa Cibernética passe a ter importância fundamental para a Defesa Nacional»[33].

Desta feita, o Brasil assume a relevância estratégica do tema (cibernético) e inicia um novo ciclo de envolvimento e desenvolvimento do setor, com vistas à defesa nacional. A partir de então, o Brasil abre espaço para discussões relativas aos inúmeros conceitos que circundam o assunto – como: domínio cibernético, espaço cibernético e poder cibernético –, bem como as perspectivas que analisam se tal componente poderia ser considerada um novo domínio operacional, a exemplo daqueles já reconhecidos (mar, terra, ar e espaço exterior). Inevitavelmente, a reflexão sobre estes conceitos leva a uma análise de como são interpretados pelos principais estudiosos contemporâneos que abordam o fenômeno, além de uma avaliação da forma como os grandes *players* do cenário internacional assumem a questão cibernética.

Neste contexto, considerando a perspectiva acadêmica, é quase unânime o reconhecimento estratégico da componente cibernética, sendo esta capaz de proporcionar vantagens significativas em uma situação de conflito, visto que possui condições de influenciar os domínios operacionais já existentes. Na visão de Nocetti[34], o domínio cibernético possui características particulares por se tratar de algo criado pelo próprio homem e que, além disso, sofre mudanças em um ciclo muito mais veloz se comparado aos demais domínios. O mesmo autor, ainda, reforça que tais especificidades proporcionam uma menor barreira de entrada para que novos atores passem a agir neste domínio, o que, em última instância, poderia gerar conflitos em tal ambiente, os quais seriam denominados como «guerra cibernética». Assim, surge o conceito de poder cibernético o qual é definido, de forma ampla, como:

> «a capacidade de proteger e promover os interesses nacionais no ciberespaço e através dele: considerar os benefícios que o ciberespaço oferece aos nossos cidadãos e à nossa economia, trabalhar com os parceiros para um ciberespaço que reflita os nossos valores e utilizar as cibercapacidades para influenciar os acontecimentos no mundo real»[35].

No âmbito de tais discussões, Lonsdale[36] introduz o conceito de infoesfera, em que este sim poderia ser considerado um domínio estratégico. Para ele, tal conceito é ainda mais amplo se comparado à interpretação de «espaço cibernético», o qual seria considerado apenas como mais uma componente da infoesfera. Já o ponto de vista exposto por Gray[37] destoa dos anteriores, uma vez que este reconhece a natureza relevante do setor cibernético, porém não o interpreta como sendo um novo domínio operacional, mas, sim, um «atuador» e «habilitador» importante naqueles já existentes. Nesta mesma esteira, Rid[38] ressalta que ataques cibernéticos não poderiam ser interpretados como atos de guerra por si só, simplesmente pelo fato de não se enquadrarem nos conceitos que definem a guerra. Para ele, tais ações são «apenas versões sofisticadas de três atividades que são tão antigas quanto a própria guerra: sabotagem, espionagem e subversão»[39].

Diante das várias discussões sobre o tema, inúmeros países assumiram o espaço cibernético como um novo domínio operacional, passando a incluí-lo de forma categórica em seus respectivos documentos estratégicos. O Brasil, por sua vez, é claro ao descrever a posição nacional em sua mais nova versão da Doutrina Militar de Defesa Cibernética[40], publicada em 2023.

INÚMEROS PAÍSES ASSUMIRAM O ESPAÇO CIBERNÉTICO COMO UM NOVO DOMÍNIO OPERACIONAL, PASSANDO A INCLUÍ-LO DE FORMA CATEGÓRICA EM SEUS RESPECTIVOS DOCUMENTOS ESTRATÉGICOS.

O Brasil, na esteira dos acontecimentos relevantes ocorridos no espaço cibernético nos últimos anos, reconhece esse ambiente como um domínio operacional, no qual ações cibernéticas ofensivas e defensivas tendem a potencializar ou complementar as ações realizadas nos demais domínios (terra, mar, ar e espaço).

A partir desta concepção e, conforme delineado na PND, na END e no *LBDN*, considerando a importância na obtenção e manutenção do conhecimento neste novo domínio operacional, a CSC se apresenta como uma ferramenta valiosa na consecução da defesa nacional, uma vez que esta propõe a percepção, compreensão e projeção de atividades que ocorram no espaço cibernético de interesse.

