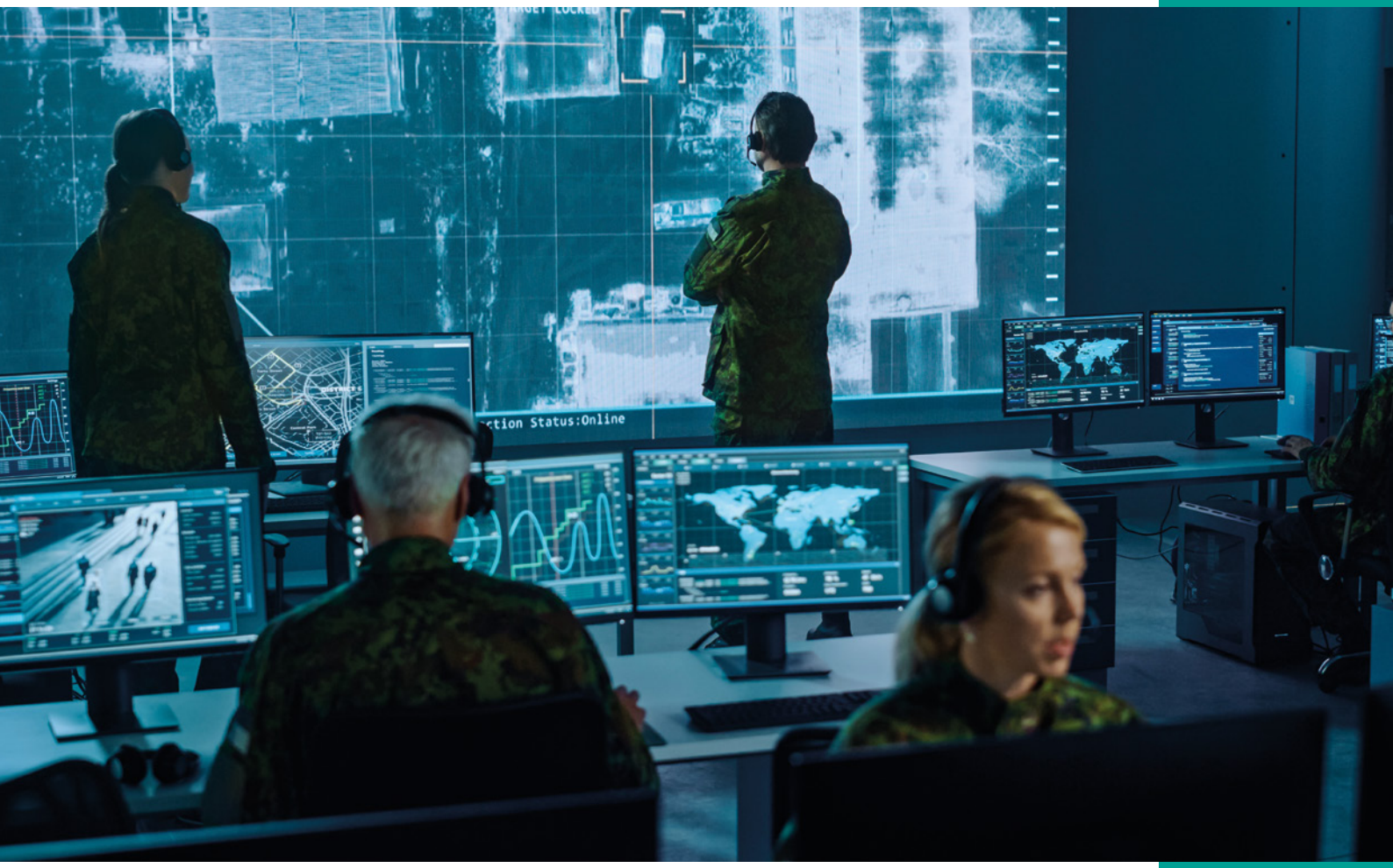
O ESPACO CIBERNÉTICO DE INTERESSE NAS FASES DO PITCIC



O artigo "O ESPAÇO CIBERNÉTICO DE INTERESSE NAS FASES DO PITCIC", buscou explicar como os dados referentes ao Espaço Cibernético de Interesse podem ser adicionados às fases do Processo de Integração terreno, Condições Meteorológicas, Inimigo e Considerações Civis, de modo a subsidiar o Exame de Situação e auxiliar no processo decisório, planejamento e condução das Operações Militares.

Luís Henrique Leal

Capitão de Artilharia do Exército Brasileiro. Bacharel em Ciências Militares – Academia Militar das Agulhas Negras (AMAN) e pós-graduado em Operações Militares – Escola de Aperfeiçoamento de Oficiais (ESAO). Atualmente serve na Escola de Inteligência Militar do Exército (EsIMEx) como instrutor de Inteligência Cibernética. Possui o Curso Básico e Intermediário de Inteligência e o Curso de Guerra Cibernética.

Ricardo Célio Chagas Bezerra Filho

Capitão de Infantaria do Exército Brasileiro. Bacharel em Ciências Militares – Academia Militar das Agulhas Negras (AMAN) e mestre em Operações Militares – Escola de Aperfeiçoamento de Oficiais (ESAO). Atualmente serve na Escola de Inteligência Militar do Exército (EsIMEx) como instrutor de Inteligência Cibernética. Possui o Curso Básico e Intermediário de Inteligência e o Curso de Guerra Cibernética.

1 INTRODUÇÃO

Para a Inteligência Militar (IM), são de interesse quaisquer condições, circunstâncias ou influências com possibilidade de afetar o desempenho das atividades e tarefas necessárias ao cumprimento da missão recebida em qualquer das dimensões, seja física, humana ou informacional, mesmo que não sejam tangíveis. Dessa forma, a compreensão do Ambiente Operacional (AmbOp) torna-se fator fundamental para o planejamento e a condução das operações (BRASIL, 2015b).

As mudanças tecnológicas e sociais forçaram a substituição da tradicional análise do AmbOp, concentrada na dimensão física em que preponderam os fatores terreno e condições meteorológicas sobre as operações, para uma visão que também considerasse a influência das dimensões humana e informacional sobre as operações militares e vice-versa (BRASIL, 2015b).

Tais evoluções também forjaram novas características aos combates modernos, dentre as quais duas das mais marcantes são: o uso maciço de tecnologia e a capacidade de operar no espaço cibernético (E Ciber) (BRASIL, 2015a).

Outra característica, a de combater no Amplo Espectro dos conflitos, exige dos decisores em todos os níveis a compreensão de aspectos que podem exercer influência sobre as operações, tais como o inimigo, o terreno e as condições meteorológicas, dentre outras (BRASIL, 2015b).

