DOI 10.21544/1809-3191.v25n1.p89-128

O ENCONTRO DA GUERRA CIBERNÉTICA COM AS GUERRAS ELETRÔNICA E CINÉTICA NO ÂMBITO DO PODER MARÍTIMO

Alan Oliveira de Sá [1]
Raphael Carlos Santos Machado[2]
Nival Nunes Almeida [3]

RESUMO

A busca por melhores capacidades operacionais e gerenciais no Poder Marítimo tem motivado o aumento do uso de sistemas híbridos, em que componentes cibernéticos interagem com plantas físicas e com sensores/dispositivos que exploram o espectro eletromagnético. Entretanto, ao mesmo tempo em que esta integração traz vantagens, ela também expõe tais sistemas a novas ameaças, resultantes do encontro da guerra cibernética com as guerras eletrônica e cinética. O presente artigo analisa como estas novas ameaças podem afetar o Poder Marítimo, caracterizando, por meio de exemplos, seus possíveis alvos. Para dar suporte a esta discussão, propõe-se uma taxonomia que abarca novas classes de ataque que exploram os domínios cibernético, eletrônico e cinético. A análise aponta para a necessidade de políticas capazes de promover a segurança dos sistemas cibernéticos do Poder Marítimo. Neste viés, são discutidas políticas de qualificação de pessoal e de homologação e certificação de produtos cibernéticos, ambas com o potencial de contribuir de forma abrangente para a segurança do Poder Marítimo.

Palavras-chave: Guerra Cibernética; Guerra Eletrônica; Guerra Cinética; Poder Marítimo Doutor. Escola de Guerra Naval (EGN), Rio de Janeiro (RJ), Brasil.

[1] Doutor.Professor do Centro de Instrução Almirante Wandenkolk (CIAW), Rio de Janeiro (RJ), Brasil. E-mail: alan.oliveira.sa@gmail.com
ORCID: http://orcid.org/0000-0001-6311-9672

[2] Doutor. Professor pela Universidade Federal Fluminense (UFF), Rio de Janeiro (RJ), Brasil. E-mail: rcmachado@inmetro.gov.br

[3] Doutor. Escola de Guerra Naval (EGN), Rio de Janeiro (RJ), Brasil.
E-mail: nivalnunes@yahoo.com.br

INTRODUÇÃO

A inclusão do domínio cibernético[4] na arte da guerra vem sendo amplamente discutida nas áreas de Ciência e Tecnologia, Defesa, Estratégia e Relações Internacionais. Por sua complexidade e peculiaridades, as ameaças cibernéticas têm feito com que pesquisadores e estrategistas revisitem os princípios da guerra erguidos ao longo do tempo com base nas literaturas de Sun Tzu, Nicolau Maquiavel, Carl von Clausewitz, Antoine-Henri Jomini, Basil Liddell Hart, dentre outros. Tais princípios, originalmente formulados considerando milênios de guerras cinéticas[5], não aderem integralmente à guerra praticada no domínio cibernético. Segundo a avaliação de Parks e Duggan (PARKS; DUGGAN, 2011), dentre os princípios da guerra cinética (WEIGLEY, 2013; MINISTÉRIO DA DEFESA, 2007; MINISTRY OF DEFENSE, 2014), há aqueles que se aplicam à guerra cibernética, há aqueles que não têm significado na guerra cibernética, e há alguns poucos que, de fato, podem ser considerados antagônicos à guerra cibernética. Todavia, desde os primeiros estrategistas e teóricos da guerra cinética aos pesquisadores atuais da guerra cibernética, observa-se uma característica comum entre os dois tipos de guerra. Ambas devem produzir efeito no mundo real.

Na guerra cibernética tal característica está explícita em um dos oito princípios propostos por Parks e Duggan o princípio de Efeitos Cinéticos. Este princípio enuncia que a guerra cibernética deve produzir efeitos no mundo cinético, só tendo sentido quando afeta alguém ou alguma coisa no mundo real. Em outras palavras, podemos dizer que a energia dispendida por guerreiros cibernéticos em combate só resulta em trabalho quando os resultados afetam – direta ou indiretamente – o mundo físico.

