ESCOLA DE GUERRA NAVAL

CC Emanuel Ferreira Jesus

SISTEMA DE MONITORAMENTO CONTÍNUO PARA REDES DE TECNOLOGIA DA AUTOMAÇÃO.

Rio de Janeiro

2021

CC Emanuel Ferreira Jesus

SISTEMA DE MONITORAMENTO CONTÍNUO PARA REDES DE TECNOLOGIA DA AUTOMAÇÃO.

Monografia apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso Superior.

Orientador(a): Miguel Henrique Alexandre Dias Alves

Rio de Janeiro

Escola de Guerra Naval

2021

AGRADECIMENTOS

A Deus por ter me dado saúde, força e sabedoria para suplantar os obstáculos e me permitir êxito nesta importante etapa profissional.

À minha família, pela compreensão, paciência, apoio e incentivo que sempre serviram de alicerce para as minhas realizações.

Ao meu orientador, Capitão de Corveta Miguel Henrique Alexandre Dias Alves, pela paciência e pelas contribuições que enriqueceram este trabalho. Estimo muito tê-lo como companheiro de turma.

Aos coordenadores e instrutores do C-Sup 2021, pelos conhecimentos transmitidos, sempre prezando pela qualidade e excelência do ensino.

Por fim aos meus amigos e amigas do C-Sup 2021 que compartilharam dos inúmeros desafios com o espírito de colaboração e camaradagem.

RESUMO

Este trabalho intenciona identificar ameaças em redes de tecnologia da automação e propor uma estrutura capaz de monitorar ataques nessas mesmas redes e, por fim, propor requisitos que devem ser observados para que novos meios navais sejam capazes de monitorar tais eventos. Para isso apresenta incidentes que foram observados em redes industriais e, os danos gerados por esses ataques e os possíveis impactos aos navios de guerra. Sua relevância vem do fato de não existir, no presente momento, um sistema capaz de detectar ações adversas em redes industriais usadas nos navios da MB. A pesquisa bibliográfica revisou *frameworks*, normas internacionais, conceitos e procedimentos relacionados à defesa cibernética, que podem ser usados em redes de automação. A partir disso, propõe-se um sistema de monitoramento contínuo para incrementar a maturidade e proteção cibernética desses sistemas, em especial aos novos meios navais. Este sistema será formado por um conjunto de procedimentos, software e hardware já consolidados na MB, que, com adaptações, é aplicável também nessas redes. A solução apresentada aponta um caminho para solucionar o problema da falta de monitoramento contínuo em redes de TA nos meios operativos da MB, contribuindo para o incremento da proteção cibernética dos navios da MB.

Palavras-chave: defesa cibernética, rede de automação industrial, sistemas de controle, monitoramento contínuo.

SUMÁRIO

1 INTRODUÇÃO

As redes de Tecnologia da Automação (TA) servem para controlar o fluxo de dados e gerenciam os processos de automação, para isso fazem uso de sensores, computadores, atuadores, posicionadores e controladores lógicos programáveis (PLC). A interação de todos esses ativos e dispositivos é responsável pelas mais diversas ações, desde o simples monitoramento de temperatura até o controle e coordenação de processos físicos, como controle de motores (CHRISTIANO, 2018). Além da indústria, essas redes estão mudando significativamente os meios militares, pois permitem melhora no suporte à manutenção preditiva e integração entre os sistemas.

A grande maioria das implementações de redes de TA são industriais, mas, devido ao seu alcance e melhoria de processos, estão cada vez mais presente em todas as implementações que requerem uso de controle industrial, inclusive em meios navais. É possível notar seu crescente uso na Marinha através da sua presença na modernização dos meios navais com a instalação dos sistemas SCMPA[1] e SCAV[2] (PEREIRA, 2011). Também estão presentes na construção e aquisição de novos meios como navios patrulhas oceânicos, submarinos da classe *Scorpène*, e recentemente, a aquisição, por construção, de fragatas classe Tamandaré. Essa classe de navio possui seus sistemas de navegação, controle de propulsão e sistemas de armas baseados em algum tipo de rede de TA (AGUAS, 2021). Além dos exemplos acima, podemos encontrá-la também nos sistemas de apoio à manutenção preditiva (CAMBRA, 2016).

A evolução das redes de TA passou por avanços ao longo do tempo. Essa evolução ocorreu principalmente por causa das limitações relacionadas ao tempo de resposta dos dispositivos. A necessidade de melhoria levou ao desenvolvimento de novas topologias, aumento da velocidade de comunicação, e de largura de banda. Mas, um grande problema é a priorização dada às garantias de envio e recebimento de dados, que são voltadas ao desempenho em detrimento da segurança.

A Segurança da Informação e Comunicações (SIC) está madura, mas os esforços destinados aos programas de segurança cibernética voltados às redes de TA ainda são incipientes. Vemos a escalada dos ciberataques a redes de automação e precisamos nos preparar. Logo a implementação de medidas de segurança cibernética devem ocupar um lugar

1SCMPA: Subsistema de Controle e Monitoração de Propulsão e Auxiliares, tem por objetivo monitorar e controlar a propulsão do navio (IPQM, 2021)

2 SCAV: Sistema para uso em navios civis e militares que controla e indica, em tempo real, a presença de fumaça, temperatura e alagamento, fornecendo informações para tomada de decisão (EMGEPRON, 2021).

de destaque também nessas redes. *Frameworks*[3] de segurança, como o "NIST *Cybersecurity Framework*" e o "IEC 62443", recomendam a adoção de mecanismos de monitoramento contínuo. O monitoramento contínuo das mensagens do protocolo durante a operação proporcionam, além, do conhecimento do status da sua rede a qualquer momento, a detecção e a ocorrência de um ataque cibernético.

A estrutura de uma rede de automação envolve uma topologia complexa, mas a tecnologia envolvida, normalmente, demora anos para sofrer uma atualização, o que a torna alvo potencial para ataques. Quando ocorre um ataque o faz-se necessário que o processo para a tomada de decisão seja rápido, pois o tempo decorrido entre o ataque cibernético e a ocorrência de um incidente de rede é curto (QUEIROZ, 2018). O que evidencia a necessidade de ferramentas com a capacidade detecção.

O problema a ser discutido é a falta de tecnologias que dotem os novos navios da Marinha com a capacidade de detectar anomalias nas redes de TA. Pretende-se também, elaborar requisitos de sistemas que precisam ser observados quando da aquisição de um novo meio naval. Para tanto, pretende-se responder a seguinte questão: Como preparar os novos navios da Marinha para serem capazes de detectar ataques cibernéticos nas redes de Tecnologia da Automação?

Existem normas para segurança de sistemas de TIC na MB, como a DGMM 0540 (BRASIL, 2019), no entanto, os modelos e requisitos de TIC não são totalmente aderentes às redes de TA. Pois, nas redes corporativas dá-se prioridade à confidencialidade, integridade e disponibilidade, nessa ordem, e as redes de TA se baseiam em disponibilidade, integridade e confidencialidade (CHRISTIANO, 2018). Assim, é mister que se busque na literatura e nos manuais de boas práticas o conhecimento dos fundamentos de TIC que garantam as redes TA a segurança necessária.

Dessa forma, para os pressupostos teóricos, serão usados as principais ameaças presentes no espaço cibernético, e serão adotadas as Cartilhas de Segurança para Internet (CERT.BR, 2012) e Segurança da Informação: princípios e práticas (STALLINGS e BROWN, 2014). Estes normativos não abordam especificamente a questão da segurança física e lógica das redes de TA, mas são referências para a definição de ameaças e boas práticas. Para tratar das redes industriais serão adotados como pressupostos teóricos os *frameworks* NIST (NIST, 2018 e NIST, 2015) e IEC-62443 (ISA, 2010).

3 Framework: é uma estrutura de apoio, formada por padrões, guias e melhores práticas para gerenciamento de risco cibernético (NIST, 2018).

Tendo em vista a amplitude do assunto, esta pesquisa se limita a destacar os aspectos de segurança da informação, os principais ataques cibernéticos que afetam as redes de TA, enfatizando o alcance, e os problemas causados por esses ataques.

Será apresentado a descrição do sistema de monitoramento contínuo e como esse sistema pode ser empregado para aumentar a consciência situacional da rede de TA e descrever como o processo de monitoramento é capaz de identificar comportamentos anômalos nessas redes.

Por último, para elaborar os requisitos de sistemas relacionados ao monitoramento e a segurança cibernética que devem ser avaliados quando a Marinha adquirir um novo meio naval será empregada a norma ISO-15408 (ISO, 2008).

Proteger os meios Navais contra ameaças sofisticadas é desafiador. Há lacunas sobre como detectar e apresentar os eventos de segurança coletados nas redes de TA. Dessa forma, este estudo é relevante por identificar como o monitoramento contínuo ajuda na detecção dos eventos de segurança, consequentemente, aumentando a consciência situacional cibernética.

De forma para atingir esse objetivo, foi realizada uma pesquisa bibliográfica em artigos, órgãos governamentais dedicados na área e sites com informações pertinentes aos diversos assuntos. Para dar fundamento ao objetivo geral foram definidos os seguintes objetivos específicos:

- Descrever as diversas tecnologias disponíveis para implementar um sistema de monitoramento contínuo em rede de TA;

- Elaborar requisitos de sistemas de monitoramento de segurança necessários para aquisição de um novo meio; e

- Identificar os principais tipos de ameaças às redes de TA existentes no espaço cibernético;

As seguintes respostas serão buscadas pelo estudo:

- Como preparar os navios da marinha para serem capazes de detectar ataques cibernéticos nas redes de TA?

- Quais Requisitos de Sistemas são necessários quando da aquisição de um novo meio naval?

- Quais são as principais ameaças às redes de TA existentes no espaço cibernético que podem prejudicar o funcionamento dos sistemas dos navios?

Será realizada uma pesquisa descritiva, seguindo um processo por etapas, de forma lógica e sucessiva, por meio de análise textual e interpretativa partindo dos documentos

em referência (NIST, 2015; NIST, 2018; ISA, 2010; ISO, 2017), com uma compreensão global, baseada em análise pessoal. Este trabalho será baseado em pesquisa bibliográfica e documental, investigando o problema descrito, tendo como partida dos estudos um referencial teórico existente e busca por fontes primárias, coletadas em monografias e teses da EGN e em periódicos especializados.

