MARINHA DO BRASIL

DIRETORIA DE ENSINO DA MARINHA

CENTRO DE INSTRUÇÃO ALMIRANTE WANDENKOLK

CURSO DE APERFEIÇOAMENTO AVANÇADO EM GUERRA ELETRÔNICA

1 TEN RICARDO DOS SANTOS BACELLAR

A IMPORTÂNCIA DA SEGURANÇA CIBERNÉTICA PARA A MARINHA DO BRASIL

TRABALHO DE CONCLUSÃO DE CURSO

Rio de Janeiro

2018

1 TEN RICARDO DOS SANTOS BACELLAR

A IMPORTÂNCIA DA SEGURANÇA CIBERNÉTICA PARA A MARINHA DO BRASIL

Monografia apresentada ao Centro de Instrução Almirante Wandenkolk como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Guerra Eletrônica.

Orientador: Prof. Dr. Anderson Oliveira da Silva.
Coorientador: Prof. Me. Alan Oliveira de Sá.

Rio de Janeiro
2018

1T RICARDO DOS SANTOS BACELLAR

A IMPORTÂNCIA DA SEGURANÇA CIBERNÉTICA PARA A MARINHA DO BRASIL

Monografia apresentada ao Centro de Instrução Almirante Wandenkolk como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Guerra Eletônica.

Aprovada em 14 de junho de 2018

Banca Examinadora:

Anderson Oliveira da Silva, Dr. – PUC Rio _____

Cesar Augusto Lampe Linhares da Fonseca, DSc – CIAW_____

Gian Karlo Huback Macedo de Almeida, Me. – CIAW _____

CIAW
Rio de Janeiro
2018

Dedico esse trabalho aos amigos do Curso de Aperfeiçoamento Avançado em Guerra Eletrônica, que com espírito de camaradagem, fez com que o curso ocorresse de maneira exemplar e de grande aprendizado.

Agradecimentos

Primeiramente a Deus, que me deu forças para a longa caminhada desse curso, fazendo com que o fogo sagrado diário não se apagasse.

À minha família, que me incentivou e apoiou nesse período do curso.

Aos meus orientadores, Anderson Oliveira da Silva e Alan Oliveira de Sá, pelo direcionamento na confecção desse trabalho.

Ao professor, Marco Grivet, pela coordenação exemplar por parte da PUC-Rio do referido curso.

Aos amigos do Curso de Aperfeiçoamento Avançado em Guerra Eletrônica, que com muita alegria ajudaram a prosseguir a minha caminhada na carreira naval.

"A arte da guerra é de importância vital para o Estado. É a província da vida ou da morte; o caminho à segurança ou à ruina. Portanto, é um objeto de investigação que não pode, sob nenhuma circunstância, ser negligenciado."

Sun Tzu

Resumo

As concepções de guerra e campo de batalha evoluíram surpreendentemente, passando de uma visão tradicional de munição militar realizada em terra, mar ou ar, para os mais novos dispositivos eletrônicos que dominam as estratégias dos conflitos internacionais no ciberespaço. Alguns exemplos destas novas armas operando no chamado quinto domínio, como computadores, drones e malware, são considerados inofensivos em uma primeira análise, especialmente quando comparados a outras categorias de artilharia clássica. No entanto, esses dispositivos foram os que fomentaram a atual corrida cibernética, notavelmente iniciada pelo ataque cibernético ocorrido na Estônia (2007). Desde então provou-se ser capaz de causar consequências muito mais alarmantes, principalmente visando infraestruturas nacionais críticas. Este trabalho tratará dos conceitos de Guerra Cibernética (GC) alinhados com o surgimento deste quinto domínio, denominado de ciberespaço, presente no contexto da guerra convencional atualmente. A seguir, o foco do estudo se concentrará em tornar explícita a importância da segurança cibernética, atualmente, frente ao crescente número de ameaças que surgem no ciberespaço. Por fim, serão apontados os meios vulneráveis a ataques cibernéticos presentes nos navios da Marinha do Brasil (MB).

Palavras-chave: Guerra Cibernética; ciberespaço; segurança cibernética; e ataque cibernético.

Lista de ilustrações

Lista de abreviaturas e siglas

AIS	Sistema de Identificação Automática (Automatic Identification System)
CIA	Confidencialidade, Integridade e Disponibilidade
COC	Centro de Operações de Combate
DDoS	Negação de Serviço Distribuída (Distributed Denial of Service)
DoD	Departamento de Defesa dos EUA (Department of Defense)
DoS	Negação de Serviço (Denial of Service)
ECDIS	Sistema de Apresentação de Cartas e Informações (Electronic Chart Display and Information System)
ENC	Carta Eletrônica de Navegação (Electronic Navigation Charts)
EUA	Estados Unidos da América
GC	Guerra Cibernética
GE	Guerra Eletrônica
IEC	Comissão Eletrotécnica Internacional (International Electrotechnical Commission)
IP	Protocolo de Internet (Internet Protocol)
IPqM	Instituto de Pesquisas da Marinha
ISO	Organização Internacional de Normalização (International Organization of Standardization)
LAN	Rede de Área Local (Local Area Network)
MAGE	Medidas de Apoio a Guerra Eletrônica
MB	Marinha do Brasil
NAVSTAR GPS	Navegação Satélite por Sistema de Posicionamento Global (Navigation Satellite with Global Positioning System)
NAVTEX	Navigational Telex
OTAN	Organização do Tratado do Atlântico Norte
SCADA	Sistema de Supervisão e Aquisição de Dados (Supervisory Control and Data Acquisition)

SICONTA	Sistema de Controle Tático
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação
UIT	União Internacional de Telecomunicações
UK	Reino Unido (United Kingdom)
VPN	Rede Privada Virtual (Virtual Private Network)

Sumário

1 INTRODUÇÃO

Cibernética, palavra de origem grega *"kibernetikós"* (DICIO, 2018), é um dos conceitos mais utilizados no mundo de hoje. A partir desse conceito nasce um novo ambiente denominado de ciberespaço e, ao mesmo tempo, surgem ameaças de ataques cibernéticos tanto por parte dos Estados e seus governos, como por agentes desconhecidos. Assim "o mundo passa a conviver com a sombra do ciberterrorismo e, no caso dos Estados, com a possibilidade de hostilidades no ciberespaço, ou seja, uma Guerra Cibernética" (NUNES, 2010).

Do ponto de vista da segurança cibernética, os navios são uma das estruturas mais críticas por serem tecnologicamente equipados. Como os sistemas de bordo são controlados e programados através de Tecnologias da Informação (TI), os navios podem encontrar-se vulneráveis no ciberespaço. Essas vulnerabilidades podem ser transformadas em ameaças cibernéticas ou ataques cibernéticos.

Neste trabalho veremos que os ataques cibernéticos contra navios são normalmente efetuados através da rede e dos sistemas de bordo, como por exemplo os Sistemas de Navegação, Sistemas de Armamento, Sistemas de Propulsão, entre outros. O acesso ilegal à rede dos navios pode ser conseguido pelo uso indevido da mesma pelos seus usuários, por isso a falta de conhecimento de TI e de medidas de prevenção de riscos cibernéticos podem prejudicar a navegação segura e também por em risco a integridade do meio.

Com base nos fatos acima, a conscientização da segurança cibernética surge como tópico importante a ser observado pela MB.

1.1 Organização do Trabalho

Este trabalho está dividido em oito capítulos, estruturados de forma a, num primeiro momento, conceituar os termos atinentes a Guerra Cibernética, passando por uma profunda abordagem de segurança cibernética e uma posterior análise das vulnerabilidades dos sistemas que atuam no ciberespaço e que estão presentes nos navios da MB.

