ESCOLA DE GUERRA NAVAL

CMG MÁXIMO EDUARDO EGGER

A GUERRA CIBERNÉTICA NO NÍVEL ESTRATÉGICO

DEFESA CIBERNÉTICA DE UMA FORÇA NAVAL NO MAR

Rio de Janeiro
2014

CMG MÁXIMO EDUARDO EGGER

A GUERRA CIBERNÉTICA NO NÍVEL ESTRATÉGICO

DEFESA CIBERNÉTICA PARA UMA FORÇA NAVAL NO MAR

Monografia apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso de Política e Estratégia Marítimas.

Orientador: CMG (RM1) Marco Aurélio Del Sarto Vendramini

Rio de Janeiro
Escola de Guerra Naval
2014

AGRADECIMENTOS

À minha família pelo apoio e compreensão de minhas ausências familiares para a dedicação a este trabalho e ao Curso de Política e Estratégia Marítimas.

RESUMO

Com o aumento da interligação das redes computacionais e dos sistemas de informação, cresce também a exploração de suas vulnerabilidades visando obter vantagens por meio de acessos não autorizados, podendo, inclusive, comprometer informações de relevância para a organização ou para o indivíduo. Neste contexto, a Política Nacional de Defesa brasileira, que é o documento de mais alto nível do planejamento de defesa, preconiza como orientação estratégica, aperfeiçoar os dispositivos de segurança e adotar procedimentos que minimizem a vulnerabilidade dos sistemas que possuam suporte de tecnologia da informação e comunicação para se opor a possíveis ataques cibernéticos. Assim, é essencial estabelecer ações de defesa cibernética visando à proteção dos ativos de informação da MB. Neste trabalho foi analisado o impacto do nível de interoperabilidade dos sistemas comando e controle na defesa cibernética de uma força naval no mar. Deste modo, o presente trabalho baseou-se no método hipotético-dedutivo seguindo preponderantemente um enquadramento qualitativo e empregando a pesquisa bibliográfica para realizar uma análise de risco da infraestrutura da rede prevista para cada nível de interoperabilidade.

Palavras-chave: Defesa Cibernética, Interoperabilidade, Força naval, Comando e controle.

ABSTRACT

With the increasing interconnection of computing and information systems networks also grows exploiting their vulnerabilities to obtain advantages by means of unauthorized access, and may also compromise information relevant to the organization or the individual. In this context, the Brazilian National Defense Policy, which is the document of the highest level of defense planning, as advocated strategic direction, improving the safety and adopt procedures to minimize the vulnerability of systems with support for information technology and communication to counter possible cyber attacks? Thus, it is essential to establish cyber defense actions aimed at protecting the information assets of Brazilian Navy. This work analyzed the impact of the level of interoperability of command and control systems and cyber protection of a naval force at sea. Thus, this study was based on the hypothetical-deductive method following mainly a qualitative framework and employing a literature search to perform a risk analysis of network infrastructure provided for each level of interoperability.

Keywords: Cyber security, Interoperability, Naval Force, Command and Control.

LISTA DE ABREVIATURAS E SIGLAS

APF	Administração Pública Federal
BIA	Business Impact Analysis
CIM	Centro de Inteligência da Marinha
ComOpNav	Comando de Operações Navais
COTS	Commercial-off-the-shelf
CTIM	Centro de Tecnologia de Informação da Marinha
DC	Defesa Cibernética
DCTIM	Diretoria de Comunicações e Tecnologia de Informação da Marinha
DGMM	Diretoria-Geral do Material da Marinha
DGPM	Diretoria-Geral do Pessoal da Marinha
DMDC	Doutrina Militar de Defesa Cibernética
DoD	Departamento de Defesa dos EUA
ECiber	Espaço cibernético
EMA	Estado-Maior da Armada
END	Estratégia Nacional de Defesa
ETIR	Equipe de Tratamento de Incidente de Rede
EUA	Estados Unidos da América
GC	Guerra Cibernética
GCR	Guerra Centrada em Rede
GSI/PR	Gabinete de Segurança Institucional da Presidência da República
ISP	Internet service providers
LAN	Local Area Network
LISI	Levels of Information System Interoperability
MB	Marinha do Brasil
MD	Ministério da Defesa
OM	Organização Militar
P2P	peer-to-peer
PCD	Política Cibernética de Defesa
PND	Política Nacional de Defesa
PPTP	Point-to-Point Tunneling Protocol

RU	Reino Unido
SIC	Segurança da Informação e Comunicação
SisGAAz	Sistema Gerenciamento da Amazônia Azul
SISTRAM	Sistema de Informações Sobre o Tráfego Marítimo
SMDC	Sistema Militar de Defesa Cibernética
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação
USNAVY	United States Navy – Marinha dos Estados Unidos
WAN	Wide Area Network
WLAN	Wireless Local Area Network

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

Com o aumento da interligação das redes computacionais e dos sistemas de informação, cresce também a exploração de suas vulnerabilidades por aqueles que genericamente chamaremos de adversários, visando obter vantagens por meio de acessos não autorizados, podendo, inclusive, comprometer informações de relevância para a organização ou para o indivíduo. Nesse mundo virtual interligado estão inseridos os conceitos de espaço cibernético (ECiber), ataques cibernéticos e Guerra Cibernética (GC).

O ECiber pode ser definido como o espaço virtual, composto por dispositivos computacionais conectados em redes ou não, por onde as informações digitais transitam, são processadas e/ou armazenadas. Este ambiente é caracterizado por ser pouco conhecido, muito dinâmico, com alcance global e ausência de fronteira, podendo ser utilizado para a prática de atos ilícitos, como invasões à rede, destruição ou roubo de informações, por meio de ataques cibernéticos. Quando esses ataques são entre Estados, constitui uma GC. No Glossário das Forças Armadas é definida como um:

> [...] conjunto de ações para uso ofensivo e defensivo de informações e sistemas de informações para negar, explorar, corromper ou destruir valores do adversário baseados em informações, sistemas de informação e redes de computadores. Estas ações são elaboradas para obtenção de vantagens tanto na área militar quanto na área civil (BRASIL, 2007b, p. 123).

O setor cibernético foi destacado na Estratégia Nacional de Defesa (END), como um dos três setores estratégicos essenciais para a defesa nacional.

A Política Nacional de Defesa (PND), que é o documento de mais alto nível do planejamento de defesa, preconiza como orientação estratégica aperfeiçoar os dispositivos de segurança e adotar procedimentos que minimizem a vulnerabilidade dos sistemas que possuam suporte de tecnologia da informação e comunicação para se opor a possíveis ataques

cibernéticos. Neste contexto, é essencial estabelecer ações de defesa cibernética visando à proteção dos ativos de informação da MB.

Com a solicitação, pela Diretoria-Geral de Material da Marinha (DGMM), para incluir um tema de um estudo referente à defesa cibernética dos meios navais no mar, o presente trabalho procurou identificar as características da defesa cibernética dos sistemas de informação empregados na força naval, respondendo a seguinte pergunta:

Qual é o impacto do nível de interoperabilidade dos sistemas comando e controle na defesa cibernética de uma força naval no mar?

Ao responder a pergunta, este trabalho pretende contribuir na identificação das características da defesa cibernética de uma força naval de acordo com os níveis de interoperabilidade dos sistemas de informação utilizados por uma força naval no mar. Estes níveis de interoperabilidade utilizados foram criados pelo Departamento de Defesa (DoD) dos Estados Unidos para estudar o desenvolvimento dos sistemas de comando e controle. O estudo foi publicado no documento "*Levels of Information System Interoperability*" (LISI).

Para desenvolver o trabalho foi utilizado o método hipotético-dedutivo seguindo preponderantemente um enquadramento qualitativo e empregando a pesquisa bibliográfica, para o qual foi formulada a seguinte hipótese:

Um maior nível de interoperabilidade dos sistemas de TI empregados pela força naval representa uma maior dificuldade para realizar a defesa cibernética desta força naval no mar.

O presente trabalho está estruturado em cinco capítulos: o primeiro capítulo é composto desta introdução para situar o leitor no contexto do assunto abordado, o segundo capítulo apresenta o referencial teórico com os principais conceitos da Guerra Cibernética, da guerra centrada em rede e da interoperabilidade de sistemas. O terceiro capítulo apresenta as os conceitos da segurança de uma rede. No quarto capítulo é realizada uma análise de

segurança de rede para cada um dos níveis de interoperabilidade de sistemas para identificar as principais características. E no capítulo 5 é apresentada a conclusão do trabalho, com uma síntese dos pontos mais importantes abordados.

2 CONCEITOS

Neste capítulo são apresentados os conceitos referentes ao Espaço Cibernético (ECiber), a Segurança Cibernética, a Defesa Cibernética, a Guerra Cibernética, a Guerra Centrada em Rede, a Interoperabilidade dos sistemas de informação e a segurança de redes de computadores.

2.1 ECIBER, SEGURANÇA, DEFESA E GUERRA CIBERNÉTICA

Segundo Richard A. Clarke[1] (2010) o ECiber é composto por todas as redes de computadores do mundo e por tudo que a elas se conectam e controlam, mesmo aquelas que não estão acessíveis a partir da Internet.

No Brasil o ECiber foi definido como "espaço virtual, composto por dispositivos computacionais conectados em redes ou não, por onde as informações digitais transitam, são processadas e/ou armazenadas" (BRASIL, 2011a). Para proteger o ECiber, a Segurança e a Defesa Cibernética brasileira foram inicialmente organizadas de acordo com os níveis de decisão (BRASIL, 2011a): político, estratégico, operacional e tático.

No nível político, o Gabinete de Segurança Institucional da Presidência da República (GSI/PR) é o órgão da Administração Pública Federal (APF) responsável por definir os objetivos para realizar a segurança cibernética. A segurança cibernética refere-se à proteção e à garantia de utilização de ativos de informação estratégicos, principalmente os ligados às infraestruturas críticas da informação (redes de comunicações e de computadores e

[1] Richard A. Clarke é professor da *Kennedy School of Government* da Universidade de Harvard. No governo americano, trabalhou para as administrações de Ronald Reagan, George Bush (pai), Bill Clinton e George Bush (filho) até pouco antes do início da guerra do Iraque.

seus sistemas informatizados) que controlam as infraestruturas críticas nacionais. No Livro Verde, segurança cibernética do Brasil é definida como:

> […] a arte de assegurar a existência e a continuidade da sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas (BRASIL, 2010, p. 19).

No nível estratégico realiza-se a defesa cibernética, em que o MD é o responsável pelo conjunto de ações defensivas, exploratórias e ofensivas, no contexto de um planejamento militar, realizadas em um espaço cibernético, com as finalidades de proteger os sistemas de informação, obter dados para a produção de conhecimento de inteligência e causar prejuízos aos sistemas de informação do oponente (BRASIL, 2011a); e

Nos níveis operacional e tático ocorrem o preparo e o emprego operacional, nos quais as ações de proteção, de exploração e de ataque cibernéticos são executadas pelas Forças Armadas e caracterizam a Guerra Cibernética (GC). As ações de proteção, de exploração e de ataque cibernético executadas pelas Forças Armadas de per si estão no nível tático, mas quando são coordenadas por um Comando Conjunto estão no nível operacional e a GC se restringirá ao Teatro de Operações estabelecido. (BRASIL, 2011b).

Com relação às características da GC, Paul Cornish[2] *et al*. (2010) apresentam no relatório *On Cyber Warfare* do *Chatham House*[3] que a Guerra Cibernética pode ser um conflito entre Estados, mas também pode envolver atores não estatais de várias maneiras. Na Guerra Cibernética, é extremamente difícil empregar uma força precisa e proporcional, em que o alvo pode ser militar, industrial ou civil, ou uma sala de servidor que hospeda uma grande variedade de clientes, sendo que apenas um entre eles é o alvo pretendido (CORNISH, 2010). Para definir melhor a GC, o autor identifica as suas principais características:

---

[2] Dr. Paul Cornish é professor do *International Security and Head of the International Security Programme at Chatham House*.