Apesar das dificuldades para descobrir e dissecar ataques cibernéticos – por vezes mantidos sob sigilo –, o princípio de Efeitos

[4] O conceito de domínio cibernético adotado neste artigo agrega a definição de mundo cibernético apresentada por Parks e Duggan (PARKS; DUGGAN, 2011). Segundo aqueles autores, um mundo cibernético é "qualquer realidade virtual contida em um conjunto de computadores e redes". Note que esta definição admite a existência de diversos mundos cibernéticos, em que a Internet seria o mais relevante. Sendo assim, o termo domínio cibernético é usado neste artigo para representar o conjunto de todos os mundos cibernéticos existentes.

[5] Na definição apresentada por Parks e Duggan (PARKS; DUGGAN, 2011), também adotada neste artigo, o termo guerra cinética refere-se à guerra praticada em terra, mar, ar e espaço. É a guerra protagonizada por tanques, navios, aeronaves, soldados etc.

Cinéticos é frequentemente identificado nos casos estudados. Dentre os ataques mais conhecidos, cujos efeitos produzidos/alegados reforçam a pertinência deste princípio, citamos o ataque associado à explosão no gasoduto transiberiano (REED, 2005; CLARK; KNAKE, 2010), o ataque cibernético que apoiou a Operação Orchard (ADEE, 2008; CLARK; KNAKE, 2010; DIPERT, 2013), e o *worm* Stuxnet (LANGNER, 2011; ZETTER, 2014) que impactou o programa nuclear iraniano.

Os três casos são exemplos de ataques em que os efeitos no mundo físico conferiram aos atacantes – Estados-Nações, segundo (CLARK; KNAKE, 2010; ZETTER, 2014) – vantagens táticas ou estratégicas, seja impondo danos físicos diretos ao inimigo ou manipulando informações táticas referentes ao Teatro de Operações. Tais exemplos reforçam a necessidade de compreender as formas de manifestação do princípio dos Efeitos Cinéticos para, a partir de então, estabelecer contramedidas – sejam elas políticas ou técnicas. Isso tem motivado estudos sobre a segurança cibernética nos mais diversos setores, principalmente naqueles classificados como infraestrutura crítica[6] o que, inevitavelmente, abarca o Poder Marítimo[7] . De fato, dependendo das circunstâncias, um incidente – cibernético ou não – em um sistema naval (civil ou militar) pode trazer impactos aos setores de transporte, energia, defesa, alimentos etc. com prováveis prejuízos econômicos, ambientais e à segurança.

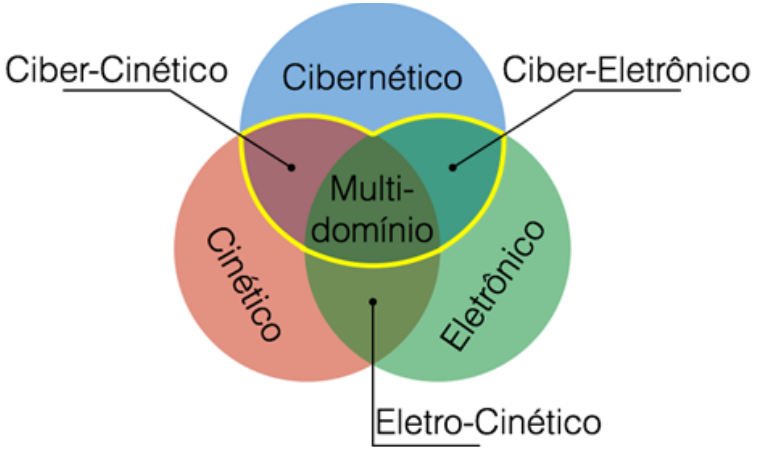
Nesse contexto, o presente artigo discute algumas formas pelas quais ataques com componentes cibernéticas podem alcançar o princípio

[6] De acordo com (Mandarino Junior,(2010) entende-se por infraestruturas críticas (IEC) "as instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provocará sério impacto social, econômico, político, ambiental, internacional ou à segurança do Estado e da sociedade." Dentre as infraestruturas críticas de um país podemos citar, por exemplo: Energia, Defesa, Transporte, Telecomunicações, Finanças, dentre outras, (WHITE HOUSE, 2003; MANDARINO JUNIOR, 2010).