No primeiro capítulo, encontra-se a introdução, que contextualiza o assunto referente a Guerra Cibernética nos dias atuais. Além disso, expõe a organização do trabalho, a justificativa e relevância para a realização deste estudo e os objetivos gerais e específicos do mesmo.

O segundo capítulo compreende o referencial teórico da pesquisa, onde são citadas as principais referências utilizadas neste estudo e o que as mesmas agregaram de conhecimento para o desenvolvimento deste trabalho.

O terceiro capítulo aborda a metodologia utilizada na realização deste trabalho.

No quarto capítulo, são descritos os conceitos de definição de Guerra Cibernética, com as concepções dos atores e os seus métodos de atuação nesta guerra.

O quinto capítulo contempla a explicação do ambiente de atuação da Guerra Cibernética, denominado de ciberespaço.

O sexto capítulo desenvolve o conceito de segurança no ambiente cibernético, sendo abordados os termos de segurança da informação e segurança cibernética.

No sétimo capítulo, são citados os sistemas vulneráveis encontrados a bordo dos navios da MB.

Por fim, no capítulo oito é feita a conclusão do estudo, seguida das referências utilizadas para a realização deste trabalho.

1.2 Justificativa e Relevância

A crescente importância do ciberespaço para a sociedade moderna, paralelamente com o seu crescente uso para novas formas de disputas, estão se tornando uma preocupação de segurança nacional para governos e forças armadas em todo o mundo. As características especiais do ciberespaço, tais como a sua natureza assimétrica, o baixo custo de entrada e seu papel como meio eficiente para protestos, crimes, espionagem e agressão militar, o torna um domínio atraente para os Estados, bem como para os atores não estatais no conflito cibernético. O ciberespaço está emergindo como uma nova ferramenta para o poder estatal que provavelmente reformulará a guerra no futuro.

Dessa forma, o estudo cada vez mais aprofundado do ciberespaço torna-se um assunto de vital importância, assim como o conhecimento sobre segurança cibernética.

1.3 Objetivos

1.3.1 Objetivos Gerais

O presente estudo tem como objetivo evidenciar a importância da segurança cibernética para a MB, mostrando as vulnerabilidades dos seus meios frente às ameaças cibernéticas. Dessa forma, pretende-se diminuir potenciais causas de um incidente indesejado.

1.3.2 Objetivos Específicos

Além do objetivo principal, o estudo possui os seguintes objetivos específicos:

Entender o conceito de Guerra Cibernética e a sua influência no contexto da guerra convencional;

Definir o que é ciberespaço e como o mesmo é utilizado pelos atores envolvidos nas questões cibernéticas ; e

Compreender como a segurança cibernética ajuda no combate às ameaças do ciberespaço.

2 REFERENCIAL TEÓRICO

Na tese de “Nunes, Luiz Artur Rodrigues. Guerra Cibernética**:** está a MB preparada para enfrentá-la?”, foram encontradas os conceitos sobre Guerra Cibernética, desde sua definição, aos métodos de ataque cibernético, passando pelos atores que estão presentes no ciberespaço. Neste artigo, foram observados, também, os conceitos de ciberespaço.

Nos documentos “The WhiteHouse. International strategy for cyberspace.” e Minister for the Cabinet Office and Paymaster General. The UK cyber security strategy.”, foram observadas as medidas de segurança cibernéticas, bem como as definições sobre esse conceito, adotados pelos governos americano e do Reino Unido.

E do site www.marinha.mil.br/ipqm/grupo_sistemas_digitais, foram tirados os sistemas digitais utilizados a bordo dos navios da MB.

3 METODOLOGIA

3.1 Classificação da Pesquisa

3.1.1 Classificação Quanto aos Fins

Adotou-se uma metodologia descritiva em grande parte do trabalho, com a exposição dos conceitos e dos recursos empregados, descritos em todo o desenvolvimento.

Também realizou-se uma metodologia explicativa, após a análise dos conceitos e recursos utilizados, explicitando-se uma necessidade de atualização e acompanhamento, por parte da MB, do assunto em questão.

3.1.2 Classificação Quanto aos Meios

Adotou-se uma metodologia basicamente bibliográfica e documental.

Bibliográfica porque grande parte do referencial teórico deriva de artigos, teses e publicações relativos ao problema abordado. Tratam-se de pesquisas na área de TI e de estratégias no âmbito cibernético, que trazem conceitos essenciais para o desenvolvimento desse trabalho.

Quanto a parte metodológica documental são documentos ostensivos, muitos de origem estrangeira, que mostram a preocupação de diversos países em relação à utilização do ciberespaço.

3.2 Limitações do Método

Não foi possível estudar em grande escala outras fontes bibliográficas, devido ao alto nível de considerações técnicas nas teses, artigos e dissertações sobre o assunto. Muitas publicações existentes na internet não puderam ser consultadas devido ao sigilo que as forças armadas nacionais e internacionais definiram sobre seus conteúdos.

4 GUERRA CIBERNÉTICA

No dia 27 de abril de 2007, a Estônia foi atingida por uma série de ataques cibernéticos que afetaram os sites do governo, bancos e os principais jornais estonianos, chamando bastante atenção da comunidade europeia e, principalmente, da OTAN (Organização do Tratado do Atlântico Norte). Estes ataques do tipo negação (DDoS) ocorreram através de redes botnets e consistiu, basicamente, no envio de pedidos de informações aos servidores num volume muito maior do que a sua capacidade de processamento (GAMA NETO, 2017).

A gravidade dos ataques cibernéticos da Estônia serviu como um alerta para o mundo sobre uma nova forma de guerra que utiliza o ciberespaço como arma de ataque.

4.1 Definição

A Guerra Cibernética é uma forma emergente de guerra que não é explicitamente abordada pelo direito internacional existente. Atualmente, a Guerra Cibernética tornou-se uma das formas mais distintas de combate, com o desenvolvimento da tecnologia de rede de computadores e tecnologia de Guerra Eletrônica (GE).

A evolução tecnológica das últimas décadas deu origem à revolução da informação que envolve o processamento e disseminação de informações. As TI continuam a se desenvolver em um ritmo acelerado, e uma nova era surge na revolução da informação.

O rápido crescimento nas áreas de computação e comunicações e a melhoria contínua no desempenho de sistemas informatizados criaram um espaço no mundo, o ciberespaço, um espaço criado não pela natureza, mas por seres humanos, e que tem um potencial para benefícios tremendos, mas também para riscos desconhecidos.

A crescente presença de diversos agentes que podem atuar no ciberespaço o tornam cada vez mais complexo. Essas atuações combinam crimes, espionagem e ações militares que podem ocasionar algum tipo de incidente nas redes de um navio, por exemplo.

"Ainda não existe concordância entre especialistas de segurança cibernética, tecnologia e relações internacionais sobre que tipo de ações, se é que há alguma, constituem a guerra no ciberespaço[1]" (MCAFEE, 2009) .

Entretanto, diante dos fatos supracitados e para uma melhor compreensão deste trabalho, pode-se entender como Guerra Cibernética a utilização do ciberespaço para promover ações de ataque, defesa e exploração destinadas a corromper, negar ou destruir os sistemas do inimigo (NUNES, 2010).

[1] Yet there is disagreement among cyber security, technology and international relations experts as to what kind of actions, if any, constitute warfare in cyberspace.

4.2 Atores

O ciberespaço também trouxe consigo várias novas ameaças. Pelo fato da dependência cibernética tornar-se tão difundida na sociedade, com interconexões complexas entre vários setores, aumentou-se a vulnerabilidade a ataques cibernéticos contra civis e infraestruturas militares. Assim, foi observado mais foco na defesa cibernética dentro das forças armadas e organizações de segurança nacional em várias partes do mundo.