Este estudo está dividido em cinco capítulos. A divisão foi feita desta forma com o objetivo de facilitar a leitura e percepção. Iniciamos com esta introdução, onde apresentamos o problema de pesquisa e os objetivos. O segundo capítulo tem a função de mostrar, com exemplos reais, a relevância do problema, sua extensão e os grandes impactos que pode causar. O terceiro capítulo busca identificar as ameaças e as principais vulnerabilidades das redes de TA. No quarto capítulo são apresentados os benefícios de um sistema de monitoramento, uma proposta de topologia usando ferramentas desenvolvidas na Marinha e são apresentados os requisitos mais importantes para que novos meios possam dispor de um sistema de monitoramento contínuo. Por fim, no quinto capítulo o trabalho é concluído correlacionando os assuntos expostos com os benefícios da solução proposta para a detecção de incidentes. Mostrando que o monitoramento feito da forma adequada contribui para a prontidão do meio e que para construir um sistema de monitoramento contínuo eficiente alguns requisitos devem ser observados.

2 HISTÓRICO DE ATAQUES

É necessário entender a evolução dos ataques às redes de TA e seus agentes causadores, a fim de preparar uma defesa eficaz. Neste capítulo, serão apresentados vários incidentes de segurança cibernética envolvendo infraestruturas críticas[4] para permitir o entendimento da natureza desses ataques e como eles podem ser realizados no futuro. Como não há ataques relatados a redes de TA de navios de guerra, usaremos os estudos e relatos de ataques a infraestruturas críticas. O objetivo deste capítulo é mostrar que existem precedentes de ataques às redes de TA e os impactos decorrentes, com isso mostrar a necessidade da preparação dos meios navais para enfrentar essas ameaças. Existem diversas medidas de proteção, sendo uma delas o monitoramento contínuo, que será apresentado no Capítulo 4.

Historicamente, os sistemas SCADA eram usados em redes segregadas usando protocolos não padronizados para protegê-los de ataques. Conforme a tecnologia foi difundida

4 infraestruturas críticas: São aquelas instalações, serviços e bens cuja interrupção ou destruição provocará sério impacto social, econômico, político, internacional ou à segurança nacional (BRASIL, 2020)

e ganhou escala, essas redes também começaram a ser conectadas a redes corporativas. Devido a sua natureza crítica começaram a ser alvos mais atrativos para grupos *hacktivistas*[5] e atividades de agentes estatais. Esses fatores somados contribuem para o aumento do número de ataques ao longo do tempo. Esse fato é corroborado pelo relatório semestral do centro de resposta a incidentes cibernéticos em redes industriais elaborado pela *karsperky* (2020). De acordo com o relatório, no segundo semestre de 2020, ocorreu um aumento de 62% de *malwares* em 2019.

2.1 Eventos passados

O primeiro caso analisado é o *Stuxnet*[6]. Esse artefato malicioso foi projetado para trabalhar de forma modular. Primeiro realiza uma infecção indiscriminada, se espalhando de um computador para outro até encontrar seu alvo. A próxima etapa é a busca pelo alvo, característica que o diferencia de outros da mesma categoria. Nesta etapa fica evidenciado o propósito de construção do *malware*, ele foi projetado para atacar somente quando encontrar um sistema industrial específico, nesse caso, os controladores lógicos programáveis (PLC) da central de enriquecimento nuclear do Irã. Por fim, sua última etapa é alterar as configurações que realizam o controle de velocidade das centrífugas, com essa alteração as centrífugas giram de forma desordenada (DENNING, 2012). O impacto no programa nuclear iraniano foi grande, paralisando-o por anos. Outro aspecto que chama muita atenção é a sua complexidade, fato que leva a crer que os agentes estatais foram responsáveis pelo seu desenvolvimento (FALLIERE *et al.*, 2011).

Do ponto de vista da segurança é preciso identificar os pontos fracos que permitiram a execução do *malware*. É possível citar duas vulnerabilidades críticas que contribuíram para que o *Stuxnet* fosse bem sucedido na infiltração da rede, na propagação interna e na alteração das configurações dos PLC. O primeiro ponto foi a infiltração manual. Os responsáveis pela implementação da segurança não consideraram o agente interno durante as avaliações de risco, com isso medidas de segurança deixaram de ser implementadas para a proteção contra uso de dispositivos portáteis, e mesmo que o uso seja permitido a sua utilização deve ser monitorada. O segundo ponto foi a propagação na rede interna, que era uma rede segregada, até encontrar um PLC de controle da centrífuga. Essa propagação bem sucedida mostra que não havia qualquer sistema de monitoramento para alarmar comportamentos anormais na rede (LENDVAY, 2016).

5 Atividade hacktivista: é o uso de ferramentas digitais com fins políticos, é a junção de ferramentas usadas para invasão a sistemas de informação com o ativismo político (MACHADO, 2013).
6 Stuxnet: é o nome de um malware. Maiores informações sobre malware vide anexo A.

O segundo caso analisado é a operação *Orchard* (ERICH e HOLGER, 2009). Operação militar realizada por Israel com o objetivo de destruir uma instalação nuclear Síria. As aeronaves da força aérea israelenses sobrevoaram a Síria sem serem detectadas, realizaram o ataque sem que houvesse resistência e retornaram à base em segurança. Diversas foram as teorias aventadas para explicar como os aviões não foram detectados. Duas dessa teorias dizem respeito à segurança cibernética. A primeira teoria é que o sistema de defesa antiaéreo da Síria possuía uma bomba lógica[7], que foi ativada com auxílio da guerra eletrônica. Os radares da defesa foram irradiados com uma determinada forma de onda que ativou o código da bomba lógica. A segunda teoria afirma que os israelenses entraram nas redes sírias muito antes do ataque, e com isso tiveram tempo para conhecer o sistema e realizar alterações no código do sistema de defesa antiaéreo (WIRED, 2007; CLARK e ROBERT, 2014). Do ponto de vista da guerra cibernética é a primeira vez que se tem notícia do seu uso em apoio a uma operação militar, o que mostra a importância do domínio dessa dimensão da guerra (PARMENTER, 2013).

Embora não haja ataques relatados a navios de guerra, existe histórico de navios mercantes como alvo. Segundo a ZNET (2020) as quatro maiores empresas de navegação comercial sofreram ataques cibernéticos nos últimos anos. Além de seus *data centers* em terra, alguns navios também foram alvos dos ataques. As empresas notaram aumento nos incidentes de *malware* em busca de sistemas embarcados, em resposta a isso criaram uma série de guias e boas práticas a serem observadas a bordo dos navios.

Por último, o evento do *malware* denominado *BlackEnergy* (PETERSON, 2016). Este fato marca a primeira vez na história que um atacante usou a interrupção da distribuição de energia elétrica como uma forma de guerra cibernética. A lição mais importante a observar neste ataque é que o *malware* não foi projetado, inicialmente, para explorar vulnerabilidades em redes de TA ou sistemas SCADA. Os atacantes dividiram o ataque em três fases, realizaram uma campanha silenciosa e sem pressa. Durante dez anos espalharam um *trojan*[8] pela internet. Na segunda fase, após milhares de computadores infectados, realizou-se uma análise nos dispositivos alvo e descobriram que um dos computadores infectados controlava um sistema SCADA. Por fim, iniciaram a última fase quando ganharam acesso ao sistema que controlava trinta subestações de energia da Ucrânia, e realizaram alterações de forma a garantir o acesso. Com isso, desde 2015 a Rússia vem realizando blecautes seletivos na

7 Bomba lógica: é um código malicioso inserido secretamente em uma rede de computadores, sistema operacional ou aplicativo de software. Ele permanece adormecido até que uma condição específica ocorra. Quando essa condição é atendida, a bomba lógica é acionada (AVAST, 2021).

8 Trojan: vide anexo A

Ucrânia. Esta é a primeira vez que um ataque cibernético foi usado por um estado em um conflito internacional, na visão do autor (OTW, 2018).

2.2 Importância

O ataque do *Stuxnet* ao Irã em 2010 e os demais exemplos chamam a atenção para as vulnerabilidades das redes de TA. Eles ilustram uma necessidade premente de readequação das técnicas de segurança também nesses ambientes, a exemplo das redes corporativas.

Estes ambientes consistem em sistemas de controle industrial, geralmente em grande escala, que monitoram, gerenciam e administram infraestruturas críticas em áreas, como energia elétrica, gasodutos, energia nuclear, e rede de água. Ao contrário da rede de TI convencional, um ambiente de TA interliga os sistemas cibernéticos e industriais (físicos), tais como válvulas e sistemas de controle de armas e de propulsão. São os chamados sistemas ciber-físicos[9].

Embora redes de TA sejam implementadas principalmente na indústria , está cada vez mais presente no ambiente naval, especificamente podemos encontrá-las nos diversos sistemas de bordo que estão sendo embarcados nas modernizações dos meios navais ou na construção de novos meios. A administração sobre os sistemas físicos, realizada pelos PLC, usa um conjunto de protocolos padronizado. Para os sistemas SCADA, a comunicação é realizada com os protocolos MODBUS, DNP3 e IEC 60870-5-101[10]. Logo, é possível observar que qualquer alteração nos dados trafegados pode causar um grande impacto. Por este motivo, a integridade dos dados de controle das redes de TA é primordial.

Em determinadas situações o tempo que o dado leva para chegar ao destino é um fator crítico. Quando um sensor (radar, sonar, alça optrônica, etc) identifica que o navio está sofrendo um ataque o tempo de reação do meio é um fator capital para sua autodefesa. Logo a disponibilidade do dado na hora em que ele for necessário é outro fator crítico. Neste ponto já é possível observar a importância de evitar, ou identificar, alteração e atraso nos dados que trafegam nas redes de TA dos navios de guerra.

Ryan Hilger, Capitão de Corveta da Marinha dos Estados Unidos da América, realizou um ensaio analisando os impactos caso a China conseguisse se infiltrar nas redes norte-americanas, efetuando um ataque cibernético preventivo contra a Marinha dos EUA (HILGER, 2021). Cabe salientar que, embora o artigo tenha se baseado em ataques reais

9 Sistemas ciber-físicos: O termo refere-se a uma nova geração de sistemas com a capacidade de integrar sistemas recursos computacionais e sistemas físicos (BAHETI e GILL, 2011).