[7] Adotamos neste estudo o conceito de Poder Marítimo definido na Doutrina Básica da Marinha (MARINHA DO BRASIL, 2014): "*O Poder Marítimo é a capacidade resultante da integração dos recursos de que dispõe a Nação para a utilização do mar e das águas interiores, quer como instrumento de ação política e militar, quer como fator de desenvolvimento econômico e social". Segundo a referida doutrina, o poder marítimo é formado pelos seguintes elementos: "o Poder Naval; a Marinha Mercante, as facilidades, os serviços e as organizações relacionados com os transportes aquaviários (marítimo e fluvial); a infraestrutura hidroviária: portos, terminais, eclusas, meios e instalações de apoio e de controle; a indústria naval: estaleiros de construção e de reparos; a indústria bélica de interesse do aprestamento naval; a indústria de pesca: embarcações, terminais e indústrias de processamento de pescado; as organizações e os meios de pesquisa e de desenvolvimento tecnológico de interesse para o uso do mar, das águas interiores e de seus recursos; as organizações e os meios de exploração ou de aproveitamento dos recursos do mar, de seu leito e de seu subsolo; e o pessoal que desempenha atividades relacionadas com o mar ou com as águas interiores e os estabelecimentos destinados à sua formação e ao seu treinamento".*

dos Efeitos Cinéticos, afetando, por exemplo, um combate naval, a navegação, ou mesmo a exploração/uso do mar e de águas interiores. Mais especificamente, discute-se como o princípio dos Efeitos Cinéticos pode ser alcançado quando a guerra cibernética encontra outros dois tipos de guerra comumente praticados no ambiente naval – a guerra eletrônica e a guerra cinética. A análise considera, portanto, três domínios de atuação para os ataques ora estudados: domínio cibernético; o domínio eletrônico; e o domínio cinético. Mais estritamente, o foco deste trabalho está nos subconjuntos de ataques contidos nas interseções destacadas no diagrama da **Figura 1.**

Figura 1 - Classificação dos ataques quanto aos seus domínios de influência/ impacto.



O restante deste artigo está organizado da seguinte forma. Primeiramente, são descritos alguns ataques cibernéticos relevantes já ocorridos, bem como as suas formas de impacto no mundo real. Em seguida, é apresentada uma taxonomia que abrange ataques que exploram os domínios cibernético, eletrônico e cinético. Esta taxonomia visa apoiar a discussão sobre possíveis ataques envolvendo estes três domínios. Posteriormente, o trabalho discute as classes de ataques ciber-cinéticos, ciber-eletrônicos e multidomínio, caracterizando, por meio de exemplos, seus possíveis alvos no Poder Marítimo. Em seguida, são discutidas políticas com o potencial de mitigar os referidos ataques. Por fim, são apresentadas as conclusões.

ATOS DE GUERRA CIBERNÉTICA

Até o presente, a humanidade não experimentou a guerra cibernética de forma tão ampla quanto o fez com a guerra cinética. Se, por um lado, os conhecimentos sobre a guerra cinética foram construídos com base em observações e registros feitos ao longo de milhares de anos, por outro, os conceitos sobre a guerra cibernética se baseiam em experiências adquiridas ao longo de algumas décadas. Ainda assim, os ataques cibernéticos já ocorridos representam uma valiosa fonte de informações para o estudo da guerra cibernética e suas vertentes. Esta seção, portanto, apresenta exemplos de ataques de guerra cibernética com diferentes propósitos e formas de emprego. Embora os ataques aqui descritos não tenham sido praticados em áreas navais – isto é contra belonaves, embarcações civis ou infraestruturas existentes nas margens, sob ou sobre a superfície da água –, eles servem, de forma geral, como referência ou prova de conceito para possíveis ataques que possam vir a causar incidentes em jurisdições navais.

ATAQUE À ESTÔNIA

Em 2007, a Estônia foi alvo de uma série de ataques cibernéticos que afetaram de forma significativa serviços essenciais do país. Para compreender a motivação dos ataques é necessário retornar ao final da Segunda Guerra Mundial. Com a Grande Guerra Patriótica[8], o Exército Vermelho tirou a Estônia do domínio nazista, forçando-a se integrar à União das Repúblicas Socialistas Soviéticas (URSS). Após o período de domínio Soviético, com a desintegração da URSS, a Estônia se tornou independente e estabeleceu novamente sua capital em Tallin. Durante seu domínio, para que os povos do leste europeu se lembrassem dos sacrifícios feitos para libertá-los dos nazistas, a URSS ergueu em muitas capitais da região grandes estátuas de um heroico soldado do Exército Vermelho. E assim também o fez em Tallin.