[3] *Chatham House*, o *Royal Institute of International Affairs*, é um instituto independente, sem fins lucrativos, não governamental, sediada em Londres, cuja missão é analisar o conhecimento e promover uma melhor compreensão dos principais temas políticos internacionais. Ver <http://www.chathamhouse.org>.

a) Guerra Cibernética pode permitir atingir seus objetivos políticos e estratégicos, sem a necessidade de um conflito armado;

b) ECiber dá poder desproporcional a atores pequenos;

c) Utilizando endereços do protocolo de Internet[4] falsos nos computadores, os atacantes podem agir com quase completo anonimato e impunidade, pelo menos a curto prazo;

d) No ECiber as fronteiras não são claras entre o militar e o civil, e entre o físico e o virtual, no qual o poder pode ser exercido por Estados ou atores não-estatais, ou por intermediários;

e) O espaço cibernético deve ser visto como o "quinto campo de batalha", ao lado das arenas mais tradicionais da terra, mar, ar e espaço. A Guerra Cibernética é melhor compreendida como um componente novo, mas não inteiramente separada destes ambientes de conflito multifacetado; e

f) Ações bélicas no ciberespaço são mais prováveis de ocorrerem em conjunto com as outras formas de coerção e de confronto. No entanto, as formas e meios da GC continuam inegavelmente distintos desses outros modos de conflito.

O relatório apresenta, ainda que, embora possa haver falta de políticas associadas com os diferentes atos de Guerra Cibernética em todo o mundo, estes atos ainda não podem ser descritos como um fenômeno político restrito da maneira que Clausewitz, o soldado-filósofo do século XIX e autor de “Da Guerra”, entenderia (CORNISH, 2010).

[4] Endereço do protocolo de internet (Internet Protocol address – IP address). Um número único atribuído a cada computador na Internet, que consiste de quatro números, onde cada número tem valor menor que 256, sendo separados por um ponto, como 129.16.255.0 (TIPTON, 2007, p. 3028).

O ECiber é descrito por Cornish (2010) como terra *nullius*, que atualmente encontra-se fora do alcance político. Cornish ainda considera que a ausência de uma política restritiva estruturada em torno da Guerra Cibernética faz com que o ECiber seja um lugar atraente para perseguir objetivos culturais, religiosos, econômicos, sociais e até mesmo políticos.

A tarefa de proteger o ECiber não é simples, principalmente pelo anonimato do atacante e a falta de uma fronteira definida.

A mesma evolução da tecnologia da informação que criou o ECiber e o conflito cibernético permitiu também alterações na forma de as forças armadas combaterem, criando a teoria da guerra centrada em rede. O próximo tópico apresenta esta definição.

2.2 GUERRA CENTRADA EM REDE

O conceito de Guerra Centrada em Redes (GCR) pode ser definido como sendo uma forma de atuar em combate utilizando a Tecnologia da Informação e Comunicações (TIC), para estabelecer uma arquitetura de Comando e Controle (C^2) que resulta na criação de um espaço virtual de compartilhamento da informação em todos os níveis de decisão para permitir o aumento da consciência situacional e contribuir para a obtenção da superioridade da informação independente da distância geográfica dos elementos das forças componentes (BRASIL, 2014). Este ECiber criado pelo uso da TIC para estabelecer a arquitetura de C^2 possui importância vital para a redução da incerteza da guerra e permitir o incremento indireto do poder de combate, o aumento na letalidade dos ataques, a rapidez das decisões, a precisão das armas e a correção da identificação de alvos e, ainda, a diminuição dos danos causados às forças amigas (BRASIL, 2014).

Esta forma de atuar foi desenvolvida pelos EUA para permitir que forças dispersas geograficamente atingissem um alto nível de consciência de batalha, de modo a alcançar objetivos estratégicos, operacionais e táticos, de acordo com a intenção do comandante; e está baseada em uma força conectada por redes de computadores e operando de forma conjunta e integrada (EUA, 2005).

> [...] Esta ligação entre as pessoas, plataformas, armas, sensores e auxiliares de decisão em uma única rede cria um todo que é claramente maior do que a soma de suas partes. Os resultados são as forças que operam em rede com o aumento de velocidade e de sincronização, e que são capazes de produzir efeitos, reunidas em muitas situações, sem a aglomeração física das forças necessárias no passado. Este aumento de velocidade e sincronização direta das operações impacta em todo o campo de batalha, a partir de áreas de apoio através de zonas de combate (EUA, 2005, p. ii, tradução nossa)[5].

Com a implementação da GCR, o Departamento de Defesa (DoD) dos EUA também identificou a possibilidade de exploração e o ataque das redes de computadores utilizadas nas operações centradas em rede (2005, p. 4).

> É razoável esperar que as organizações terroristas também estejam analisando as vulnerabilidades e fraquezas de nossas redes e planejando para explorá-las no futuro (2005, p. 4, tradução nossa)[6].

Para desenvolver o compartilhamento de dados entre os sistemas de informação heterogêneos empregados no apoio aos usuários nos níveis operacionais e táticos, os EUA estabeleceram padrões de interoperabilidade e arquiteturas de sistemas (EUA, 2005).

A dependência do ECiber pelas Forças Armadas cresce com o desenvolvimento dos sistemas de comando e controle e o aumento da interoperabilidade.

Esta interoperabilidade será abordada no próximo tópico.

---

[5] This linking of people, platforms, weapons, sensors, and decision aids into a single network creates a whole that is clearly greater than the sum of its parts. The results are networked forces that operate with increased speed and synchronization and are capable of achieving massed effects, in many situations, without the physical massing of forces required in the past. This increased speed and synchronization directly impacts operations across the battlespace, from support areas through combat zones. (EUA, 2005, p. ii),

[6] It is reasonable to expect that terrorist organizations are also analyzing the vulnerabilities and weaknesses of our networks and planning to exploit them in the future (2005, p. 4).

2.3 INTEROPERABILIDADE DE SISTEMAS DE TI

A interoperabilidade de sistemas de informação está relacionada com a habilidade de acessar, processar e trocar informações com outros sistemas (EUA, 1998).

Para descrever o processo de interoperabilidade entre os sistemas, o Departamento de Defesa (DoD) dos Estados Unidos publicou o documento "*Levels of Information System Interoperability*" (LISI) (EUA, 1998). Este documento foi utilizado para orientar o desenvolvimento dos sistemas de informação de modo a incrementar a interoperabilidade. O mesmo é considerado uma referência mundial e ponto de partida para o desenvolvimento de outras metodologias (STADEN, 2012).

Independente do modelo de interoperabilidade adotado, os princípios de aplicação são os mesmos para se determinar a interação entre os sistemas (STADEN, 2012). O enquadramento em níveis obedece quatro de cinco aspectos dependendo do modelo empregado (EUA,1998; STADEN, 2012):

a) existência e tipo de canal de conexão entre os sistemas (ex: inexistente, existente em baixa taxa de transmissão ou existentes em alta taxa de transmissão);

b) tipos e capacidades dos protocolos de comunicação de rede empregados (ex: permissão para comunicação unidirecional, bidirecional, em LAN, em WAN);

c) habilidade dos aplicativos empregados pelos sistemas em trocarem e compartilharem dados, corrigindo diferenças entre eles;

d) grau de facilidade dos modelos de dados empregados serem perfeitamente compreendidos pelos diferentes sistemas que o utilizarão; e

e) políticas e procedimentos técnicos estabelecidos para a troca de informação, capacidades e serviços entre sistemas.

Para esse trabalho será utilizado o modelo de interoperabilidade LISI desenvolvido pelo DoD (EUA,1998) que utiliza os níveis de interoperabilidade apresentados a seguir.

2.3.1 Níveis de interoperabilidade

A LISI define um conjunto de "níveis" cada vez mais sofisticados ou maduros em relação a interoperabilidade. Cada nível representa uma caracterização específica de vários elementos e o conjunto associado de capacidades presentes para promover a interoperabilidade (EUA, 1998).

O conceito divide a interoperabilidade entre sistemas de TI em cinco níveis distintos (EUA,1998):

a) Nível 0 – ISOLADO — abrange os sistemas isolados ou autônomos. Sem ligação eletrônica direta permitida ou disponível, onde a única interface entre esses sistemas é pelo método manual (digitação ou via mídia removível). A fusão de informações, se houver, é feito off-line pelo tomador de decisão individual por outros meios automatizados (FIG. 1).

FIGURA 1 – Nível de interoperabilidade isolado em um ambiente manual
Fonte: EUA, 1998, p. 3-3.

b) Nível 1 – CONECTADO — existe uma conexão eletrônica entre os sistemas. Este tipo de conexão em ambiente computacional é conhecida como *peer-to-peer*

(P2P)[7] em que um sistema troca informação com outro sistema via conexão física. Estes sistemas têm uma capacidade limitada, geralmente passando tipos de dados homogêneos entre os sistemas, tais como voz, e-mail de texto simples, ou arquivos gráficos fixos, como GIF ou TIFF. A comunicação é somente em um sentido de cada vez, quando a transmissão e a recepção não ocorrem simultaneamente. Os enlaces de rádio que funcionam desta maneira são considerados nível 1. (FIG. 2).

FIGURA 2 – Nível de interoperabilidade conectado em um ambiente ponto a ponto
Fonte: EUA, 1998, p. 3-4.

c) Nível 2 – FUNCIONAL — neste nível os sistemas estão interconectados por LAN e WAN[8], o que permite a troca de dados mais complexos entre os sistemas. O ambiente computacional é distribuído[9] com vários servidores ao longo da rede, permitindo que um aplicativo de um servidor troque dados com outros sistemas. Estes sistemas são geralmente *base web*[10]. Este nível permite que os tomadores de decisão sejam capazes de compartilhar informações correlacionadas entre sistemas ou funções, tal como uma imagem com uma sobreposição anotada,

[7] *Peer-to-peer* ou P2P abreviado, é um tipo de rede em que cada estação de trabalho (*peer*) tem capacidades e responsabilidades equivalentes. É diferente de arquiteturas cliente / servidor, no qual alguns computadores são dedicados a servir os outros. As redes *peer-to-peer* são geralmente mais simples, mas não oferecem o mesmo desempenho sob cargas pesadas (TIPTON, 2007, p. 3107)

[8] Local Area Network (LAN) é uma rede de computadores formada dentro de uma pequena área geográfica e a Wide Area Network (WAN) é uma rede de computadores que abrange um grande espaço geográfico. A internet pode ser considerada uma WAN (TIPTON, 2007).

[9] Ambiente distribuído é um ambiente de rede onde diferentes sistemas estão distribuídos por diferentes servidores ao longo da rede. Este ambiente permite que um aplicativo de um servidor troque ou utilize dados de outros sistemas de forma direta ou distribuída.

[10] Acesso em base web é o acesso de um sistema a dados ou a outros sistemas por meio da intranet ou internet.

documentos com hiperlink[11] e mapas em várias camadas (FIG. 3). O enlace de satélite pode operar em nível 2, porque diferente do enlace rádio este transmite e recebe simultaneamente e pode conectar LANs.