No âmbito militar, o ciberespaço foi identificado como uma nova área de atuação, em que as operações militares podem ser realizadas. Estas operações no ciberespaço são tanto ofensivas quanto defensivas e, podem ser realizadas de forma independente ou como complemento da guerra convencional.

Devido a sua maior capacidade de gerar recursos que possibilitam o desenvolvimento de ferramentas para a realização de ataques cibernéticos com elevado grau de sofisticação, o Estado pode ser considerado o principal ator presente no espaço cibernético (NUNES, 2010). Entretanto, existem vários outros agentes que atuam de diversas formas no ciberespaço e que também podem exercer o papel principal na realização de um ataque cibernético.

No evento ocorrido na Estônia em abril de 2007, foi observado o ativismo cibernético, onde um grupo de "voluntários" participaram ativamente de um conflito cibernético, mobilizando-se para sobrecarregar vários recursos do ciberespaço estoniano, como sites governamentais, por exemplo.

Os criadores de malware e os criminosos cibernéticos organizados também têm sido muito ativos durante os últimos anos, motivados principalmente pelo ganho econômico.

Em 2009, foi descoberta uma rede de ciberespionagem chamada GhostNet que havia acessado informações confidenciais pertencentes as organizações governamentais e privadas em mais de 100 países ao redor do mundo. Posteriormente, foi alegado que o software era, aparentemente, controlado por servidores localizados na ilha de Hainan, na China. Devido a este fato, suspeitou-se que a GhostNet seria uma ferramenta utilizada pelo governo chinês. No entanto, a China negou oficialmente responsabilidades pela GhostNet, e não há provas conclusivas de que os chineses estariam envolvidos nessa operação (INFORMATION WARFARE MONITOR, 2009).

Outro tipo de ameaça, não menos importante, é o elemento interno, que atua no ciberespaço introduzindo uma vulnerabilidade operacionalmente por meio de ação humana direta, ou seja, por meio físico (NUNES, 2010).

4.3 Métodos de Ataque

Em face ao exposto neste trabalho até agora, pode-se observar que existem diversas formas de ataques cibernéticos. Para uma melhor compreensão deste estudo, os métodos de

ataque serão divididos em três categorias diferentes: sabotagem, espionagem e subversão (RID, 2012).

A Sabotagem é explicada como um ataque cibernético através do uso de malware, visando enfraquecer ou destruir um sistema. O exemplo mais comum desse tipo de ataque é a utilização de programas nocivos, também conhecidos como vírus.

A Espionagem tem como objetivo interceptar ou recuperar informações de redes ou sistemas de computadores da maneira mais sigilosa possível. É imprescindível nesse tipo de ataque o anonimato e também a possibilidade não ser descoberto. Anteriormente, foi citado o exemplo da rede GhostNet como um tipo de ator que utiliza o método de espionagem.

A subversão é um tipo de ataque cibernético que visa enfraquecer uma autoridade ou uma ordem estabelecida. É o método de ataque mais usado pelos movimentos ativistas cibernéticos. Nesta categoria são utilizados métodos de ataques prejudiciais e perturbadores da rede, como Defacement, DoS (Denial of Service) e DDoS. Ataques Defacement realizam uma espécie de desfiguração da rede, já os ataques DoS e DDoS são mais destinados a sobrecarregar a rede com informações.

5 OS AMBIENTES DA GUERRA CIBERNÉTICA

5.1 Ciberespaço

O ciberespaço é composto por todas as redes informatizadas do mundo, bem como todos os pontos que estão conectados às redes e são controlados através de comandos que passam por essas redes. “O ciberespaço é um “ambiente” artificial caracterizado por uma complexa e não centralizada rede de emissões e transmissores de informações” (GAMA NETO, 2017).

O Departamento de Defesa dos EUA (DoD) define o ciberespaço como um domínio caracterizado pelo uso do espectro eletromagnético para armazenar, modificar e trocar dados via sistemas em rede e infraestruturas físicas associadas. “O ciberespaço é um domínio de combate” (BOLENG; SCHWEITZER; GIBSON, 2008)

5.2 Ciberespaço Marítimo

No domínio marítimo, as tecnologias e sistemas de informação de computadores e redes de portos e navios são os principais constituintes do ciberespaço marítimo. Além disso, os sensores dos radares e armamentos dos navios de guerra, assim como os sistemas de navegação também são vulneráveis a ataques cibernéticos. Por conseguinte, esses sistemas e sensores também podem ser membros do ciberespaço marítimo.

Devido ao contínuo desenvolvimento das tecnologias da informação, as redes dos navios foram conectadas à rede mundial, aumentando a probabilidade de riscos a segurança dos meios navais. Assim, cada parte dos sistemas de máquinas, navegação, comunicação, radar e armamento de um navio podem sofrer ameaças cibernéticas. Esses ataques podem ser causados pelo inimigo que encontra as vulnerabilidades do sistema na rede dos navios.

6 SEGURANÇA NO AMBIENTE CIBERNÉTICO

O termo segurança cibernética é frequentemente usado atualmente, assim como o termo segurança da informação. Embora exista uma certa semelhança entre segurança cibernética e segurança da informação, esses dois conceitos possuem algumas diferenças entre si. Além disso, verifica-se neste estudo que a segurança cibernética vai além dos limites da segurança da informação tradicional, incluindo não apenas a proteção dos recursos de informação, mas também a de outros ativos, como o próprio indivíduo. Na segurança da informação, a referência ao fator humano geralmente relaciona-se com o papel do indivíduo no processo de segurança. Já na segurança cibernética, esse fator tem uma dimensão adicional, pois considera o homem como alvo em potencial de ataques cibernéticos ou, até mesmo sem saber, parte de um ataque cibernético. Essa dimensão adicional tem implicações éticas para a sociedade na totalidade, já que a proteção de certos grupos vulneráveis, por exemplo, crianças, pode ser vista como uma responsabilidade social.

A segurança cibernética tornou-se uma questão importante e de interesse global. Atualmente, mais de 50 nações já publicaram oficialmente algum tipo de documento estratégico relacionado a suas posições no ciberespaço, ao crime cibernético e/ou a segurança cibernética (KLIMBURG, 2012). Em 2011, a Casa Branca delineou uma "ciberestratégia" que define a postura dos Estados Unidos da América (EUA) sobre questões relacionadas a cibernética e descreve uma abordagem do envolvimento americano com outros países nessas questões (EUA, 2011). O Reino Unido (UK) lista a segurança cibernética como prioridade máxima e comprometeu 650 milhões de libras, em quatro anos, para o desenvolvimento de um programa nacional de segurança cibernética (UK, 2011). No entanto, poucas fontes parecem fazer uma distinção entre os conceitos de segurança cibernética e segurança da informação ou uma relação entre eles.

As definições de segurança cibernética variam, esse termo para alguns autores podem ser definido como um conjunto de ideias e ações que permitem o usuário do ciberespaço proteger-se de possíveis ataques cibernéticos (BOYES; ISBELL, 2017). Entretanto, a União Internacional de Telecomunicações (UIT) define a segurança cibernética como:

> A coleção de ferramentas, políticas, conceitos de segurança, salvaguardas de segurança, diretrizes, gerenciamento de riscos, ações, treinamentos, melhores práticas, garantias e tecnologias que podem ser usadas para proteger o ambiente cibernético e os recursos da organização e do usuário. Os recursos da organização e do usuário incluem dispositivos de computação conectados, pessoal, infraestrutura, aplicativos, serviços, sistemas de telecomunicações, e a totalidade dos dados transmitidos e/ou informações armazenadas no ambiente cibernético. A segurança cibernética se esforça para garantir a obtenção e a manutenção das propriedades de segurança da organização e dos recursos do usuário contra riscos de segurança relevantes no ambiente cibernético.[1] (ITU, 2008).