Assim, é possível identificar um novo desafio a ser superado pelos tomadores de decisão, qual seja: como se organizar para obter uma CSC efetiva e que, de fato, colabore diante dos conflitos contemporâneos? Nesse aspecto, países e organizações buscam encontrar um modelo que seja aplicável às suas necessidades.

A partir desse objetivo, em uma de suas várias iniciativas em torno do assunto, os Estados Unidos, por intermédio de seu Departamento de Defesa, financiam pesquisadores no âmbito do programa Multidisciplinary University Research Initiative para tratar do assunto. Alguns desses pesquisadores, Sushil Jajodia e Massimiliano Albanese, conceberam um modelo conhecido como «Integrated Framework for Cyber Situation Awareness»[41]. Nele, são abordadas capacidades necessárias para uma CSC eficaz, como as habilidades de: enxergar o cenário de defesa cibernética de forma holística; gerenciar incertezas; raciocinar, mesmo diante de um ambiente «ruidoso» e com nível de conhecimento limitado, dentre outras.

Outro exemplo, na busca por uma CSC que atenda às necessidades identificadas, é o modelo proposto pelo coronel da Força Aérea dos Estados Unidos, Rizwan Ali, no âmbito da Task Force Cyber do Supreme Headquarters Allied Powers Europe (SHAPE-NATO), e conhecido como «cyber situational awareness for the NATO Alliance»[42]. O modelo é baseado em três componentes: consciência das ameaças existentes; consciência da rede de dados e demais componentes tecnológicos de interesse; consciência do objetivo a ser alcançado.

No Brasil, há iniciativas em torno da busca por uma melhor CSC. No âmbito da defesa nacional, é possível destacar as iniciativas que envolvem o Sistema Militar de Defesa Cibernética que, de acordo com a Doutrina Militar de Defesa Cibernética[43],

é estruturado nos níveis estratégico, operacional e tático, e implicam tanto o Ministério da Defesa, quanto as estruturas de defesa cibernética das Forças Armadas, tendo o Comando de Defesa Cibernética (ComDCiber) como órgão central do sistema.
De forma geral, a partir das ações de considerar o domínio cibernético em documentos estratégicos, bem como a busca por modelos e estruturas organizacionais que colaborem para uma CSC eficaz, demonstra como os países, inclusive o Brasil, enxergam a componente cibernética como estratégica para a defesa nacional.

CONCLUSÃO

No arcabouço dos estudos estratégicos e da influência exercida pela componente cibernética sobre os domínios tradicionais, o presente artigo se propôs a identificar o papel estratégico da CSC no âmbito da defesa nacional. Para tanto, foram descritas as bases teóricas e modelos do seu conceito ascendente, ou seja, da CS, e como essa vem sendo aplicada em atividades complexas e operacionais desde a década de 1980. Dessa forma, quatro modelos teóricos foram identificados. O primeiro deles, e mais amplo, descrito por Mica Endsley. Em seguida, aqueles definidos por Bedny e Meister; Staton; e Smith e Hancock. Todos com suas peculiaridades, porém, mantendo a mesma base interpretativa de Mica Endsley.
A partir desses modelos, foi possível traçar um paralelo entre a CS e os princípios estratégicos delineados por Sun Tzu, Clauzewitz e Giulio Douhet. Além disso, o artigo buscou detalhar o conceito de CS no âmbito cibernético, se referindo a CSC. Essa, por sua vez, também encontrando aplicabilidade em ambientes críticos, os quais requerem um nível de atenção elevado e grande capacidade de decisão. Ou seja, no escopo do espaço cibernético de interesse, foi possível perceber a necessidade de percepção, compreensão e projeção de um determinado evento cibernético. Por fim, uma vez que os principais documentos estratégicos de defesa no Brasil como a PND, a END e o LBDN tratam e consideram a importância da componente cibernética para a Defesa Nacional, torna-se latente a capacidade de a CS ser utilizada como ferramenta estratégica no âmbito da defesa cibernética. RI