10 Protocolos MODBUS, DNP3 e IEC 60870-5-101: protocolos são as regras que governam a comunicação entre dispositivos eletrônicos. Os protocolos mais comuns na indústria são os MODBUS, DNP3 e IEC 60870-5-101 (ELETRICO, 2010)

sofridos pelos EUA, o cenário é um exercício mental. Assim, os chineses infectariam as redes alvo há uma década, conseguindo se infiltrar na cadeia de suprimento das empresas que produzem os navios de guerra, infectando todos os sistemas das redes de TA. Os *malwares* permaneceriam dormentes até que os chineses resolvessem realizar o ataque preventivo, ativando os *malwares*, o que resultaria em navios sem energia, à deriva no mar. Após a identificação do problema e retorno às condições operacionais diversos outros problemas ocorreriam, tais como falha nas comunicações e sistema de armas atirando em alvos fantasma. Neste cenário fictício haveria uma vitória sem luta. Apesar de obra de ficção, este artigo levanta questões importantes sobre a segurança cibernética dos navios: engenharia social; espionagem; controle da cadeia de suprimentos; e monitoramento de ativos.

As operações iniciam com o planejamento que tem o propósito de alcançar um determinado objetivo. Do ponto de vista cibernético, o objetivo durante uma missão é garantir que os ativos necessários se mantenham operacionais.

Nos navios o monitoramento deve ocorrer durante todas as fases da execução de uma operação, desde a preparação até a ação tática. Durante a preparação, o navio executa uma série de testes e rotinas que podem identificar se algum sistema está comprometido. Normalmente na preparação é de se esperar que alguns sistemas sejam acessados com novos dados para a missão. Podemos citar o carregamento da biblioteca de emissões magnética no MAGE[11], que pode servir de porta de entrada para um malware no sistema.

No teatro de operações pode ocorrer um evento de bomba lógica, como ensaiado por Hilger (2021) e o navio ficar totalmente paralisado. O navio pode, também, sofrer um ataque cibernético, ataque preemptivo, como ocorreu na operação *Orchard* (ERICH, 2009). Parmenter (2013) mostra a evolução dos ataques preemptivos israelenses em apoio às operações aéreas com o uso da guerra cibernética. Traçando um paralelo com as operações navais, a detecção de um ataque cibernético no curso de uma operação real, no teatro de operações, pode significar que um ataque cinético[12] está prestes a acontecer, servindo como um alarme antecipado.

Assim, o monitoramento é essencial. Com efeito, a detecção de um ataque cibernético em curso pode prejudicar o desempenho e a operacionalidade desses ativos. Além disso, quando há um evento, este deve ser analisado para determinar sua abrangência e descobrir o impacto na missão em andamento.

11 MAGE: são as medidas de apoio à guerra eletrônica, equipamento eletrônico usado para detectar e classificar emissões de radares (BRASIL, 2021).

12 Considerando que a cinética é a parte da física que estuda as mudanças de movimento produzidas pela força, pode-se estabelecer que o domínio da guerra cinética reside no mundo real – isto é não virtual – sujeito a mudanças mediante a aplicação de forças (ALMEIDA *et al.*, 2019).

3 SEGURANÇA CIBERNÉTICA E AMEAÇAS

O crescente histórico de ataques às redes de TA e a importância dessas redes para o funcionamento de diversos sistemas dos novos meios navais motivam a descrever as suas ameaças, vulnerabilidade e riscos a que essas redes estão expostas. Desta forma o objetivo deste capítulo é fornecer uma visão holística da aplicação dos protocolos SCADA, apresentar uma pesquisa que aborde as deficiências desses ativos, e identificar suas principais ameaças e vulnerabilidades. Conhecer esses riscos é importante para mostrar como um sistema bem especificado e que conte com um sistema de monitoramento contínuo pode contribuir com a preparação dos novos navios da Marinha para serem capazes de detectar ataques cibernéticos.

3.1 Redes de TA

Primeiro é interessante saber o que distingue as redes de TI das redes de TA. Segundo Gartner (2021) Tecnologia da Informação é um termo geral para sistemas e tecnologias que possuem a capacidade de processar informação, normalmente usadas para fins corporativos. Já a Tecnologia da Automação além de envolver o uso e processamento de informação também possui a capacidade de interagir com o meio físico.

A definição e o uso do termo Tecnologia da Automação não é um consenso. Há diversas nomenclaturas e sistemas que são tratados como TA: Sistema de Controle Industrial (ICS); Sistema de Controle de Supervisão e Aquisição de Dados (SCADA); Sistemas de Controle Distribuído (DCS); e Sistemas ciber físicos (Cyber Physical System – CPS) (STOUFFER *et al.*, 2014). Neste trabalho o termo Tecnologia da Automação será usado como um termo abrangente, um termo geral que envolve vários tipos de sistemas de controle, frequentemente encontrados no setores industriais e em infraestruturas críticas.

Como os sistemas de TI e TA têm finalidades diferentes, eles também possuem requisitos de segurança cibernética diversos. A segurança da TI tem o objetivo de evitar a modificação, o roubo, e a alteração de dados da empresa e garantir que esses dados somente sejam acessados por usuários autorizados. Já a segurança da TA busca controlar e manter a continuidade de processos industriais com segurança (HU, 2010). Isso acarreta uma mudança brusca nos requisitos de segurança cibernética. A SIC da TI tem como pedra basilar o tripé Confidencialidade, Integridade e Disponibilidade, com maior importância dada a Confidencialidade. Já os sistemas de TA a ordem de importância muda para Disponibilidade, Integridade e Confidencialidade (B. ZHU, 2011). Isso impacta diretamente todas as propostas

de implementação de sistemas de monitoramento e detecção de intrusão nesses sistemas, visto que a adição de um monitor não pode impactar no funcionamento dos processos industriais, pois a interrupção, ou degradação pode gerar danos físicos aos sistemas e pessoas.

Tabela 1: comparativo entre os sistemas de TI e TA

	TA	TI
Performance	- Execução em tempo real - O tempo de resposta é crucial - Controle de acesso restrito	- A execução não é em tempo real - Sem restrição de tempo de resposta - Controle de acesso baseado em necessidade de uso do sistema, normalmente todos tem acesso.
Disponibilidade	- 100% de disponibilidade, desligamentos não são aceitáveis.	- Desligamentos são tolerados.
Riscos	- Sistema ciber físico, controla algo no mundo real. - Segurança é crucial	- Gerencia dados - Confidencialidade e integridade são cruciais
Sistema Operacional	- Sistemas proprietários - Atualizações e alterações nas aplicações são menos frequentes.	- Sistema de amplo uso comercial e bem conhecidos - Atualizações são frequentes e normalmente automáticas.
Hardware	- Os equipamentos são projetados com o mínimo necessário para realizar o trabalho, normalmente possuem pouca capacidade de processamento, disco e memória.	- Os Servidores possuem farta capacidade de recursos.

Fonte: compilado de diversos (NIST, 2015; KNOWLES *et al.*, 2015; SULLIVAN, 2015; PLIATSIOS *et al.*, 2020; LAMBA *et al.*, 2017).

3.2 *Frameworks* de cibersegurança

Um *framework* é uma abstração conceitual, um conjunto de conceitos usados com a finalidade de resolver um problema. Um *framework* busca funcionalidades em comum a processos e é criado de forma que possa ser adaptado para inúmeras situações e casos de uso. De modo geral, é um sistema de padrões, diretrizes e melhores práticas que, caso sejam implementados, irão reduzir significativamente a probabilidade de incidentes (NIST, 2021). A revisão bibliográfica dos principais *frameworks* de segurança proporcionam uma visão abrangente dos pontos mais importantes a serem buscados quando implementamos a

segurança de forma gerencial, e ajuda a identificar as principais vulnerabilidades que o sistema deve evitar, e com isso será possível buscar quais ameaças podem explorar essas vulnerabilidades.

3.2.1 NIST *Cybersecurity Framework*

O *Framework* do NIST (2021) foi concebido para melhorar a segurança cibernética de infraestruturas críticas, como usinas de energia, sistema bancário e sistemas de abastecimento de água, de ataques cibernéticos. Mas, seus princípios são flexíveis e podem ser facilmente aplicados a qualquer segmento, desde pequenas empresas, passando por grandes indústrias, e até Estados.

O *framework* é composto por três partes: a Estrutura Básica, os Níveis de Implementação e as Avaliações da Estrutura. Para esse trabalho o foco será a sua Estrutura Básica, que é um conjunto de funções básicas que identificam os principais resultados de defesa cibernética que precisam ser alcançados, os quais descreve-se abaixo:

- identificar: busca desenvolver uma compreensão holística de toda a infraestrutura onde será implementada a segurança, englobando: sistemas, pessoas, ativos dentro de um determinado contexto que podem ser um risco cibernético;

- proteger: busca garantir o correto funcionamento e a contenção dos impactos causados por um incidente. Esta função tem como foco principal a disponibilidade de serviços críticos e vitais;

- detectar: busca identificar a ocorrência de anomalias, eventos, ou incidentes de segurança, com base em um sistema de monitoramento contínuo de modo que ações de contenção possam ser tomadas a tempo;

- responder: desenvolver e implementar as atividades e ações que serão realizadas quando ocorrer um incidentes de segurança, buscando minimizar seus impactos;

- recuperar: busca implementar os planos de restauração dos recursos afetados. Essa função busca prover resiliência ao sistema.

Para fins deste trabalho cabe ressaltar a função de detecção. Pois nela está incluída a categoria do sistema de monitoramento contínuo, que busca identificar se a rede é monitorada para detectar potenciais incidentes de segurança cibernética, código malicioso, ou conexão de dispositivos não autorizados.

3.2.2 Outras Normas

A norma ISO 27001 (2013) é o padrão internacional para segurança cibernética em redes de TI. Sua estrutura pressupõe que uma organização que a adota terá um sistema de gerenciamento de segurança da informação que exige que a administração gerencie proativamente seus riscos de segurança da informação, levando em consideração as ameaças e vulnerabilidades. A norma requer que a organização projete e implemente controles com o objetivo de mitigar os riscos identificados. A partir daí, sugere que seja criado um processo de gerenciamento de risco e um processo de melhoria contínua. Outra grande contribuição desta norma é o estabelecimento dos princípios fundamentais da segurança da informação: Confidencialidade; Integridade; e Disponibilidade. Esses princípios são a base para análise de risco e vulnerabilidades dos ativos e sistemas.

