QUANTIFICANDO A GUERRA CIBERNÉTICA: MÉTRICAS DE PROTEÇÃO E INDICADORES DE DESEMPENHO PARA A OBTENÇÃO DE UMA CONSCIÊNCIA SITUACIONAL CIBERNÉTICA

Capitão de Fragata Flávio de Queiroz Guimarães
Diretoria de Comunicações e Tecnologia da Informação da Marinha – DCTIM
Edifício Barão de Ladário, 118 – 4º andar – Centro – Rio de Janeiro – RJ
flavio.queiroz@marinha.mil.br

RESUMO

O avanço tecnológico vem aumentando a dependência dos ativos de informação das organizações, expandindo a superfície de ataque do Espaço Cibernético (ECiber). O desenvolvimento de uma Consciência Situacional Cibernética (ConSitCiber) – formada pelos níveis de Percepção, Compreensão, Projeção e Resolução – tornou-se fundamental para o processo de tomada de decisão sobre as ações ofensivas e defensivas de Guerra Cibernética (GC). Assim, para se obter uma ConSitCiber mais precisa, propõe-se estabelecer métricas e indicadores que representem as características quantitativas da condição de proteção de um ECiber, categorizadas em proteção de perímetro, cobertura e disponibilidade/confiabilidade. Há, no entanto, um esforço ainda maior para se estabelecer uma ConSitCiber plena, ao superar uma série de desafios: a complexidade das redes de computadores; a evolução tecnológica; os excessivos alarmes falsos positivos; a detecção de um ataque em tempo real; e a diversidade de vetores de ataque.

Palavra-chave: Consciência Situacional Cibernética; Guerra Cibernética; Métricas.

ABSTRACT

The technological progress has been increasing the dependence of information assets, expanding the attack surface of Cyberspace. The development of Cyber Situational Awareness (CSA) – composed of Perception, Comprehension, Projection and Resolution levels – have become fundamental to the offensive and defensive decision-making process on Cyber Warfare (CW). Thus, for a more accurate CSA, have proposed to establish metrics and indicators that represent the quantitative characteristics on the protection condition of the Cyberspace, categorized in terms of perimeter protection, coverage, and availability/ reliability. There is, however, an even greater effort to set up an ample CSA, by overcoming a series of challenges: computer networks complexity, technological evolution, excessive false positive alarms, detection of real-time attack, and a variety of attack vectors.

Keywords: Cyber Situational Awareness; Cyber Warfare; Metrics.

Como Citar:
GUIMARÃES, Flávio de Queiroz. Quantificando a Guerra Cibernética: Métricas de proteção e indicadores para a obtenção de uma consciência situacional cibernética. In: SIMPÓSIO DE

PESQUISA OPERACIONAL E LOGÍSTICA DA MARINHA, 19., 2019, Rio de Janeiro, RJ. **Anais** […]. Rio de Janeiro: Centro de Análises de Sistemas Navais, 2019.

1. INTRODUÇÃO

O constante avanço tecnológico vem causando um impacto substancial na Tecnologia da Informação e Comunicações (TIC), não só aumentando a dependência dos ativos informacionais pelas organizações para o cumprimento da missão, mas também expandindo a superfície de ataque do Espaço Cibernético (ECiber). Como consequência, as instituições vêm incrementando suas capacidades de proteção contra as ameaças iminentes neste novo domínio da guerra, uma vez que as ações ofensivas contra as infraestruturas críticas estatais mostram-se viáveis [11]. Para um gerenciamento efetivo dessa capacidade, faz-se necessário conhecer o ECiber de interesse, mantendo sua Consciência Situacional Cibernética (ConSitCiber), contribuindo para o processo decisório em função do impacto de um incidente de segurança provocado por ações ofensivas de Guerra Cibernética (GC).

A composição do ECiber das instituições envolve uma complexa topologia de rede de computadores, compreendida em um ambiente de rápida evolução tecnológica, onde o intervalo de tempo entre um ataque cibernético empreendido com sucesso e seu efeito desejado é potencialmente curto, evidenciando a necessidade de um rápido processo de tomada de decisão. Nesse contexto, considerando o ponto de vista da proteção cibernética, destaca-se a relevância de se identificar e padronizar as métricas de proteção e indicadores de desempenho para se obter uma ConSitCiber.

A regularidade da proteção cibernética contra as ameaças de diferentes níveis de sofisticação é uma atividade desafiadora. Embora já exista arcabouços técnicos essenciais normatizados [2], há uma carência de compreensão sobre como se adotar as métricas mais relevantes coletadas no ECiber visando estabelecer uma ConSitCiber aceitável que contribua para o processo decisório. Em 2012, um estudo sobre operações cibernéticas realizado pela Força Aérea dos Estados Unidos da América (EUA) tendo 2025 como horizonte, concluiu que a Força não dispunha de uma ConSitCiber, considerada como um dos pré-requisitos para a garantia da proteção do seu ECiber [5]. Em 2016, o Exército norte-americano divulgou que para se obter uma vantagem no ambiente cibernético é preciso entender como e quando os adversários empregarão suas capacidades cibernéticas contra a força e quais ações devam ser tomadas com efetividade para atenuar as consequências de um ataque. Além disso, consideraram a ConSitCiber como um dos elementos principais para as operações cibernéticas, incluindo a defesa de perímetro, análise e monitoramento das ameaças externas e internas, a assistência às equipes de proteção e ataque, monitoramento das comunicações e forense computacional [7].

A contribuição deste artigo é identificar as métricas de segurança relevantes para a modelagem do processo de ConSitCiber, verificando os motivos que tornam o seu desenvolvimento tão crítico para uma efetiva proteção do ECiber. Buscando fundamentar o alcance deste objetivo, apresenta-se na Seção 2 o conceito de consciência situacional e o estabelecimento de uma ConSitCiber a partir de um modelo mental, na Seção 3 são identificadas as métricas de proteção que contribuem para o desenvolvimento de uma ConSitCiber pelo analista de proteção cibernética, na Seção 4 são apontados os desafios a serem superados para a obtenção de uma ConSitCiber plena e, por fim, na Seção 5 são apresentadas as considerações finais.