[1] Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices,

Essas definições são muito semelhantes às de segurança da informação. Neste trabalho, será observado a definição de segurança da informação e, posteriormente, será analisado os limites da segurança cibernética como um conceito mais amplo do que os da segurança da informação.

Neste capítulo, será dado um enfoque na natureza de segurança, em geral e tentará mostrar, através de exemplos, que os recursos de segurança cibernética visam incluir uma dimensão que se estenda além dos limites formais de segurança da informação. Além disso, este estudo afirma que os seres humanos, em termos pessoais e de sociedade, podem ser diretamente prejudicados ou afetados pelos ataques cibernéticos, no que diz respeito a segurança cibernética. Por outro lado, este não é necessariamente o caso da segurança da informação, onde o dano é sempre indireto. Os autores veem tais diferenças como uma importante contribuição para o conhecimento no campo da informação e da segurança cibernética. Tais conhecimentos fornecem uma base para entender os termos e conceitos em questão e, atuam como uma sistemática de tópicos relevantes para profissionais de todo o mundo (THEOHARIDOU; GRITZALIS, 2007).

6.1 Segurança da Informação

O objetivo da segurança da informação é garantir a continuidade dos negócios e minimizar os seus danos , limitando o impacto dos incidentes de segurança (SOLMS, 1998). Segurança da informação pode ser definida de várias maneiras, conforme destacado abaixo.

A ISO (International Organization of Standardization) / IEC (International Electrotechnical Commission) (2013), define segurança da informação como a preservação da confidencialidade, integridade e disponibilidade (CIA) de informações. No contexto da ISO/IEC (2013), a informação pode assumir muitas formas, podendo ser impressa ou escrita em papel, armazenada eletronicamente, transmitida por correio ou por meio eletrônico, mostrada em filmes, transmitida em conversas, e assim por diante. WHITMAN e MATTORD (2009) definem segurança da informação como "a proteção da informação e dos sistemas e hardware que usam, armazenam e transmitem essa informação[2]". Esses autores também identificam várias características críticas da informação segura. Essas características incluem confidencialidade, integridade e disponibilidade, conforme a definição encontrada na ISO/IEC (2013), porém, a informação não se limita apenas a estas três características. Segundo WHITMAN e MATTORD (2009), a tríade CIA também conhecida em segurança da informação como o "triângulo da CIA", têm sido tradicionalmente o padrão utilizado pela indústria de computadores. Por conseguinte, estes autores acrescentam precisão, autenticidade, utilidade e posse como novas características da informação que precisam ser protegidas.

personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment.

[2] The protection of information and the systems and hardware that use, store, and transmit that information.

Alguns conceitos nas definições acima precisam de um exame mais detalhado. Em primeiro lugar, deve ficar claro que a segurança da informação não é um produto ou uma tecnologia, mas um processo (MITNICK; SIMON, 2002). Segundo WOOD (2004) segurança da informação costumava ser um problema estritamente técnico. No entanto, como o uso de computadores e redes evoluíram, o processo de segurança desses meios também tiveram que evoluir, tornando-o não apenas técnico. O processo de segurança da informação pode exigir o uso de certos produtos, e não é algo que pode ser comprado na prateleira. O segundo fator importante a ser observado nas definições acima é que a segurança da informação é comumente definida em termos das propriedades ou características que protegem as informações. Estes geralmente incluem a confidencialidade, integridade e disponibilidade, mas podem incluir características adicionais. É importante notar que há uma diferença entre segurança da informação e segurança de Tecnologia da Informação e Comunicação (TIC).

6.2 Segurança de TIC

A segurança de Tecnologia da informação e Comunicação é definida como a proteção da tecnologia baseada em sistemas tecnológicos nos quais a informação é normalmente armazenada e/ ou transmitida. A ISO/IEC (2004) define segurança de TIC como todos os aspectos necessários para alcançar e manter a confidencialidade, integridade, disponibilidade, responsabilidade, autenticidade, e confiabilidade dos recursos de informação. Como a segurança da informação inclui a proteção dos recursos de informação, pode-se argumentar que a segurança de TIC é um subcomponente da segurança da informação. A definição de segurança de TIC é muito semelhante à de segurança da informação. No entanto, possui características adicionais que, neste contexto, poderiam ser melhor descritas como aspectos que devem ser fornecidos por recursos de informações seguras. Estes aspectos incluem, responsabilidade, autenticidade e confiabilidade. DHILLON (2007) se refere ao conceito de segurança de dados como proteção dos dados reais em um sistema de informação. A definição dada por DHILLON (2007) inclui a maioria das características, já vistas, de segurança de TIC. Pelo fato da segurança de dados depender, em grande medida, da segurança geral da informação, sistema onde os dados residem, pode-se argumentar que esta definição usada por DHILLON (2007) tem o mesmo conceito utilizado na ISO/IEC (2004) para definir segurança de TIC.

Como mencionado anteriormente, as três primeiras características da informação segura, confidencialidade, integridade e disponibilidade, têm sido consideradas como padrão para segurança de computadores desde o desenvolvimento do mainframe (WHITMAN; MATTORD, 2009). As demais características foram adicionadas à definição de segurança da informação para atender as necessidades da segurança das organizações de negócios em ambientes de redes. Um claro entendimento do significado de todas as características acima mencionadas é essencial para uma compreensão da segurança de TIC, sem a confidencialidade, integridade, disponibilidade, autenticidade e confiabilidade dos recursos da informação, a mesma não pode ser considerada

segura. Todos os itens acima (incluindo precisão, utilidade e posse de informações) desempenham papel essencial na segurança da informação e devem ser igualmente importantes. No entanto, é possível que uma ou mais dessas características sejam mais aplicáveis em cenários específicos do que em outros, dependendo da natureza da informação em si. Por exemplo, a integridade das estatísticas de inflação é de importância óbvia para os economistas, enquanto a confidencialidade dos mesmos dados parece não ter tanta importância porque todos, provavelmente, deveriam ter permissão para ter acesso à tal informação. Contudo, por definição, uma violação da confidencialidade só ocorre se uma entidade não autorizar o acesso à determinada informação. Como todos seriam usuários autorizados a terem acesso às estatísticas de inflação, neste caso, a confidencialidade da informação seria realmente mantida. Portanto, no contexto de uma organização, garantir a segurança das informações não é um caso de decidir quais características são aplicáveis, mas de definir a forma de acesso à essas características.

Ao analisar a segurança de TIC, como descrito acima, fica claro que várias ameaças visam as vulnerabilidades que, eventualmente, terão um impacto negativo na infraestrutura de TIC. Neste caso, conclui-se que a infraestrutura tecnológica é considerada um recurso que precisa de proteção. No caso da segurança da informação, as TIC são a infraestrutura que processa, armazena e comunica informações. Nesse caso, a informação é considerada o ativo que requer proteção. Então, a TIC pode ser classificada como, entre outras coisas, uma vulnerabilidade, sendo alvo de vários ameaças na tentativa de comprometer o ativo, isto é, a informação.

Assim, é importante notar que, no caso da segurança da informação, a informação é o ativo que deve ser protegido. Posteriormente, será visto que, na segurança cibernética, as ameaças, vulnerabilidades e ativos diferem a partir da segurança da informação.