Center for Internet Security (CIS, 2021) é outro *framework* de segurança. Trabalha com métricas e diretrizes baseadas em padrões comumente usados, como NIST e ISO 27001. Diferente dos demais, este *framework* além de mapear os padrões de segurança oferece configurações básicas para ajudar as empresas a cumpri-los.

A IMO[13] estabeleceu que a partir de janeiro de 2021 o setor marítimo deveria entrar em conformidade com a sua resolução "MSC.428 (98)" (IMO, 2017), que incentiva as empresas a contemplarem os riscos cibernéticos na gestão de segurança existente. Essa resolução baseia-se na estrutura do *framework* do NIST, adequando-o à indústria marítima, com o objetivo de aplicar e avaliar os controles de segurança dentro de uma rede de TA em um ambiente naval.

3.3 Avaliação de riscos

A avaliação de riscos pode ser realizada utilizando-se os princípios da norma ISO 27001 (2013): Confidencialidade, Integridade e Disponibilidade. Conforme vimos no item 3.1 a importância da confidencialidade, da integridade e da disponibilidade dependem do propósito da utilização da informação e dados disponíveis nos sistemas do navio. Para exemplificar, em navios de guerra, sistemas de TI contendo informações e dados de operações, geralmente armazenadas em computadores portáteis, têm como maior vulnerabilidade a confidencialidade e integridade. No entanto, para sistemas das redes de TA, especialmente sistemas críticos e sensíveis (como o sistema de governo, por exemplo), o acesso à sua disponibilidade e integridade é mais preocupante, haja vista que o navio depende

13 Organização Marítima Internacional: é a agência especializada das Nações Unidas responsável pela segurança e proteção dos navios e pela prevenção da poluição marinha e atmosférica por navios (IMO, 2021).

de sua capacidade operacional em boas condições – confiáveis e disponíveis – para navegar de forma segura e eficiente.

Como sistemas de controle e automação são inseridos no rol de sistemas de TA de um navio, a avaliação de riscos cibernéticos de cada sistema deve compreender todos equipamentos, sistemas baseados em computador, mapa das conexões de redes (caso existente), além de pontos de acesso e dispositivos de comunicação. O objetivo final desse processo é uma lista com os principais ativos e sistemas, identificando os que são críticos para o navio.

A norma DGMM-0540 (BRASIL, 2019) define vulnerabilidade como a fraqueza de um sistema ou ativo. Também define que a ameaça é a causa potencial de um evento. Quando o agente malicioso explora a vulnerabilidade e esse evento causa impacto em um ativo, temos o incidente. Logo, uma das maneiras de aumentar a segurança da rede é conhecer as principais ameaças a que ela está exposta e monitorar as vulnerabilidades a fim de evitar sua exploração.

3.3.1 Vulnerabilidades

Após a pesquisa realizada é possível sintetizar em quatro as principais vulnerabilidades aos sistemas das redes de TA (CHIFFLIER, 2014; KNOWLES *et al.*, 2015; SULLIVAN, 2015; PLIATSIOS *et al.*, 2020; ISA, 2010; MITNICK, 2003):

— Pessoal: O ciberespaço vai além do hardware, software, e sistemas de rede, há também pessoas e sua interação com toda a infraestrutura. Conforme observou Kevin Mitnick (2003), o desenvolvimento novas barreiras de segurança e à medida que os especialistas dificultam a exploração de vulnerabilidades, a tendência dos atacantes é se voltar para a exploração do elemento humano, considerado o elo mais fraco da segurança. Assim, o pessoal deve ser visto como a principal vulnerabilidade em qualquer sistema tecnológico.

— Falhas no sistema: As brechas nos sistemas permitem sua exploração por um agente malicioso. Essas falhas podem ocorrer por negligência dos engenheiros e programadores, ditas não intencionais, ou por ação direta e dolosa. Mesmo com o desenvolvimento de aplicações novas e mais seguras, o ciclo de vida longo que esses tipos de sistemas geram um problema: quanto mais tempo uma aplicação sobrevive maior é a quantidade de vulnerabilidades exploráveis encontrada (PLIATSIOS *et al.*, 2020).

— Negação de Serviço: Os ataques conhecidos como negação de serviço causam a paralisação da função para a qual o sistema ou ativo foi projetado (SCHUBA *et al.*, 1997). O tipo mais comum de ataque de negação de serviço é a inundação, aquele onde o atacante envia

uma quantidade de dados maior que o alvo consegue tratar. Outro tipo é o que o atacante envia uma série de comandos com a finalidade de travar o dispositivo. Em ambos os casos, o objetivo é tornar o uso do sistema inacessível aos usuários (PALOALTO, 2021).

— Espionagem: Com o intuito de diminuir os custos de produção diversos fabricantes de equipamentos buscam usar hardware e sistemas amplamente difundidos no mercado, são os chamados dispositivos de prateleira. Há um mercado negro para venda de "vulnerabilidades de dia zero[14]" (FASTCOMPANY, 2008). Essas vulnerabilidades podem ser usadas para conseguir acesso aos dados que trafegam nessas redes. Outro ponto importante é o controle da cadeia de suprimentos. Conforme apontado na revista *Defense Science Board* (DOD, 2007) agentes estatais alteram equipamentos, incluindo *backdoors*[15], antes de enviá-los aos seus destinatários.

3.3.2 Agentes causadores

Além das principais ameaças conhecidas, é também mister conhecer os seus agentes causadores, Cristiano (2018) realizou uma extensa pesquisa bibliográfica e identificou que existem cinco tipos de agentes, combinado com o *white paper da Armor Shield* (ARMOR, 2021), é possível agrupá-los em agentes internos, fazem parte da instituição, e externos. Esses dois grupos por sua vez podem ser classificados como:

— Grupos de hackers organizados: podem ser grupos estatais, grupos terroristas, organizações criminosas com propósito financeiro; ou ativistas com motivação política;

— Aventureiro: são usuários que realizam ataques por curiosidade ou desafio pessoal;

— Pesquisador: tem por objetivo melhorar a segurança realizando pesquisa e testando sistemas em busca de fragilidades;

3.3.3 Tipos de impacto gerados

Um ciberataque pode gerar muitos impactos em um navio, desde a indisponibilidade de um sistema até acidentes fatais ou perda total do meio naval (BOARD, 2010). Os principais impactos estudados foram:

— dano físico: qualquer evento que gere dano material ao navio, ferimentos ou mortes, ou algum tipo de impacto ao meio ambiente;

14 Ataques de dia zero: são aqueles que aproveitam falhas de software que os desenvolvedores desconhecem para atacar as vítimas sem aviso prévio (AVAST, 2021)

15 Programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para esse fim. Normalmente esse programa é colocado de forma a não a ser notado (CERT.BR, 2012)

— vazamento de dados: exposição de informações que podem comprometer a segurança do navio em situações de conflito, cita-se: posição, rumo, velocidade, e situação operacional dos equipamentos;

— alteração dos dados: Este tipo de impacto normalmente acarreta operação incorreta dos sistemas. A alteração de dados em trânsito pode afetar o correto funcionamento de sistemas essenciais, tais como: controle da propulsão, posicionamento do navio, inclusão de erro na solução de tiro, dentre outros;

— interrupção: ataques do tipo de negação de serviço causam esse tipo de impacto. A rede fica sobrecarregada de dados e não consegue processar adequadamente os dados reais.

— fabricação: muito similar a alteração de dados, a fabricação também afeta o funcionamento correto dos sistemas, o que os diferencia é que na fabricação os dados são enviados independentemente de haver tráfego de dados para ser alterado.

3.3.4 Ameaças

Seguindo a metodologia dos principais normativos (ISO, 2013; BRASIL, 2019; NIST, 2021) busca-se fazer uma correlação entre a capacidade dos agentes causadores descritos no item anterior com as principais ameaças: *Malware, Man-in-the-Midle,* Engenharia Social, *Backdoor, Sniffer,* Bomba Lógica, *Spyware*, e Cavalo de Tróia[16]. A análise correlativa descrita acima pode ser observada na tabela 2.

Tabela 2. Correlação entre ameaças, vulnerabilidades e impacto.

Ameaças	**Vulnerabilidades**				**Impacto**
	Pessoal	Falha nos Sistemas	Negação de Serviço	Espionagem	
Spyware				X	Vazamento de dados
Backdoor		X	X	X	Vazamento de dados, dano físico, alteração, interrupção, e fabricação
Malware	X	X	X	X	Vazamento de dados, dano físico, alteração, interrupção, e fabricação.

16 As definições estão descritas no Anexo A.

Man-in-the-Midle	X	X	X	Vazamento de dados, dano físico, alteração, interrupção, e fabricação.
Engenharia Social	X	X	X	Vazamento de dados, dano físico, alteração, interrupção, e fabricação.
Sniffer	X		X	Vazamento de dados.
Bomba Lógica		X		dano físico, e interrupção.
Cavalo de Tróia	X		X	-

Fonte: (CERT.BR, 2012; NIST, 2010; NIST, 2018; ISO, 2013; ISA, 2010)

4 SISTEMA DE MONITORAMENTO E REQUISITOS

O capítulo dois apresenta casos notórios de ataques às redes de TA. Esses ataques demonstram a sofisticação dos agressores e suas graves consequências. No capítulo três, com o auxílio de um análise de risco sucinta, foram identificadas as vulnerabilidades, impactos e ameaças.

Este Capítulo busca apresentar um conjunto de tecnologias e processos capazes de contribuir para melhorar a maturidade cibernética dos meios navais: o monitoramento contínuo. Processo fundamental no *framework* do NIST incluído na função “detectar”. A intenção é descrever as diversas tecnologias disponíveis para implementar um sistema de monitoramento contínuo em rede de TA.

Inicialmente serão apresentados os principais sistemas que podem ser ou são interconectados, o protocolo de comunicação das redes de TA, como monitorá-la, e por último será feita uma descrição dos principais requisitos funcionais que essas redes e sistemas devem possuir para que o monitoramento possa ser implementado.