A compreensão dos aspectos que influenciam no espaço de batalha passa pelo desenvolvimento do Exame de Situação de Inteligência, que constitui parte fundamental em qualquer processo decisório. Nas operações militares, sua execução é caracterizada e materializada pela elaboração do Processo de Integração Terreno, Condições Meteorológicas, Inimigo e Considerações Civis (PITCIC) (BRASIL, 2015b).

Adotado experimentalmente na Força Terrestre em 1999, o PITCIC foi aperfeiçoado e atualizado no ano de 2016, com a publicação do manual EB70-MC-10.307: Planejamento e Emprego da Inteligência Militar. Nessa oportunidade foram inseridos diversos aspectos, como as considerações civis, porém, não foi contemplada a inserção das evoluções tecnológicas no espaço de batalha (BRASIL, 2016).

Corroborando com a necessidade de inclusão das novas tecnologias no Exame de Situação de Inteligência, no ano de 2017, ocorreu nos Estados Unidos da América (EUA) um *workshop* com a finalidade de discutir a atualização do manual de *Intelligence Preparation of the Battlefield* (IPB), o processo estadunidense correspondente ao PITCIC (McMillian Junior, 2019).

A preocupação principal era garantir que o manual que estavam revisando proveria a orientação necessária para a análise das complexidades presentes no espaço de batalha e na descrição de ameaças híbridas que possivelmente explorariam áreas tecnológicas (McMillian Junior, 2019).

No *workshop* identificou-se que as fases do IPB favorecem a consideração do uso do E-Ciber pelos analistas, e concluiu-se que o uso de tecnologias avançadas também força os analistas a determinarem como essas tecnologias podem afetar o ambiente operacional, de uma forma que não haviam sido analisadas previamente, uma vez que o E-Ciber pode estender a área de influência e a área de interesse durante determinada operação (McMillian Junior, 2019).

Na Doutrina Militar Terrestre (DMT) brasileira ainda não existe documentação que leve em consideração os aspectos mencionados. Dessa forma, verifica-se que dados importantes ou decisivos podem não estar sendo analisados no processo de planejamento das operações militares, o que representa uma notável oportunidade de melhoria no processo de desenvolvimento do PITCIC.

Com base nos aspectos mencionados, definiu-se como objetivo do trabalho explicar como os dados referentes ao espaço cibernético de interesse podem ser adicionados às fases do PITCIC, de modo a subsidiar o Exame de situação. Para tanto também será necessário definir o que vem a ser o espaço cibernético de Interesse.

2 AS DIMENSÕES DO AMBIENTE OPERACIONAL

Com a evolução da DMT e dos conflitos no século atual, foi apresentado pelo Estado Maior do Exército (EME), em 2013, o conceito de "Operações de Amplo Espectro", conforme cita PAIXÃO JÚNIOR (2013):

> A designação "Operações no Amplo Espectro" enfatiza que os conflitos atuais envolvem não somente o combate entre oponentes armados. As operações constituem-se, também, na aplicação dos

> meios de combate, de forma simultânea ou sucessiva, combinando atitudes ofensiva, defensiva, de pacificação, de garantia da lei e da ordem, de apoio às instituições governamentais e internacionais e de assistência humanitária, em ambientes interagências (Paixão Júnior, 2013).

Com a adoção do novo conceito e a transformação da doutrina brasileira, ocorreu um avanço no entendimento de ambiente operacional, que, de acordo com o Manual de Operações, é caracterizado pela existência de três dimensões: física, humana e informacional, e se constitui no conjunto de condições e circunstâncias que afetam o espaço onde atuam as forças militares e que interferem na forma como são empregadas (BRASIL, Exército, 2017a, pp. 2-2).

Já o Manual de Operações de Informação define ambiente operacional como:

> [...] a composição de condições, circunstâncias e influências que afetam o emprego de recursos e apoiam as decisões do comandante, abrangendo áreas físicas e fatores relativos aos domínios marítimo, terrestre e aeroespacial, aspectos humanos, bem como a dimensão informacional, que inclui o **espaço cibernético (ciberespaço)** (BRASIL, 2014a, pp. 2-2).

A análise do ambiente operacional, por tradição, tinha seu foco voltado à dimensão física. Porém, na atualidade, essa análise deve considerar as três dimensões de maneira igualitária (BRASIL, Exército, 2017a, pp. 2-2), uma vez que os fatores a serem analisados interagem entre si, formando o seu caráter único e indivisível.

A dimensão informacional, cerne desse trabalho, abrange os sistemas utilizados para obter, produzir, difundir e atuar sobre a informação. É subdividida em três perspectivas inter-relacionadas que interagem continuamente entre si: a física, a lógica e a cognitiva (BRASIL, 2014a, pp. 2-3). O Manual de Operações de Informação define cada uma das perspectivas da dimensão informacional, conforme segue:

> **A perspectiva física** é composta por sistemas de comando e controle (C2), pelo apoio de infraestruturas que propiciam aos indivíduos e às organizações criarem efeitos desejados. É a dimensão em que residem as plataformas físicas e as redes de comunicação que as conectam
>
> **A perspectiva lógica** engloba onde e como as informações são obtidas, produzidas, armazenadas, protegidas e difundidas. É onde o C2 das forças militares é exercido e por meio da qual a intenção do comandante é transmitida. As ações nessa perspectiva afetam o conteúdo e o fluxo de informações.
>
> **A perspectiva cognitiva** abrange as mentes daqueles que têm a responsabilidade de obter, produzir, difundir e atuar sobre a informação. Ela se refere a indivíduos ou grupos de processamento da informação, percepção, avaliação e tomada (BRASIL, 2014a, pp. 2-4, grifo nosso).

3 O PITCIC

O PITCIC é cíclico e contínuo, de caráter eminentemente gráfico, e visa subsidiar o processo decisório dos comandantes, nos mais diversos níveis, por meio da análise integrada de informações sobre o terreno, condições meteorológicas, inimigo e considerações civis e seus impactos sobre as operações. Dessa forma, constitui-se em um processo de apoio ao exame de situação e integra todo o Processo de Condução das Operações Terrestres (BRASIL, 2016, pp. 5-1).

De acordo com o Manual de Planejamento e Emprego da Inteligência Militar:

> O PITCIC permite ao decisor visualizar como o terreno e as condições meteorológicas condicionam ou poderiam condicionar as nossas operações ou as do inimigo e, em consequência, a partir dessa imagem gráfica, tomar decisões mais adequadas, maximizando o poder de combate em pontos críticos de tempo e espaço (BRASIL, 2016, pp. 5-1).

A doutrina estadunidense também define o correlato IPB como um processo contínuo e que a análise e avaliação desenvolvidas nele são necessárias para manter a compreensão situacional de um ambiente operacional em fluxo constante (EUA, 2019a).