Data de receção: 5 de janeiro de 2024 | Data de aprovação: 5 de abril de 2024

André Lucas Alcântara da Silva Capitão engenheiro da computação no Comando de Operações Aeroespaciais (COMAE) – Força Aérea Brasileira (FAB).
> Força Aérea Brasileira (FAB), SHIS – Lago Sul, Brasília DF, 70297-400, Brasil | alcantaraalas@fab.mil.br

Gills Vilar Lopes Professor permanente do Programa de Pós-Graduação em Ciências Aeroespaciais (PPGCA) da Universidade da Força Aérea (UNIFA).
> Universidade da Força Aérea (UNIFA) Av. Marechal Fontenele, 1200, Jardim Sulacap, Rio de Janeiro/RJ, 21750-000, Brasil | gillsgvl@fab.mil.br

NOTAS

1 A presente investigação foi realizada com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001.

2 SINGER, Peter W.; FRIEDMAN, Alan – *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford: Oxford University Press, 2017. Disponível em: https://doi.org/10.1093/wentk/9780199918096.001.0001. Tradução livre dos autores.

3 SMITH, Kip; HANCOCK, Peter A. – «Situation awareness is adaptive, externally directed consciousness». In *Human Factors Journal*. Vol. 37, N.º 1, 1997, pp. 137-148.

4 STANTON, Neville A. – «Hierarchical task analysis: developments, applications, and extensions». In *Applied Ergonomics*. Vol. 37, N.º 1, 2006, pp. 55-79.

5 WOODS, David D. – «Coping with complexity: the psychology of human behaviour in complex systems». In *Tasks, Errors and Mental Models: A Festschrift to Celebrate the 60th Birthday of Professor Jens Rasmussen*. Londres: Routledge, 1988.

6 KABER, David B.; ENDSLEY, Mica R. – «Out-of-the-loop performance problems and the use of intermediate levels of automation for improved control system functioning and safety». In *Process Safety Progress*. Vol. 16, N.º 3, 1997, pp. 126-131. DOI: https://doi.org/10.1002/prs.680160304.

7 ENDSLEY, Mica R. – «Design and evaluation for situational awareness enhancement». In *Proceedings of the Human Factors Society 32nd Annual Meeting*. Anaheim: 24-28 de outubro de 1998, pp. 97-101. Tradução livre a partir do original.

8 BEDNY, G.; MEISTER, D. – «How do professionals reason in real-world situations? Implications for the design of decision support». In *Handbook of Human Factors and Ergonomics*. 2.ª edição. 1999, pp. 1118-1142.

9 STANTON, Neville A.; CHAMBERS, Peter R. G.; PIGGOTT, John – «Situational awareness and safety». In *Safety Science*. Vol. 39, N.º 3, dezembro de 2001, pp. 189-204.

10 SMITH, Kip; HANCOCK, Peter A. – «Situation awareness is adaptive...».

11 ENDSLEY, Mica R. – «Toward a theory of situation awareness in dynamic systems». In *Human Factors Journal*. Vol. 37, N.º 1, 1995, pp. 32-64.

12 BEDNY, G.; MEISTER, D. – «How do professionals reason in real-world situations?...».

13 STANTON, Neville A.; CHAMBERS, Peter R. G.; PIGGOTT, John – «Situational awareness and safety».

14 HOLLAN, James; HUTCHINS, Edwin; KIRSH, David – «Distributed cognition: toward a new foundation for human-computer interaction research». In *ACM Transactions on Computer-Human Interaction*. Vol. 7, N.º 2, 2000, pp. 174-196.

15 STANTON, Neville A. – «Hierarchical task analysis...».

16 SMITH, Kip; HANCOCK, Peter A. – «Situation awareness is adaptive...».

17 STANTON, Neville A.; CHAMBERS, Peter R. G.; PIGGOTT, John – «Situational awareness and safety».

18 ENDSLEY, Mica R. – «Design and evaluation for situational awareness enhancement».

19 TZU, Sun – *A Arte da Guerra*. São Paulo: Martin Claret, 2010.

20 ENDSLEY, Mica R. – «Toward a theory of situation awareness in dynamic systems». Tradução livre dos autores.

21 SMITH, Kip; HANCOCK, Peter A. – «Situation awareness is adaptive...».

22 CLAUSEWITZ, Carl von – *Da Guerra*. Brasília, DF: Editora UnB, 1984.

23 ENDSLEY, Mica R. – «Design and evaluation for situational awareness enhancement».

24 STANTON, Neville A. – «Hierarchical task analysis...».

25 *Ibidem*.