Tais estátuas eram vistas com muito apreço pelos líderes soviéticos. No entanto, aos olhos dos estonianos, a estátua erguida em Tallin representava um símbolo das cinco décadas de opressão que eles foram obrigados a passar como parte da URSS (CLARK; KNAKE, 2010).

[8] Termo usado pelos russos para se referir à Segunda Guerra Mundial.

Assim, em 2007, atendendo aos sentimentos da população, o legislativo da Estônia aprovou a Lei das Estruturas Proibidas que determinava a remoção da estátua do soldado do Exército Vermelho, o que desagradou Moscou. Para evitar um incidente, o então presidente da Estônia vetou a lei. Nesse contexto, as pressões em torno da preservação, ou não, do símbolo soviético aumentaram.

De um lado, a opinião pública estoniana defendia a remoção da estátua e um grupo nacionalista a tentava destruir. De outro, grupos étnicos russos dedicados a protegê-la se tornavam cada vez mais ativos. conflito culminou em uma revolta, conhecida como a Noite de Bronze (KAISER, 2015), que se seguiu da remoção da estátua para um cemitério militar. Foi quando o conflito migrou para o ciberespaço. A Estônia foi atingida por um ataque DDoS[9] de grande escala – até então o maior registrado. O ataque, lançado por diversas *botnets*[10] , durou semanas e derrubou serviços eletrônicos do governo, bancos, sites de jornais e servidores da rede de telefonia. Devido ao grande impacto, o País Báltico levou o caso ao Conselho do Atlântico Norte, da OTAN. A Estônia alegou que os computadores que controlavam as botnets estavam na Rússia que, por sua vez, negou estar envolvida nos ataques cibernéticos (CLARK; KNAKE, 2010).

GUERRA RUSSO-GEORGIANA

Outro ataque cibernético conhecido – também envolvendo uma antiga república soviética – ocorreu em 2008 na Geórgia (SHAKARIAN, 2011), durante a chamada Guerra Russo-Georgiana. Na época, a Ossétia do Sul era reconhecida internacionalmente como território da Geórgia, no entanto se considerava independente e recebia proteção, financiamento e vivia sob influência russa (CLARK; KNAKE, 2010). Naquele ano, rebeldes

[9] No contexto dos serviços de internet, um ataque de negação de serviço, ou Denial of Service (DoS), é um tipo de ataque em que o serviço executado por um determinado servidor é interrompido devido à quantidade de requisições maior do que a sua capacidade de processamento e resposta. Um ataque distribuído de negação de serviços, ou Distributed Denial of Service (DDoS), por sua vez, é um ataque DoS em que um grande conjunto de equipamentos – composto por até milhares de máquinas – é usado para gerar o tráfego responsável por sobrecarregar o servidor e negar o seu serviço. Os equipamentos atacantes, denominados zumbis, podem ser computadores, servidores, equipamentos de rede ou mesmo dispositivos de Internet das Coisas, ou Internet of Things (IoT).

[10] Rede de dispositivos zumbis, ou bots, controlados remotamente por um computador mestre que, por sua vez comanda os ataques DDoS.

da Ossétia do Sul organizaram uma série de ataques com mísseis contra aldeias da Geórgia. Em resposta, a Geórgia bombardeou a capital da Ossétia do Sul e invadiu a região. No dia seguinte à invasão georgiana, veio a resposta do exército russo expulsando os militares georgianos da Ossétia do Sul. Ocorre que a ofensiva física não foi a única deflagrada contra a Geórgia.