2. CONCEITO DE CONSCIÊNCIA SITUACIONAL

Embora venha ocorrendo uma evolução do setor cibernético das nações ao longo

dos anos, as ameaças ao ECiber vêm gradativamente incrementando a sofisticação e a complexidade dos seus ataques, sendo necessário um maior esforço para se evitar um possível conflito cibernético. Ao se executar as ações de proteção cibernética é preciso obter e manter uma ConSitCiber do ambiente operacional que permita identificar, compreender e projetar as ações dessas ameaças, assim como ter o conhecimento das vulnerabilidades do ECiber de interesse e do impacto de um possível ataque.

Apesar das diferentes interpretações de consciência situacional disponíveis na literatura [10], a definição amplamente utilizada, em função da sua divisão em níveis é aquela que a descreve como a percepção dos elementos no ambiente, dentro de um volume de tempo e espaço, a compreensão de seu significado e a projeção da condição no futuro próximo [4]. Com base nesta definição, a consciência situacional é composta pelo nível 1 (Percepção), nível 2 (Compreensão) e nível 3 (Projeção), que se alimentam diretamente do ciclo de decisão e ação denominado Modelo de Endsley [4], representado pela Figura 1.

A Percepção envolve a detecção sensorial de informações significativas sobre o ambiente em que se está operando. Considerando o ambiente cibernético, os analistas de proteção precisam perceber as alterações relevantes no seu ECiber, seja de forma manual através de análise de registros ou automática por alarmes, incluindo a percepção dos ativos críticos da rede e do tráfego anômalo.

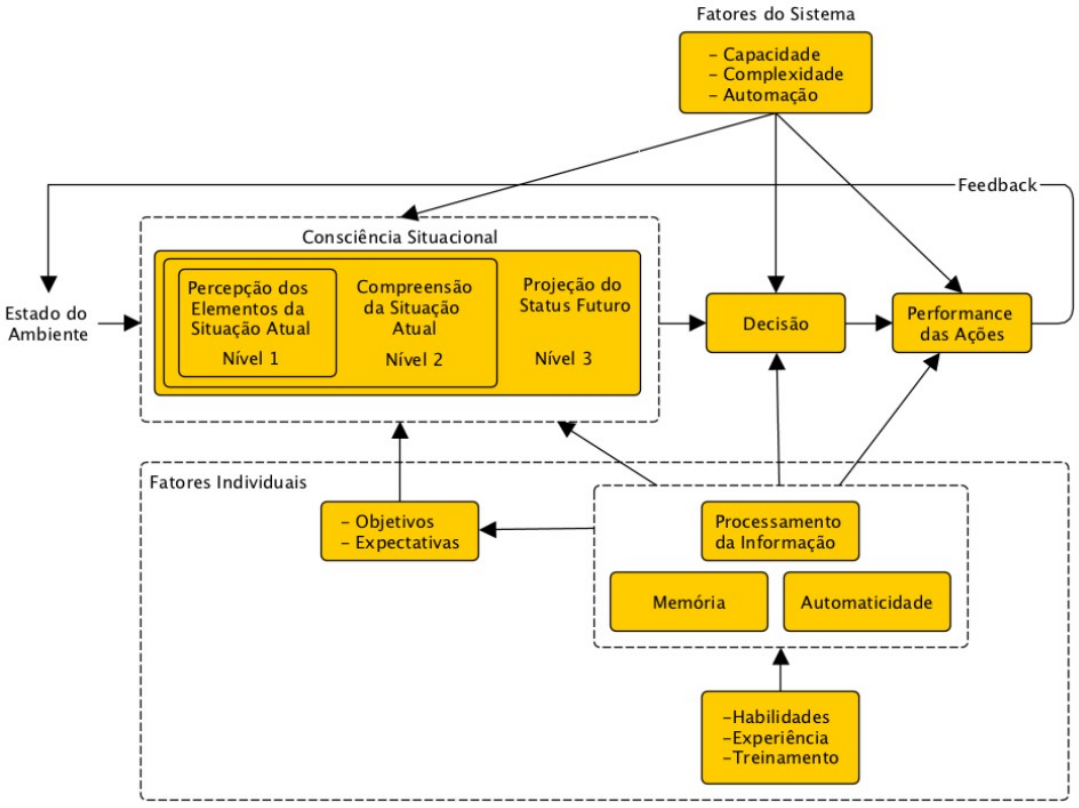

Figura 1 – Modelo de Endsley de Consciência Situacional [4].

A Compreensão envolve a assimilação do significado ou da importância dessas informações em relação aos objetivos a serem alcançados. Este nível é denominado de entendimento das informações percebidas da situação. Considerando o ambiente cibernético, os analistas de proteção precisam entender as causas que tornam um ativo da rede

vulnerável, entender as táticas, técnicas e procedimentos de um ataque, quais incidentes isolados podem estar inter-relacionados, o efeito de um determinado incidente nas operações atuais e a priorização correta de tratamento de incidentes concorrentes.

A Projeção, o nível mais alto de consciência, representa o planejamento das informações adiante no tempo, determinando como elas afetarão os estados futuros do ambiente operacional. Considerando o ambiente cibernético, os analistas de proteção precisam projetar o impacto de uma atividade identificada como ofensiva sobre outros sistemas ou sua consequência ao se propagar através da rede.

Além dos níveis de Percepção, Compreensão e Projeção previstos no Modelo de Endsley foi proposta posteriormente a inclusão do nível de Resolução [8], visando identificar qual o melhor método a seguir para se alcançar uma mudança de estado entre a situação em que se encontra e uma situação desejada.

Portanto, uma vez que o conceito de consciência situacional não depende do tipo do ambiente operacional, considera-se apropriada a adequação dos seus níveis ao ambiente operacional cibernético, estabelecendo uma ConSitCiber, representando-a como a Percepção, Compreensão, Projeção e Resolução inerentes ao ambiente operacional cibernético, ao contribuir para o processo de tomada de decisão nas ações de proteção cibernética.