Tanto na doutrina brasileira quanto na estadunidense (EUA, 2019a, p. 8) o PITCIC é dividido em quatro fases: definição do ambiente operacional, identificação dos efeitos ambientais sobre as operações, avaliação da ameaça e a determinação das possíveis linhas de ação da ameaça; que ocorrem de forma simultânea, uma vez que os seus produtos podem estar sendo utilizados em uma operação, enquanto outros planejamentos ocorrem em paralelo (BRASIL, 2016, pp. 5-2).

Figura 3 – Fases do PITCIC
Fonte: Brasil (2016, pp. 5-3).

4 O ESPAÇO CIBERNÉTICO

O Espaço Cibernético (E-Ciber) é definido doutrinariamente como o "espaço virtual composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam e são processadas e/ou armazenadas" (BRASIL, Exército, 2017b, pp. 2-2). Tal conceito deixa evidente a amplitude abrangida por ele.

Complementarmente, o E-Ciber constitui um ambiente complexo que ultrapassa fronteiras organizacionais e entre nações, abrangendo também espaços internacionais e de uso coletivo (Brandão & Izycki, 2019). Resulta da interação entre pessoas, *softwares* e serviços disponibilizados na internet por intermédio de dispositivos físicos e redes lógicas (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2012).

Neste item, serão apresentadas as características do E-Ciber consideradas relevantes para a argumentação do presente estudo e a sugerida definição do E-Ciber de interesse.

4.1 Características do E-Ciber

A Doutrina Militar de Defesa Cibernética elenca as características da Defesa Cibernética: por sua natureza, torna-se válido considerar que essas também são assumidas pelo E-Ciber como um todo. Dessas, verifica-se que o alcance global e a vulnerabilidade das fronteiras geográficas vão ao encontro do que se propõe esse estudo.

Por alcance global, entende-se que o E-Ciber possibilita o desencadeamento de ações em diferentes frentes e em proporção global, já que não se aplicam as limitações físicas de espaço e distân-

cia nesse espaço (BRASIL, Ministério da Defesa, 2014b, p. 21).

Já a vulnerabilidade das fronteiras geográficas materializa-se pela não limitação das ações pelas fronteiras geograficamente definidas, tendo em vista que ações originadas de qualquer localização podem provocar efeitos, cinéticos ou não, em qualquer lugar (BRASIL, Ministério da Defesa, 2014b).

Portanto, o E-Ciber pode se estabelecer como um ambiente operacional por si só ou parte dele em uma operação de amplo espectro, podendo, dessa forma, afetar as dimensões física, informacional e humana do campo de batalha.

4.2 Definição do E-Ciber de interesse

A amplitude do E-Ciber é uma de suas características intrínsecas e irrefutáveis. Esse superdimensionamento e a virtualização do espaço de batalha, todavia, dificultam as ações executadas na 1ª fase do PITCIC, ou seja, na Definição do Ambiente Operacional, notadamente para o estabelecimento dos limites da área de influência e da área de interesse, fundamentais para o planejamento das operações militares.

Na pesquisa realizada verificou-se a existência de menções ao termo "Espaço Cibernético de Interesse" em diversos tipos de documentos e manuais doutrinários.

Dessas, salienta-se que a Doutrina Militar de Defesa Cibernética, primeira publicação sobre cibernética, publicada em 2014, utilizou o termo na conceituação de ameaças cibernéticas e na caracterização dos níveis de alerta cibernético (BRASIL, 2014b).

Posteriormente, no ano de 2017, o Manual de Campanha Guerra Cibernética utilizou o termo na definição da tarefa "Consciência situacional" contida na atividade "Proteção Cibernética" na seção do manual referente às atividades e tarefas da Guerra Cibernética (BRASIL, 2017b).

Em observância ao contexto que o termo foi utilizado nos referidos manuais, torna-se evidente que em ambos foi empregado com a conotação de alguma delimitação para a análise dos aspectos do E-Ciber, corroborando com a necessidade de restrição anteriormente apontada por esse trabalho. Contudo, em que pese a utilização do termo em publicações doutrinárias, nenhuma delas apresenta uma definição formal.

Em virtude da conjuntura apresentada, verificou-se necessário criar delimitações, usando como base os termos já consagrados pela doutrina, mas também levando em consideração as características do E-Ciber: o Espaço Cibernético de Interesse.

A área de interesse, já consolidada, é assim definida:

> É constituída por áreas adjacentes ou não à zona de ação, tanto à frente como nos flancos e retaguarda, onde os fatores e acontecimentos que nela se produzam possam repercutir no resultado ou afetar as ações, as operações atuais e as futuras. Também pode ser definida como o espaço, incluindo a área de responsabilidade e a área de influência, onde, embora o comandante não possa atuar, os acontecimentos poderão influenciar no cumprimento de sua missão. É assinalada pelo próprio Comando da Força (BRASIL, 2016).

A área de interesse não representa uma área específica, com limites definidos, e deve evoluir constantemente (BRASIL, 2016). Dessa forma, analogamente, o Espaço Cibernético de Interesse seria definido como: **"parcela do espaço cibernético onde os fatores e acontecimentos que nele se produzam possam repercutir no resultado ou afetar as ações, cinéticas ou não, atuais e futuras na Área de Operações da Força Terrestre Componente (FTC) considerada"**.

Diante do exposto, considera-se que a necessidade de delimitação seria alcançada com a utilização da conceituação de E-Ciber de Interesse proposta, tanto na execução do PITCIC, viés desse trabalho, quanto para os demais contextos em que o termo for utilizado.

4.3 Doutrina estrangeira sobre camadas do E-Ciber

Na doutrina americana, verifica-se a divisão do E-Ciber em três camadas: social (*Social Layer*), lógica (*Logical Layer*) e física (*Physical Layer*), como se verifica na Figura 7.

A camada física inclui o componente geográfico, que representa a localização espacial dos elementos de rede e o componente da rede física, que inclui todo o *hardware* e infraestrutura que suporta as redes e seus conectores (EUA, 2010, pp. 9, tradução nossa).

A lógica é a camada eminentemente técnica e talvez a mais representativa do E-Ciber, que consiste nas ligações lógicas, nas conexões entre nós da rede. Por nó entende-se qualquer dispositivo conectado a uma rede (EUA, 2010, pp. 9, tradução nossa).

A camada social compreende as relações humanas e os aspectos cognitivos. Pode ser subdividida em social, identidade e identidade cibernética. A social é representada pelas interações humanas, a identidade representada pelas pessoas propriamente ditas e as identidades cibernéticas correspondem a uma identificação pessoal na rede (*e-mail*, telefone, endereço IP, credenciais de acesso, dentre outros) (EUA, 2010, pp. 9, tradução nossa).