4.1 Monitoramento

A identificação de eventos de segurança pode ser realizada tanto em tempo de operação quanto para verificação de eventos passados. Com monitoramento em tempo real os operadores podem verificar se o tráfego da rede está ocorrendo em condições normais, ou se há algum alarme de eventos em curso. A busca histórica se concentra em analisar registros

armazenados, com a finalidade de estudar mais a fundo se ocorreu alguma condição anormal que passou despercebida, ou seja, que pode não ter sido detectada. Isso ocorre pois para novas vulnerabilidades não há assinaturas disponíveis para atualização do sistema e ela pode ter sido explorada sem que ninguém tenha percebido de imediato. Nessas ocasiões, a equipe de analistas de segurança pode ser acionada para analisar o registro de eventos e identificar se a vulnerabilidade foi explorada, ou até mesmo criar uma assinatura nova para ser usada para alertas em tempo real.

4.1.1 Conectividade em meios navais modernos

Os navios modernos possuem muita tecnologia, com a maioria de seus sistemas controlados por algum ativo computacional. A comunicação entre esses sistemas é fundamental para a correta operação, quer na navegação quer em postos de combate[17]. Todo esse tráfego de informações representa um risco, e o monitoramento contínuo é uma forma de identificar a ocorrência de eventos e incidentes. Seu objetivo principal é acompanhar o correto funcionamento dos sistemas e seu desempenho, sendo capaz de emitir notificações caso ocorram quaisquer problemas.

Diferente das gerações anteriores que possuíam redes de controle analógicas, ou quando possuíam rede de TA, eram isoladas fisicamente. Por definição, um sistema isolado não está conectado, em teoria, a nenhum outro sistema, mas, continuam sofrendo com riscos associados à manutenção e atualização. Basta uma entrada de dados, como portas seriais e unidades USB para que um agente malicioso possa infiltrar e infectar esses sistemas. A introdução de sistemas modernos e interconectados traz esse tipo de preocupação. Detectar anomalias e eventos de segurança em redes de TA representa algo desafiador, pois são inúmeros sistemas e pontos de entrada de dados.

Os principais sistemas presentes em um navio moderno, que podem ser ou são interconectados (AGUAS, 2021; NAVAL, 2021; SECURE, 2020) são:

— Propulsão: Controle dos motores (propulsão e geração de energia), controle do leme, controle de passo, sensor de combustível;

— Navegação: GPS, AIS, carta eletrônica e, radar, sistemas meteorológicos;

— Sistema de estabilidade: Sistemas de lastro, tensão de casco, controle de estabilidade;

— Sistemas de Segurança: Sensores de incêndio e inundação, CCTV;

17 Quando o navio está pronto para fazer frente aos trabalhos que envolvem toda a tripulação de bordo ao mesmo tempo, ou parte dela, para um fim específico. Podem se fainas gerais, comuns, especiais ou de emergência (BRASIL, 2021).

— Comunicações: Comunicações via satélite e RDS;

— Segurança física: Salas de servidores, controle de acesso, Centro de controle de máquinas, Centro de Operações de Combate;

— Infraestrutura de rede;

— Rede de TA: HMI, PLCs, sensores digitais e analógicos; e

— Sistemas de Armas: Radar de direção de tiro, Sistema de armas (mísseis, torpedos, flair, canhão).

4.2 Sistema de Monitoramento

As principais referências para o desenvolvimento de sistemas seguros são as normas ISA/IEC-62443 e o *framework* do NIST. Assim é importante verificar e entender como esses normativos tratam o sistema de monitoramento, onde ele deve ser implementado e o que deve monitorar.

A norma ISA/IEC-62443 (ISA, 2010) foi desenvolvida para atender à necessidade de projetar sistemas de controle de automação industrial levando em conta a segurança cibernética como um de seus requisitos desde a fase de projetos do sistema. Foi criado como uma coleção de requisitos para pessoas, hardware, software e políticas envolvidas na operação dos controles industriais, que podem afetar sua segurança. Esse *framework* possui 7 requisitos de segurança fundamentais: Controle de identificação e autenticação; Controle de uso; Integridade do sistema; Confidencialidade; Fluxo de dados restrito; Resposta aos eventos; e Disponibilidade. Além disso, a norma também define os perímetros de segurança, depois que os sistemas e redes são mapeados para criar um plano de segurança, essas redes podem ser separadas por uma função, e caso necessário serem interligadas. Todos os perímetros e interligações devem possuir alguma tecnologia que permita monitorar eventos de segurança (DesRuisseaux, 2018; ISA, 2010).

O NIST (2021) identificou um conjunto de ferramentas de avaliação para que uma organização tenha um alto nível de maturidade de segurança cibernética[18]. O estudo dessa norma permite identificar quais funções, práticas e processos de segurança cibernética estão atreladas ao monitoramento contínuo. As seguintes recomendações são feitas pela função detectar:

18 Os diversos modelos de cibersegurança costumam avaliar os programas implementados com o objetivo de identificar em qual nível a organização se encontra, e fazer sugestões de melhorias. Quanto maior o nível, mais madura é a mentalidade de segurança da organização (AZAMBUJA, 2020).

— Implementar uma *baseline*[19] para os fluxos de dados, com procedimentos e processos para detectar e analisar eventos, de preferência, de várias fontes e sensores.

— Implementar ferramentas para monitorar os perímetros isolados e os interligados. Também é necessário monitorar os ambientes físicos para detectar acesso de pessoal não autorizado.

— Implementar processos de análise de *logs*[20], como forma de melhorar continuamente esses processos para garantir que eventos anômalos passados possam ser identificados no futuro.

O monitoramento é realizado em três etapas: captura dos dados, que normalmente é feita por dispositivos especializados, que são capazes de ler o tráfego de rede na camada física. estes dispositivos são comumente chamados de *sniffers*[21]. Outra forma de capturar dados é utilizar a própria infraestrutura de rede, caso ela possua a capacidade de encaminhar os dados para uma porta de diagnóstico (BARNES e SAKANDAR, 2005).

A segunda camada é a identificação dos dados, nela está a inteligência do sistema. Esses sistemas de identificação por sua vez são classificados em dois tipos: os baseados em anomalias; e os baseados em assinaturas (BORKAR *et al.*, 2017).

Já a apresentação, terceira e última etapa, é a responsável por informar ao usuários que algo está errado. pode ser feita desde um simples conjunto de luzes indicando algum evento, até sistemas mais complexos com painéis, gráficos e linhas do tempo para monitoramento em tempo real (MALIN e HEULE, 2013). O painel de monitoramento deve fornecer imediatamente, os eventos que estão ocorrendo na rede, a fim de auxiliar os usuários do sistema a tomar decisões sobre como tratar os possíveis incidentes (CIMPAN *et al.*, 2019).

4.2.1 Captura dos dados

O Modbus (FOVINO *et al.*, 2009) é o protocolo padrão de camada de aplicação para as redes de TA. Por ser versátil, e de fácil implementação esse protocolo é utilizado em muitas aplicações como: instrumentação, usinas nucleares, plantas industriais, automação residencial, e automação de navios. Sua implementação pode ser realizada com uma

19 Baseline é um ponto de referência de determinado serviço. O fluxo de dados normal de uma rede é sua base line (GSTI, 2016).

20 Log é o registro dos eventos que ocorrem nos sistemas e redes de uma organização. Os registros são compostos de entradas que contém informações relacionadas a um evento específico que ocorreu em um sistema ou rede. Muitos logs dentro de uma organização contêm registros relacionados à segurança do computador (NIST, 2010).

21 Dispositivos físicos que são colocados na rede, que possuem a capacidade de detecção e interceptação de cada pacote à medida que ele flui pela rede (CLINCY e NAEL, 2005).

variedade de meios físicos de rede, tais como: RS-232, RS-485, ou TCP/IP[22]. O padrão RS-232 é um tipo específico voltado para aplicações ponto a ponto, ou seja, só admite dois dispositivos na rede. Já os padrões RS-485 e TCP/IP, além de trabalharem com maior largura de banda, também operam em rede com diversos dispositivos. Assim o dispositivo que será usado para captura dos dados deve ser capaz de suportar os três protocolos.

A arquitetura típica do protocolo define um cabeçalho, um quadro para os códigos de função e a área de dados. O cabeçalho é usado para identificação dos ativos de rede envolvidos no tráfego de dados, checagem de erro e outros bytes para controle. Os códigos de função identificam que operação está sendo realizada, informação de dados, apresentação do ativo de rede, nova configuração de parâmetros, comandos de ligar ou desligar. Já a área de dados, transporta os dados úteis que serão consumidos, tais como: temperatura, ângulo do leme, rumo e velocidade (DENG *et al.* 2016).

4.2.2 Identificação

Segundo Sharmila (2013), os sistemas de detecção de intrusão[23] (IDS) buscam encontrar padrões nos fluxos de rede e classificá-los em tráfego normal ou tráfego suspeito. Apesar de não haver uma classificação formal para esses sistemas é possível categorizá-los em dois grupos distintos baseado em sua abordagem de detecção:

— Sistemas baseados em detecção de anomalias: este tipo de sistema monitora os fluxos de rede e usam técnicas de aprendizado de máquina[24] para entender o fluxo normal da rede. Os fluxos que estão fora do que é considerado normal são classificados como anômalos. A grande vantagem dessa abordagem é ser capaz de detectar ataques novos. Em contrapartida gera muitos falsos positivos (LIAO, 2013; WAGH, 2013).

— Sistemas baseados em detecção por assinatura: assinatura é uma sequência de dados ou comandos previamente conhecidos que caracterizam um ataque. Armazena-se as assinaturas em uma base de dados, chamada de base de ataques conhecidos. O IDS compara com o fluxo que rede com o banco de assinaturas, e caso haja uma combinação, classifica o tráfego como malicioso. São o tipo mais usado, pela sua simplicidade e assertividade (LIAO, 2013; WAGH, 2013).

---

22 TCP/IP significa protocolo de controle de transmissão/protocolo da internet (Transmission Control Protocol/Internet Protocol). É um conjunto de regras padronizadas que permitem que os computadores se comuniquem em uma rede como a internet (AVAST, 2021).

23 Sistema de detecção de intrusão é o sistema usado para automatizar a detecção de incidentes em uma rede (LIAO, 2013).

24 O aprendizado de máquina, machine learning, é um conjunto de algoritmos e métodos que permitem que sistemas de computador adquiriram conhecimento autonomamente (EL NAQA, 2015)

4.2.3 Apresentação

A apresentação pode ser definida como uma exibição visual de informações usadas para monitorar condições e auxiliar na compreensão do que está sendo monitorado. Seu objetivo principal é alertar que há algo errado no sistema monitorado, por meio da visualização de dados através de gráficos, tabelas e linhas de tempo. Esses elementos fornecem em tempo real visualizações analíticas dos dados e permitem que os usuários façam buscas e pesquisas.