2.1. Estabelecimento de uma Consciência Situacional Cibernética a partir de um modelo mental

A proteção cibernética é uma ação multidisciplinar que depende da combinação de conhecimentos de técnicas de defesa e ataque, de modo a preveni-los, rastreá-los ou mitigá-los. Considera-se que deva haver uma proatividade dos analistas, onde as ações de proteção não se limitem somente a impedir um comprometimento inicial do ECiber, mas que também detectem os ativos de informação já comprometidos, reduzam a superfície de ataque, implementem as configurações de proteção dos dispositivos e estabeleçam uma capacidade adaptativa e contínua de defesa e resposta que possa ser mantida e aprimorada.

Os analistas de proteção cibernética possuem a função principal de empreender as atividades de detecção, identificação e resposta às ações conduzidas contra o ECiber de interesse empregando uma estratégia de defesa em profundidade e examinando os testes de vulnerabilidades e de invasão como uma avaliação do nível de resiliência dos ativos de informação de interesse. Assim, considera-se que a manutenção de uma ConSitCiber sobre uma ampla variedade de eventos e quantidades de dados gerados seja um desafio analítico.

Para minimizar este desafio, foi proposto que um analista de proteção cibernética utilize um modelo mental [9], baseado em questões a serem respondidas, durante o curso de um evento de segurança de rede para direcionamento de uma ConSitCiber. O modelo é composto por uma taxonomia de questões centradas no usuário, derivadas de uma série de pesquisa dos autores [9], sendo divididas em duas categorias: Detecção de Eventos e Orientação do Evento. A primeira com perguntas onde os analistas devem responder antes e durante um evento, visando o desenvolvimento da percepção da situação e a segunda, com perguntas em proveito da compreensão do estágio de análise da situação, representado pelo Quadro 1 e 2, respectivamente.

A categoria de Detecção de Eventos é dividida nas subcategorias: (i) baseline da rede, quando funcionando em um estado “normal”; (ii) detecção de alterações, capacidade de comparar estados da rede identificando diferentes tendências; e (iii) atividade de rede, refletindo uma mudança de um estado “normal” para “anormal”, atuando como uma sugestão para que o analista estreite sua atenção para uma análise mais aprofundada. Considera-se um estado normal da rede, aquele cujo tráfego de dados e elementos operacionais estejam sob condições habituais, sem indício de uma anomalia ou suspeita de

um comprometimento de um ativo de informação.

Quadro 1 – Detecção de Eventos

Tipo	Questões
Baseline de rede	Meus ativos de rede estão configurados corretamente? Como está a minha rede? O que está acontecendo na rede agora? O que é normal para minha rede? O que não é normal para minha rede? Qual é o status da minha rede? Quais sistemas estão disponíveis e indisponíveis?
Detecção de Alterações	O que aconteceu na minha rede na noite anterior? Minha rede está diferente desde a última semana?
Atividade de Rede	Há uma anormalidade ocorrendo na minha rede? A anormalidade é ruim, boa ou apenas diferente? O tráfego da minha rede está compatível? O que não está acontecendo na minha rede? Qual significado do evento na minha rede? Qual o evento mais importante da minha rede?

Fonte: PAUL,2013 [9].

A categoria de Orientação do Evento é dividida nas subcategorias: (i) identificação de evento, para uma análise detalhada a fim de identificar os fatores motivadores de um ataque e os vinculem a uma ameaça; (ii) impacto na missão, de forma a priorizar a importância de uma ameaça identificada; e (iii) avaliação de danos, para detectar os prejuízos causados.

Quadro 2 – Orientação do Eventos

Tipo	Questões
Identificação de Evento	Este é um tipo de ataque conhecido? Como minha rede está sendo atacada? Como é o ataque? Onde minha rede está sendo atacada? Quem está atacando minha rede? Qual a origem do ataque? Por que minha rede está sendo atacada?
Impacto na Missão	O ataque causa algum prejuízo para a missão? Quão ofensivo é o ataque? Quais as contramedidas necessárias?
Avaliação de Danos	O ataque tem um efeito negativo nas operações? O que o atacante empreendeu? Foi exfiltrado algum dado?

Fonte: PAUL,2013 [9]

A ConSitCiber, formada pelos níveis de Percepção, Compreensão, Projeção e Resolução mostra-se fundamental no contexto da proteção cibernética. Considerando-se a complexidade do ambiente cibernético das instituições, buscou-se minimizar este desafio analítico através da proposta de utilização de um modelo mental [9], baseado em questões voltadas para o analista. No entanto, quantificar qualquer degradação ou melhoria alcançada do ambiente cibernético é um obstáculo para este modelo, tendo em vista a subjetividade das

respostas. Assim sendo, para se obter uma percepção mais precisa da ConSitCiber, propõe-se estabelecer métricas significativas, que possam representar as características quantitativas da condição de proteção de um ECiber.

3. MÉTRICAS DE PROTEÇÃO CIBERNÉTICA

Em razão da multiplicidade do ambiente cibernético, faz-se necessário que os analistas de segurança utilizem métodos sistemáticos para avaliar quantitativamente as vulnerabilidades da rede e prevejam os riscos de ataques e seus possíveis impactos, de forma a minimizar os danos e garantir o cumprimento da missão da organização. O estabelecimento de métricas de proteção fornece uma melhor compreensão aos analistas sobre a adequação dos controles para a segurança do ECiber de interesse.

3.1. DEFINIÇÃO DE MÉTRICA E INDICADOR DE DESEMPENHO

Conceitua-se métrica como uma medida sistemática – dimensão comparada a um padrão – relacionada à quantificação de alguma característica. Por conseguinte, define-se métrica de proteção cibernética como uma dimensão sistemática relacionada à quantificação do grau da possibilidade de sofrer um dano ou perda por um ataque cibernético [1]. Já os indicadores de desempenho são compostos pelas métricas, possuindo uma visão mais ampla e direcionada da ConSitCiber, avaliando a performance organizacional, auxiliando a análise de tendência, a melhoria contínua e a atuação proativa.