FIGURA 3 – Nível de interoperabilidade funcional em um ambiente distribuído
Fonte: EUA, 1998, p. 3-6.

d) Nível 3 – DOMÍNIO — neste nível o ambiente computacional é considerado integrado[12] no qual diferentes sistemas se integram e trabalham juntos, compartilhando um banco de dados comum na rede em que estão conectados, utilizando um modelo de dados de domínio, permitindo que vários usuários acessem os dados deste banco de dados por meio de aplicações independentes. Estes sistemas operam por meio de redes de longa distância (WAN), onde cada entidade possui um identificador global único. Este identificador permite melhorar o controle de acesso e controlar como os pacotes de informação são trocados, evitando a transmissão desnecessária. (FIG 4).

[11] Hiperlink é o recurso que permite a um documento apontar para outra parte dele mesmo ou para um documento novo. Normalmente é identificado com um sublinhado ou uma cor diferente em seu texto, onde o leitor consegue seguir facilmente para o novo conteúdo clicando no hiperlink.

[12] Ambiente de computação integrado é um ambiente de rede no qual diferentes sistemas se integram e trabalham juntos, compartilhando um banco de dados comum na rede em que estão conectados (EUA, 1998).

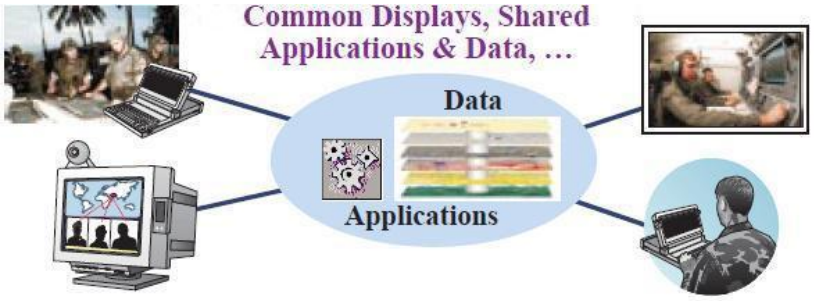


FIGURA 4 – Nível de interoperabilidade domínio em um ambiente integrado
Fonte: EUA, 1998, p. 3-6.

e) Nível 4 – CORPORATIVO — neste nível o ambiente computacional é considerado universal, compartilhando em uma rede, a mesma base de dados por meio de um modelo corporativo comum a todos os aplicativos. É o ambiente mais avançado em interoperabilidade, permitindo a colaboração de sistemas distribuídos geograficamente, criando um espaço de trabalho virtual e a computação em nuvem que utiliza recursos de computação oferecidos por sistemas em um espaço global de informações ou ECiber. A figura a seguir representa a colaboração entre a força naval, o nível político, parceiros estatais e agências, onde vários usuários podem acessar e interagir com dados complexos simultaneamente (FIG. 5).

FIGURA 5 – Nível de interoperabilidade corporativo em um ambiente universal
Fonte: EUA, 1998, p. 3-10

Em estudo realizado pelo RAND National Defense Research Institute foi apresentado que a Marinha e o Departamento de Defesa (DoD) dos EUA estão cada vez mais dependentes de redes e operações centradas em redes para realizar missões militares, resultando em um objetivo vital de estabelecer e manter redes seguras para as redes de navios (PORCHE III *et al.*, 2010).

Quanto maior for o nível de interoperabilidade, maior será o uso de TI e a capacidade de comando e controle, mas ao mesmo tempo aumenta a dependência das forças armadas dos EUA deste ECiber criado pelos sistemas de comando e controle. Esta dependência pode ser explorada por um ataque cibernético.

Para analisar a segurança dos sistemas de comando e controle em cada nível o próximo tópico abordará a segurança de uma rede de computador.

3 SEGURANÇA DE UMA REDE DE COMPUTADORES

Os autores Harold F. Tipton e Micki Krause *et al*., no *Information Security Management Handbook* (2007), definem a segurança de rede como multifacetada, envolvendo todos os níveis de uma organização.

> A segurança de Rede pode ser pensada como a provisão de acesso consistente e adequada às informações e a garantia de que a integridade e a confidencialidade de informações são mantidas, conforme apropriado. Ao contrário do que possa parecer intuitivo, a segurança de rede não é simplesmente uma solução de tecnologia. Envolve os esforços de todos os níveis de uma organização, das tecnologias e dos processos que eles usam para projetar, construir, administrar e operar uma rede segura[13] (TIPTON, 2007, p. 1739, tradução nossa).

Segundo Tipton *et al.* (2007), uma rede segura deve ser caracterizada pela existência de mecanismos para garantir que a informação esteja disponível somente para quem tem a necessidade de conhecer (confidencialidade); assegurar que os dados estejam sempre íntegros (integridade); que os recursos da rede estejam sempre disponíveis para usuários autorizados (disponibilidade); que as ações tomadas possam ser associadas a um único usuário, sistema ou rede (responsabilidade); e de controles que permitam auditoria (auditabilidade).

As redes de computadores representam ativos críticos para a organização e a avaliação do risco de perda desses ativos é uma importante responsabilidade da administração. A indústria de segurança da informação tem utilizado técnicas de análise de risco por muitos anos. Em geral, a análise de risco é usada para determinar qual a posição que uma organização deve tomar em relação ao risco de perda dos bens. A gestão de risco é definida como um processo para minimizar as perdas por meio da avaliação periódica de

[13] "Network security" can be thought of as the provision of consistent, appropriate access to information and the assurance that information confidentiality and integrity are maintained, also as appropriate. Contrary to what may seem intuitive, network security is not simply a technology solution. It involves the efforts of every level of an organization and the technologies and the processes that they use to design, build, administer, and operate a secure network (TIPTON *et al*., 2007).

riscos potenciais e aplicação sistemática de medidas corretivas. Quanto maior o valor dos ativos, maior será a perda potencial (O'HANLEY *et al.*, 2013).

As **ameaças** podem ser pessoas, tais como hackers, funcionários descontentes, programadores propensos a erros, operadores que cometem erros por descuido, quando entram com dados, ou coisas como o hardware não confiável, ou até mesmo a própria natureza, como terremotos, enchentes e relâmpagos (O'HANLEY *et al.*, 2013) . Em outras palavras, as ameaças são agentes ou ações, que podem atuar de modo espontâneo ou proposital, aproveitando das vulnerabilidades de um sistema para conseguir seu intento. A ameaça é um fator externo ao sistema.

As **vulnerabilidades** são falhas na proteção de ativos que podem ser exploradas, parcial ou totalmente, pelas ameaças, resultando em perda ou dano. A vulnerabilidade é um fator interno ao sistema e a sua existência permite a ação de ameaças externas. Para impedir ou mitigar as vulnerabilidades deve-se aplicar as salvaguardas. (O'HANLEY *et al.*, 2013).

Para exemplificar os conceitos de ameaças e vulnerabilidades, pode-se utilizar o recebimento pela organização de um e-mail com um arquivo anexo, onde este arquivo está infectado por um vírus (ameaça) que tenta explorar a ausência de um programa antivírus (vulnerabilidade) no computador do usuário. Outra situação possível é a ocorrência de picos de tensão causados por raios (ameaça) durante uma tempestade na região de um edifício sem para-raios (vulnerabilidade) que pode causar danos aos equipamentos da rede local instalados neste edifício. Nesses dois exemplos, o risco criado pela ação da ameaça em um ativo com vulnerabilidade possui um impacto (danos e perdas causados) e uma probabilidade de ocorrer. Esses riscos devem ser reduzidos pela aplicação das salvaguardas que minimizem ou eliminem as vulnerabilidades (instalação de antivírus no computador e de para-raios no edifício).

Gerenciar riscos não envolve apenas a identificação de ameaças, mas também determinar o seu impacto e a gravidade. Até que os gestores compreendam a magnitude do problema e as áreas em que as ameaças são mais prováveis de ocorrer, proteger recursos vitais continuará a ser uma proposta arbitrária e ineficaz. A complexidade dos ambientes das redes de computadores criam maiores desafios para a compreensão e a gestão de riscos (O'HANLEY *et al.*, 2013).

A análise de risco é um exercício formal, que inclui:

a) Identificar, classificar e avaliar os ativos;
b) Definir e estimar o potencial das ameaças;
c) Identificar as vulnerabilidades dos ativos em relação às ameaças; e
d) Avaliar a eficácia provável de garantias existentes e os benefícios de salvaguardas adicionais.

Para conceber e instalar uma arquitetura segura utilizando gestão de risco, Tipton *et al.* (2007) identificam que é necessário uma compreensão abrangente da arquitetura de rede. E que para proteger a rede e os ativos disponíveis sobre a mesma, um profissional de segurança deve entender claramente:

a) a natureza hierárquica dos ativos de informação que requerem proteções;
b) a estrutura da própria arquitetura da rede; e
c) o perímetro da rede (ou seja, os pontos de entrada e saída e as associações de proteção a estes pontos).

3.1 ARQUITETURAS DE REDE

De acordo com Tipton *et al.* (2007), para a compreensão das arquiteturas de rede, várias fontes podem ser utilizadas tais como diagramas de rede, entrevistas ou relatórios técnicos.

Um entendimento comum entre as instituições e para quase todos os profissionais de rede é a diferença entre o conceito de rede local e rede de longa distância[14], independentemente de serem termos antigos. A LAN, ou rede de área local, é uma rede de computadores instalados em uma pequena área geográfica, como um conjunto de salas, um prédio ou campus universitário. A WAN ou rede de longa distância é um arranjo de instalações de transmissão de dados que fornece capacidade de comunicação através de uma ampla área geográfica. Pode-se descrever com precisão a estrutura da LAN e da WAN utilizando três critérios: (1) localização – identifica-se a localização física da rede na organização por meio de desenhos ou listas e em seguida relacionam-se hierarquicamente estas localizações; (2) ligações (links) – identificam-se as ligações entre as localizações relacionadas na etapa anterior, criando uma relação com índice destas ligações. Nesta fase é importante identificar todas as ligações, tais como as ligações redundantes, para balanço de carga e linhas discadas para situação de emergência; e (3) topologias – identificam-se as topologias, que representam a relação entre os locais e as ligações, podendo ser simples ou complexas dependendo do número de ligações e locais (TIPTON *et al.*, 2007).

O mapeamento da LAN é similar ao da WAN, com as localizações dentro de edifícios que possuem equipamentos e cabos de rede.

Uma vez que a arquitetura de rede está claramente entendida, o perímetro da rede pode ser investigado e devidamente mapeado (TIPTON *et al.*, 2007).

[14] Local Area Network – LAN e Wide Area Network – WAN (TIPTON, 2007).

3.1.1 Perímetro da Rede

Após o entendimento da arquitetura das redes, a organização precisa definir o limite em que a informação deixa seu controle imediato e direto. Este limite é o perímetro da rede. Ele representa o conjunto dos pontos de entrada e saída de dados e informação da rede de uma organização (TIPTON *et al.*, 2007).

O perímetro de rede inclui conexões com provedores de serviços de Internet (ISPs), conexões de acesso remoto, redes privadas virtuais (VPNs) e conexões com outros parceiros. Estes pontos de entrada e saída de rede que muitas vezes passam sem exame e sem proteção incluem componentes de LAN e WAN, como links, salas de servidores, armários de cabeamento, portas de rede sem restrições, e até mesmo as próprias estações de trabalho (TIPTON, 2007).

Uma variação da rede local é a rede local sem fio (Wireless LANs ou WLAN) que com relação à localização pode-se existir dentro ou fora das instalações físicas da organização. As considerações sobre este tipo de rede local incluem a sua existência e a localização dos pontos de acesso individuais que irão determinar a distinção entre rede local sem fio em uso no interior do perímetro ou fora do perímetro da rede (TIPTON *et al*., 2007).