Antes que os ataques cinéticos começassem, ataques cibernéticos já atingiam sites do governo georgiano. Ao longo do conflito, a Geórgia sofreu ataques DDoS direcionados aos seus meios de comunicação, com o objetivo de dificultar que os georgianos percebessem o que estava acontecendo. Os sistemas bancários, de cartões de crédito e de telefonia móvel foram afetados. A maioria dos roteadores que conectavam a Geórgia à Internet, via Turquia e Rússia, foram atacados. A Geórgia perdeu o acesso às fontes de informação e notícia externas. No auge da ofensiva, seis botnets foram mobilizadas para gerar o tráfego de ataque (CLARK; KNAKE, 2010). Embora alguns especialistas considerem que a coordenação entre os ataques cibernéticos e cinéticos tenha sido baixa (SHAKARIAN, 2011), e os russos alegarem que os ataques cibernéticos estavam fora do comando do Kremlin (CLARK; KNAKE, 2010), alguns eventos identificados sugerem ter havido tal coordenação. As instalações físicas da mídia e de sistemas de comunicação, por exemplo, não sofreram ataques cinéticos, apenas cibernéticos. Além disso, hackers russos atacaram um site usado para aluguel de geradores elétricos a diesel, provavelmente em complemento aos ataques convencionais que atingiram a infraestrutura elétrica do país (SHAKARIAN, 2011). É digno de nota que, segundo Shakarian (2011), os objetivos de isolar e desgastar a Geórgia foram limitados em seu escopo, tendo os atacantes evitado causar danos permanentes às redes georgianas e aos seus sistemas SCADA[11] .

STUXNET

O ataque a sistemas SCADA, com consequências cinéticas diretas no mundo real, é verificado em um contexto diferente da Guerra Russo-Georgiana, com o emprego da – possivelmente – mais emblemática arma

[11] Os sistemas de Supervisão e Aquisição de Dados, ou Supervisory Control and Data Acquisition (SCADA), são sistemas usados para controlar, monitorar e fazer a aquisição de dados de sistemas físicos automatizados. Os sistemas físicos controlados vão desde plantas industriais até infraestruturas críticas.

cibernética já usada: o *malware* Stuxnet. Seu propósito estratégico não foi a negação de serviços de internet, mas sim a negação de armas nucleares ao Irã de forma furtiva e sem o emprego de armas físicas. Mais especificamente, seu alvo eram as centrífugas de enriquecimento de urânio que operavam na usina de Natanz. Tais centrífugas, que funcionavam em um sistema de cascatas, eram controladas e operadas por meio de um sistema SCADA composto por controladores Siemens STEP 7.

Utilizando a analogia feita em (ZETTER, 2014), podemos descrever o Stuxnet como um míssil digital usado para transportar dois tipos de ogiva. A porção "míssil" se encarregava de transportar as ogivas digitais até os Controladores Lógicos Programáveis (CLP) que controlavam as centrífugas. Em outras palavras, a parte "míssil", era responsável por fazer com que o malware – mais especificamente um worm – se propagasse e replicasse até encontrar um sistema que tivesse a assinatura do sistema a ser atacado. Uma vez encontrando o sistema alvo – CPLs Siemens conectados às centrífugas –, o worm liberava as ogivas digitais que se instalavam nos CLPs e iniciavam ações sutis de degradação e destruição das centrífugas. Uma das ogivas digitais continha um código que alterava a velocidade de rotação das centrífugas de forma a reduzir a eficiência do processo de enriquecimento, causando também vibrações destrutivas. A outra ogiva atuava na abertura e fechamento das válvulas que interconectavam as centrífugas em cascata, causando aumento de pressão interna e avaria das centrífugas. Cabe ressaltar que o sistema de controle das centrífugas do Irã não estava diretamente conectado à Internet, de forma que, para alcançar a rede de controle, o malware precisava vencer o *air gap*[12] existente entre as duas redes. Sendo assim, dentre outras formas de difusão, o Stuxnet se propagava através de mídias removíveis (pen drives) e instalava seu código malicioso nos CLPs através das máquinas que eram utilizadas para programá-los.

Após a descoberta do Stuxnet, pesquisas demonstraram que, ele além de complexo, dispunha de uma quantidade de recursos nunca antes vistos juntos em uma arma digital. Em sua parte "míssil", o malware reunia ao todo oito formas de propagação (ZETTER, 2014), das quais quatro eram *zero-day exlpoits*[13] (FALLIERE, 2011), o que demonstra o grau

[12] *Air gap* é o termo utilizado para se referir à medida de segurança de redes onde a rede a ser protegida é fisicamente isolada das redes inseguras – como a Internet, por exemplo –, não havendo conectividade entre elas

[13] *Zero-day exploits* são ferramentas que exploram vulnerabilidades do tipo zero-day – i.e. vulnerabilidades desconhecidas por quem estaria interessado em mitigá-las.

de comprometimento e investimento aplicado no projeto.