Já a doutrina empregada no Reino

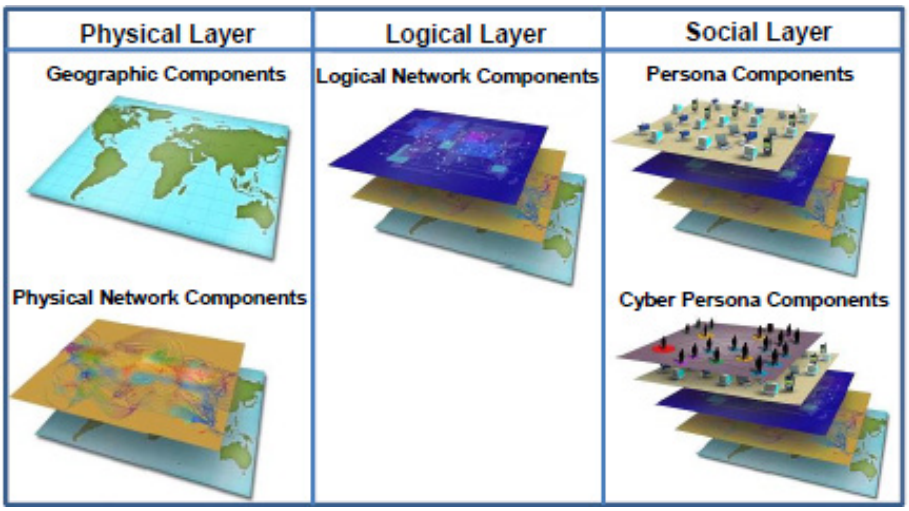


Figura 7 – Camadas do E-Ciber (doutrina estadunidense)
Fonte: EUA (2010, p. 8).

Unido divide o E-Ciber em seis camadas: social, pessoa (*people*), identidade (*persona*), informação (*information*), rede (*network*) e real, conforme Figura 8.

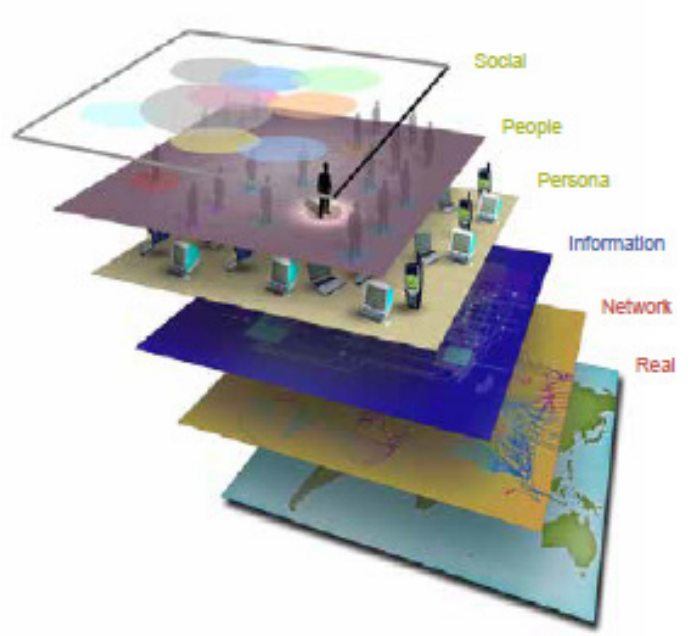


Figura 8 – Camadas do E- Ciber (doutrina britânica)
Fonte: Reino Unido (2016, p. 5)

As camadas Social, Pessoa e Identidade consistem nos "detalhes que conectam as pessoas ao E-Ciber e as pessoas e grupos que interagem e operam as redes. Endereços ou títulos exclusivos são combinados com endereços virtuais, que, por sua vez, direcionam para as camadas real e de rede". Ainda pode ser dividida em quatro subcamadas: rede social, procedimentos de operação e manutenção, pessoas e segurança (REINO UNIDO, 2016, pp. 5, tradução nossa).

A camada Informação representa as conexões existentes entre os pontos de rede. Incluem ainda configurações de rede, dados, aplicações e protocolos que conduzem a interação por meio da camada física, dos detalhes dos provedores de serviços, dos nomes de domínio na Internet e dos dados de propriedade (REINO UNIDO, 2016, p. tradução nossa).

A camada de Rede utiliza estruturas lógicas como método primário de segurança e integridade. Essa, geralmente, é a camada alvo da Inteligência do Sinal, Inteligência Cibernética e Reconhecimento e Vigilância (REINO UNIDO, 2016, pp. 7, tradução nossa).

Já a camada Real engloba os aspectos geográficos e físicos. Os geográficos são relacionados com a localização dos elementos de uma rede e os físicos, a quais componentes estão presentes etc. (REINO UNIDO, 2016, pp. 7, tradução nossa).

4.4 Divisão de camadas do E-Ciber adotada

Comparando a divisão proposta por estadunidenses e britânicos verifica-se que, de maneira geral, apesar da diferença do número de camadas e de alguns aspectos conceituais, as divisões se assemelham, ou pelo menos se equivalem. Diante dessa comparação e, ainda, utilizando as perspectivas da dimensão informacional do ambiente operacional, já mencionadas, Vasquez (2020) formulou proposta conforme a Figura 9.

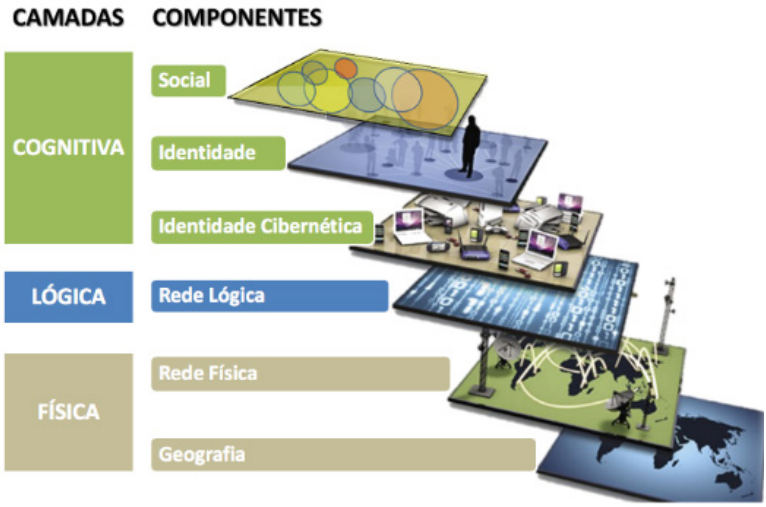


Figura 9 – Camadas e subcamadas do E Ciber
Fonte: VASQUEZ (2020, p. 43).

Na proposta de Vasquez (2020, p. 44):

A camada física é caracterizada pelo *hardware* e pela infraestrutura computacional responsáveis pelo armazenamento, transporte e processamento de informações, distribuídos em um espaço geográfico. Seus componentes podem ser aproveitados para a obtenção do acesso lógico. Ela também define a localização geográfica e a estrutura legal apropriada a ser aplicada nas operações militares. (VASQUEZ, 2020, p. 44)

A camada lógica constitui-se em uma abstração da camada física e consiste nos códigos de programação, protocolos e dados responsáveis pela comunicação dos componentes de uma rede. Por ser a camada mais característica do E-Ciber, "restringe o engajamento de seus alvos por meios inerentes ao espaço cibernético, ou seja, um dispositivo ou aplicação projetada para criar um efeito no ciberespaço ou por meio dele" (Vasquez, 2020, p. 44).