Todos os pontos de entrada e saída devem ser documentados e indexados para que o perímetro da rede possa ser avaliado e as salvaguardas apropriadas definidas para cada ponto de entrada e saída. Segundo Tipton, um equívoco comum em segurança de redes é acreditar que a proteção contra as ameaças de fora da organização é mais importante do que proteger contra ameaças vindas do interior da organização. Os dois tipos devem ser abordados para que o perímetro de rede seja seguro (TIPTON *et al.*, 2007).

3.1.2 Identificação dos Ativos que Necessitam de Proteção

O próximo passo apresentado é a identificação dos ativos que necessitam de proteção. O autor observa que a identificação inicia com a organização determinando quais são os ativos críticos para a sua atividade e a sua classificação. A classificação dos ativos, especialmente os sistemas e os dados, orientam os usuários sobre o manuseio apropriado dos bens, sendo essencial para evitar erros, tais como a divulgação inadequada de informações sensíveis. As organizações normalmente identificam os ativos por meio do processo de análise de impacto nos negócios[15] (BIA – *Business Impact Analysis*) (TIPTON *et al.*, 2007).

3.1.3 Identificação das Ameaças para os Ativos

Outro passo importante é a identificação das ameaças aos ativos da organização. Esta identificação permitirá montar uma boa defesa para os mesmos. Os principais exemplos de ameaças para a maioria dos ambientes estão relacionados no QUADRO 1 (TIPTON *et al*., 2007, p. 1748):

QUADRO 1 - Ameaça aos ativos

Ameaças aos ativos	Descrição
Malícia	As pessoas podem ser motivadas a prejudicar ativos de uma organização por raiva da gestão, dos colegas de trabalho ou da própria organização. Um tema comum entre esses indivíduos é a intenção de fazer mal à organização. Um exemplo de um ato malicioso é um administrador de rede deixar acessos a uma organização para atacar após a sua saída da mesma;

[15] Existem vários métodos para realizar uma BIA. O *Disaster Recovery Institute International* (www.drii.org) apresenta várias informações para organizações envolvidas nessa atividade.

Ganho monetário	Necessidade ou ganância também podem ser um motivador para intrusão em uma rede. Muitos exemplos de roubo de propriedade intelectual ou pessoal, como números de cartão de crédito, são vistos em todo o mundo;
Curiosidade	Os seres humanos são curiosos por natureza; muitos são igualmente inteligentes. Curiosidade pode levar uma pessoa a pôr em risco os ativos, seja intencionalmente ou acidentalmente;
Acidentes	Apesar dos melhores esforços, as pessoas cometem erros e acidentes acontecem. Apesar do fato de que eles não são intencionais, os acidentes podem causar danos aos ativos da organização e devem ser contabilizados no planejamento de segurança;
Desastres naturais	Relacionados com o tempo e emergências geográficas também devem ser considerados no planejamento de segurança. Nos EUA, os dados coletados pela *Federal Emergency Management Agency* (FEMA) são um exemplo deste tipo de ameaça.

Fonte: TIPTON *et al*. (2007, p. 1748).

3.1.3.1 Ameaças para a segurança da LAN/WAN

Segundo Steven F. Blanding (O'HANLEY *et al.*, 2013, p. 1017), uma ameaça é um risco identificado que tem alguma probabilidade de ocorrer. E estas ameaças são agrupadas em três grandes áreas: ameaças de pessoas, ameaças de vírus e ameaças físicas. As LANs e WANs são particularmente suscetíveis às ameaças de pessoas e relacionadas a vírus por causa do grande número de pessoas que têm direitos de acesso.

A maior ameaça para LANs e WANs são pessoas e essa ameaça ocorre principalmente dentro da organização, onde os empregados comentem erros e omissões, estão descontentes ou são desonestos. No QUADRO 2 são relacionadas algumas ameaças de pessoas (O'HANLEY *et al.*, 2013):

QUADRO 2 - Ameaça de Pessoas

Ameaças de Pessoas	Descrição
Erro na administração do sistema	Inclui todos os erros humanos que ocorrem na instalação, administração e operação dos sistemas de rede local, que vão desde a falta de habilitar adequadamente os controles de acesso e outros recursos de segurança até a falta de backups adequados. As possíveis consequências incluem a perda da confidencialidade, integridade e disponibilidade do sistema, bem como os possíveis constrangimentos para a empresa ou indivíduo.
Erro do operador de computador	Inclui todos os erros humanos que ocorrem na operação de sistemas de computador e LAN, incluindo o uso indevido de log-on e senhas, exclusão acidental de arquivos e backups inadequados. Possíveis consequências incluem violações de privacidade de dados e perda de capacidades, tais como a exclusão acidental de programas críticos ou dados.
Erro de programação/software	Incluem todos os erros, problemas de incompatibilidade e problemas relacionados que ocorrem no desenvolvimento, instalação e manutenção de software em uma LAN. Possíveis consequências incluem a degradação, interrupção ou perda de capacidade da LAN.
Divulgação não autorizada	Qualquer liberação de informações confidenciais na rede local que não é sancionado pela autoridade competente, incluindo aqueles causados por descuido e liberação acidental. Possíveis consequências são violações da lei e da política, limitar os direitos dos indivíduos, constrangimento para os indivíduos e para a empresa e perda de confiança dos acionistas na empresa.
Uso não autorizado	Emprego dos recursos da empresa para fins não autorizados pela empresa e o uso de recursos não adquiridos pela empresa na rede, como o uso de software de propriedade pessoal no escritório. Possíveis consequências incluem a introdução de vírus e violações de direitos autorais para o uso de software não licenciado.

Fraude/estelionato	Supressão ilegal de ativos registrados da empresa por meio da manipulação enganosa dos controles internos, arquivos e dados, muitas vezes por meio do uso de uma LAN. Possíveis consequências incluem a perda monetária e pagamentos ilegais a terceiros.
Modificação de dados	Qualquer mudança não autorizada de dados, que podem ser motivadas por coisas tais como ganho pessoal, o favoritismo, um sentido equivocado de dever, ou uma intenção maliciosa de sabotagem. Possíveis consequências incluem a perda de integridade dos dados e a tomada de decisão potencialmente falha. O maior risco é o funcionário insatisfeito.
Alteração do software	Qualquer alteração não autorizada de software, que pode ser motivado por coisas como descontentamento, ganho pessoal, ou um senso equivocado de dever. Possíveis consequências incluem todos os tipos de erros de processamento e perda de qualidade de produtos de saída.
Roubo de bens de informática	Inclui a remoção não autorizada/ilegal de dados, hardware ou software a partir das instalações da empresa. Possíveis consequências para a perda de hardware podem incluir a perda de importantes dados e programas residentes em disco rígido ou em mídias removíveis.

Fonte: O'HANLEY *et al.* (2013, p. 1017-1019).

As ameaças de vírus de computador são o exemplo mais amplamente reconhecido de uma classe de programas escritos para causar algum tipo de perturbação intencional ou danos aos sistemas de computadores ou redes. Um vírus de computador executa duas funções básicas: ele se copia junto a outros programas, infectando-os e executa as suas instruções. Um programa infectado com um vírus, dependendo das instruções, pode causar danos imediatamente após a sua execução, ou pode esperar até que um determinado evento ocorra, como uma hora ou uma data especial. O dano pode variar amplamente e pode ser tão extenso que exija a reconstrução completa de todos os dados e programas de um sistema. Como os vírus podem se espalhar rapidamente para outros programas e sistemas, o dano pode ser multiplicado geometricamente (O'HANLEY *et al.*, 2013).

As ameaças de vírus ainda incluem outras formas de programas destrutivos, como cavalos de Tróia e vermes (*worms*) de rede. Coletivamente, eles são conhecidos como programas maliciosos. Estes programas na maioria das vezes são escritos para se mascarar como programas úteis, de modo que os usuários são induzidos a copiá-los e compartilhá-los com seus amigos. O fenômeno do programa malicioso é, fundamentalmente, um problema associado a pessoas, pois é frequentemente, transmitido por indivíduos que usam os sistemas de forma não autorizada. Assim, a ameaça de uso não autorizado, por usuários não autorizados e autorizados, deve ser tratada como parte da prevenção de vírus (O'HANLEY *et al.*, 2013).

As ameaças físicas mais frequentes para as LANs estão relacionadas com problemas de energia elétrica, mas o fogo ou danos causados pela água são os mais graves. No QUADRO 3 são relacionadas algumas ameaças físicas (O'HANLEY *et al.*, 2013):

QUADRO 3 - Ameaças Físicas

Ameaças Físicas	Descrição
Quedas/distúrbios de energia	Qualquer interrupção ou perturbação na continuidade da energia elétrica da LAN que seja suficiente para causar interrupção operacional, desde picos de alta-tensão a quedas de energia ("brownouts"). As possíveis consequências variam de perda da entrada de dados ao desligamento temporário de sistemas.
Falha de hardware	Qualquer falha de componentes de rede local (particularmente falhas de disco rígido). As possíveis consequências incluem a perda de dados ou de integridade dos dados, perda de tempo de processamento e interrupção de serviços, e também pode incluir a degradação ou perda de capacidades do software.
Danos causados pelo fogo/água	Inclui a destruição do edifício inteiro, destruição parcial dentro de uma área de escritório, fogo na sala dos ativos da LAN e danos causados pela água do sistema de incêndio e/ou pela fumaça. As possíveis consequências incluem a perda de todo o sistema, por longo período de tempo.
Outras ameaças físicas	Incluem acidentes ou falhas ambientais envolvendo ar condicionado, umidade, aquecimento, vazamento de líquido, explosão e contaminação; ameaças de acesso físico que

	incluem sabotagem, terrorismo, tumulto, distúrbios civis, ameaça de bomba e vandalismo; e desastres naturais que incluem inundação, terremoto, furacão, neve, tempestade de gelo, vendaval, furacão e relâmpagos.

Fonte: O'HANLEY *et al.* (2013, p. 1017-1019).

3.1.4 Vulnerabilidades

As falhas na proteção de ativos que podem ser exploradas, parcial ou totalmente, por meio das ameaças, resultando em perda são conhecidas por vulnerabilidades (O'HANLEY *et al*., 2013).

As LAN/WAN foram desenvolvidas para fornecer aos usuários designados acesso compartilhado a hardware, software e dados, onde a maior a vulnerabilidade da rede local é o controle de acesso. O controle de acesso possui áreas de vulnerabilidade que incluem o computador pessoal, as senhas, o servidor de rede e os equipamentos de conectividade (O'HANLEY *et al*., 2013).

Apenas algumas vulnerabilidades genéricas serão destacadas no QUADRO 4, uma vez que as vulnerabilidades dos ativos são pontos fracos específicos de determinado ambiente de LAN /WAN, identificados na avaliação do ambiente e que devem ser corrigidas sempre que forem descobertas.