O Stuxnet foi encontrado em 2010 e investigado por diversos especialistas ao redor do mundo (ZETTER, 2014), tanto da área de sistemas de controle industriais (LANGNER, 2011), quanto da área de segurança da informação (FALLIERE, 2011). As evidências e investigações apontam para a autoria conjunta de EUA e Israel (ZETTER, 2014). O Stuxnet é considerado uma prova de conceito de como as armas digitais podem afetar diretamente o mundo físico, sendo capazes de cumprir os mesmos propósitos estratégicos de ataques com armas cinéticas como mísseis e bombas.

ATAQUE AO GASODUTO TRANSIBERIANO

Embora o Stuxnet seja considerado um marco nos ataques a sistemas ciberfísicos, a literatura (WEISS, 1996; CLARK; KNAKE, 2010; MILLER, 2012) indica a existência de outra bomba lógica de impacto físico anterior ao referido worm. A arma teria sido usada para causar destruição em uma tubulação de transporte de gás situada na Sibéria, no início da década de 1980 (CLARK; KNAKE, 2010) – ou seja, antes mesmo de a Internet estar difundida como nos dias do Stuxnet. À época, sem a grande conectividade da rede mundial de computadores, os atacantes – isto é a CIA com o apoio de Canadenses, segundo (CLARK; KNAKE, 2010) – utilizaram outra estratégia para fazer o código malicioso chegar ao sistema de controle do gasoduto. Para tal, implantaram o código malicioso diretamente no controlador, antes mesmo de o equipamento ser obtido pela Rússia e instalado em seu sistema de automação de dutos (CLARK; KNAKE, 2010).

O controlador seria utilizado para comandar a abertura e o fechamento de válvulas, bem como para controlar o acionamento de bombas que faziam fluir gás na tubulação. Sendo assim, segundo (CLARK; KNAKE, 2010), o código malicioso foi programado para comandar o fechamento da válvula de um segmento do gasoduto, ao mesmo tempo em que a bomba era acionada em capacidade máxima para injetar gás dentro da tubulação. O acionamento indevido dos atuadores do sistema – i.e. a bomba e a válvula – resultou no aumento da pressão interna do duto, causado, por sua vez, a maior explosão não nuclear até então registrada, acima de três quilotons (CLARK; KNAKE, 2010; MILLER, 2012).

Vulnerabilidades zero-day são raras e seus exploits, quando comercializadas no mercado cinza ou negro (ZETTER, 2014) de armas digitais, são caros.

OPERAÇÃO ORCHARD

Um novo tipo de ataque veio à discussão com a Operação Orchard, lançada em 2007 pelo Estado de Israel contra a Síria. Na madrugada de 06 de setembro de 2007, aeronaves da Força Aérea Israelense entraram no espaço aéreo sírio e bombardearam uma instalação industrial que estava sendo construída no território daquele país. Tal instalação era uma planta nuclear que, segundo Clark e Knake (2010), a Síria estava construindo com o apoio da Coréia do Norte. Na ocasião, além da repercussão do próprio bombardeio e das discussões em torno do propósito da planta atacada, chamou a atenção internacional o fato de a Síria, que já havia investido bilhões de dólares em sistemas de defesa aérea (CLARK; KNAKE, 2010), não ter reagido ao ataque. Naquela noite, a Síria estava em alerta, uma vez que Israel, na manhã anterior, havia posicionado suas tropas nas colinas de Golã. Os militares sírios observavam atentamente seus radares. No entanto, no momento em que as aeronaves F-15 Eagles e F-16 Falcons de Israel invadiram o espaço aéreo sírio, nada de incomum apareceu nas telas dos radares do sistema de vigilância.

Na busca por explicações plausíveis para a falha do sistema de vigilância sírio, alguns analistas sugerem que aquele país tenha sido vítima de um ataque de guerra eletrônica. No entanto, o ataque se diferenciava das demais Medidas de Ataque Eletrônico[14] (MAE) conhecidas, por explorar uma vulnerabilidade implantada no domínio cibernético do sistema de vigilância sírio (ADEE, 2008; CLARK; KNAKE, 2010).