26 DOUHET, Giulio – *O Domínio do Ar*. São Paulo: Bibliex, 2010.

27 STANTON, Neville A. – «Hierarchical task analysis...».

28 GUTZWILLER, Robert – *Situation Awareness in Defensive Cyberspace Operations: An Annotated Bibliographic Assessment Through 2015*. San Diego: NIWC Pacific, 2019.

29 HOLLNAGEL, Erik; WOODS, David D. – *Joint Cognitive Systems: Patterns in Cognitive Systems Engineering*. CRC Press. 2005.

30 JAJODIA, Sushil; ALBANESE, Massimiliano – «An integrated framework for cyber situation awareness». In *Theory and Models for Cyber Situation Awareness*. Berlim: Springer, 2017.

31 *POLÍTICA NACIONAL de Segurança da Informação*. Brasília, DF: Gabinete de Segurança Institucional, 2018.

32 *LIVRO BRANCO de Defesa Nacional*. Brasília, DF: Ministério da Defesa, 2012.

33 *Ibidem*.

34 NOCETTI, Julien – «Cyber power». In *Routledge Handbook of Russian Foreign Policy*. Londres: Routledge, 2018, pp. 182--198; «DEVELOPMENTS IN the field of information and telecommunications in the context of international security». United Nations. 2019. DOI: https://www.un.org/disarmament/ict-security/.

35 DEVANNY, Joseph – «The review and responsible, democratic». In *Centre for Defence Studies. The Integrated Review in Context*. 2021, p. 62. Tradução livre a partir do original.

36 LONSDALE, David J. – «Information power: strategy, geopolitics, and the fifth dimension». In *Journal of Strategic Studies*. Vol. 22, N.º 2-3, junho de 1999, pp. 137-157.

37 GRAY, Colin S. – *Making Strategic Sense of Cyber Power: Why the Sky is not Falling*. Washington, DC: Strategic Studies Institute, US Army War College, 2013.

38 RID, Thomas – «Cyber war will not take place». In *Journal of Strategic Studies* Vol. 35, N.º 1, 2012, pp. 5-32.

39 *Ibidem*. Tradução livre dos autores.

40 *DOUTRINA MILITAR de Defesa Cibernética*. Brasília, DF: Ministério da Defesa, 2023.

41 JAJODIA, Sushil; ALBANESE, Massimiliano – «An integrated framework for cyber situation awareness».

42 ALI, Colonel Rizwan – «Situational awareness for The Nato Alliance». In *The Three Swords Magazine*. N.º 30, 2016, pp. 72-75. Disponível em: https://www.jwc.nato.int/images/stories/_news_items_/2016/Cyber_Situational_Awareness.pdf.

43 *DOUTRINA MILITAR de Defesa Cibernética*.

BIBLIOGRAFIA

ALI, Colonel Rizwan – «Situational awareness for the Nato Alliance». In *The Three Swords Magazine*. N.º 30, 2016, pp. 72-75. Disponível em: https://www.jwc.nato.int/images/stories/_news_items_/2016/Cyber_Situational_Awareness.pdf.

BEDNY, G.; MEISTER, D. – «How do professionals reason in real-world situations? Implications for the design of decision support». In *Handbook of Human Factors and Ergonomics*. 2.ª edição. 1999, pp. 1118--1142.

CLAUSEWITZ, Carl von – *Da Guerra*. Brasília, DF: Editora UnB, 1984.

DEVANNY, Joseph – «The review and responsible, democratic». In *Centre for Defence Studies. The Integrated Review in Context*. 2021, p. 62.

«DEVELOPMENTS IN the field of information and telecommunications in the context of international security». United Nations. 2019. DOI: https://www.un.org/disarmament/ict-security/.