QUADRO 4 - Vulnerabilidades genéricas

Vulnerabilidades	Descrição
Computador pessoal	A redução das vulnerabilidades depende da conscientização do usuário e o seu treinamento para garantir um grau mínimo de proteção. Áreas vulneráveis de PC incluem: **Controle de acesso -** Faltam mecanismos internos de hardware que forneçam aos usuários funções de sistemas relacionados com a segurança. Sem esses recursos de hardware (por exemplo, proteção

	de memória), é praticamente impossível evitar que os programas do usuário acessem ou modifiquem partes do sistema operacional e contornando assim todos os mecanismos de segurança pretendidos. **Unidade de mídia removível** - Permite introdução de software não autorizado (incluindo vírus) e a remoção não autorizada de dados sigilosos. Este problema é grave em certos ambientes de dados sensíveis, e indústria de computadores tem respondido com estações de trabalho sem disco, projetadas especificamente para operações em LAN. **Disco rígido** - A maioria dos computadores atuais têm discos rígidos de grande capacidade de armazenamento online. Os dados sensíveis que residem nesses discos rígidos são vulneráveis a roubo, modificação ou destruição. **Reparos** - deve ser dada a devida atenção para a reparação e a alienação de equipamentos para evitar roubo ou perda de dados.
Vírus	PCs são especialmente vulneráveis a vírus e softwares maliciosos relacionados, tais como cavalos de Tróia[16], bombas lógicas e *worms*[17]. O mais importante é determinar a origem do vírus e da vulnerabilidade e instituir salvaguardas apropriadas do sistema.
Acesso à LAN	**Controle de Acesso**. A senha do sistema é o método mais básico e amplamente utilizado para controlar o acesso às redes de computadores e também é o mais fraco do ponto de vista humano. **Acesso discado**. O acesso telefônico discado via modems fornece uma janela única para LANs e WANs, permitindo que qualquer pessoa com um ID de usuário, senha e um computador entre no sistema. Hackers são conhecidos por utilizar recursos discados para o acesso.
Conectividade (Internetworking)	Internetworking é a conexão do servidor de rede local com outros servidores de LAN / WAN através de vários dispositivos de conexão, que consistem de roteadores e gateways. Cada interligação adicional de LAN/WAN pode adicionar usuários externos e aumentar os riscos para o sistema.

Fonte: O'HANLEY *et al.* (2013, p. 1017-1019).

As vulnerabilidades são corrigidas pelas salvaguardas, onde a mais importante e básica delas continua sendo a conscientização da segurança e os treinamentos adequados (O'HANLEY *et al.*, 2013).

[16] Cavalo de Troia (*Trojan Horse*) é um virus que aparenta ser um programa de computador útil, mas que permite acesso não autorizado ao computador (O'HANLEY *et al*., 2013).

[17] *Worm* (verme) é um tipo especial de vírus que não se junta a programas existentes, ele se autorreplica e se espalha pela rede usando algum recuso disponível no computador, onde a forma mais comum de propagação é pelo email (O'HANLEY *et al.*, 2013).

3.1.5 Identificação das Contramedidas para as Ameaças

Após a identificação das ameaças para a organização, Tipton *et al.* (2007) apresentam que o próximo passo é projetar e implementar as contramedidas adequadas para neutralizar ou minimizar as ameaças identificadas, observando que algumas ameaças representam um perigo maior do que outras e que as ameaças possuem diferentes probabilidades de ocorrer.

3.1.6 Avaliação do Ambiente

A avaliação de segurança é normalmente feita por meio da "caça" e da "coleta" . A “caça” refere-se à inspeção da tecnologia de modo intrusiva que pode ser feita utilizando tanto ferramentas de software *commercial-off-the-shelf* [18] (COTS), como de código aberto. E a "coleta", refere-se à coleta de dados obtida por meio de da revisão de avaliações anteriores, políticas e procedimentos existentes, visitas a locais da organização, entrevistas do pessoal da organização e demonstrações de sistemas realizados por pessoal apropriado (TIPTON *et al.*, 2007).

Os métodos de avaliação não intrusiva são muito úteis na coleta de dados sobre pessoas, processos e instalações, enquanto os métodos de avaliação intrusiva são classificados geralmente em duas categorias: (1) verificação de vulnerabilidades e (2) ataque de penetração, sendo úteis para construir uma imagem da rede, servidores e estações de trabalho semelhante à imagem que um atacante externo poderia encontrar (TIPTON *et al.*, 2007).

[18] Software comercial, com código fonte não disponível e com versões periódicas. Souza, F.M., Alencar, F.M.R., Castro, J.F.B. “O Impacto dos COTS no processo de engenharia de requisitos”, UFPE Universidade Federal de Pernambuco. 1999.

As avaliações de segurança não intrusivas são consideradas muito importantes para verificar a saúde da rede, devido ao fato de que a segurança da rede é conduzida por pessoas, processos, tecnologia e instalações. Esta avaliação fornece um instantâneo da situação atual da organização e possui os seguintes métodos apresentados no QUADRO 5 (TIPTON *et al.*, 2007):

QUADRO 5 - Métodos não intrusivos

Método não intrusivo	Descrição
Revisões de documentos	Realizadas para fornecer informações de base para a avaliação de segurança;
Entrevistas	Entrevista com representantes de cada setor da organização de acordo com o escopo da avaliação;
Demonstrações do sistema	Demonstrações conduzidas pelas pessoas que foram entrevistadas para verificar as informações obtidas durante as entrevistas;
Visitas aos locais	Avaliar a segurança física das instalações;
Análise de impacto nos negócios	Determinar como a perda de um determinado ativo ou conjunto de ativos impactam na organização. Este método também avalia as ameaças aos ativos e tem como fatores importantes para o sucesso do método o inventário e a classificação dos ativos da organização;
Avaliação de risco ou análise de risco	Método que utiliza métricas para verificar a exposição no ambiente e a sua probabilidade de ocorrer;
Auditoria	Verifica o cumprimento das normas de segurança pela organização.

Fonte: TIPTON *et al.* (2007, p. 4574-4575).

Em conjunto com a “coleta”, os métodos intrusivos são utilizados para fornecer uma visão mais completa dos riscos da organização. A seguir será apresentado alguns destes métodos intrusivos no QUADRO 6 (TIPTON *et al.*, 2007):

QUADRO 6 - Métodos intrusivos

Método intrusivo	Descrição
Reconhecimento (footprinting) e enumeração	Este método procura em sítios Web, listas de discussão, salas de chat ou outros recursos da web a existência de informações públicas com conteúdo sensível sobre a organização obtida de maneira ilícita ou postada pela equipe como resposta a algum questionamento à organização. A importância desta busca é que a informação sensível possa dar a um atacante uma vantagem sobre a organização.
Engenharia Social	Atividade que testa diretamente os processos de uma organização e sua conscientização de segurança. Os engenheiros sociais tentam obter acesso às informações sensíveis ou às instalações de acesso restrito por meio de distração, desorientação, representação, ou de outros meios. Esta atividade é surpreendentemente eficaz. O teste verifica a possibilidade de obtenção de informações sensíveis por meio de funcionários ingênuos, de informações encontradas no lixo (*dumpster diving*) ou de observação direta (*shoulder surfing*) de modo a obter acesso a um recurso da organização. Uma técnica de engenharia social comum é a aquisição do número telefônico de uma organização e chamar o *help desk* se passando por um gerente ou um empregado e exigir que a senha do alvo seja alterada para uma simples palavra ou frase. Esta técnica funciona especialmente quando os turnos estão terminando. Outros métodos, mais imaginativos podem empregar engenheiros sociais disfarçados como entregadores de materiais ou como funcionário da organização.
Quebra de senha	Verifica a construção e a manutenção das senhas de uma organização. Embora muitas organizações orientem os funcionários sobre a construção e manutenção de senhas, algumas não fazem. Por meio de ferramentas de software é possível "quebrar" ou descobrir as senhas. Estas ferramentas realizam várias tentativas para forçar a descoberta de senhas usadas no ambiente. Este método é chamado de "força bruta". A maioria das senhas de uma organização podem ser descobertas em um período muito curto de tempo.
Mapeamento de rede	Técnica usada para "desenhar" a arquitetura de rede atual. Esse "mapa" é usado pelo avaliador e pelos administradores de rede para verificar os dispositivos que são capazes de acessar os recursos da organização. Quando é encontrado algum dispositivo na rede desconhecido, ou não aprovado pela organização, este pode pertencer a um atacante e, como tal, deve ser desligado da arquitetura em conformidade com o plano de resposta a incidentes de segurança da organização.
Varredura de	A varredura busca vulnerabilidades técnicas específicas. O alvo pode ser uma estação de trabalho, equipamentos de rede (switch, roteador,

vulnerabilidade	firewall), servidor ou um intervalo inteiro de rede. As informações obtidas pelo scanner podem ser bastante extensas e representam informações específicas sobre o(s) alvo(s), tais como os endereços de rede e físicos (IP e MAC[19]), o sistema operacional e versão, e uma lista de vulnerabilidades técnicas encontradas no alvo. Os dados obtidos pela varredura de vulnerabilidades não devem ser avaliados de forma isolada. Varreduras de vulnerabilidades frequentemente revelam informações que necessitam mais investigação para serem entendidas e confirmadas. Acima de tudo, varredura de vulnerabilidades não deve ser considerada uma substituta para a conscientização de segurança.
Ataque e Penetração	Exploração de uma vulnerabilidade específica, ou um conjunto de vulnerabilidades, identificadas pela varredura de vulnerabilidades, para determinar o impacto que a exploração bem-sucedida teria. Este método pode ter um objetivo específico, como, por exemplo, um determinado arquivo ou uma informação, ou pode ser mais geral. Em um exemplo hipotético, a penetração bem-sucedida de um *firewall* pode permitir o acesso a um determinado serviço interno ou a um diretório em um servidor. Este acesso ao diretório pode permitir a instalação de um programa *keystroke logger* que registra o que é digitado no teclado e permite obter os nomes de contas e suas senhas para serem utilizadas pelo atacante no futuro.
War dialing e *War driving*	*War dialing* usa programas para verificar grandes blocos de números de telefone para localizar modems em computadores ou em outros dispositivos para serem explorados. Para acelerar essa busca pode-se usar programas comerciais que operam vários modems de cada vez e verificam grandes blocos de números de telefone em pouco tempo. *War driving* usa programas comerciais ou de código aberto instalados em um computador com um modem e antena externa para detectar redes locais sem fio em uma região, determinando suas características e obter acesso à rede.

Fonte: TIPTON *et al.* (2007, p. 4576-4578).

3.1.7 Remediar

Quando as atividades de avaliação são concluídas e os dados analisados para determinar onde a organização está exposta, esses riscos são então priorizados para que

[19] Endereço MAC, endereço de hardware ou endereço físico. É o endereço padronizado da camada de enlace de dados associado a cada placa de rede, necessário para cada porta ou dispositivo que se conecta a uma LAN. Os endereços MAC possuem 6 bytes de comprimento e são controlados pelo IEEE.

possam ser adequadamente tratados. O tratamento e a correção dos riscos em um ambiente são chamados de remediação. Essas correções são normalmente atividades que resultam em uma solução que pode ser uma política, um procedimento, uma correção técnica ou de atualização da instalação que aborda a questão criada pelo risco identificando de forma satisfatória (TIPTON *et al.*, 2007).

Como qualquer iniciativa organizacional, a correção deve ser cuidadosamente planejada antes da sua execução, para ser bem-sucedida. Os resultados da avaliação não intrusiva e intrusiva devem ser cuidadosamente revistos; os riscos devem ser priorizados por nível de gravidade. Essa priorização diz à organização, de maneira séria, como ela será afetada se uma vulnerabilidade exposta for explorada com êxito. Uma organização pode optar por corrigir todos os seus riscos de gravidade "alta" como medida de precaução, ou pode corrigir as vulnerabilidades pelos resultados. Uma boa regra é nunca corrigir alguma coisa onde o custo da correção é maior do que deixá-la sem correção. Por exemplo, se uma organização perde dez centavos em uma transação particular, que custa vinte dólares para ser reparada, o valor seria muito elevado para realizar a remediação da exposição. Uma exceção seria qualquer exposição que resulte em ferimentos ou perda de vida; estes riscos devem sempre ser corrigidos. E finalmente, se há uma exposição que custa pouco ou nada para corrigir, deve-se fazê-la mesmo que ela tenha uma prioridade mais baixa (TIPTON *et al.*, 2007).