Essas informações visuais ajudam a identificar tendências, padrões e anomalias. O conceito é desenvolvido a partir de telas interativas com múltiplas visualizações e tem o propósito de apoio à tomada de decisão (SARIKAYA, 2018). A vantagem de uma tela é reduzir a sobrecarga de informações e melhorar o desempenho dos usuários.

Segundo CIMPAN (2019), a apresentação pode fornecer visualização de dados de diversos tipos: Dados Históricos, são aqueles que fornecem uma visão geral dos eventos anteriores; Dados em tempo real, o conteúdo é atualizado automaticamente com os dados mais atuais. O uso de dados históricos é relevante para análise de log e investigação. Os dados em tempo real são usados para a operação.

4.2.4 Proposta de Sistema de Monitoramento

Coletar eventos de rede e ativos para detecção cibernética não é um problema, existe uma infinidade de ferramentas e tecnologias desenvolvidas para as redes de TI que podem facilmente ser adaptadas para as redes de TA, observando algumas restrições (MONITORAMENTO, 2020, MODBUS, 2018).

A largura de banda da redes é uma restrição, pois limita o volume dados que trafega por ela. A complexidade das arquiteturas dos sistemas dos navios impõe que o sistema de monitoramento cibernético deve estar isolado, em uma rede distinta dos sistemas monitorados, pois os dados gerados pelos eventos de monitoramento não devem impactar o funcionamento normal da rede de TA.

Diante dessa restrição Chifflier (2014) descreve um sistema de IDS com uma arquitetura capaz de monitorar as redes usando uma rede secundária. Os dados coletados podem então ser enviados para serem processados e analisados em um sistema central. Assim, é possível instalar diversos coletores de dados sem interferir na operação normal da rede de TA e ao mesmo tempo lidar com a complexidade e heterogeneidade de sistemas.

A Marinha do Brasil possui dois sistemas que, com pequenas modificações, podem ser usados para o monitoramento das redes de TA dos navios. O primeiro é o Sistema Militar de Proteção Cibernética, desenvolvido pelo Comando Naval de Operações Especiais. É um conjunto de hardware e software que reúne vários serviços de segurança em um único dispositivo: uma ferramenta de detecção, um *firewall* e uma central de gerenciamento, que analisa o tráfego de rede e tem a capacidade de identificar atividades maliciosas.

O Segundo é o SIEM (*Security Information and Event Management*) CÈUS, desenvolvido pelo Centro de Tecnologia da Informação da Marinha. Um SIEM possuí uma tecnologia que permite agregar, analisar, coletar e normalizar eventos gerados por qualquer dispositivo da rede. Esses dados combinados tem o poder de contextualizar os eventos de segurança, provendo dados úteis para a segurança, tais como: comportamento dos usuários, fluxo de rede, tentativas de acesso e falha dos sistemas. Esses dados podem ser analisados em tempo real, aumentando a capacidade de gerenciamento e visibilidade de toda a rede. Além de receber dados dos dispositivos de segurança e rede, o SIEM também pode receber dados dos próprios sistemas da rede de TA, por exemplo mudanças nos arquivos de configuração e tentativas de acesso. A coleta de eventos de segurança independente da fonte de dados e do formato de envio confere flexibilidade ao sistema. Essa coleta e posterior análise de todos esses dados possibilita uma rápida identificação e resposta aos incidentes e eventos. Um SIEM também tem uma capacidade grande de retenção de dados, o que permite armazenar, analisar e alertar ou visualizar os dados tanto em tempo real quanto seu histórico, de forma resiliente e segura.

Desta forma, é possível dotar o SMPC com placas de rede apropriadas para as redes de TA (WEIS, 2020, MODBUS, 2018) e instalar as unidades coletoras pelos diversos sistemas do navio. Essas unidades serão responsáveis por realizar as duas primeiras etapas, quais sejam: coleta de dados e identificação. Posteriormente os dados são enviados ao console central com o sistema de SIEM, onde será possível monitorar todas as redes e sistemas de forma centralizada.

4.3 Requisitos

Um bom sistema de monitoramento é mais do que simplesmente coletar dados, é preciso que haja um processo bem estabelecido, saber o que se quer identificar, qual seu impacto e se há tempo hábil para medidas corretivas. O foco do monitoramento, neste trabalho, é voltado para a coleta de dados de ativos e de rede, incidentes e eventos que possam ter um impacto nos ativos e sistemas de TA dos meios navais.

Na engenharia de software os requisitos de um sistema podem ser divididos em funcionais e não funcionais (GHEZZI *et al.*, 2002). Os requisitos funcionais ditam o que o sistema deve fazer, ou seja quais funcionalidades deve prover. Enquanto, os requisitos não funcionais dizem respeito a propriedades de qualidade do sistema, tais como segurança e performance (BASS *et al.*, 2003). Esta divisão ser adotada para descrever o escopo de cada requisito.

A ISO/IEC 15048 (2017), também chamada de *Common Criteria,* é um *framework* voltado para especificação de requisitos de segurança. A norma implementa uma escala de avaliação chamada de "*Evaluation Assurance Level* (EAL)". Essa escala varia entre 1 a 7, que mede o grau de maturidade de segurança, que segundo a norma, um determinado sistema possui. Assim, quanto mais alta a escala, maior a segurança do sistema avaliado.

O principal benefício da norma é a existência de critérios globalmente aceitos. Esses critérios servem para auxiliar a produção de requisitos de segurança e também ajudam os fabricantes a buscarem uma conformidade técnica de seus produtos em atendimento aos requisitos.

Por exemplo, um requisito que consta na norma é "o sistema precisa ser capaz de monitorar o fluxo de informações erradas na rede", ou "o sistema de monitoramento precisa receber regras, de forma a verificar se há alguma violação de integridade no fluxo de rede", dentre outros, a norma enumera diversos pontos que necessitam de monitoramento: acesso não autorizado; erro do fluxo de dados; dispositivos conectados; e integridade dos dados são alguns exemplos. Com isso, caso um sistema seja certificado na ISO 15408 significa que ele possui um certo grau de maturidade e segurança cibernética, incluindo alguma forma de monitoramento.

Seguindo a metodologia de Ricardo Ribeiro Gudwin (2015), primeiramente é necessário identificar dois aspectos: os problemas a serem resolvidos e os pré-requisitos. A compreensão do problema envolve a sua descrição e detalhamento de tal forma que a solução não esteja incluída na sua formulação. É necessário descrever as particularidades e características. Os pré-requisitos devem ser escritos na forma de funções e atributos. Enquanto o primeiro deve descrever o que o sistema deve fazer, o segundo deve descrever o que o sistema deve ter. A partir de então define-se quais serão os requisitos funcionais e não funcionais do sistema (GHEZZI *et al.*, 2002). Os problemas principais foram os apontados no capítulo 2, quais sejam: Falhas no sistemas; Negação de serviço; Espionagem; e Abuso de Privilégio. A partir de então define-se quais serão os requisitos funcionais e não funcionais do sistema. Para fins deste trabalho serão abordados apenas requisitos funcionais.

Os requisitos do sistema devem acompanhar as necessidades do sistema de monitoramento. Com base na pesquisa realizada é possível então dividir a maneira da coleta de dados em duas fontes distintas: dados provenientes de ativos (sistema), ou dados em trânsito (rede) coletados em dispositivos de interconexão. Que por sua vez possuem requisitos distintos para monitoramento.

4.3.1 – Requisitos de Rede

O monitoramento de rede busca detectar atividades potencialmente maliciosas na rede. É possível detectar ataques cibernéticos em um estágio inicial, coletando e agregando dados de diversos pontos da rede, comparando-os com indicadores conhecidos. Logo, o requisito fundamental para esse segmento é que a infraestrutura de rede deve possuir a capacidade de espelhar o tráfego de rede de todas as suas interfaces em uma interface de monitoramento. São dados úteis os coletados dos seguintes pontos:

— Conexões IP entre os Ativos da rede: É útil monitorar os dados destas conexões, pois através desse dado podemos ver conexões anômalas, entre sistemas que não deveriam trocar dados e até mesmo dispositivos desconhecidos conectados na rede. É normal esperar que um sensor de lastro do tanque envie dados para o seu servidor, mas não é esperado que os sensores troquem dados entre si. Esse fato é um indicador de que um destes dispositivos foi comprometido e está tentando comprometer outros na rede (ISA, 2010).

— Conexões entre perímetros: em redes de TA é comum separar as redes em segmentos comuns. Sendo a comunicação entre elas realizada por um acordo de interfaces entre os servidores destas zonas. É então necessário monitorar esse tráfego em busca de evidências e indicadores de comprometimento (ISA, 2010).

4.3.2 Requisitos dos ativos

O monitoramento dos ativos e sistemas busca detectar atividades não autorizadas nos próprios sistemas. Os dados enviados devem considerar o monitoramento de usuários regulares quanto administradores de sistema, nas camadas do aplicativo e do sistema operacional. Isso ajuda a identificar o comportamento suspeito do usuário para um invasor ou interno. Para isso é necessário que os ativos e sistemas sejam capazes de fornecer os seguintes dados (NIST, 2015; NIST, 2018; ISA, 2010):

— dados de acesso aos sistemas: com esses dados é possível identificar tentativas sem sucesso e os acessos concedidos. Esse dado é importante também para identificar o

ataque do insider, que são pessoas, internas, que possuem o privilégio necessário para realizar a operação;

— Controle de alteração: sempre que um houver alteração em qualquer configuração do ativo este deve informar que a alteração, ou a tentativa, ocorreu; e

— Controle de usuários: sempre que um usuário novo for cadastrado essa informação deve ser informada.

Este capítulo, apresentou uma estrutura de monitoramento contínuo para redes de TA. Essa estrutura é composta por dois sistemas em uso na Marinha, o SMPC e o CEUS. Também foram propostos requisitos funcionais de sistema para que o monitoramento possa ser implementado atendendo as especificações dos padrões internacionais. Esta estrutura foi descrita em alto nível, e por isso, precisa ser melhor estudada com apoio de outros setores da Marinha.