6.3 Segurança Cibernética

Como mencionado anteriormente, muitas publicações atuais sobre segurança cibernética usam esse conceito em conformidade com o termo segurança da informação. Se a segurança cibernética fosse um sinônimo de segurança da informação, seria razoável assumir que os incidentes de segurança cibernética também poderiam ser descritos com as mesmas características usadas para definir os incidentes da segurança da informação. Assim, um incidente de segurança cibernética, por exemplo, também levaria em conta a violação da confidencialidade, integridade ou disponibilidade da informação. Na verdade, para a maioria dos serviços de segurança cibernética, a violação das características citadas a cima são alvos frequentes das ameaças a que um usuário e/ ou organização podem estar expostos. No entanto, será visto nesse trabalho que existem ameaças a segurança cibernética que não fazem parte do sistema de segurança da informação. A seguir serão apresentados alguns exemplos dessas ameaças.

Com os avanços nas TIC, bem como os avanços no campo da eletrônica, originou-se uma infinidade de aplicações de automação. Muitas dessas permitem a integração de sistemas de

propulsão naval, sistema de navegação, sistemas radares e sistemas de armamento de um navio de guerra, por exemplo, com o sistema de rede de dados dos navios, que podem estar ligados na web. Portanto, através dessa rede de dados, ocorre o risco de que alguém possa ter acesso a tais sistemas e causar danos. Esses danos poderiam variar de falhas leves, como desligar o sistema de ar condicionado, a sérias avarias como interromper o sistema de propulsão ou até mesmo causar alguma pane no sistema de armas. Mais uma vez, neste caso, pode-se argumentar que a informação não foi necessariamente afetada, mas outros recursos da vítima se tornaram alvo do cibercrime.

Nos EUA, a infraestrutura crítica é definida através de sistemas e redes, sejam físicos ou virtuais, tão vitais para os americanos que a sua incapacitação ou destruição teria um efeito debilitante na segurança nacional, na economia, ou até mesmo na saúde pública. A infraestrutura que fornece eletricidade e água, controla o tráfego aéreo e suporta transações financeiras é vista como sustentação da vida americana e todos dependem diretamente dela (EUA, 2011). A proteção de tal infraestrutura crítica forma uma parte significativa da segurança cibernética. e é incluída como uma importante estratégia dos EUA na segurança nacional (EUA, 2011). Ciberterroristas ou inimigos podem ter como alvo essa infraestrutura crítica via ciberespaço. Isso poderia ser indiretamente, por exemplo, influenciando a disponibilidade de informações usando ataques de negação de serviço ou, mais diretamente, através de um ataque à rede elétrica americana. No caso de ataques contra essa infraestrutura crítica, a perda implica não apenas na integridade ou disponibilidade de recursos das informações, mas também o acesso a esses recursos. Neste caso, não é a informação em si nem o usuário da informação que está em risco, mas sim o bem-estar da sociedade na totalidade. Um bom exemplo de tais ataques são os ataques à Estônia em abril de 2007. Esses cenários lidam com um aspecto específico da segurança cibernética, onde os interesses de uma pessoa, sociedade ou nação, incluindo seus ativos não baseados em informações, precisam ser protegidos dos riscos decorrentes da interação com o ciberespaço. Isso serve para destacar a diferença entre a segurança da informação e segurança cibernética.

Toda a segurança é sobre a proteção de ativos das várias ameaças colocadas por certas vulnerabilidades inerentes. Processos de segurança geralmente lidam com a seleção e implementação de controles de segurança (também chamados de contramedidas) que ajudam reduzir o risco representado por essas vulnerabilidades (GERBER; SOLMS, 2005).

No caso de segurança de TIC, os ativos que precisam ser protegidos são a infraestrutura de TIC. A segurança da informação, por outro lado, estende essa definição dos ativos a serem protegidos, incluindo todos os aspectos da informação em si. Inclui assim a proteção dos ativos de TIC e, em seguida, vai além da tecnologia para incluir informações que não são armazenadas ou comunicada diretamente utilizando as TIC.

No entanto, como demonstrado nos cenários acima, na segurança cibernética, os ativos que precisam ser protegidos podem variar entre a própria pessoa e os meios tecnológicos

inventados pelo homem, a interesses da sociedade, em geral, incluindo os interesses nacionais. Na verdade, esses ativos incluem absolutamente qualquer um ou qualquer coisa que possa ser acessada via ciberespaço.

Por esses motivos citados, conclui-se que o termo segurança cibernética está relacionado, mas não é análogo, ao termo segurança da informação. Na segurança cibernética, as informações e as TIC são a base da causa da vulnerabilidade. Contudo, a característica mais definidora da segurança cibernética é o fato de que todos os ativos que precisam de proteção devem ser protegidos por causa das vulnerabilidades que existem como resultado do uso das TIC que formam a base do ciberespaço.

Tomando os exemplos acima mencionados em conta, pode-se afirmar que na segurança cibernética os ativos que precisam ser protegidos se estendem para além dos limites da informação. Em primeiro lugar, deve-se ficar claro que, na segurança cibernética, os ativos incluem os aspectos pessoais ou físicos, de um ser humano. Além disso, como pode ser visto, a segurança cibernética inclui também a proteção dos valores sociais (intangíveis) e de infraestrutura (tangível). Na segurança cibernética os ativos incluem, assim, ativos tangíveis e intangíveis relacionados com o bem-estar do indivíduo ou da sociedade, em geral. No caso de segurança cibernética, a informação em si pode ser classificada como uma vulnerabilidade. Em todos os exemplos acima, o comprometimento de informações leva diretamente a um impacto sobre o ativo, seja de caráter pessoal, ou na sociedade, em geral.

Assim como a segurança da informação se expandiu nos conceitos de segurança de TIC, de modo a proteger a informação em si, independentemente da sua forma e/ ou localização atual, a segurança cibernética precisa ser vista como uma expansão da segurança da informação. A segurança cibernética deve proteger mais do que apenas a informação, ou recursos de sistemas de informação de uma pessoa e/ ou organização. A segurança cibernética trata da proteção do pessoal, usando recursos em um ambiente cibernético, e também da proteção de quaisquer outros ativos, incluindo os que pertencem à sociedade, em geral, os quais foram expostos aos riscos ocasionados pelas vulnerabilidades decorrentes do uso das TIC.

A partir da discussão acima, conclui-se que na segurança de TIC o que deve ser protegido é a tecnologia subjacente. No caso da segurança da informação, os ativos a serem assegurados são a informação em conjunto com as tecnologias subjacentes. No entanto, no caso da segurança cibernética, o objetivo não é garantir o ciberespaço, mas sim proteger aqueles que utilizam o ciberespaço, sejam indivíduos, organizações ou nações.

Diante do exposto, a segurança cibernética pode ser resumidamente definida como a proteção do próprio ciberespaço com o objetivo principal de proteger aqueles que utilizam este meio, sendo estes o próprio indivíduo, organizações ou até mesmo as nações, representadas pelos seus governos. O próximo capítulo irá mostrar as vulnerabilidades existentes a bordo dos navios de guerra brasileiros, realçando a importância que deve ser dada a segurança cibernética pela MB.

7 SISTEMAS VULNERÁVEIS USADOS A BORDO DOS NAVIOS DA MB

Neste capítulo, serão apontados os sistemas existentes a bordo dos navios da MB vulneráveis a ataques cibernéticos. Também serão mostradas as aberturas, passíveis de penetração por um intruso, existentes nas redes dos navios.

7.1 Sistemas SCADA

As ameaças contra segurança dos ativos de serviços públicos foram reconhecidas por décadas. Após os ataques terroristas em 11 de setembro de 2001, foi dada uma grande atenção a segurança de infraestruturas críticas. Sistemas de computador inseguros podem levar a perturbações catastróficas, divulgação de informações sensíveis, e fraudes. As ameaças cibernéticas resultam da exploração de vulnerabilidades do sistema cibernético por usuários com acesso não autorizado. Uma potencial ameaça cibernética aos sistemas de controle de supervisão e aquisição de dados (SCADA), é observada desde o sistema de computador até os aspectos do sistema de energia. Um ataque pode ser executado a qualquer momento, uma vez que a segurança do sistema de computador esteja comprometida. O poder cada vez maior da internet facilita ataques simultâneos de vários locais. O mais alto impacto de um ataque ocorre quando um intruso ganha acesso ao controle de um sistema SCADA e inicia o domínio das ações que podem causar danos catastróficos.