As atividades de remediação para as organizações variam, mas podem incluir segundo Tipton *et al.* (2007):

a) recomendação de modelos para servir como base de uma política de segurança corporativa;

b) recomendação para a criação de procedimentos de segurança de destino adequados;

c) revisão dos planos de continuidade de negócios de uma organização, de catástrofes ou

de resposta a incidentes;

d) revisão e implementação das arquiteturas e das tecnologias da organização do ponto de vista da segurança;

e) identificação de um escopo adequado de responsabilidades e nível de habilidade para os profissionais de segurança;

f) prestação de consultoria em estratégia de segurança no nível executivo em curso;

g) alto nível de identificação no processo educacional e na formação contínua necessária para apoiar o programa de implementação de segurança da organização; e

h) outras atividades de remediação perseguida pela organização para atingir os seus objetivos de negócios, de regulamentação e tecnologia.

3.2 VULNERABILIDADES CIBERNÉTICAS

Ações hostis contra um sistema de informação ou de rede podem assumir duas formas: ataque cibernético e exploração cibernética. Um ataque cibernético é o uso de ações deliberadas para alterar, interromper, enganar, degradar ou destruir sistemas de TI adversários, redes ou as informações que transitam nestes sistemas. E a exploração cibernética é a utilização de ações para obter informação a respeito dos sistemas TI de interesse, normalmente de maneira clandestina, conduzida com a menor intervenção possível que ainda permita a extração da informação pretendida (SCHREIER, 2014).

Os ataques cibernéticos e as explorações cibernéticas só são possíveis porque os sistemas de TI e de redes são vulneráveis. A maioria das vulnerabilidades existentes são

introduzidas acidentalmente na implementação do projeto (LIBICKI, 2009) conforme o QUADRO 7.

QUADRO 7 - Fontes de falhas

Vulnerabilidades	Descrição
Software	Aplicativos ou programas de sistema podem ter acidentalmente ou deliberadamente falhas introduzidas cuja utilização pode subverter a finalidade para o qual o programa foi projetado.
Hardware	As vulnerabilidades podem ser encontradas no hardware, incluindo microprocessadores, microcontroladores, placas de circuitos, fontes de alimentação, periféricos (impressoras e *scanners)*, dispositivos de armazenamento e equipamentos de comunicação, tais como placas de rede. A adulteração de tais componentes pode secretamente alterar a funcionalidade pretendida do componente ou fornecer oportunidades para introduzir *malware*.
Na linha entre *hardware* e *software*	Um exemplo de uma tal linha pode ser a memória só de leitura de um computador reprogramável (*firmware*) que pode ser de forma abusiva e clandestinamente reprogramado.
Canais de comunicações	Os canais de comunicação entre um sistema ou rede e o mundo "de fora" pode ser usado por um adversário de muitas maneiras. Um adversário pode fingir ser um usuário autorizado do canal, bloqueá-lo, e, portanto, negar a sua utilidade para o seu adversário, ou espionar o canal para obter informações sigilosas do seu adversário.
Configurações	A maioria dos sistemas oferece uma variedade de opções de configuração que os usuários podem definir com base em suas próprias vantagens e desvantagens entre segurança e conveniência. Porque conveniência muitas vezes é mais valorizada do que a segurança, muitos sistemas são - na prática - configurados de forma insegura.
Usuários e operadores	Usuários e operadores autorizados de um sistema ou rede podem ser enganados ou chantageados de modo a cumprir uma ordem de um adversário, ou vender seus serviços.
Provedores de serviço	Muitas instalações de computadores dependem de terceiros para prestar serviços relacionados com a informática, como manutenção ou serviço de Internet. Um adversário pode ser capaz de convencer um provedor de serviços para tomar alguma ação especial em seu nome, como a instalação de software ataque em um computador de destino.

Fonte: SCHREIER (2014).

O ataque cibernético e a exploração cibernética necessitam da existência de vulnerabilidade, acesso à vulnerabilidade, e uma carga útil[20] a ser executada. A diferença técnica principal entre ataque cibernético e a exploração cibernética é da natureza da carga a ser executada. A carga de ataque cibernético é destrutiva ao passo que uma carga de exploração cibernética adquire dados ou informações de forma não destrutiva.

A seguir são apresentados os métodos e as categorias de um ataque cibernético (SCHREIER, 2014):

QUADRO 8 - Métodos e categoria de ataque cibernético

Ataques	Descrição
Ataque de negação de serviço (Denial-of-Service)	
Inundação (*flooding*)	Envio de dados irrelevantes ou respostas para bloquear um serviço
Inundação de conexão (*Synchronize*/*reset flooding*)	Exploração da limitação no protocolo IP para um bloco de conexões
Smurfing	Usando o sistema de divulgação IP e a falsificação de IP (IP *spoofing*) para multiplicar o ataque de inundação
Exploração de protocolo	Exploração de vulnerabilidades da implementação do protocolo IP
Nuking	Usa mensagens para reiniciar as conexões ativas
Negação de serviço especifica	Geração de solicitações que bloqueiam um serviço específico
	Ataque de programas maliciosos
Backdoor	Programa que permite execução remota de comandos em um computador
Verme (*worm*)	Programa autorreplicante que invade o computador. É projetado para tomar ações maliciosas após infestar um sistema.
Vírus	Código que "infecta" pela alteração de arquivos e causa danos e destruição de dados no computador.
Cavalo de Troia (*Trojan*)	Programa malicioso dentro de outro programa que permite o acesso ao computador onde o arquivo se encontra.

[20] A carga útil (*payload*) é o termo para descrever as coisas que podem ser feitas quando uma vulnerabilidade é explorada. Por exemplo, um código, como um vírus, que entrou em um sistema TI, que pode ser programado para fazer muitas coisas como reproduzir, se retransmitir e destruir ou alterar arquivos no sistema. As cargas úteis (*payloads*) podem ter múltiplas capacidades programáveis (SCHREIER, 2014, tradução nossa).

Permissão de acesso	Explora a leitura ou a escrita de sistemas de arquivos
Força Bruta	Usa senhas fracas ou fáceis para conseguir acesso ao sistema.
Overflow	Transbordamento de dados ou estouro de *buffer*. Escreve códigos arbitrários para causar falha na memória e ganhar acesso ao sistema.
	Manipulação do pacote IP
Port spoofing	Usando as portas de origem comumente utilizados (pontos de entrada) para evitar as regras de filtragem
Tiny fragments	Usando pequenos pacotes para ignorar a verificação do *firewall*
Blind IP *spoofing*	Alterar origem do IP para acessar os serviços de senha sem senha
Name-server ID "*snoofing*"	*Spoofing* cego com cálculo falso de número ID server-caches
Sequence-number guessing	Calcular a seqüência TCP / número *acknowledge* para falsificar um host confiável
Remote-session hijacking	Usando spoofing para interceptar e redirecionar as conexões
	Ataque de invasão
Backdoor daemons	Porta aberta para acesso futuro
Log manipulation	Remoção de traços de um ataque e acesso não autorizado
Cloaking	Substitui o sistema de arquivo para esconder um acesso não autorizado
Sniffing	Monitora a rede para encontrar dados sensíveis (Ex.: senhas)
Nonblind spoofing	Monitora a rede para roubar conexões ativas ou esquecidas

Fonte: SCHREIER (2014).

Neste capítulo foram apresentados os aspectos da segurança de uma rede, a forma de avaliar esta segurança e os principais métodos de ataque cibernético para permitir o correlacionamento com as características de cada nível de interoperabilidade.

A FIG. 6 apresenta um resumo do capítulo e a FIG. 7 apresenta como atuar sobre as ameaças, as vulnerabilidades, os ataques e os impactos a fim de reduzir o risco e diminuir o impacto.

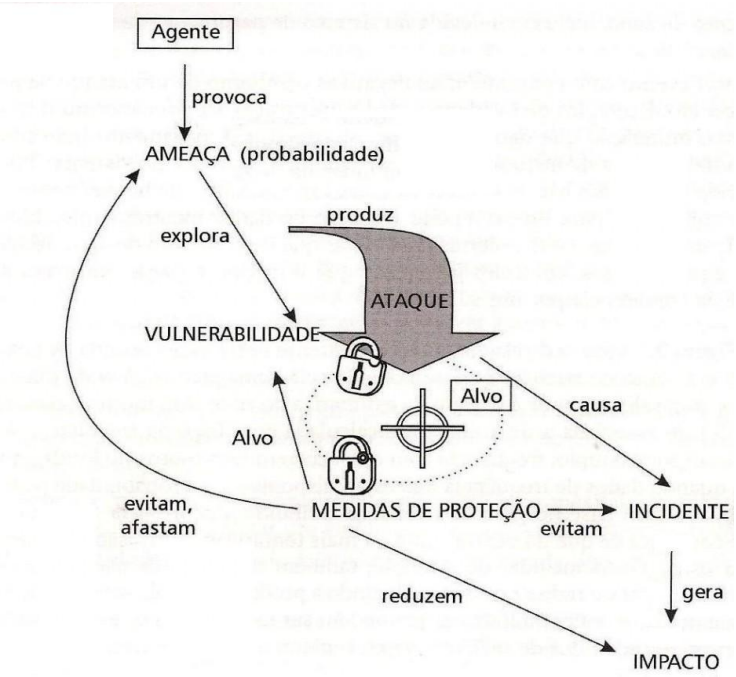
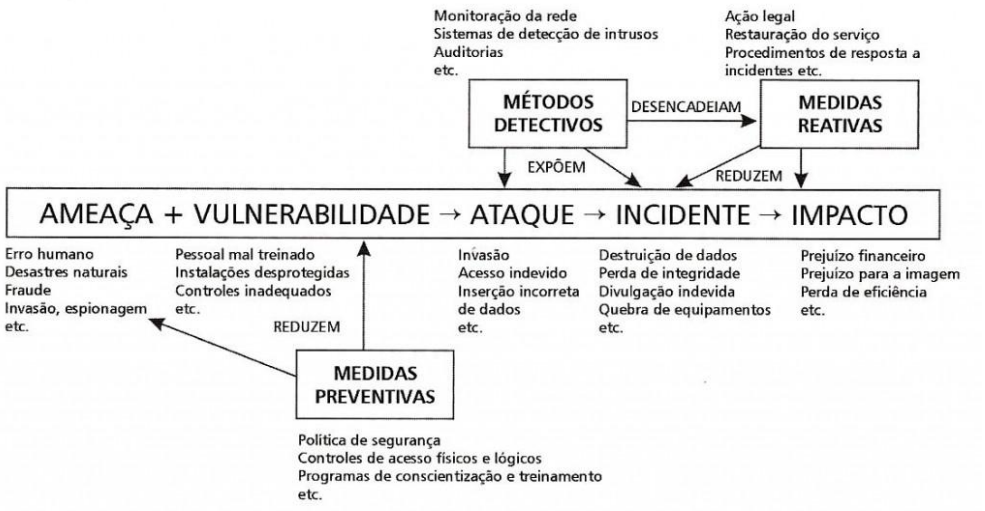


FIGURA 6 - Relacionamentos na segurança de uma rede
Fonte: http://analistati.com/gestao-de-riscos-em-ambientes-seguros/



Componentes do risco e medidas de proteção usadas para reduzi-lo.

FIGURA 7 - Medidas para reduzir o risco
Fonte: http://analistati.com/gestao-de-riscos-em-ambientes-seguros/

4 SISTEMAS DE TI EM UMA FORÇA NAVAL

Neste capítulo, será analisado como uma força naval utilizando sistemas de TI em cada um dos cinco níveis de interoperabilidade (isolado, conectado, funcional, domínio e corporativo) pode realizar a defesa cibernética.

4.1 FORÇA NAVAL COM SISTEMAS NO NÍVEL ISOLADO

Como foi apresentado no capítulo 2, no nível 0 os sistemas de TI se caracterizam por não estarem conectados diretamente e a troca de informação é realizada pelo usuário.