DOUHET, Giulio – *O Domínio do Ar*. São Paulo: Bibliex, 2010.

DOUTRINA MILITAR de Defesa Cibernética. Brasília, DF: Ministério da Defesa, 2023.

ENDSLEY, Mica R. – «Toward a theory of situation awareness in dynamic systems». In *Human Factors Journal*. Vol. 37, N.º 1, 1995, pp. 32-64. DOI: https://doi.org/10.1518/001872095779049543.

ENDSLEY, Mica R. – «Design and evaluation for situational awareness enhancement». In *Proceedings of the Human Factors Society 32nd Annual Meeting*. Anaheim: 24-28 de outubro de 1998, pp. 97-101. DOI: https://doi.org/10.1177/154193128803200221.

GRAY, Colin S. – *Making Strategic Sense of Cyber Power: Why the Sky is not Falling*. Washington, DC: Strategic Studies Institute, US Army War College, 2013.

GUTZWILLER, Robert – *Situation Awareness in Defensive Cyberspace Operations: An Annotated Bibliographic Assessment Through 2015*. San Diego: NIWC Pacific, 2019.

HOLLAN, James; HUTCHINS, Edwin; KIRSH, David – «Distributed cognition: toward a new foundation for human-computer interaction research». In *ACM Transactions on Computer-Human Interaction*. Vol. 7, N.º 2, 2000, pp. 174-196. DOI: http://dx.doi.org/10.1145/353485.353487.

HOLLNAGEL, Erik; WOODS, David D. – *Joint Cognitive Systems: Patterns in Cognitive Systems Engineering*. CRC Press. 2005.

JAJODIA, Sushil; ALBANESE, Massimiliano – «An integrated framework for cyber situation awareness». In *Theory and Models for Cyber Situation Awareness*. Berlim: Springer, 2017.

KABER, David B.; ENDSLEY, Mica R. – «Out--of-the-loop performance problems and the use of intermediate levels of automation for improved control system functioning and safety». In *Process Safety Progress*. Vol. 16, N.º 3, 1997, pp. 126-131. DOI: https://doi.org/10.1002/prs.680160304.

LIVRO BRANCO de Defesa Nacional. Brasília, DF: Ministério da Defesa, 2012.

LONSDALE, David J. – «Information power: strategy, geopolitics, and the fifth dimension». In *Journal of Strategic Studies*. Vol. 22, N.º 2-3, junho de 1999, pp. 137-157.

NOCETTI, Julien – «Cyber power». In *Routledge Handbook of Russian Foreign Policy*. Londres: Routledge, 2018, pp. 182-198.

POLÍTICA NACIONAL de Segurança da Informação. Brasília, DF: Gabinete de Segurança Institucional, 2018.

RID, Thomas – «Cyber war will not take place». In *Journal of Strategic Studies* Vol. 35, N.º 1, 2012, pp. 5-32. DOI: https://doi.org/10.1080/01402390.2011.608939.

SINGER, Peter W.; FRIEDMAN, Alan – *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford: Oxford University Press, 2017. DOI: https://doi.org/ 10.1093/wentk/9780199918096.001.0001.

SMITH, Kip; HANCOCK, Peter A. – «Situation awareness is adaptive, externally directed consciousness». In *Human Factors Journal*. Vol. 37, N.º 1, 1997, pp. 137-148. DOI: https://doi.org/10.1518/001872095779049444.

STANTON, Neville A. – «Hierarchical task analysis: developments, applications, and extensions». In *Applied Ergonomics*. Vol. 37, N.º 1, 2006, pp. 55-79. DOI: https://doi.org/10.1016/j.apergo.2005.06.003.

STANTON, Neville A.; CHAMBERS, Peter R. G.; PIGGOTT, John – «Situational awareness and safety». In *Safety Science*. Vol. 39, N.º 3, dezembro de 2001, pp. 189-204.

TZU, Sun – *A Arte da Guerra*. São Paulo: Martin Claret, 2010.

WOODS, David D. – «Coping with complexity: the psychology of human behaviour in complex systems». In *Tasks, Errors and Mental Models: A Festschrift to Celebrate the 60th Birthday of Professor Jens Rasmussen*. Londres: Routledge, 1988.