A última das camadas, a cognitiva, é a que representa a conexão das pessoas e dos grupos à sua ou suas representações no E-Ciber (identidades cibernéticas). Nessa camada se refletem aspectos humanos e sociais dos indivíduos, os quais consomem dados, formam grupos e se relacionam por intermédio de suas contas de usuários (humanas ou automatizadas) (Vasquez, 2020, p. 44).

Nesse contexto, salienta-se que uma pessoa pode possuir diversas identidades cibernéticas, bem como a mesma identidade cibernética pode ser utilizada ou controlada por mais de uma pessoa.

5 O E-CIBER DE INTERESSE NO PITCIC

Atualmente existe uma dependência, global e massiva, do uso do E-Ciber para a troca de informações, inclusive em campos de batalha. Com essa dependência e com vulnerabilidades inerentes a ele, o E-Ciber deve ser considerado em cada uma das fases do PITCIC, conforme será visualizado a seguir.

5.1 Dados do E-Ciber que podem ser inseridos no PITCIC

Dartnall (2017) considerou a existência de um PITCIC específico para o Ambiente Cibernético, o qual denominou *Intelligence Preparation of Cyber Environment*. Nesse processo sistemático e contínuo, deve-se analisar: os meios e motivos dos atores da ameaça; e seu ambiente digital e o ambiente digital no qual se está operando, a fim de compreender os cenários prováveis em que se enfrentará as ameaças. Tal conceito salienta um direcionamento para alguns dos tipos de dados obtidos diretamente do E-Ciber ou versando sobre ele.

Nessa seção, além dos aspectos apontados por Dartnall (2017), serão apresentadas outras sugestões de dados possíveis de serem inseridos no PITCIC.

5.2 As fases do PITCIC e as camadas do E-Ciber de interesse

5.2.1 1ª fase – Definição do ambiente operacional

Nessa fase, devem ser buscadas informações pertencentes as três camadas do E-Ciber sobre indivíduos, organizações ou sistemas que processam, disseminam ou agem na informação. Diante disso, visualizam-se como sugestões de dados pertinentes os apresentados no quadro a seguir.

Quadro 2 – Dados x Camadas do E-Ciber na 1ª fase do PITCIC

1ª FASE – DEFINIÇÃO DO AMBIENTE OPERACIONAL	
Camada do E-Ciber	**Aspectos a serem observados**
Física	Sistemas de TIC do oponente (ameaça ou alvo); pontos de entrada para redes; dispfís de rede na A Op; medidas de segurança implementadas; e infraestruturas críticas da informação
Lógica	Sites que influenciam ou tenham impacto social na A Op; configurações e vulnerabilidades das redes; os meios de compartilhamento de dados e quais *softwares* são utilizados; e técnicas e *softwares* de criptografia comumente utilizados.
Cognitiva	Presença da ameaça e uso do E-Ciber com efeitos na A Op; consumidores de dados e informações na A Op; hacktivistas com capacidade de atuação na A Op; e entidades com capacidade de penetrar em redes.

Fonte: adaptado de EUA (2019b, pp. D-2).

Dados de qualquer natureza, obtidos pelas diversas disciplinas de Inteligência, podem contribuir para essa fase com os aspectos do E-Ciber de Interesse. Salienta-se que a representação da camada lógica pode revelar como e onde a ameaça conduz operações usando o E-Ciber. Já na camada cognitiva, torna-se relevante entender a estrutura organizacional da ameaça, pois esse entendimento conduz a identificação das identidades cibernéticas chave para tal estrutura, como as utilizadas para representar a organização (EUA, 2019b, pp. D-3).

5.2.2 2ª *fase – Identificação dos efeitos ambientais sobre as operações*

Embora a análise mais detalhada da ameaça deva ser oferecida na 3ª e na 4ª fases do PITCIC, é na 2ª que o tipo de ameaça e sua capacidade de utilização do E-Ciber deve ser definida (EUA, 2019b, pp. D-4).

O terreno, no escopo desse trabalho, é analisado utilizando os tradicionais aspectos militares do terreno, adicionando a eles considerações do E-Ciber, conforme apresentado no Quadro 3 (EUA, 2019b, pp. D-5).

Quadro 3 – Análise do terreno

2ª FASE - ANÁLISE DO TERRENO	
Aspectos Militares do Terreno	**Aspectos a serem observados**
Observação e campos de tiro	É essencial entender qual porção da rede pode ser vista e de onde ela pode ser vista. Isso pode incluir a habilidade de ver a utilização de vigilância física. Adicionalmente, redes fechadas podem prevenir a observação em redes amigáveis e nas redes de ameaças.
Cobertas e abrigos	A assinatura eletromagnética da ameaça, higiene no ciberespaço, disciplina de ruídos e a habilidade de limitar a atribuição de ações são considerados cobertas e abrigos no domínio do E-Ciber. Levantar: se atores da ameaça estão escondendo sua identidade real usando múltiplas identidades cibernéticas ou outras técnicas, medidas defensivas e tempo e volume de atividade da rede (isso pode apoiar o acobertamento de atividades na rede).
Obstáculos	Configurações de rede que podem impedir operações no E-Ciber (IPS, IDS etc)
Acidentes capitais	Podem ser aplicados nas três camadas do E-Ciber. Podem ser considerados nós físicos ou dados que sejam essenciais para o cumprimento da missão, tais como principais linhas de telecomunicação, *Domain Name Server* (DNS), *switches*, principais provedores de Internet. No E-Ciber, é possível que forças amigas e as ameaças ocupem os mesmos acidentes capitais ao mesmo tempo, sem que um saiba a presença do outro.
Vias de acesso	Métodos de acesso a redes, intrusão de ameaça ou caminhos para acidentes capitais físicos ou lógicos, tais como *switches*, roteadores, servidores e vetores. Corredores de mobilidade podem ser identificados e agrupados de acordo com a velocidade da rede, onde baixas velocidades podem causar restrições ou severas restrições ao terreno. O volume de atividade de rede pode criar vias de acesso adicionais.

Fonte: EUA (2019b, pp. D-5, tradução nossa).

Salienta-se que componentes de rede podem ser associados a mais de um aspecto do terreno simultaneamente. Como exemplo, um *firewall* pode tanto constituir um obstáculo como pode prover cobertura contra fogos não cinéticos sobre a rede (EUA, 2019, p. D-9).