A **arquitetura da rede** não é formada por ligação eletrônica e a **topologia** pode ser entendida como sendo um "ponto a ponto" manual onde o usuário realiza a conexão entre os sistemas.

O **perímetro da rede**, definido pelas entradas e saídas dos sistemas, é composto pelo acesso do usuário aos sistemas por meio da visualização das informações, por mídias removíveis ("*pen drive*", "*hard disk"* portáteis) ou impressão dos dados e das informações.

Como exemplo de sistemas neste nível temos os sistemas de inteligência.

Ao ser avaliado, o ambiente foi identificado que o **ativo** a ser protegido é o computador que executa o sistema e as **vulnerabilidades** existentes são o controle de acesso ao ativo, o controle da manutenção e da utilização do sistema e o usuário.

Utilizando os principais exemplos de **ameaças** para a maioria dos ambientes apresentados no item 3.1.3 (malícia, ganho monetário, curiosidade, acidentes e desastres naturais), verificamos que no caso destes sistemas de TI onde a conexão é realizada pelo usuário, os controles sobre as pessoas, que realizam a manutenção e operam os sistemas e os

controles das alterações realizadas, são necessários para proteger os sistemas. Assim, a defesa cibernética da força naval utilizando sistemas no nível 0 depende de:

a) controlar o acesso físico aos equipamentos que contém os sistemas TI identificados;
b) controlar o acesso do usuário ao sistema, de modo a garantir que somente terá acesso quem tem a necessidade de conhecer;
c) controlar a entrada de dados externos (injeções manuais, "pen drives", atualizações do programa); e
d) ter o registro (*log*) das alterações e atualizações do sistema, dos dados e das informações que entraram e saíram dos sistemas.
e) controlar a transferência dos dados e das informações de um sistema para outro para impedir o acesso não autorizado.

4.2 FORÇA NAVAL COM SISTEMAS NO NÍVEL CONECTADO

No nível 1, já existe uma conexão eletrônica *peer-to-peer* entre os sistemas de TI que permite a troca de dados em formato simples e predefinido.

O exemplo de sistema neste nível é o sistema de controle tático enviando mensagens curtas via barramento de dados para o sistema de controle de armas ou enviando mensagens via link de dados táticos, quando a conexão é realizada por meio de rádio enlace.

A arquitetura da rede é formada por computadores conectados diretamente por cabo ou por rádio enlace. A localização da rede está dentro e fora, no caso do enlace rádio, de cada plataforma da força naval que utiliza estes sistemas e a topologia da rede é do tipo barramento internamente e *peer-to-peer* para o rádio enlace criado pelo link de dados táticos.

Os ativos identificados que necessitam de proteção são os computadores que possuem o sistema de TI, as suas conexões físicas e o rádio.

O perímetro da rede, que é definido pelos pontos de entrada e saída de dados e informação da rede, são as entradas e saídas dos computadores conectados diretamente e o link de dados.

As ameaças ou riscos identificados com probabilidade de ocorrerem, para a segurança do sistema em nível 1 de interoperabilidade com ligação física e link de dados, de acordo com o item 3.1.3.1, incluem as ameaças de pessoas, de vírus e físicas. Após o levantamento da arquitetura da rede foram relacionadas as seguintes ameaças listadas no QUADRO 9.

QUADRO 9 - Ameaças para os sistemas do nível 1

Ameaças	Descrição
Pessoas	Erros de programação, do operador do computador e na administração do sistema. Modificação de dados Alteração do programa
Vírus	A ameaça de vírus transferidos por mídia removível
Físicas	Interferência do enlace rádio Falha de hardware Distúrbios de energia Danos causados pelo fogo e pela água Falha do ar condicionado Umidade Sabotagem

Fonte: Autor.

As vulnerabilidades dos ativos ou falhas que podem ser exploradas por meio das ameaças para causar dano, aplicáveis ao sistema de nível 1, são associadas aos ativos e às pessoas que operam e realizam a manutenção do sistema que incluem o controle de acesso, as unidades removíveis, disco rígido, reparos e alienação; vírus e *malware* (QUADRO 4).

No QUADRO 10 são relacionadas as vulnerabilidades possíveis de serem encontradas no sistema de nível 1, pois se trata de um modelo teórico. Em um ambiente real

deve-se executar a avaliação de segurança pela “caça” e a “coleta” como descrito no item 3.1.6 utilizando métodos intrusivos e não intrusivos para levantar as vulnerabilidades dos ativos.

QUADRO 10 - Vulnerabilidades para os sistemas do nível 1

Vulnerabilidades	Descrição
Controle de acesso	Acesso aos dados transmitidos pelo link Acesso aos compartimentos dos ativos. Acesso por terceiros para reparo
Programação do sistema	Permite o que ocorram erros durante a operação
Componentes do sistema	Mau funcionamento devido à falha dos componentes (unidades removíveis, disco rígido, reparos e alienação). Interferência, bloqueio do link de dados.
Programa malicioso e vírus	Exploração de erros do sistema.

Fonte: Autor.

Para reduzir o risco produzido pelas ameaças explorando as vulnerabilidades, corrigem-se as vulnerabilidades encontradas durante a avaliação de segurança.

Alguns exemplos de correções seriam: codificar os dados transmitidos pelo link de dados; estabelecer o controle dos compartimentos dos ativos; reparos dos equipamentos somente por empresas certificadas; encaminhar relatórios de falhas ao setor responsável pela manutenção; acompanhar as avarias e buscar a causa; monitorar o espectro eletromagnético para localizar a fonte de interferência; estabelecer controle de emprego de mídias removíveis.

4.3 FORÇA NAVAL COM SISTEMAS NO NÍVEL FUNCIONAL.

No nível 2, os sistemas estão interconectados por uma rede local (LAN) utilizando o protocolo TCP/IP, o que permite a troca de dados mais complexos. Os sistemas

disponibilizam as informações em páginas *web* utilizando protocolos: HTTP (*Hypertext Transfer Protocol*) e NITF (*National Imagery Transmission Format*).

O exemplo de sistema neste nível é o sistema de controle tático enviando mensagens via rede de local para o sistema de controle de armas ou utilizando um link rádio conectado à rede local para trocar informações com outras plataformas.

A arquitetura da rede do nível 2 é formada por computadores conectados pela LAN e a topologia da rede é do tipo *full mesh* (transmitir e receber de qualquer nó da rede sem um controle central).

O perímetro da rede é definido pelas entradas e saídas dos vários computadores que fazem parte da rede e enlace satélite.

Os ativos identificados que necessitam de proteção são os computadores que fazem parte da rede, os sistemas e aplicativos, e os equipamentos de conectividade e as conexões e o enlace satélite.

As ameaças aos ativos identificados dos sistemas em nível 2 de interoperabilidade, continuam ser as ameaças de pessoas, de vírus e as ameaças físicas (QUADRO 11):

QUADRO 11 - Ameaças para os sistemas do nível 2

Ameaças	Descrição
Pessoas	Erros de programação de cada sistema que opere na LAN, Erros dos operadores dos computadores e Erros na administração dos sistemas. Modificação de dados dos vários sistemas que operam na rede Alteração dos vários programas que operam na rede Acesso não autorizado via link de dados
Vírus	A ameaça de vírus transferidos por mídia removível A ameaça de vírus transferidos pela rede
Físicas	Interferência do enlace rádio Falha de hardware Distúrbios de energia Danos causados pelo fogo e pela água Falha do ar condicionado Umidade

	Sabotagem

Fonte: Autor.

As vulnerabilidades dos ativos dos sistemas de nível 2 foram relacionadas no QUADRO 12. A principal diferença entre as vulnerabilidades do nível anterior estão relacionadas com uma maior quantidade de ativos. Esta quantidade maior de ativos representa um número maior de vulnerabilidades pelo fato que mais erros poderão ser cometidos na programação de sistemas e na configuração de equipamentos de conectividade. Em um ambiente real deve-se realizar a avaliação de segurança como descrito no item 3.1.6 utilizando métodos intrusivos e não intrusivos para levantar as vulnerabilidades dos ativos.

QUADRO 12 - Vulnerabilidades para os sistemas do nível 2

Ativos com Vulnerabilidades	Descrição
Computadores e servidores	Acesso aos compartimentos dos ativos. Acesso de terceiros para reparo. Falha de funcionamento dos componentes (unidades removíveis, disco rígido, reparos e alienação).
Sistemas	Acesso aos sistemas disponíveis na rede TCP/IP por falhas no programa. Falhas nos códigos dos sistemas permitindo que ocorram erros durante a operação.
Conectividade	Acesso aos compartimentos dos ativos. Acesso aos equipamentos de conectividades. Interferência, bloqueio do link de dados. Acesso aos dados transmitidos pelo link. Acesso aos sistemas disponíveis na rede LAN via enlace satélite.
Vírus e programas maliciosos	Exploração de mais erros dos sistemas e de equipamentos de conectividade.

Fonte: Autor

4.4 FORÇA NAVAL COM SISTEMAS NO NÍVEL DOMÍNIO.

No nível 3, os sistemas estão interconectados por uma rede de longa distância (WAN), na qual diferentes sistemas são integrados e compartilham um banco de dados comum na rede utilizando um modelo de dados de domínio, permitindo que vários usuários acessem este banco de dados por meio de aplicações independentes. Neste nível foi utilizado um identificador global único para cada entidade na rede. Este identificador permite melhorar o controle de acesso. Outra alteração foi um controle a respeito de como os pacotes de informação são trocados para evitar a transmissão desnecessária.

Um exemplo de sistema neste nível é o sistema de comando e controle de uma força naval que atualiza via WAN um banco de dados que também é atualizado por outras forças. Este nível permite ter acesso a informações compartilhadas pelas outras forças.

A arquitetura da rede do nível 3 é formada por computadores, servidores de banco de dados, equipamentos de conectividade e enlace satélite, em uma topologia da rede *full mesh*.

O perímetro da rede é definido pelas entradas e saídas de todos os computadores, servidores e do enlace satélite.

Os ativos identificados que necessitam de proteção são os computadores que fazem parte da rede, os sistemas e aplicativos, o banco de dados comum, os equipamentos de conectividade, as conexões e o enlace satélite.

As ameaças aos ativos identificados do sistema em nível 3 de interoperabilidade, continuam ser as ameaças de pessoas, de vírus e físicas (QUADRO 1), aplicadas a um conjunto de ativos maior (QUADRO 13):

QUADRO 13 - Ameaças para os sistemas do nível 3

Ameaças	Descrição
Pessoas	Erros na programação de cada sistema que opere na LAN e WAN, dos operadores dos computadores e na administração dos sistemas. Modificação de dados dos vários sistemas que operam na rede Alteração dos vários programas que operam na rede Acesso não autorizado via link de dados
Vírus	Vírus e *malware* transferidos por mídia removível Vírus recebido pela rede
Físicas	Interferência no enlace satélite Falha de hardware Distúrbios de energia Danos causados pelo fogo e pela água Falha do ar condicionado Umidade Sabotagem

Fonte: Autor

As vulnerabilidades dos ativos dos sistemas de nível 3 foram relacionadas no QUADRO 13. A principal diferença entre as vulnerabilidades do nível anterior estão relacionadas com uma maior quantidade de ativos. Esta quantidade maior de ativos representa um número maior de vulnerabilidades pelo fato de que mais erros poderão ser cometidos na programação de sistemas e na configuração de equipamentos de conectividade. Em um ambiente real deve-se realizar a avaliação de segurança como descrito no item 3.1.6 utilizando métodos intrusivos e não intrusivos para levantar as vulnerabilidades dos ativos.