O National Institute of Standards and Technology (NIST) define uma métrica como uma ferramenta facilitadora na tomada de decisões e melhora de desempenho através da coleta, análise e geração de relatórios de dados relevantes. Considera-se que as métricas de proteção cibernética sejam implementadas para medir quantitativamente a postura de segurança de uma organização, se tornando essenciais para o gerenciamento da ConSitCiber. Seu objetivo é garantir a continuidade da missão, prevenindo ou minimizando o potencial impacto de incidentes de segurança no ECiber [3].

As métricas de proteção cibernética podem cobrir uma grande categoria de recursos mensuráveis, desde todos os registros de uma auditoria de Segurança da Informação Digital e Comunicações (SIC) até a quantidade total de sistemas atualizados em um período. Busca-se com as métricas, identificar os pontos fracos, determinar as tendências para melhorar a utilização das soluções de segurança e julgar o seu sucesso ou o fracasso das soluções de segurança implementadas.

3.2. MÉTRICAS PARA A CONSCIÊNCIA SITUACIONAL CIBERNÉTICA

As métricas de proteção são utilizadas como quantificadores de segurança, servindo de suporte à tomada de decisões. Para isso, deve-se ter a preocupação de se adotar métricas adequadas, com um padrão consistente de medição, que reflita a ConSitCiber desejada. Para que uma métrica seja eficiente, devem-se prevalecer algumas características já identificadas [6]: aferição consistente; sem subjetividade; fácil coleta, de preferência de forma automatizada; expressa por um número ou um percentual e não utilizar rótulos qualitativos como “alto”, “médio” e “baixo”; usar pelo menos uma unidade de medida; e ter um contexto específico, sendo suficientemente relevante para que os tomadores de decisão possam agir [6].

Ao analisar a aplicação inicial de métricas de proteção para uma instituição, considerando a complexidade do ECiber, foram abordadas aquelas que não somente focassem nas questões defensivas, mas que também pudesse contribuir para o processo de gerenciamento de risco, considerando uma abordagem inicial mínima de consciência situacional. Durante a pesquisa, identificou-se aquelas que poderiam avaliar a postura de segurança, o diagnóstico de problemas e as atividades de segurança associadas à

infraestrutura do ECiber [6].

Considera-se que o ECiber a ser protegido tenha três áreas básicas: uma Rede Externa, composta pela Internet; uma Rede Desmilitarizada (DMZ), onde estão disponibilizados os serviços à Rede Externa; uma Rede Interna (Rede Local); Sensores de Proteção de Perímetro (antispam, firewall e Intrusion Prevention System - IPS) e Proteção de host (antivírus), como representado pela Figura 2. Além disso, considera-se um ECiber com ativos de informação gerenciados por diferentes Sistemas Operacionais (SO) como Windows e Linux.

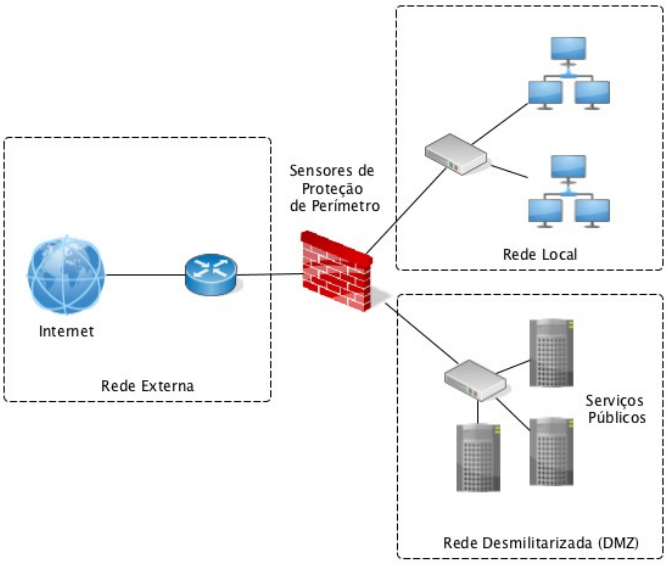

Figura 2 – Topologia de rede básica considerada.

Em razão da diversidade do ambiente operacional cibernético para implementação inicial, considera-se necessário que as métricas abordadas sejam coletadas com periodicidade máxima de 30 dias.

As métricas de proteção foram agrupadas em três categorias, de acordo com os principais elementos operacionais: (i) métricas de proteção de perímetro; (ii) métricas de cobertura; e (iii) métricas de disponibilidade e confiabilidade.

3.2.1. Métricas de Cobertura

As métricas de cobertura buscam entender a extensão e a eficácia dos sistemas de gerenciamento de configuração, correção e vulnerabilidade, caracterizando o alcance da política de segurança adotada pela instituição. Considera-se cobertura como o grau em que um determinado controle de segurança foi aplicado nos ativos de informação. Estas métricas são divididas em: (i) métricas de cobertura de antivírus; (ii) métricas de gerenciamento de atualizações; e (iii) métricas de gerenciamento de vulnerabilidades.

As métricas de cobertura de antivírus, representadas pela Figura 3 e Quadro 3, são coletadas pelo sistema de gerenciamento do software, servindo para identificar as lacunas de implementação do antivírus na rede, quantificando o nível de potencial exposição à infecção interna dos clientes e servidores.

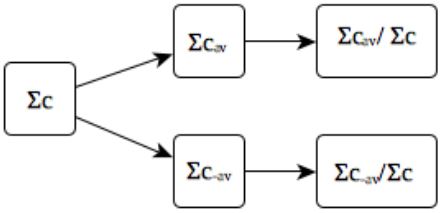

Figura 3 – Métricas básicas de cobertura de antivírus.

Quadro 3 – Métricas básicas de cobertura de antivírus

Cobertura de antivírus		
Variável	**Métrica**	**Propósito**
Σc	Quantidade total de clientes e servidores da organização.	Estabelecer um *baseline* de dimensão do ECiber da organização a ser protegido.
Σc_{av}	Quantidade total de clientes e servidores protegidos com software antivírus instalado e atualizado.	Estabelecer um *baseline* de proteção dos ativos de informação do ECiber da organização.
Σc_{-av}	Quantidade total de clientes e servidores sem software antivírus instalado.	Estabelecer um *baseline* de ativos de informação do ECiber vulneráveis à vírus.
Variável	**Indicador de desempenho**	**Propósito**
$\Sigma c_{av}/\Sigma c$	Índice de proteção por antivírus.	Analisar a variação de proteção dos ativos por antivírus.
$\Sigma c_{-av}/\Sigma c$	Índice de exposição à infecção por vírus.	Analisar a variação da superfície de ataque desprotegida por antivírus.