As considerações civis são analisadas de acordo com a metodologia consolidada. São analisados aspectos sobre área de responsabilidade, estruturas, capacidades, organizações, população, considerações civis complementares, refugiados e deslocados e eventos, porém com a inserção das considerações do E-Ciber. No Quadro 4 é possível visualizar exemplos de dados de cada um dos fatores, relacionados com as camadas do E-Ciber.

Quadro 4 – Análise das considerações civis

ANÁLISE DAS CONSIDERAÇÕES CIVIS		
Fator	**Camadas E-Ciber**	**Aspectos a serem observados**
Área de responsabilidade	Física	Provedores de serviço de Internet.
	Lógica	Cobertura de rede celular, qualidade dos serviços de internet.
	Cognitiva	-
Estruturas	Física	Plantas energéticas, infraestrutura de comunicação, torres de telefonia.
	Lógica	Conectividade, acesso a redes de interesse.
	Cognitiva	-
Capacidades	Física	-
	Lógica	Possibilidade de criar acesso a redes de interesse.
	Cognitiva	Atores com capacidade de agir ciberneticamente, identidades cibernéticas com influência, histórico de ataques cibernéticos e vazamento de dados.
Organizações	Física	Grupos e instituições (universidades, imprensa, indústrias) com possibilidade de influenciar na A Op.
	Lógica	Provedores de serviço de internet.
	Cognitiva	Identidades cibernéticas com influência, grupos com múltiplas identidades cibernéticas.
População	Física	*Hackers*, administradores de sistemas e redes, pessoas com notório saber.
	Lógica	Distribuição residencial dos serviços de internet.
	Cognitiva	Pessoas controlando múltiplas identidades cibernéticas, identidades cibernéticas com influência.
Considerações civis complementares	Física	-
	Lógica	-
	Cognitiva	Idiomas e dialetos usados por identidades cibernéticas, impactos da falta de infraestrutura de comunicações em regiões.
Refugiados e deslocados	Física	Meios para comunicação com refugiados/deslocados.
	Lógica	-
	Cognitiva	Identidades cibernéticas com características análogas a refugiados/deslocados.
Eventos	Física	Rotinas que podem impactar na A Op, simpósios/palestras, encontros religiosos ou políticos.
	Lógica	Redes providas para os eventos programados.
	Cognitiva	-

Fonte: Adaptado de EUA (2019b, pp. D-5).

Já as condições meteorológicas devem ser analisadas sob o aspecto de como condições climáticas extremas podem impactar na utilização do E-Ciber de Interesse no transcurso de Operações Militares, cinéticas ou não (EUA, 2019, p. D-9).

Nessa fase também devem ser obtidos dados sobre a ameaça. A indicação de sua atual localização física, identificação, tamanho e força estão entre os dados necessários. Deve-se avaliar sobre a perspectiva do E-Ciber as camadas física e lógica, com a identificação, por exemplo, de servidores locais, infraestrutura de comunicações ou o uso de mídias sociais por parte da ameaça (EUA, 2019, p. D-7).

Para cada uma das ameaças consideradas, deve-se descrever suas capacidades de modo geral, considerando a possibilidade de interdependências entre as capacidades militares e cibernéticas e o conhecimento do uso de capacidades técnicas e programas suspeitos (EUA, 2019, p. D-7).

Dessa forma, concluindo os trabalhos atinentes a essa fase, os dados devem ser combinados e inseridos nas diversas camadas de calcos produzidos. Adiciona-se que as considerações cibernéticas podem tanto ser representadas em camadas exclusivas para o E-Ciber quanto adicionadas às camadas tradicionalmente confeccionadas.

5.2.3 3ª fase – Avaliação da ameaça

A 3ª fase tem como característica o detalhamento das características da ameaça de modo a permitir que possa ser corretamente avaliada (EUA, 2019b). A correta condução dessa fase impacta decisivamente na delineação das possíveis linhas de ação da ameaça, as quais devem retratar com fidelidade sua capacidade de agir nas condições identificadas nas fases anteriores (BRASIL, 2016).

Nesse contexto, busca-se determinar suas capacidades; seus princípios doutrinários; e que Técnicas, Táticas e Procedimentos (TTP) emprega no e por meio do E-Ciber. Torna-se importante identificar como a ameaça executou ou integrou operações independentes no E-Ciber ou em conjunto com operações tradicionais (EUA, 2019b).

Detalhes específicos podem incluir a atribuição de dispositivos eletrônicos a determinadas identidades cibernéticas, as TTP historicamente utilizadas, capacidade de utilizar ou desenvolver *malwares*, tendência de optar por ações no E-Ciber, nós de comando e controle e as intenções da ameaça nas redes amigas, o potencial de ferramentas utilizadas, dentre outros (EUA, 2019b).

Uma das etapas para o processo de avaliação da ameaça é a identificação de sua capacidade de agir. Tal etapa tem como resultado a identificação dos alvos de alto valor (BRASIL, 2016). Ao identificar possíveis alvos dessa natureza no E-Ciber, deve-se levar em consideração a sua disposição em alguma das camadas do E-Ciber de Interesse, suas características, configurações e vulnerabilidades (EUA, 2019b).

Dessa forma, verifica-se que as considerações do E-Ciber na análise da ameaça são adicionadas às utilizadas para verificar qualquer ameaça tradicional. Os dados levantados nesse contexto podem ser inseridos aos modelos de ameaça tradicionais, ou considerados separadamente.

5.2.4 4ª fase – Possíveis linhas de ação da ameaça

Na 4ª fase, representação gráfica dos dados integrados permite uma melhor visualização das reais possibilidades da ameaça e permite determinar as possíveis linhas de ação do inimigo, na forma de hipóteses, bem como priorizá-las em ordem de probabilidade ou nível de perigo oferecido (EUA, 2019b).

Para o sucesso dessa fase deve-se buscar quando, onde, como e porque a ameaça vai tentar obter a superioridade no E-Ciber de Interesse. Para tanto, deve ser levantada e considerada a capacidade de agir da ameaça (EUA, 2019b).

Salienta-se que o nível de utilização do E-Ciber pela ameaça vai determinar em que proporção os aspectos cibernéticos devem aparecer o calco de situação, produto final desta 4ª e última fase do PITCIC (EUA, 2019b).

5.2.5 Sobreposição de dados do Espaço Cibernético de Interesse

De acordo com o que foi apresentado, verifica-se que os dados relevantes citados anteriormente fornecem uma melhor consciência situacional aos decisores no que tange à utilização do E-Ciber de Interesse. Em todas as fases do PITCIC tais dados devem ser espacializados de forma a materializar o trabalho realizado, tal qual os dados tradicionalmente considerados.

Como produto da 1ª fase, a Figura 11 apresenta inserções de dados relevantes como cabos de fibra óptica, provedores de internet e infraestrutura de telecomunicações. Note-se que nessa figura os aspectos do E-Ciber foram representados de forma estanque ao calco tradicional, ressaltando a região do calco tradicional que está sendo evidenciada.