5 CONCLUSÃO

Os ataques cibernéticos voltados para as redes de TA, embora não inteiramente novos, têm crescido bastante nos últimos anos. Ainda que não existam registros oficiais de ataques voltados a navios de guerra, há estudos e ensaios que demonstram quão devastador eles poderiam ser. Além disso, há inúmeros exemplos da aplicação das mesmas técnicas de ataque que seriam empregadas nas redes de TA dos navios, e conforme foi mostrado no capítulo 2, muitos países têm dado atenção ao seu uso militar.

Foi apresentado no capítulo 3 que existem ameaças reais às redes de TA, assim, foram identificadas as principais ameaças que podem afetar os pilares da segurança cibernética dessas redes em um meio naval. Também foram mapeadas as vulnerabilidades e os agentes maliciosos que podem comprometer os sistemas navais.

Conforme mostrou a pesquisa, é importante proteger os sistemas de TA, pois eles são tão vulneráveis quanto os sistemas de TI, existem diversas vulnerabilidades exploráveis nesses sistemas e há agentes dispostos a atacá-los. Com isso, o capítulo 4 identificou a preocupação da comunidade normativa internacional com o tema criando normas específicas com a finalidade de produzir sistemas seguros. Todas as normas e *frameworks* incluem o monitoramento como essencial a ser implementado para a defesa cibernética. Foi apresentado

também, que o sistema de monitoramento é dividido em três partes: coleta de dados, detecção, e apresentação. Apresentou que existem na Marinha dois sistemas que, em conjunto, realizam essas três etapas: o SMPC e o CÈUS. Após isso foi proposto um esquema de monitoramento que pode ser aplicado às redes de TA dos navios, demonstrando assim como preparar os navios da marinha para serem capazes de detectar ataques cibernéticos nessas redes. Por fim, foram elaborados requisitos de sistemas que devem ser observados quando a marinha for adquirir um novo meio de forma a permitir a instalação de um sistema de monitoramento de segurança para as redes de TA.

Particularmente em navios de guerra esse tipo de ataque pode ser mais danoso que os ataques a redes de TI tradicionais, pois, no curso de uma ação tática é mais importante manter o sistema funcionando do que aplicar uma correção perfeita e demorada que, embora seja a melhor solução, pode ter impacto direto no tempo de resposta de um evento. Isso requer que além de se implementar um sistema de monitoramento é necessário atualização da doutrina de tratamento de incidentes nessas redes.

Assim, o monitoramento contínuo tem se tornado a pedra fundamental para detectar ataques cibernéticos e tomar atitudes proativas com o intuito de mitigar seus efeitos e de proteger ativos e sistemas críticos. Garantindo que os incidentes e eventos sejam resolvidos de forma rápida e adequada, contribuindo para que esses sistemas continuem a operar sem prejudicar a missão.

Concluindo, a probabilidade de um incidente cibernético ocorrer é alta. Por isso é necessário estar preparado para detectá-lo e mitigá-lo da forma adequada, garantindo a prontidão do meio. Um dos sistemas que ajudam nessa preparação é o monitoramento contínuo. E, para que haja um sistema de monitoramento contínuo eficiente alguns requisitos devem ser observados quando da aquisição de um sistema de TA.

Para trabalhos futuros sugere-se um estudo de ferramentas para realização de coleta de dados e um estudo para criação de uma doutrina de tratamento de incidentes em redes de TA.

REFERÊNCIAS

AGUAS, Azuis. **Fragatas classe Tamandaré: o mais moderno e inovador projeto naval do Brasil.** 2021. Disponível em: https://aguasazuis.com.br/. Acesso em: 12/07/2021.

ALMEIDA, Nival Nunes; MACHADO, Raphael Carlos Santos; DE SÁ, Alan Oliveira. **O Encontro da Guerra Cibernética com as Guerras Eletrônica e Cinética no Âmbito do Poder Marítimo**. 2019. Revista da Escola de Guerra Naval, v. 25, n. 1, 2019.

AVAST, **What is a logic bomb**. 2021. Disponível em: https://www.avast.com/c-what-is-a-logic-bomb. Acessado em: 10 de julho de 2021.

AVAST, **O que é um TCP/IP e como ele funciona?**. 2021. Disponível em: https://www.avast.com/pt-br/c-what-is-tcp-ip. Acessado em: 10 de julho de 2021.

ARMOR, Shield. **Guia prático para gerenciamento de riscos e segurança cibernética de navios**. 2021. White paper. 12 p. 14 de abril de 2021.

AZAMBUJA, Antonio João Gonçalves de; NETO, João Souza. **Modelo de maturidade de segurança cibernética para os órgãos da administração pública federal**. 2020.

BAHETI, Radhakisan e GILL, Helen. **Cyber-physical systems.** ***The impact of control technology***. 2011.

BARNES, David; SAKANDAR, Basir. **Cisco LAN switching fundamentals**. 2005. Cisco Press.

BASS, Len *et al.*. **Software architecture in practice**. 2003. Addison-Wesley Professional.

BOARD, Naval Studies *et al.*. **Information assurance for network-centric naval forces**. 2010. National Academies Press.

BORKAR, Amol *et al.*. **A survey on Intrusion Detection System (IDS) and Internal Intrusion Detection and protection system (IIDPS)**. 2017. International conference on inventive computing and informatics (ICICI). IEEE, 2017. p. 949-953.

BRASIL, Diretoria Geral do Material da Marinha. DGMM 0540: **Normas de Tecnologia da Informação da Marinha**. Rio de Janeiro, 2019.

BRASIL, Decreto n° 10569 de 9 de dezembro de 2020. **Estratégia Nacional de Segurança de Infraestruturas Críticas**. 9 dez. 2020.

BRASIL, Marinha. **Equipamento de medidas de apoio à guerra eletrônica, mage defensor**. 2021. disponível em: https://www.marinha.mil.br/ipqm/node/38. Acesso em: 05 de junho de 2021.

BRASIL, Marinha. **A Organização de Bordo**. 2021 Disponível em: https://www.marinha.mil.br/tradicoes-navais/organizacao-de-bordo. Acesso em: 15/07/2021.

CAMBRA, A.C. **Manutenção Centrada na Confiabilidade: Uma proposta de aprimoramento da manutenção dos meios navais da Marinha do Brasil. Monografia** (Curso de Política e Estratégia Marítima). Escola de Guerra Naval, Rio de Janeiro, 2016.

CERT.BR. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Cartilha de Segurança para Internet. São Paulo**. 2012. Disponível em: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf. Acesso em: 05 abr. 2021.

CHIFFLIER, Pierre; FONTAINE, Arnaud. **Architecture système sécurisée de sonde IDS réseau**. 2014. Computer & Electronics Security Applications Rendez-vous (C&ESAR).

CIS, Center for Internet Security. "**Cis controls v8**". 2021.

CIMPAN, Andra *et al.*. **Applying design system in cybersecurity dashboard development**. 2019. Computing, v. 593, p. 224-236

CLARKE, Richard e ROBERT, K. Knake. **"Cyber war"**. 2014. Old Saybrook: Tantor Media, Incorporated.

CLINCY, Victor A.; NAEL, Halaweh Abu. **A Taxonomy of free Network Sniffers for teaching and research**. 2005. Journal of Computing Sciences in Colleges, v. 21, n. 1, p. 64.

CRISTIANO S.C. **Ameaça da guerra cibernética aos sistemas de comando e controle: O impacto que um ataque cibernético pode gerar a um submarino nuclear de ataque**. Monografia (Curso Superior). Escola de Guerra Naval, Rio de Janeiro, 2018.

DENG, Li *et al.*. **Intrusion detection method based on support vector machine access of modbus TCP protocol**. 2016. IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, 2016. p. 380-383.

DENNING, Dorothy E. "**Stuxnet: What has changed?**." 2012. *Future Internet* 4.3 (2012): 672-687.

DESRUISSEAUX, Daniel. **Practical Overview of Implementing IEC 62443 Security Levels in Industrial Control Applications**. 2018. Schneider Electric White Paper.

DOD, U. S. **Report of the Defence Science Board Task Force on Mission Impact of Foreign Influence on DoD Software**. 2007.

ELETRICO, Revista o setor elétrico. **Automação de subestações**. 2010. Disponível em: http://www.osetoreletrico.com.br/wp-content/uploads/2010/07/ed52_fasc_automacao_subestacoes_capV.pdf. Acessado em: Acesso em: 05 abr. 2021.

EL NAQA, Issam; MURPHY, Martin J. **What is machine learning?**. 2015. In: machine learning in radiation oncology. Springer, Cham, 2015. p. 3-11.

EMGEPRON. S**istema de Controle de Avarias**. 2021. Disponível em: https://www.marinha.-mil.br/emgepron/en/en/pt-br/sistema-de-controle-de-avarias-scav. Acesso em: 30 ago. 2021.

ERICH, Follath e HOLGER, Stark. **The Story of 'Operation Orchard': How Israel Destroyed Syria's al-Kibar Nuclear Reactor.** 2009. Disponível em: http://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663-7.html. Acesso em: 05 maio 2021.

FALLIERE, Nicolas; MURCHU, Liam O.; CHIEN, Eric. W32. **stuxnet dossier**. 2011. White paper, Symantec Corp., Security Response, v. 5, n. 6, p. 29, 2011.

FASTCOMPANY, "**The Black Market Code Industry**". 2008. Disponível em: https://www.fastcompany.com/898660/black-market-code-industry. Acesso em: 01/08/2021.

FOVINO, Nai *et al.*. **Secure Modbus Protocol, a proof of concept**. 2009. In: Proc. of the 3rd IFIP Int. Conf. on Critical Infrastructure Protection, Hanover, NH, USA. 2009. p. 4-7.

GARTNER, "**Information technology (IT)**". 2020. Disponível em: https://www.gartner.com/en/information-technology/. Acesso em 05 mai 2021.

GHEZZI, Carlo *et al.*. **Fundamentals of software engineering**. 2002.

GUDWIN, Ricardo R. **Engenharia de software: uma visão prática**. 2015.

GSTI, Baseline: **Configuração de referência**. 2016. Disponível em: https://www.portalgsti.com.br/2016/11/baseline-configuracao-de-referencia.html. Acesso em 15/07/2021.

HILGER, Ryan. "**The Navy Must Hide in Plain Sight**". 2021. Disponível em: https://www.usni.org/magazines/proceedings/2021/july/navy-must-hide-plain-sight. Acessado em: 04 de junho de 2021.

HU, Yan *et al.*. **A survey of intrusion detection on industrial control systems. International.** 2018. Journal of Distributed Sensor Networks, v. 14, n. 8, p. 1550147718794615, 2018.