Fonte: Próprio autor baseado em JAQUITH, 2007 [6].

As métricas de gerenciamento de atualizações, representadas pela Figura 4 e Quadro 4, quantificam o nível de exposição a ataques aos sistemas operacionais desatualizados, caracterizando-os como vulneráveis. As métricas são estabelecidas diferenciando servidores de clientes e diferentes sistemas operacionais.

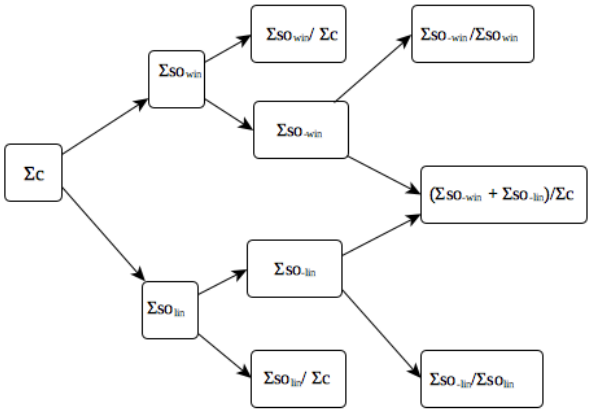

Figura 4 – Métricas básicas de gerenciamento de atualizações.

Quadro 4 – Métricas básicas de gerenciamento de atualizações

Gerenciamento de atualizações		
Variável	**Métrica**	**Propósito**
Σso_{win}	Quantidade total de clientes e servidores com SO Windows.	Estabelecer um *baseline* de dimensão de SO Windows.
Σso_{lin}	Quantidade total de clientes e servidores com SO Linux.	Estabelecer um *baseline* de dimensão de SO Linux.
$\Sigma so_{win}/ \Sigma c$	Proporção de SO Windows do total de clientes e servidores.	Estabelecer um *baseline* de proporção de SO Windows.
$\Sigma so_{lin}/ \Sigma c$	Proporção de SO Linux do total de clientes e servidores.	Estabelecer um *baseline* de proporção de SO Linux.
Σso_{-lin}	Total de clientes e servidores com SO Linux desatualizado.	Identificar a exposição a ataques vinculados ao SO Linux desatualizado.
Σso_{-win}	Total de servidores com SO Windows desatualizado.	Identificar a exposição a ataques vinculados ao SO Windows desatualizado
Variável	**Indicador de desempenho**	**Propósito**
$\Sigma so_{-win}/\Sigma so_{win}$	Índice de exposição de SO Windows.	Analisar a variação de SO Windows desatualizados.
$\Sigma so_{-lin}/\Sigma so_{lin}$	Índice de exposição de SO Linux.	Analisar a variação de SO Linux desatualizados.
$(\Sigma so_{-win} + \Sigma so_{-lin})/\Sigma c$	Índice de exposição de SO do ECiber.	Analisar a taxa de desatualização do ECiber.

Fonte: Próprio autor baseado em JAQUITH, 2007 [6].

As métricas de gerenciamento de vulnerabilidades, representadas pela Figura 5 e Quadro 5, fornecem uma visão da superfície de ataque da rede que possui vulnerabilidades conhecidas e não corrigidas. As vulnerabilidades são falhas imprevistas no projeto ou na implementação de um software que permitem a exploração por usuários maliciosos, com objetivo de causar algum prejuízo. Para identificá-las, utiliza-se processos de escaneamento dos ativos, classificando as vulnerabilidades em diferentes níveis de criticidade. Ao se obter uma ConSitCiber, faz-se necessário priorizar a correção das vulnerabilidades conhecidas mais críticas.

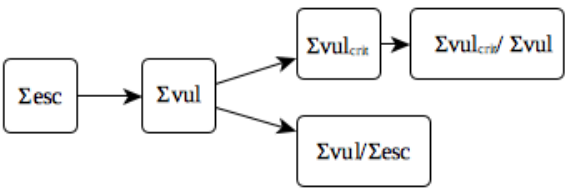

Figura 5 – Métricas básicas de gerenciamento de vulnerabilidades.

Quadro 5 – Métricas básicas de gerenciamento de vulnerabilidades

Gerenciamento de vulnerabilidades		
Variável	**Métrica**	**Propósito**
f_{vul}	Frequência de escaneamento de vulnerabilidades nos servidores.	Estabelecer um *baseline* de escaneamento de vulnerabilidades nos ativos do ECiber da organização.
Σesc	Quantidade total de ativos escaneados.	Estabelecer um *baseline* de ativos escaneados.
Σvul	Quantidade total de vulnerabilidades identificadas.	Estabelecer um *baseline* de vulnerabilidades conhecidas.
Σvul_{crit}	Quantidade total de vulnerabilidades classificadas como críticas.	Identificar as vulnerabilidades críticas do ECiber.
Variável	**Indicador de desempenho**	**Propósito**
$\Sigma vul_{crit}/\Sigma vul$	Índice de vulnerabilidades críticas.	Identificar a proporção de vulnerabilidades críticas do ECiber.
$\Sigma vul/\Sigma esc$	Índice de vulnerabilidades conhecidas.	Identificar o nível de exposição de vulnerabilidades.
t_{crit}	Tempo médio decorrido para mitigar uma vulnerabilidade crítica após sua identificação.	Identificar o nível de eficácia de resposta à mitigação de vulnerabilidades.

Fonte: Próprio autor baseado em JAQUITH, 2007 [6].