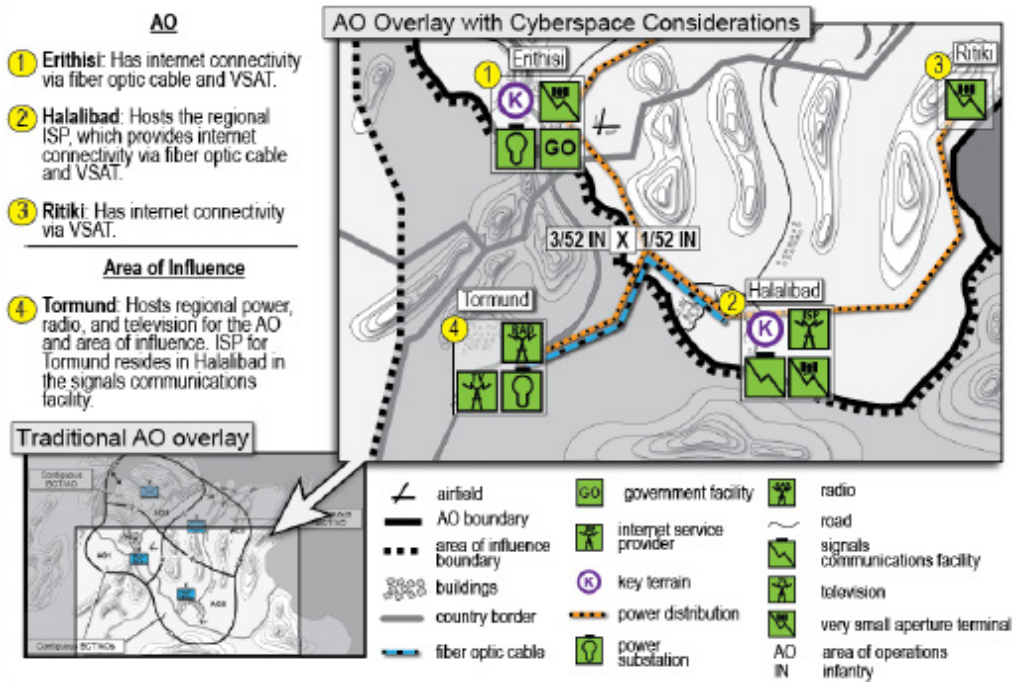


Figura 11 – Exemplo de produto gráfico da 1ª fase
Fonte: EUA (2019b, pp. D-4).

A Figura 12 apresenta a localização de possíveis pontos de acesso à internet, bem como o local que a ameaça representada pela identidade cibernética "Nefarious31" utiliza. Nessa figura, existem aspectos da camada física e da camada cognitiva do E-Ciber. Salienta-se ainda a representação de um prédio governamental definido como acidente capital por apresentar relevância em aspectos do E-Ciber.

A Figura 13 constitui um desdobramento da figura anterior com maior detalhamento na representação gráfica dos aspectos da camada lógica do E-Ciber. Nela, visualizam-se as topologias de rede do local utilizado pela ameaça como ponto de acesso, da subestação de energia e do acidente capital constituído pelo prédio governamental.

Também é possível identificar a presença de *firewalls*, IPS, roteadores e utilização de criptografia, representados como obstáculos. Outro aspecto a ressaltar é a indicação de três possíveis vias de acesso: AA1, AA2 e AA3.

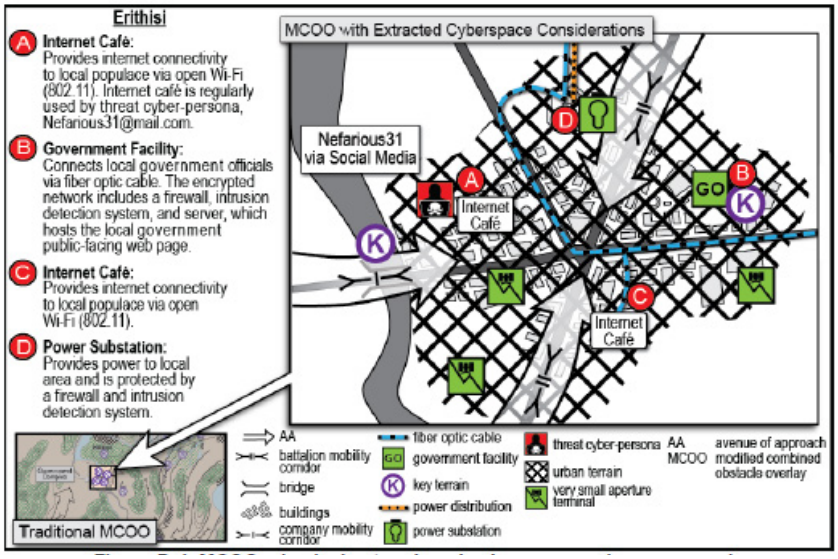


Figura 12 – Exemplo de produto 2ª fase – Obstáculos
Fonte: EUA (2019b, pp. D-8).

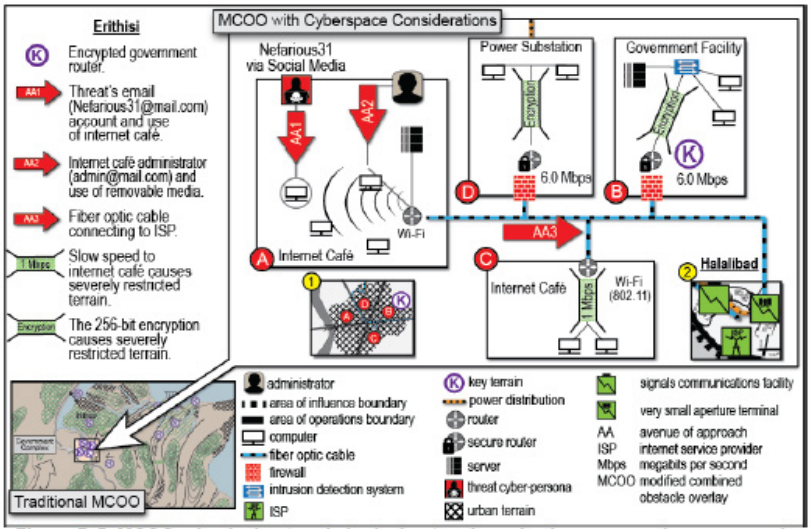


Figura 13 – Exemplo de produto 2ª fase – dados relevantes das três camadas
Fonte: EUA (2019b, pp. D-8).

A Figura 14 demonstra um exemplo de calco de situação, produto final da 4ª fase do PITCIC. Nessa figura, ressalta-se a presença de identidades cibernéticas da ameaça agindo sobre o prédio governamental e sobre os dois pontos de acesso representados pelo "Internet Café". Visualiza-se ainda a composição da fração da ameaça que atua na Área de Operações considerada.