Desde a década de 1970, a estrutura do centro de controle evoluiu gradualmente de uma estrutura de regime fechado para um ambiente de rede mais aberto. Com a tendência recente de usar protocolos padronizados, mais utilitários estão se movendo em direção ao sistema baseado em protocolos de internet (IP) para comunicação em área ampla. A compatibilidade dos padrões também alavancou o custo de implantação do sistema entre os fornecedores para melhorar a capacidade de atualização do mesmo. No entanto, uma integração mais rigorosa também pode resultar em novas vulnerabilidades. Os riscos de vulnerabilidade associados a conexão dos sistemas SCADA à internet são conhecidos (ERICSSON, 2007). A preocupação da segurança com a troca de informações entre várias entidades se torna cada vez mais desafiadora à medida que o potencial das ameaças cibernéticas crescem. A crescente dependência das comunicações pela internet contribuiu de maneira significante para o tamanho e magnitude do problema. Portanto, a conscientização de segurança e treinamento de pessoal sobre sistemas de controle de supervisão são cruciais (AMIN, 2002). Um relatório recente comparando a segurança em diferentes diretrizes e padrões foi fornecido para enfatizar os elementos críticos da segurança cibernética para sistemas SCADA (ELECTRA, 2007). Pesquisas recentes enfatizam a modelagem de dependência da segurança que inclui sabotagem deliberada e a melhoria na arquitetura de informação do sistema de energia e interação de comunicação (DONDOSSOLA et al., 2006). O desenvolvimento do banco de testes dos sistemas SCADA é uma maneira eficaz de identificar as vulnerabilidades da segurança cibernética. (DAVIS et al., 2006). LEÓN, VITTALV

e MANIMARAN (2007) propõem uma nova abordagem usando a tecnologia de sensores sem fio para avaliar a saúde mecânica de um sistema de transmissão. O desenvolvimento de técnicas quantitativas para dependência de sistemas é relatado por NICOLN, SANDERS e TRIVEDI (2004) em *"Model-based evaluation from dependability to security"*. Atualmente, existem técnicas de detecção de ataques baseadas em modelos para detectar anomalias e reconhecer assinaturas eletrônicas maliciosas (GIORDANO; FELDMAN, 2001).

Através de uma intranet, cada subestação geograficamente dispersas são configuradas com uma rede dial-up para fins de manutenção. Além disso, redes sem fio podem ser instaladas para comunicação local. A rede privada virtual (VPN) é uma tecnologia de segurança cibernética usada para se conectar a outras redes corporativas.

Programas de acesso remoto na VPN fornecem a capacidade de controlar outras máquinas dentro das redes. Esses pontos de acesso podem ser protegidos por senha (MCCLURE; SCAMBRAY; KURTZK, 2003). Um intruso bem-sucedido em uma subestação baseada em ethernet permite que um invasor realize ações potencialmente prejudiciais. Isso inclui a criação de dados falsos para causar operações indesejadas de dispositivos de proteção.

O acesso conveniente aos recursos da internet e aos recursos de pesquisa online fornecem uma base sistemática para os hackers identificarem a postura de segurança de uma organização. Existem ferramentas de invasão cada vez mais sofisticadas que incluem:

1) Discagem de guerra: Pode ser executada nos scripts para os números ao redor, de modo a detectar possíveis conexões quando o prefixo do número de telefone principal é determinado;

2) Varredura: Examina os endereços IP de destino para determinar as portas de serviço na máquina que estão sendo executadas ou em estado de escuta para conexão a possíveis pontos de acesso;

3) Farejador de tráfego: O analisador de rede é usado para capturar os pacotes que atravessam uma rede; e

4) Quebra de senha: Um programa que tenta adivinhar repetidamente uma senha para obter acesso, não autorizado, a uma rede.

Com as informações e ferramentas disponíveis, há várias maneiras possíveis de penetrar as conexões existentes de uma rede, através de VPN, conexões dial-up, conexões sem fio, qualquer programa de acesso remoto e cavalos de troia (em portas de serviço desconhecidas). Informações necessárias podem ser obtidas de diferentes ferramentas e recursos para determinar endereços IP nas redes. A detecção de uma conexão VPN por um hacker indica o que os defensores estão tentando proteger. Cavalos de Troia podem usar portas de serviço desconhecidas para estabelecer uma conexão remota.

7.2 Sistema de Navegação

Os principais equipamentos do sistema de navegação e que compõem o ciberespaço de um navio são: GPS, AIS e ECDIS.

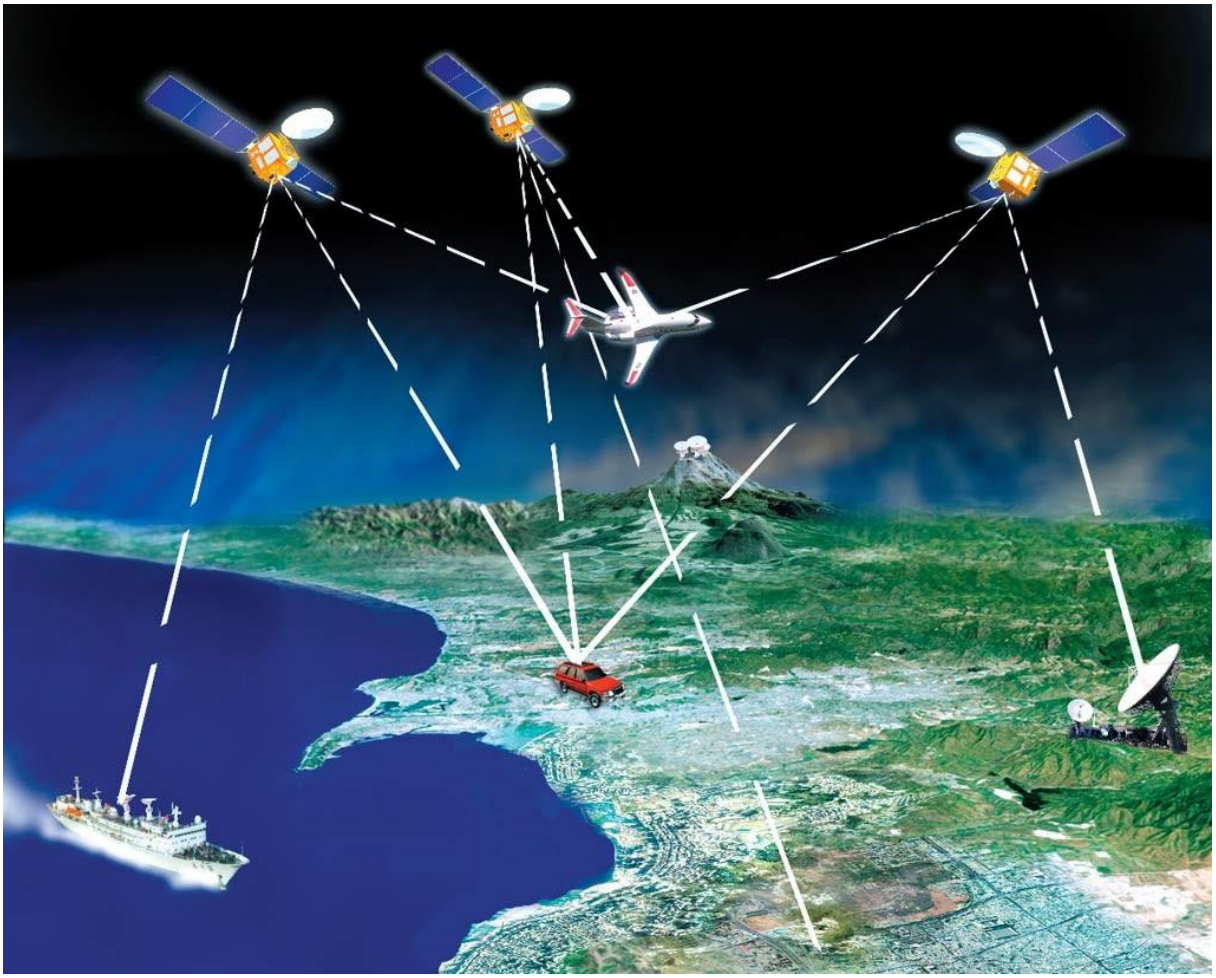
GPS: O Sistema de Posicionamento Global foi originado do projeto NAVSTAR GPS (Navigation Satellite with Global Positioning System) no ano de 1973. O desenvolvimento dessa tecnologia foi concluído no final de 1994 e começou a ser usado em sistemas de controle de embarcações. O sistema GPS que é mostrado na Figura 1, é composto por 3 segmentos principais. Estas partes podem ser classificadas como:

1) Segmento espacial: Os próprios satélites GPS;

2) Sistema de controle: Operado por uma autoridade; e

3) Segmento de usuários: Que inclui usuários militares e civis e seus equipamentos de GPS.

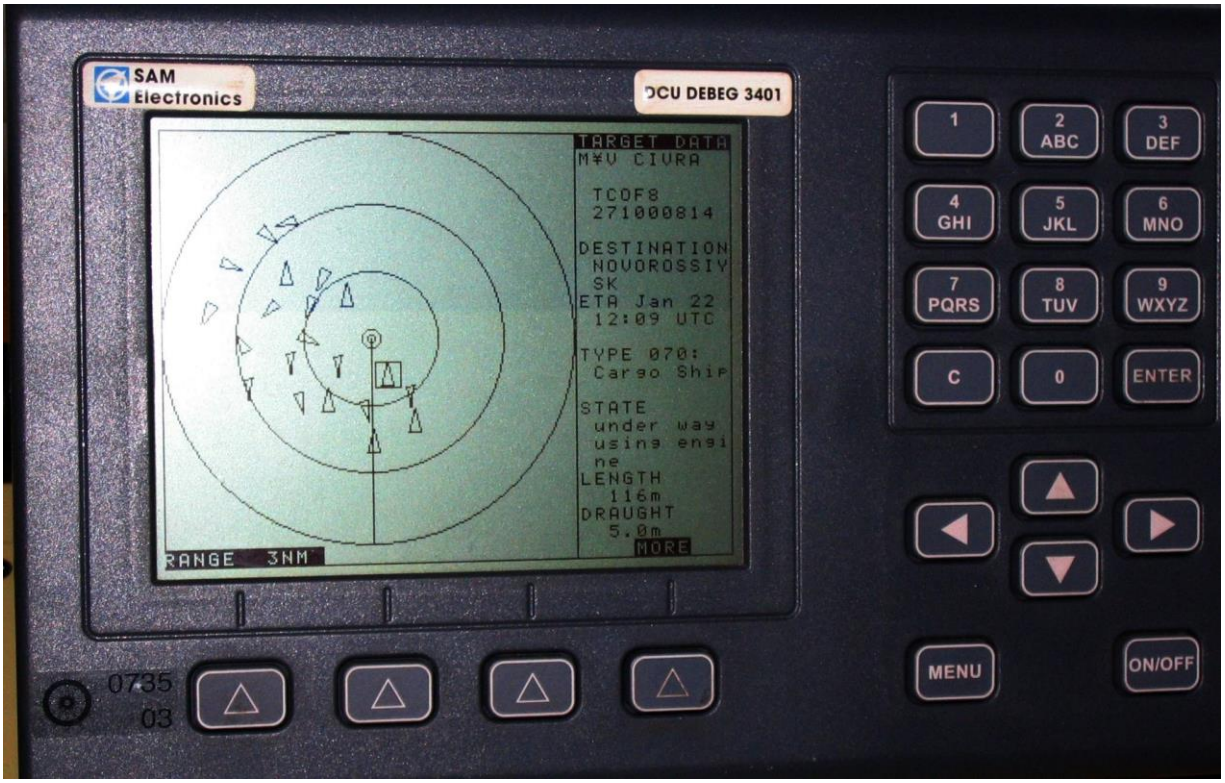
Figura 1 – Princípio do sistema GPS



Fonte: www.naval.com.br (2018).

AIS: Imagine um radar de bordo ou um mostrador de carta eletrônica que inclua um símbolo para cada embarcação significativa dentro da faixa de rádio, cada um com um vetor de velocidade (indicando velocidade e rumo). Cada símbolo do navio pode refletir o tamanho real do navio, com a posição e precisão do GPS conforme mostrado na Figura 2.

Figura 2 – Dispositivo AIS



Fonte: www.seanews.co.uk (2018).

ECDIS: O sistema ECDIS utiliza uma estação de trabalho com Windows XP. Ele normalmente inclui radar, mas também possui sensores relacionados a NAVTEX (Navigational Telex), AIS, direções de navegação, fixação de posição, registro de velocidade, ecobatímetro, anemômetro e medidor de temperatura. Esse sistema é conectado à LAN (Local Area Network) do navio (via adaptadores especiais), incluindo gateways para a internet. O ENC (Electronic Navigation Charts) é carregado no ECDIS e é usado pelo oficial do navio para pilotar, navegar e monitorar a velocidade do navio. A Figura 3 ilustra a utilização do sistema ECDIS no passadiço de um navio.

Figura 3 – Sistema ECDIS

Fonte: www.nauticexpo.com (2018).

7.3 SICONTA (Sistema de Controle Tático)

O SICONTA é um sistema de controle tático e de armamentos que possui um elevado grau de modularidade. Seu sistema é configurado para instalação em praticamente qualquer tipo de navio ou submarino. Esse sistema é um dos melhores de sua categoria ao nível mundial, pois possui um porte compacto, escalabilidade e é de simples operação, além de ter sido utilizadas várias tecnologias de ponta ao longo do seu projeto (IPQM, 2018).

O SICONTA integra as armas e os sensores do navio ao cenário tático de operação, a fim combater, com mais eficácia, às ameaças previstas. E tem por finalidade executar automaticamente as funções que, antes do advento dos computadores digitais, eram desempenhadas pelos operadores (CASTRO SOBRINHO, 2007). Na Figura 4, pode-se observar o SICONTA dentro do COC (Centro de Operações de Combate) de uma fragata classe Niterói.

Figura 4 – SICONTA

Fonte: www.naval.com.br (2018).

7.4 Sistema FÊNIX

O Sistema Fênix é um banco de dados que foi desenvolvido com o intuito de prover, aos diversos equipamentos de MAGE (Medidas de Apoio a Guerra Eletrônica) da MB, bibliotecas de emissores adequadas.

Esse sistema gera automaticamente as Ordens de Batalha Eletrônica para os diversos equipamentos de MAGE que dotam os navios da Esquadra brasileira, utilizando um banco de dados de características eletromagnéticas, formado ao longo do tempo, composto por registros obtidos pelas unidades da MB envolvidas nas atividades de GE.

8 CONCLUSÃO

O presente trabalho buscou analisar vários conceitos da Guerra Cibernética. Os aspectos apresentados foram montados a partir de pesquisas realizadas e da experiência do autor.