3.2.2. Métricas de Proteção de Perímetro

As métricas de proteção de perímetro visam compreender o risco de incidentes por ameaças externas ao ECiber de interesse, medindo a efetividade dos principais sistemas de proteção da borda da rede interna (firewall, sistema de prevenção de intrusão e sistema antispam) e proteção de host (software antivírus). Assim, foram divididas em: (i) métricas de antispam; (ii) métricas de detecção de vírus; (iii) métricas de firewall; e (iv) métricas de prevenção de intrusão.

As métricas de antispam, representadas pela Figura 6 e Quadro 6, servem para quantificar a proteção do ECiber pelo analista quanto à recepção de spam (e-mails comerciais indesejados) e ameaças por phishing, uma das principais fontes de transmissão de malwares provenientes da Internet.

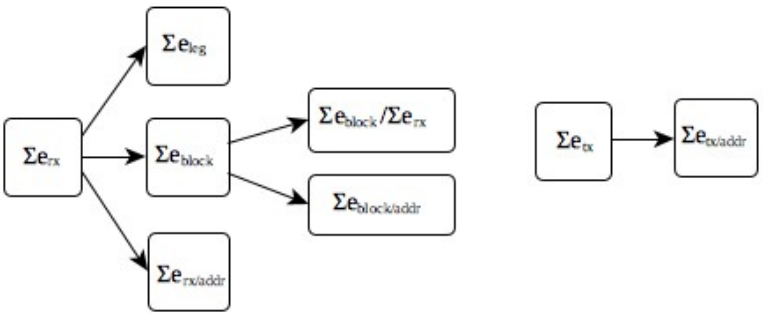

Figura 6 – Métricas básicas de antispam

Quadro 6 – Métricas básicas de antispam

Email		
Variável	**Métrica**	**Propósito**
Σe_{rx}	Quantidade total de e-mails recebidos pelo antispam originados da Internet	Estabelecer um *baseline* de tráfego de recebimento de e-mails da organização.
Σe_{leg}	Quantidade total de e-mails legítimos recebidos pelo serviço de correio originados da Internet	Estabelecer um *baseline* de tráfego de recebimento de e-mails legítimos da organização.
Σe_{tx}	Quantidade total de e-mails transmitidos pelo serviço de correio para a Internet	Estabelecer um *baseline* de tráfego de transmissão de e-mails da organização.
$\Sigma e_{tx/addr}$	Quantidade total de e-mails transmitidos pelo serviço de correio para a Internet por endereço de e-mail da organização	Identificar tráfego anômalo de transmissão de e-mails para a Internet por endereços internos da organização.
$\Sigma e_{rx/addr}$	Quantidade total de e-mails recebidos pelo serviço de correio originados da Internet por endereço de e-mail da organização	Identificar tráfego anômalo de recepção de e-mails por endereços internos da organização.
Σe_{block}	Quantidade total de e-mails originados da Internet bloqueados pelo antispam	Identificar a intensidade de recebimento de spam/ phishing pela organização.
$\Sigma e_{block/addr}$	Quantidade total de e-mails bloqueados pelo antispam por endereço de e-mail	Identificar os endereços de e-mails da organização mais vulneráveis à ataques de phishing.
Variável	Indicador de desempenho	Propósito
$\Sigma e_{block}/\Sigma e_{rx}$	Índice de detecção de spam/phishing	Analisar a taxa de poluição por e-mails.

Fonte: Próprio autor baseado em JAQUITH, 2007 [6].

As métricas de detecção de vírus, representadas pela Figura 7 e Quadro 7, são coletadas a partir de seu gerenciador central, servindo para quantificar a taxa de infecção de clientes e servidores do ECiber.

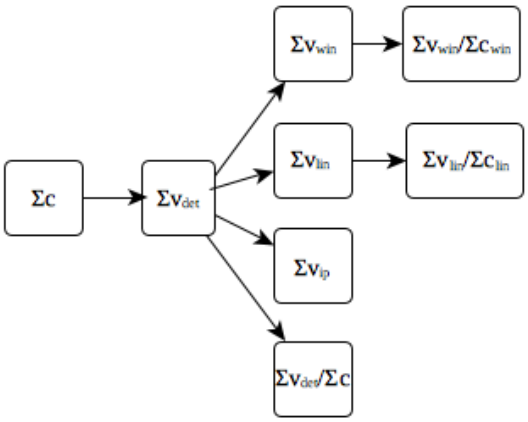

Figura 7 – Métricas básicas de de detecção de vírus

Quadro 7 – Métricas de detecção de vírus

Detecção de vírus		
Variável	**Métrica**	**Propósito**
Σv_{det}	Quantidade total de vírus detectados da organização.	Estabelecer um *baseline* de detecção de vírus no ECiber da organização.
Σv_{win}	Quantidade total de vírus detectados em servidores e clientes por SO Windows.	Estabelecer um *baseline* de detecção de vírus por SO Windows da organização.
Σv_{lin}	Quantidade total de vírus detectados em servidores e clientes com SO Linux.	Estabelecer um *baseline* de detecção de vírus por SO Linux da organização.
Σv_{ip}	Quantidade total de vírus detectados por IP.	Identificar os ativos mais visados à infecção por vírus no ECiber da organização.
Variável	Indicador de desempenho	Propósito
$\Sigma v_{win}/\Sigma c_{win}$	Índice tentativa de infecção por vírus em SO Windows.	Analisar a taxa de tentativa de infecção em SO Windows.
$\Sigma v_{lin}/\Sigma c_{lin}$	Índice de tentativa de infecção por vírus em SO Linux.	Analisar a taxa de tentativa de infecção em SO Linux.
$\Sigma v_{det}/\Sigma c$	Índice de tentativa de infecção por vírus no ECiber.	Analisar a taxa de tentativa de infecção no ECiber da organização.

Fonte: Próprio autor baseado em JAQUITH, 2007 [6].

As métricas relacionadas ao firewall, representadas pelo Quadro 8, desempenham a função de quantificar a proteção do tráfego proveniente da Internet, bloqueado por regras estáticas, definidas pela política de segurança da organização.