A Figura 15 apresenta um detalhamento maior da topologia de rede (camada lógica) do acidente capital (prédio governamental). Representam-se os obstáculos representados pelo *firewall* e pela atuação do "*Brigade Combat Team Network*" e onde a ameaça seria bloqueada. Também se identifica uma possível rota de infiltração.

Dessa forma, verifica-se que os dados obtidos no E-Ciber de Interesse são cruciais para a obtenção da consciência situacional da Área de Operações e, portanto, devem ser inseridos nos calcos em todas as fases do PITCIC.

CONCLUSÃO

Com vistas ao objetivo definido para o trabalho, as principais contribuições apresentadas foram: a definição de E-Ciber de Interesse; a indicação de tipos de dados relevantes que podem ser inseridos no

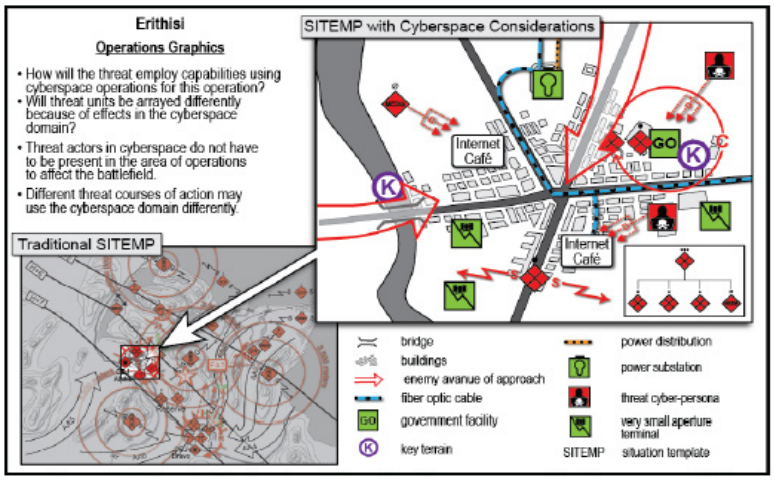


Figura 14 – Produto 4ª fase – Exemplo 1
Fonte: EUA (2019b, pp. D-15).

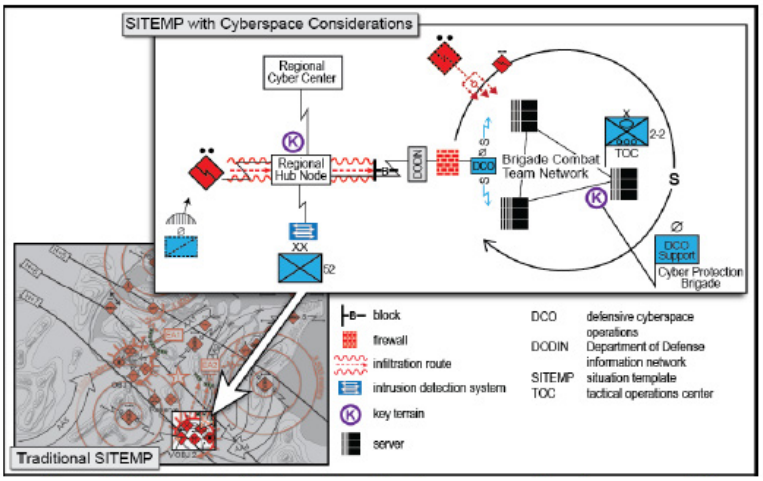


Figura 15 – Produto 4ª fase – Exemplo 2
Fonte: EUA (2019b, pp. D-16).

PITCIC; e a apresentação de um produto gráfico, configurado como uma camada adicional a um calco representando os referidos dados.

Salienta-se que esse trabalho se limitou a abordar o PITCIC considerando a inserção de dados do E-Ciber de Interesse que possam afetar a condução de qualquer operação militar cinética. Não foi objetivo discorrer sobre o aludido processo em proveito de operações exclusivamente cibernéticas, o que fica como sugestão para trabalhos futuros.

Diante do apresentado, verifica-se que os dados relevantes do E-Ciber de Interesse devem ser inseridos na forma de camadas adicionais aos calcos que compõem o PITCIC. Dessa forma, pela sobreposição dos calcos já tradicionais com os que contemplam os dados relevantes do E-Ciber de Interesse, os comandantes e seus Estados-Maiores possuirão informações visuais mais completas para subsidiar o processo decisório no planejamento e condução de Operações Militares.

REFERÊNCIAS

BRANDÃO, J. E. M. D. S.; IZYCKI, E. A. **Desafios Contemporêneos Para o Exército Brasileiro**. Poder Ofensivo no Espaço Cibernético, Brasília, 2019.

BRASIL. Exército. **EB20-MC-10.207:** Inteligência, 2015a.

_____. _____. **EB20-MC-10.213:** Operações de Informação, 2014a.

_____. _____. **EB70-MC-10.223:** Operações, 2017a.

_____. _____. **EB70-MC-10.232:** Guerra Cibernética, 2017b.

_____. _____. **EB70-MC-10.307:** Planejamento e Emprego da Inteligência Militar Terrestre, 2016.

_____. _____. **EB20-MF-10.107:** Inteligência Militar Terrestre, 2015b.

_____. Ministério da Defesa. **MD31-M-07:** Doutrina Militar de Defesa Cibernética, 2014b.

DARTNALL, R. Palestra. **Intelligence Preparation of the Cyber Environment**. 2017.

EUA. Department of the Army. **Cyberspace Operations Concept Capability Plan 2016-2028.** 2010.

_____. _____. **MI Professional Bulletin:** Inteligence Preparation of the Battlefield, 2019a.

_____. _____. Headquarters. **ATP 2-01.3:** Intelligence Preparation of the Battlefield, 2019b.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27032:** Information Technology - Security Techniques - Guidelines for Cybersecurity. 2012.

MCMILLIAN JUNIOR, J. H. ATP 2-01.3, Intelligence Preparation of the Battlefield: Why the Update? **Military Intelligence Professional Bulletin (PB 34-19-4) October-December 2019**, v. 45 Number 4, p. 80, 2019. Disponivel em: <https://fas.org/irp/agency/army/mipb/2019_04.pdf>. Acesso em: 22 de maio de 2020.

PAIXÃO JÚNIOR, M. D. Defesanet. **A abrangente concepção de emprego da Força Terrestre**, 11 jul. 2013. Disponivel em: <http://www.defesanet.com.br/terrestre/noticia/11432/A-abrangente-concepcao--de-emprego-da-Forca-Terrestre/>. Acesso em: 3 de maio de 2017.

REINO UNIDO. Ministry of Defense. **Cyber Primer:** Second Edition, 2016.

VASQUEZ, V. L. O Processo de Elaboração da Lista de Alvos Cibernéticos no Nível Tático. **DATA & HERTZ**, Brasília, v. 1, p. 59, 2020.