Dessa forma, este trabalho apresentou em seus capítulos iniciais as definições da Guerra Cibernética. Cabe destacar o conceito de que a Guerra Cibernética é a guerra travada entre dois ou mais elementos, sendo eles o Estado ou outros agentes atuantes no ciberespaço. Portanto, esta é uma atividade que requer uma atenção especial por parte do governo representado pelas suas Forças Armadas, e no caso deste estudo, pela MB.

Além das diversas vantagens para a sociedade moderna, como a internet, o ciberespaço trouxe consigo muitas formas de ameaça, que de maneiras diversas, utilizam o ambiente cibernético para causar danos aos indivíduos, organizações ou, até mesmo, às nações. Esses métodos podem variar do acesso a informações, por meio da ciberespionagem, a danos provocados por invasores a um sistema que possa estar ligado a alguma rede de dados, por exemplo. Tem-se por meio da segurança cibernética, uma forma de se proteger dessas ameaças.

Com base nos fundamentos apresentados ao longo do trabalho, acredita-se na necessidade de se dar uma maior atenção para a questão da segurança cibernética, em paralelo a investimentos na área de Guerra Cibernética. Sugere-se que a MB envide esforços para que seus militares estejam a par desse assunto e que os mesmos possam se capacitar na defesa de seus sistemas de informação e operativos.

Referências

AMIN, M. Security challenges for the electricity infrastructure. **IEEE Secur. Priv.**, v. 35, n. 4, p. 8 – 10, 2002.

BOLENG, J.; SCHWEITZER, D.; GIBSON, D. S. Developing Cyber Warriors. U.S. Air Force Academy, EUA, 2008. Disponível em: <http://www.edocfind.com/download.pdf>. Acesso em: 19/05/2018.

BOYES, H.; ISBELL, R. Code of Practice: Cyber Security for Ships. Institution of Engineering and Technology, Londres, Reino Unido, 2017.

CASTRO SOBRINHO, A. da S. Configuração de Sistemas de Combate no Processo de Obtenção e Modernização de Navios de Superfície. Tese (Curso de Politica e Estratégia Marítimas) – Escola de Guerra Naval, Rio de Janeiro, 2007.

DAVIS, C. M.; TATE, J. E.; OKHRAVL, H.; GRIER, C.; OVERBYE, T. J.; NICOL, D. SCADA cybersecurity test bed development. **in Proc. 38th North Amer. Power Symp**, p. 483 – 488, Setembro 2006.

DHILLON, G. Principles of information systems security. John Wiley & Sons, Nova Jersey, EUA, 2007.

DICIO. Dicionário Online em Português. 2018. Disponível em: <https://www.dicio.com.br/pesquisa.php?q=cibernética>. Acesso em: 23/05/2018.

DONDOSSOLA, G.; DECONINCK, G.; GIANDOMENICO, F. D.; DONATELLI, S.; KAANICHE, M.; VERISSIMO, P. Critical utility infrastructural resilience. in Proc. Complex Network and Infrastructure Protection, p. 28 – 29, Março 2006.

ELECTRA. Security for Information Systems and Intranets for Electric Power Systems. **ELECTRA Tech. Brochure**, v. 231, n. 317, p. 70 – 81, 2007.

ERICSSON, G. N. Toward a framework for managing information security for an electric power utility—CIGRÉ experiences. **IEEE Trans. Power Del**, v. 22, n. 3, p. 1461 – 1469, 2007.

EUA. International strategy for cyberspace: prosperity, security, and openness in a networked world. THE WHITEHOUSE, EUA, 2011. Disponível em: <http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>. Acesso em: 19/05/2018.

GAMA NETO, R. B. Guerra cibernética / guerra eletrônica – conceitos, desafios e espaços de interação. **Revista Política Hoje**, v. 26, n. 1, p. 201 – 217, 2017.

GERBER, E.; SOLMS, R. V. Management of risk in the information age. **Computers & Security**, v. 24, n. 1, p. 16 – 30, 2005.

GIORDANO, J.; FELDMAN, J. A process control approach to cyber attack detection. **Commun. ACM**, v. 44, n. 8, p. 76 – 82, 2001.

INFORMATION WARFARE MONITOR. Tracking GhostNet: Investigating a Cyber Espionage Network. Information Warfare Monitor, Canadá, Março 2009. Disponível em: <http://www.nartv.org/mirror/ghostnet.pdf>. Acesso em: 19/05/2008.

IPQM. Grupo de Sistemas Digitais. INSTITUTO DE PESQUISAS DA MARINHA, 2018. Disponível em: <https://www.marinha.mil.br/ipqm/grupo_sistemas_digitais>. Acesso em: 23/05/2018.

ISO/IEC. ISO/IEC TR 13335-1:2004: Information technology security techniques management of information and communications technology security part 1: concepts and models for information and communications technology security management. Genebra, Suiça, 2004.

ISO/IEC. ISO/IEC 27002: Code of practice for information security management. Genebra, Suiça, 2013.

ITU. ITU-TX.1205: Series X: data networks, open System communications and security: telecommunication security: overview of cybersecurity. INTERNATIONAL TELECOMMUNICATIONS UNION, Genebra, Suiça, 2008.

KLIMBURG, A. National Cyber Security Framework manual. NATO CCD COE Publications, Tallin, Estônia, 2012.

LEÓN, R. A.; VITTALV, V.; MANIMARAN, G. Application of sensor network for secure electric energy infrastructure. **IEEE Trans. Power Del**, v. 22, n. 2, p. 1021 – 1028, 2007.

MCAFEE. Virtual Criminology Report 2009 - Virtually Here: The Age of Cyber Warfare. McAfee Inc, Santa Clara, EUA, 2009. Disponível em: <http://www.mcafee.com/us/local_ content/reports/virtual_criminology_2009.pdf>. Acesso em: 23/05/2018.

MCCLURE, S.; SCAMBRAY, J.; KURTZK, G. Hacking Exposed: Network Security Secrets and Solutions. Emeryville, CA: McGraw-Hill/ Osborne, 2003.

MITNICK, K.; SIMON, W. The art of deception: controlling the human element of security. Wiley Publishing, Indianápolis; EUA, 2002.

NICOLN, D. M.; SANDERS, W. H.; TRIVEDI, K. S. Model-based evaluation from dependability to security. **IEEE Trans. Depend. Secure Comput**, v. 1, n. 1, p. 48 – 65, 2004.

NUNES, L. A. R. Guerra Cibernética: está a MB preparada para enfrentá-la? Tese (Curso de Politica e Estratégia Marítimas) – Escola de Guerra Naval, Rio de Janeiro, 2010.

RID, T. Cyber War Will Not Take Place. **Journal of Strategic Studies**, v. 35, n. 1, p. 5 – 32, 2012.

SOLMS, R. V. Information security management (3): the code of practice for information security management (BS 7799). Information Management & Computer Security., Porto Elizabeth, África do Sul, 1998.

THEOHARIDOU, M.; GRITZALIS, D. Common body of knowledge for information security. Security & privacy. IEEE, 2007. Disponível em: <http://ieeexplore.ieee.org.> Acesso em: 21/05/2018.

UK. The UK cyber security strategy: protecting and promoting the UK in a digital world. MINISTER FOR THE CABINET OFFICE AND PAYMASTER GENERAL, Reino Unido, 2011. Disponível em: <http://www.cabinetoffice.gov.uk/sites/default/files/resources/WMS_The_ UK_Cyber_Security_Strategy.pdf>. Acesso em: 21/05/2018.

WHITMAN, M. E.; MATTORD, H. J. Principles of information security. Thompson Course Technology, Atlanta, EUA, 2009.

WOOD, C. C. Why information security is now multi-disciplinary, multi-departmental, and multi-organizational in nature. **Computer Fraud & Security**, v. 1, n. 1, p. 7 – 16, 2004.