Quadro 8 – Métricas de firewall

Firewall		
Variável	**Métrica**	**Propósito**
Σfw_{alt}	Quantidade total de mudanças de regras de firewall implementadas no período.	Identificar o nível de complexidade de alteração de política requerida.
Σfw_{src}	Quantidade total de tentativas de acesso de ativos da rede interna à Internet bloqueada pela política de segurança por IP de origem.	Investigar os ativos internos que estão com tráfego anômalo para a Internet.
Σfw_{dst}	Quantidade total de tentativas de acesso à Internet bloqueada pela política de segurança por IP de destino.	Investigar os destinos de tráfego anômalo para a Internet.
Σfw_{por}	Quantidade total de tentativas de acesso à Internet bloqueada pela política de segurança por porta de destino.	Investigar os protocolos e aplicações do tráfego anômalo para a Internet.

Fonte: Próprio autor baseado em JAQUITH, 2007 [6].

As métricas coletadas pelo gerenciador do Sistema de Prevenção de Intrusão (IPS), representadas pelo Quadro 9, são relacionadas aos ataques bloqueados na borda da rede pelo tráfego proveniente da Internet.

Quadro 9 – Métricas de prevenção de intrusão

Prevenção de intrusão		
Variável	**Métrica**	**Propósito**
Σips	Quantidade total de tentativas de ataques provenientes da Internet bloqueados pelo IPS por tipo de assinatura de tráfego.	Estabelecer um *baseline* de ataques bloqueados originados na Internet com destino ao ECiber da organização.
Σips_{src}	Quantidade total de tentativas de ataques provenientes da Internet bloqueados pelo IPS por IP de origem.	Identificar origem da infraestrutura utilizada pelo atacante.
Σips_{dst}	Quantidade total de tentativas de ataques provenientes da Internet bloqueados pelo IPS por IP de destino.	Identificar o IP de destino da rede interna para investigação de possível comprometimento da máquina.

Fonte: Próprio autor baseado em JAQUITH, 2007 [6].

3.2.3. Métricas de Disponibilidade e Confiabilidade

As métricas de disponibilidade e a confiabilidade, representadas pelo Quadro 10, destinam-se a entender a resistência dos sistemas, considerados críticos, às falhas de hardware, software e energia, cujo objetivo é a disponibilidade dos serviços durante o maior tempo possível.

Quadro 10 – Métricas de disponibilidade e confiabilidade

Disponibilidade e confiabilidade		
Variável	**Métrica**	**Propósito**
t_{disp}	Tempo total de disponibilidade dos servidores críticos durante o período de medição.	Estabelecer um *baseline* de disponibilidade dos servidores críticos.
t_{ind}	Tempo de indisponibilidade planejada dos servidores críticos durante o período de medição.	Estabelecer um *baseline* de indisponibilidade dos servidores devido a uma paralisação planejada dos serviços.
t_{inc}	Tempo de indisponibilidade dos servidores críticos devido a um incidente de segurança durante o período de medição.	Estabelecer um *baseline* de indisponibilidade dos servidores devido a uma paralisação planejada dos serviços.
Σin	Quantidade total de incidentes de segurança.	Estabelecer um *baseline* quantitativo de incidentes de segurança.
Σin_{type}	Quantidade total de incidentes de segurança por tipo de incidentes.	Identificar os incidentes mais recorrentes no ECiber.
Variável	**Indicador de desempenho**	**Propósito**
t_{disp}/p	Índice de disponibilidade dos servidores críticos durante o período p de medição.	Identificar o nível de disponibilidade dos servidores críticos.
t_{ind}/p	Índice de indisponibilidade planejada dos servidores críticos durante o período p de medição.	Identificar o nível de indisponibilidade dos servidores devido a uma paralisação planejada dos serviços.
t_{inc}/p	Índice de indisponibilidade dos servidores críticos devido a um incidente de segurança durante o período p de medição.	Identificar o nível de indisponibilidade dos servidores devido a uma paralisação planejada dos serviços.

Fonte: Próprio autor baseado em JAQUITH, 2007 [6].

As métricas de proteção funcionam como quantificadores, servindo de suporte à tomada de decisão, necessitando de uma adequação para que possa retratar de forma consistente a ConSitCiber desejada. Destarte, para complementar o mapa mental de questões relacionadas ao ambiente cibernético, propôs-se adotar as métricas e indicadores de desempenho que retratam uma ConSitCiber, ao coletar dados dos sistemas de gerenciamento de e-mail, antivírus, firewall, IPS e gerenciador de vulnerabilidades.

4. DESAFIOS PARA A MANUTENÇÃO DE UMA CONSCIÊNCIA SITUACIONAL CIBERNÉTICA

Além do estabelecimento do mapa mental e métricas de proteção, estima-se ainda que o processo de obtenção e manutenção de uma ConSitCiber requeira alguns aspectos específicos como o entendimento dos ataques cibernéticos, a priorização das ações, o diagnóstico contínuo e o processo de automação da defesa. A aprendizagem com os ataques fornecer uma base de conhecimento visando a construção de uma proteção eficaz. A priorização das ações remete a opção pela proteção que atuará contra a ameaça que tiver o maior impacto no ambiente cibernético. Esta priorização dar-se-á a partir de um diagnóstico contínuo automatizado, buscando atenuar a capacidade do analista de proteção, tornando a análise mais confiável. Há, no entanto, a necessidade de superar uma série de dificuldades.

4.1. AS DIFICULDADES A SEREM SUPERADAS

Há um esforço ainda maior para se estabelecer uma ConSitCiber plena, superando uma série de desafios: a complexidade das redes de computadores; a evolução tecnológica; a grande quantidade de alarmes falsos positivos; a detecção de um ataque em tempo real; e a diversidade de potenciais vetores de ataque.

A dimensão e a complexidade das redes de computadores criam um desafio significativo para se manter uma ConSitCiber. A medida que se amplia o ECiber, mais ativos e ramificações são expandidos podendo alterar significativamente a percepção dos ativos críticos, dificultando a compreensão de uma imagem precisa.

As tecnologias que provêm a infraestrutura do ECiber tendem a evoluir rapidamente. Novos softwares, sistemas e equipamentos de conectividade são incorporados dificultando não apenas o entendimento preciso da topologia da rede, mas das novas vulnerabilidades introduzidas pela evolução tecnológica, comprometendo a compreensão e a projeção da ConSitCiber.