IPQM. **Sistema de Controle e Monitoração**. 2021. Disponível em: http://www.ipqm.mb/ipqmweb/node/138. Acesso em: 30 ago. 2021.

IMO, International Maritime Organization. 2017. Disponível em: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf. Acesso em: 06 abr. 2021.

ISA, ISA/IEC-62443: **Network and system security for industrial-process measurement and control**. 2010.

ISO, International Standard Organization. **ISO 15408: Information Technology -Security Technique -Evaluation Criteria for IT Security.** Abril 2017. v. 3.1, r.5.
ISO, International Standard Organization. **ISO-27001: Sistema de gestão da segurança da informação** , Dezembro 2013.

KARSPERKY. **Threat landscape for industrial automation systems. Statistics for H2 2020**. 2021. Disponível em: https://ics-cert.kaspersky.com/reports/2021/03/25/threat-

landscape-for-industrial-automation-systems-statistics-for-h2-2020/. Acesso em: 07 maio 2021.

KNOWLES, William *et al.*. **A survey of cyber security management in industrial control systems**. 2015. International journal of critical infrastructure protection, v. 9, p. 52-80, 2015.

LAMBA, Anil *et al.*. **Mitigating Cyber Security Threats of Industrial Control Systems (Scada & Dcs)**. 2017. In: 3rd International Conference on Emerging Technologies in Engineering, Biomedical, Medical and Science (ETEBMS–July 2017).

LENDVAY, Ronald L. **Shadows of Stuxnet: Recommendations for US policy on critical infrastructure cyber defense derived from the Stuxnet attack**. 2016. NAVAL POSTGRADUATE SCHOOL MONTEREY CA MONTEREY United States.

LIAO, Hung-Jen *et al.*. **Intrusion detection system: A comprehensive review.** 2013. Journal of Network and Computer Applications, v. 36, n. 1, p. 16-24, 2013.

MACHADO, Murilo Bansi. **Por dentro dos Anonymous Brasil: poder e resistência na sociedade de controle**. 2013. Dissertação (Mestrado em Ciências Humanas e Sociais) – Universidade Federal do ABC, Santo André.

MALIN, Alex; VAN HEULE, Graham. **Continuous monitoring and cyber security for high performance computing**. 2013. In: Proceedings of the first workshop on Changing landscapes in HPC security. p. 9-14.

MITNICK, Kevin D.; SIMON, William L. **The art of deception: Controlling the human element of security**. 2003. John Wiley & Sons.

MODBUS. **Implementando Modbus RTU no Arduino**. 2021. Disponível em: https://mundoprojetado.com.br/implementando-modbus-rtu-no-arduino/. Acessado em: 10 de julho de 2021.

NAVAL. **Fragatas 'Classe Tamandaré' estão em fase avançada de configuração**. 2021. Disponível em: https://www.naval.com.br/blog/2021/06/10/fragatas-classe-tamandare-estao-em-fase-avancada-de-configuracao/. Acesso em: 07/07/2021.

NIST. **Guide to Industrial Control Systems (ICS) Security**. 2015. revisão 2, 247 p Maio 2015. Disponível em: https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final. Acesso em: 05 abr. 2021.

NIST. **Framework for Improving Critical Infrastructure Cybersecurity**, Abril 2018. v. 1.1, 55 p. Disponível em: https://www.nist.gov/cyberframework/framework. Acesso em: 05 abr. 2021.

OTW. **SCADA Hacking: Anatomy of a SCADA Malware, BlackEnergy 3**. 2018. Disponível em: https://www.hackers-arise.com/post/2018/10/10/scada-hacking-anatomy-of-a-scada-malware-blackenergy-3. Acessado em: 07 de julho de 2021.

PALOALTO. **What is a denial of service attack (DoS) ?** 2021. Disponível em: https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos. Acesso em 01/08/2021.

PARMENTER, Robert C. **The Evolution of Preemptive Strikes in Israeli Operational Planning and Future Implications for the Cyber Domain**. 2013. Army command and general staff college fort leavenworth ks school of advanced military studies,

PEREIRA L.T. **Meios Navais: Tendências de desenvolvimento de projetos de plataformas de superfície. Desenvolvimento autóctone de sistemas digitais operativos na MB: vantagens e desvantagens**. Monografia (Curso Superior). Escola de Guerra Naval, Rio de Janeiro, 2011.

PETERSON, Andrea. **Hackers caused a blackout for the first time, researchers say**. 2016. Disponível em: https://www.washingtonpost.com/news/the-switch/wp/2016/01/05/hackers-caused-a-blackout-for-the-first-time-researchers-say/. Acessado em 11 de julho de 2021.

PLIATSIOS, Dimitrios *et al.*. **A survey on SCADA systems: secure protocols, incidents, threats and tactics**. 2020. IEEE Communications Surveys & Tutorials, v. 22, n. 3, p. 1942-1976.

QUEIROZ F.G. **Possibilidades e limitações de emprego da guerra gibernética na MB: Métricas para estabelecimento de uma consciência situacional cibernética do eciber-mb**. Monografia (Curso Superior). Escola de Guerra Naval, Rio de Janeiro, 2018.

SARIKAYA, Alper *et al.*. **What do we talk about when we talk about dashboards?** 2018. IEEE transactions on visualization and computer graphics, v. 25, n. 1, p. 682-692, 2018.

SECURE, Mission. **A Comprehensive Guide to Maritime Cybersecurit**. 2020. Disponível em: https://www.missionsecure.com/hubfs/Assets/eBooks/A%20Comprehensive%20Guide%20to%20Maritime%20Cybersecurity_Final.pdf?hsCtaTracking=ca8e6bac-baa8-40f8-a744-d59df3ea98bf%7Cfb457f1d-e624-476e-96f3-bf89dbfa4747#view=Fit. Acesso em 10/07/2021.

STALLINGS, W.; BROWN, L. **Segurança de computadores: princípios e práticas**. 2014. 2. ed. Rio de Janeiro: Elsevier.

STOUFFER, Keith; FALCO, Joe; SCARFONE, Karen. **Guide to industrial control systems (ICS) security**. 2007. NIST special publication, v. 800, p. 82.

SULLIVAN, Daniel T. **Survey of malware threats and recommendations to improve cybersecurity for industrial control systems version 1.0**. 2015. RAYTHEON TECHNICAL SERVICES CO LLC DULLES VA.

WAGH, Sharmila Kishor *et al.*. **Survey on intrusion detection system using machine learning techniques**. 2013. International Journal of Computer Applications, v. 78, n. 16.

WEIS, Olga. **Duas maneiras de implementar o monitoramento serial para o Arduino**. 2021. Disponível em: https://www.virtual-serial-port.org/pt/articles/arduino-serial-monitor-alternative/. Acessado em: 10 de julho de 2021.

WIRED. **How Israel Spoofed Syria's Air Defense System.** 2007. Disponível em: https://www.wired.com/2007/10/how-israel-spoo/. Acesso em: 06 abr. 2021.

ZNET. **All four of the world's largest shipping companies have now been hit by cyber-attacks**. 2020. Disponível em: https://www.zdnet.com/article/all-four-of-the-worlds-largest-shipping-companies-have-now-been-hit-by-cyber-attacks/. Acessado em: 10 de junho de 2021.

SARIKAYA, Alper *et al.*. **What do we talk about when we talk about dashboards**? 2018. IEEE transactions on visualization and computer graphics, v. 25, n. 1, p. 682-692.

SCHUBA, Christoph L. *et al.*. **Analysis of a denial of service attack on TCP**. 1997. In: Proceedings. 1997 IEEE Symposium on Security and Privacy (Cat. No. 97CB36097). IEEE, p. 208-223.

ZHU, Bonnie; JOSEPH, Anthony; SASTRY, Shankar. **A taxonomy of cyber attacks on SCADA systems**. 2011. In: 2011 International conference on internet of things and 4th international conference on cyber, physical and social computing. IEEE, p. 380-388.

ANEXO A – Glossário

— engenharia social: Essa Técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações. É considerada uma prática de má-fé, usada por golpistas para tentar explorar a ganância, a vaidade e a boa-fé ou abusar da ingenuidade e da confiança de outras pessoas, a fim de aplicar golpes, ludibriar ou obter informações sigilosas e importantes. O popularmente conhecido "conto do vigário" utiliza engenharia social (CERT.BR, 2012).

— Backdoor: programa que permite o retorno de um invasor a um equipamento comprometido, por meio da inclusão de serviços criados ou modificados para este fim. Pode ser incluído pela ação de outros códigos maliciosos, que tenham previamente infectado o computador, ou por atacantes,que exploram vulnerabilidades existentes nos programas instalados no computador para invadi-lo (CERT.BR, 2012) .

— Root-kit: Tipo de código malicioso. Conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido. É importante ressaltar que o nome rootkit não indica que as ferramentas que o compõem são usadas para obter acesso privilegiado (root ou Administrator) em um computador, mas, sim, para manter o acesso privilegiado em um computador previamente comprometido (CERT.BR, 2012).

— Sniffer: Dispositivo ou programa de computador utilizado para capturar e armazenar dados trafegando em uma rede de computadores. Pode ser usado por um invasor para capturar informações sensíveis (como senhas de usuários), em casos onde estejam sendo utilizadas conexões inseguras, ou seja, sem criptografia (CERT.BR, 2012).

— Spyware: Tipo específico de código malicioso. Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. Keylogger, screenlogger e adware são alguns tipos específicos de spyware (CERT.BR, 2012).

— Cavalo de tróia: Tipo de código malicioso. Programa normalmente recebido como um "presente" (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo, etc.) que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas e sem o conhecimento do usuário (CERT.BR, 2012).

— Logic Bomb: Uma Bomba Lógica é uma parte de um código malicioso que é intencionalmente inserido no software. Ele é ativado na rede do host apenas quando certas condições são atendidas.(KABAY, 2008)

— Vírus: Programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo, tornando-se parte de outros programas e arquivos. O vírus depende da execução do programa ou arquivo hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção (CERT.BR, 2012).

— Worms: Tipo de código malicioso. Programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o worm não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar. Sua propagação se dá por meio da exploração de vulnerabilidades existentes ou falhas na configuração de programas instalados em computadores (CERT.BR, 2012).

— Ransomware: é um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (ransom) para restabelecer o acesso ao usuário (CERT.BR, 2012).