QUADRO 14 - Vulnerabilidades para os sistemas do nível 3

Ativos com Vulnerabilidades	Descrição da vulnerabilidade
Computadores e servidores	Acesso remoto aos dados do computador Falha de funcionamento dos componentes (unidades removíveis, disco rígido, reparos e alienação). Acesso ao equipamento por terceiros para reparo.
Sistemas	Falhas nos códigos dos sistemas permitindo que ocorram erros durante a operação. Falta de atualização de segurança
Acesso à LAN/WAN	Acesso aos sistemas disponíveis na rede LAN via enlace satélite. Interferência, bloqueio do link de dados. Acesso aos dados transmitidos pelo link.

Conectividade	Acesso aos equipamentos de conectividades. Acesso aos compartimentos dos ativos.
Vírus e programas maliciosos	Exploração de mais erros dos sistemas, equipamentos de conectividade.

Fonte: Autor

4.5 FORÇA NAVAL COM SISTEMAS NO NÍVEL CORPORATIVO.

No nível 4, a infraestrutura de rede é a mesma do nível anterior, os sistemas utilizados na rede local se conectam através do enlace satélite a outras redes. A diferença está na capacidade de configurar LAN virtuais usando protocolos como o *Point-to-Point Tunneling Protocol* (PPTP) que criam um túnel virtual entre dois pontos geograficamente distribuídos permitindo que usuários interajam e trabalhem de modo colaborativo. Os aplicativos utilizados podem estar em qualquer lugar da rede

Como exemplo de sistema neste nível são os sistemas de comando e controle utilizados pelo DoD dos EUA.

O perímetro da rede é definido pelas entradas e saídas de todos os computadores, servidores e do enlace satélite e dos túneis virtuais criados. Estes túneis virtuais permitem o acesso de um computador localizado fora da plataforma como se o mesmo estivesse conectado diretamente na rede local.

Os ativos identificados que necessitam de proteção são os computadores que fazem parte da rede, os sistemas e aplicativos, os equipamentos de conectividade, as conexões e o enlace satélite.

As ameaças aos ativos do sistema em nível 4 de interoperabilidade são as ameaças de pessoas, de vírus e físicas (QUADRO 1), aplicadas a um conjunto maior de ativos e ao túnel virtual quando criado.

As vulnerabilidades apresentadas no QUADRO 13 são aplicáveis para sistemas nível 4, incluídas aquelas associadas aos túneis virtuais.

A análise é que os níveis de interoperabilidade funcional, de domínio e corporativo demandam uma preocupação crescente com a segurança, onde os sistemas podem ser deslocados para fora do perímetro da rede da plataforma. A disponibilidade do enlace satélite e do enlace rádio deve ser protegida, pois no nível de domínio e corporativo os sistemas de comando e controle são dependentes do seu correto funcionamento.

5 CONCLUSÃO

Analisando a evolução da TI, que permitiu o desenvolvimento da teoria da guerra centrada em rede pelos EUA e a interoperabilidade dos sistemas, observa-se que os sistemas de TI empregados pelas forças armadas dos EUA e as redes de dados tiveram, ao longo dos últimos 20 anos, um incremento na capacidade de compartilhar informações aumentando a colaboração entre as forças que operam em conjunto. Este aumento ocorreu devido à evolução das redes de dados e dos sistemas empregados.

Para avaliar qual é o impacto da maturidade de interoperabilidade dos sistemas de comando e controle sobre a proteção da rede de uma força naval foi utilizada uma técnica de analise de risco empregada pela indústria de segurança. Esta técnica foi aplicada na infraestrutura de rede prevista para atender cada nível de interoperabilidade.

No nível isolado, ao ser avaliado o ambiente foi identificado que o ativo a ser protegido é o computador do sistema e as principais vulnerabilidades existentes são afetas ao controle de acesso das pessoas ao ativo e suas atividades.

No nível conectado, embora exista uma ligação física e a possibilidade utilização de enlace rádio, as informações trocadas são simples e predefinidas, e a conexão física estaria dentro da plataforma sem conexão com outras redes, tornando inviável a exploração remota. As principais vulnerabilidades dos ativos deste nível também são afetas ao controle de acesso das pessoas aos ativos e suas atividades.

Os riscos envolvidos para este sistema são as ameaças de pessoas com acesso autorizado ou não de realizarem alguma alteração no sistema de maneira a interferir no funcionamento instalando vírus ou causando falhas. Com relação ao *link* de dados, a interferência ou bloqueio são ameaças possíveis.

No nível funcional já existe uma LAN e a utilização de protocolo TCP/IP e a possibilidade de acesso por conexão via satélite, o que torna possível a exploração remota.

No nível domínio, os sistemas da LAN estão interconectados por uma WAN, na qual diferentes sistemas estão integrados e compartilhando um banco de dados comum. Neste nível, o risco de interrupção ou comprometimento do acesso com a WAN teria um impacto grande, pois impediria o acesso ao banco de dados comum e as informações compartilhadas das outras forças.

No nível corporativo a infraestrutura da rede é a mesma mais existe a capacidade de criar redes virtuais e os sistemas encontram-se em algum local da rede, fora da plataforma. A falha do enlace satélite da força naval no mar representa o risco de maior impacto.

Analisando as variações das estruturas das redes utilizadas em cada nível de interoperabilidade, verifica-se que até o nível funcional a infraestrutura de conectividade aumenta dentro do perímetro da rede da plataforma e desta forma existe um maior numero de ativos na rede que deverão ser protegidos. Nos níveis de domínio e corporativo existe uma migração dos sistemas para fora do perímetro da rede iniciando com o banco de dados e depois com os sistemas. Esta migração transfere os riscos destes ativos para o novo responsável e aumenta a necessidade de conexões estáveis e seguras.

Assim, a hipótese levantada de que um maior nível de interoperabilidade dos sistemas de TI empregados pela força naval representa uma maior dificuldade para realizar a defesa cibernética desta força naval no mar é verdadeira.

Para todos os níveis, a segurança da rede deve ser estabelecida levantando a arquitetura da rede, os ativos a serem protegidos, as ameaças aos ativos e as vulnerabilidades dos ativos. Para o levantamento das vulnerabilidades é necessário avaliar o ambiente utilizando os métodos intrusivos e não intrusivos.

Para o planejamento da defesa cibernética deste ECiber “militar” é necessário uma compreensão da arquitetura da rede de modo a identificar os riscos e aplicar os controles de proteção para reduzi-los. Para isso a força naval deve realizar:

a) o levantamento dos ativos utilizados e controlados pela Força naval;

b) a identificação da estrutura da rede,

c) a definição do perímetro da rede;

d) o levantamento das vulnerabilidades relacionadas aos ativos;

e) a identificação das possíveis ameaças;

f) a avaliação do impacto e da probabilidade para cada combinação de ativos / ameaças / vulnerabilidades;

g) a verificação do nível de risco, de modo a priorizar os mais importantes; e

h) a aplicação dos controles de proteção para mitigar os riscos identificados.

A periodicidade com que esta análise de risco deverá ser executada deve estar em um intervalo de tempo adequado com as atividades da força naval levando em conta as alterações nos ativos da rede.

O planejamento de uma defesa cibernética deve empregar o monitoramento das entradas e saídas otimizando nos pontos de concentração das informações e realizar exercícios para testar o planejamento de defesa cibernética do ECiber da Força naval no mar e a capacitação do pessoal de bordo para executá-la. E todas as informações obtidas com o monitoramento de incidentes e ataques deve produzir conhecimento cibernético de modo a ser utilizados nos próximos planejamentos de defesa cibernética.

REFERÊNCIAS

BRASIL. Marinha do Brasil. Estado-Maior da Armada. Doutrina Básica da Marinha – DBM-2a revisão. Brasília, 2014.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Livro Verde: segurança cibernética no Brasil**. Brasília. 2010.

BRASIL. **Decreto Legislativo nº 373, de 30 de setembro de 2013. Aprova a Política Nacional de Defesa (PND).** Brasília, 2013

BRASIL. **Decreto Legislativo nº 373, de 30 de setembro de 2013. Aprova a Estratégia Nacional de Defesa (END).** Brasília, 2013a

BRASIL. Secretaria de Assuntos Estratégicos da Presidência da República. **Desafios Estratégicos para a Segurança e Defesa Cibernética**. Brasília. 2011a.

BRASIL. Ministério da Defesa. **MD30-M-01**: Doutrina de Operações Conjuntas 1. Ed. Brasília, 2011b.

BRASIL. Ministério da Defesa. **MD35-G-01**: Glossário das Forças Armadas. 4. ed. Brasília, 2007b.

CLARKE, Richard A; KNAKE, Robert K. **Cyber War**: The Next Threat to National Security and What To Do About It. Nova Iorque, 2010. Ed. HarperCollins e-books.

CORNISH, Paul; LIVINGSTONE, David; CLEMENTE Dave; YORKE, Claire. **On Cyber Warfare**. United Kingdom: Chatham House, Nov. 2010. Disponível em: <http://w. chathamhouse.org/publications/papers/view/109508>. Acesso em: 1 ago. 2014.

EUA. Department of Defense. **The Implementation of Network-Centric Warfare**. Washington, DC, 2005. Disponível em: <http://www.carlisle.army.mil/DIME/documents/oft_ implementation_nwc[1].pdf>. Acesso em: 20 jul 2014.

EUA. Department of Defense. **Levels of Information Systems Interoperability (LISI)**. Washington, DC, 1998. Disponível em:<http://www.eng.auburn.edu/~hamilton/ security/DODAF/LISI.pdf >. Acesso em: 24 abr 2014.

FRANÇA, Junia Lessa; VASCONCELOS, Ana Cristina de. **Manual para normalização de publicações técnico-científicas.** 8. ed. Belo Horizonte: UFMG, 2007.

LIBICKI, Martin C. RAND Corporation. **Cyberdeterrence and Cyberwar**, Santa Monica, Project Air Force, 2009. Disponível em: <http://www.rand.org/content/dam/rand/pubs/ monographs/2009/RAND_MG877.pdf>. Acesso em: 18 ago 2014.

O' HANLEY, Richard (Ed.); TILLER, James S.(Ed.). **Information Security Management Handbook**. 2013. ed. New York: Auerbach Publications. 1 CD-ROM.

PORCHE III, Isaac R.; COMANOR, Katherine; WILSON Bradley; SCHNEIDER, Matthew J.; MONTELIBANO, Juan; ROTHENBERG, Jeff. **Navy Network Dependability: Models, Metrics, and Tools**. RAND National Defense Research Institute, Santa Monica, CA, EUA, 2010.

SCHREIER, Fred. DCAF Horizon 2015 Working Paper No. 7. **On Cyberwarfare.** 2012. Disponível em:<http://www.dcaf.ch/content/download/67316/1025687/file/OnCyberwarfare-Schreier.pdf>. Acesso em: 18 ago 2014.

STADEN, Stefanus Van; MBALE, Jameson. The Information System Interoperability Maturity Model (ISIMM): Towards Standardizing Technical Interoperability and Assessment within Government. **International Journal of Information Engineering and Electronic Business**. Modern Education & Computer Science Publisher, Online, v. 2012-5, p. 36-41, 2012. Disponível em: < http://www.mecs-press.org/ijieeb/ijieeb-v4-n5/IJIEEB-V4-N5-5.pdf >. Acesso em: 11 nov. 2014.

STOUFFER Keith; FALCO, Joe; SCARFONE Karen. NIST Special Publication 800-82, **Guide to Industrial Control Systems (ICS) Security Revision 1**. 2013. Disponível em: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r1.pdf>. Acesso em: 18 ago 2014.

TIPTON, Haroldo F. (Ed.); KRAUSE, Micki. (Ed.). **Information Security Management Handbook**. 6. ed. New York:Auerbach Publications, 2007. 3231 p.