A detecção de um ataque cibernético, em muitos casos, também pode ser difícil, dado que eventos anômalos caracterizados como falsos positivos são comuns de serem observados durante as ações de proteção cibernética. É possível descartar uma atividade maliciosa na rede como sendo um falso positivo, afetando a percepção das características de um ataque cibernético real.

Com o incremento da sofisticação dos ataques cibernéticos, ampliaram-se os potenciais vetores de ataque a serem empreendidos, assim como, a quantidade e tipos de assinaturas de ataque. Estima-se que até 2025 haveria cerca de 200 milhões de novas assinaturas de malware por ano [5]. Assim, desenvolver uma compreensão de todos os potenciais vetores de ataque de uma ameaça e seus efeitos através da aprendizagem e experiência se torna uma tarefa praticamente inexequível.

O alto nível de sobrecarga associado à percepção de dados em uma grande e complexa rede torna a proteção cibernética uma missão desafiadora para os analistas. Considera-se que, além de estabelecer métricas de proteção significativas, seja preciso estabelecer um processo de automação, de forma a se obter um monitoramento de eventos confiável e contínuo, reduzindo o desgaste cognitivo do analista.

5. CONCLUSÃO

Ao longo das seções, foram observadas a necessidade de obter e manter uma ConSitCiber que permita identificar, compreender e antecipar as ameaças ao ECiber, formulando um modelo mental baseado em questões a serem respondidas pelos analistas. No entanto, pela subjetividade das questões, propôs-se estabelecer métricas e indicadores significativos que possam representar as características quantitativas da condição de proteção de um ECiber. Para garantir o sucesso da missão de proteção cibernética, os analistas de segurança precisam manter uma ConSitCiber eficiente, de forma monitorar continuamente as atividades da rede, identificar eventos suspeitos e mitigar as possíveis vulnerabilidades em tempo hábil. Nesse contexto, considerando o ponto de vista da proteção cibernética de forma a proporcionar o apoio ao processo de tomada de decisão, foram identificadas as métricas de proteção que possam contribuir para obtenção de uma ConSitCiber, divididas nas categorias de Defesa de Perímetro, Cobertura e Controle e Disponibilidade e Confiabilidade.

Ainda assim, estima-se que, além da implementação de um modelo mental e métricas de proteção, faz-se necessário ter o entendimento dos ataques, saber priorizar as ações, manter um diagnóstico contínuo e automatizar o processo da proteção, além de superar a complexidade das redes de computadores, a evolução tecnológica, a grande quantidade de alarmes falsos positivos, a detecção de um ataque em tempo real e os potenciais vetores de ataque.

6. REFERÊNCIAS BIBLIOGRÁFICAS

[1] ABBADI, Z. **Security Metrics, What Can We Measure?**. Open Web Application Security Project (OWASP), 2007. Disponível em: https://www.owasp.org/images/b/b2/Security_Metics-_What_can_we_measure-_Zed_Abbadi.pdf. Acesso em: 14 abr. 2019.

[2] BARABANOV, R.; KOWALSKI, S.; YNGSTRÖM, L. **Information security metrics**: State of the art: State of the art, Stockholm Univ., Stockholm, Sweden, Tech. Rep. DSV Report series 11-007, 2011. Disponível em: https://www.researchgate.net/publication /279476237_Information_Security_Metrics_State_of_the_Art_State_of_the_art. Acesso em: 14 abr. 2019.

[3] CHEW, E.; SWANSON M.; STINE, K.; BARTOL, N.; BROWN, A; ROBINSON, W. **Security Metrics Guide for Information Technology Systems**, NIST Special Publication 800-55, 2003. Disponível em: https://nvlpubs.nist.gov/nistpubs/Legacy /SP/nistspecialpublication800-55.pdf. Acesso em: 14 abr. 2019.

[4] ENDSLEY, M.R. **Human Factors and Ergonomics Society**. Toward a theory of situation awareness in dynamic systems, 1995. Disponível em: http://www.realtechsupport.org/ UB/I2C/SituationAwarenessTheory_1995.pdf. Acesso em: 14 abr. 2019.

[5] ESTADOS UNIDOS. U.S. Air Force. **United States Air Force Cyberspace Science and Technology Vision 2012-2025**, 2012. Disponível em: https://www.globalsecurity.org/ security/library/policy/usaf/cybervision2025_afd-130327-306.pdf. Acesso em: 14 abr. 2019.

[6] JAQUITH, A. **Security Metrics: Replacing Fear, Uncertainty, and Doubt**, Addison-Wesley Professional, 2007.

[7] MARTIN, W. J.; KAEMMER, E. **Entendimento Situacional Cibernético para os Comandantes Táticos do Exército**. Military Review, p.72, 2016. Quarto trimestre. Disponível em: https://www.armyupress.army.mil/Portals/7/militaryreview/Archives/PortugueseMilitaryReview_20161231_art011POR.pdf. Acesso em: 14 abr. 2019.

[8] MCGUINNESS, B.; FOY, J. L. **A subjective measure of SA: The crew awareness rating scale (CARS)**. Proceedings of the first human performance, situation awareness, and automation conference, 2000. Savannah, Georgia, USA.

[9] PAUL, C.; WHITLEY, K. A . **Taxonomy of Ciber Awareness Questions for the User-Centered design of Cyber Situation Awareness**. Lecture Notes in Computer Science, pp.145-154, 2013. Springer, Disponível em: https://pdfs.semanticscholar.org/0ba6/8b5f0ef35ef94fa238275e2f571bce446538.pdf. Acesso em: 14 abr. 2019.

[10] STANTON, N.A.; CHAMBERS, P.R.G.; PIGGOTT, J. **Situational Awareness and Safety**, Safety Science 39, p. 189-204, 2001.

[11] ZHANG, N.; KANT, K.; DAS, S. K. **Handbook on Securing Cyber-Physical Critical Infrastructure**, Morgan Kaufmann Publishers, 2012.