Radares, como sensores, são interfaces abertas para o ambiente. Para captar informações sobre possíveis alvos, um radar transmite pulsos por meio de sua antena e capturam, de uma forma geral, todo e qualquer eco que chegue de volta ao seu receptor. Os ecos recebidos, por sua vez, são digitalizados, armazenados em uma memória e processados por um sistema computacional que apresenta ao operador informações relevantes sobre os alvos detectados como, por exemplo, posições e velocidades (BOLE, 2005). Dessa forma, é possível afirmar que um transmissor,

[14] De acordo com (MARINHA DO BRASIL, 2014), as Medidas de Ataque Eletrônico (MAE) correspondem a um "*conjunto de ações tomadas para evitar ou reduzir o uso efetivo, por parte do inimigo, do espectro eletromagnético e, também, degradar, neutralizar ou destruir sua capacidade de combate por meio de equipamentos e armamentos que utilizem este espectro*". As MAE têm natureza fundamentalmente tática e representam um dos três ramos das Medidas de Guerra Eletrônica (MGE) – que também englobam as Medidas de Proteção Eletrônica (MPE) e as Medidas de Apoio à Guerra Eletrônica (MAGE) (MARINHA DO BRASIL, 2014).

apto a transmitir pulsos no mesmo padrão dos transmitidos pelo radar, seja capaz de fazer com que ecos falsos – sinteticamente produzidos – cheguem à antena do radar (ABDALLA et al., NENG-JING; YI-TING, 1995). Estes ecos falsos, uma vez digitalizados, passam a ser representados na forma de bits na memória do radar (BOLE; DINEY; WALL, 2005). Isto significa dizer que é possível manipular os bits da memória de dados de um radar por meio de MAE conhecidas – o que não representa grande novidade em face do estado da arte da guerra eletrônica (ABDALLA et al.; 2015). No entanto, neste ataque, é possível que houvesse no sistema de vigilância um gatilho digital – isto é uma vulnerabilidade implantada em software e/ou hardware – observando constantemente as informações captadas e salvas na memória do radar, em busca de informações com um padrão específico que acionasse tal gatilho digital (ADEE, 2008; CLARK; KNAKE, 2010). Tal gatilho digital, por sua vez, iniciaria rotinas maliciosas no sistema computacional dos radares. Basicamente seriam duas rotinas maliciosas: uma rotina de gravação e outra de reprodução de cenários. As informações, ou bits, com tal padrão específico de acionamento seriam introduzidas na memória pela MAE, por meio da antena do próprio radar. Uma vez identificado o padrão de acionamento da rotina de gravação, o gatilho digital dava início a gravação de um cenário a priori normal – i.e. sem alvos que representassem ameaças. Posteriormente, ao identificar o padrão de acionamento da rotina de reprodução, o gatilho digital passava a reproduzir para os operadores o cenário de operação normal, previamente gravado durante a rotina de gravação. Dessa forma, estima-se que uma MAE em conjunto com um gatilho digital no sistema computacional do radar tenha sido capaz de negar aos operadores sírios a detecção de aeronaves inimigas durante a execução do bombardeio (CLARK; KNAKE, 2010).

SÍNTESE DOS ATAQUES

As ações de guerra cibernética apresentadas nesta seção não esgotam os ataques cibernéticos já ocorridos. No entanto, demonstram a diversidade dos ataques, bem como as formas em que eles foram eficazmente usados como ferramenta para causar danos físicos ou econômicos a nações adversárias, ou mesmo para apoiar a execução de ataques cinéticos em operações militares. No caso do ataque à Estônia, notamos que os ataques executados foram exclusivamente cibernéticos, causando impacto no

mundo real por meio da negação de serviços essenciais para a economia e sociedade estonianas. Na guerra Russo-Georgiana, os ataques cibernéticos foram empregados para apoiar ataques de forças convencionais (SHAKARIAN, 2011), com algum grau de coordenação entre eles. Nos exemplos do Stuxnet e do ataque ao gasoduto transiberiano, as armas digitais foram empregadas para causar danos físicos diretos ao inimigo, sem a necessidade do uso de forças convencionais. Já na operação Orchard um ataque envolvendo ações de guerra cibernética e eletrônica foi usado para apoiar, de forma coordenada, a execução de ataques usando forças convencionais. É possível, portanto, perceber nesses exemplos três tipos de ataque:

- ataques cibernéticos com o objetivo de afetar sistemas de informação e de comunicação, porém sem o propósito de afetar diretamente sistemas físicos (ataques à Estônia e da Guerra Russo-Georgiana);

- ataques cibernéticos com o propósito de afetar diretamente sistemas físicos (Stuxnet e o ataque ao gasoduto transiberiano); e

- ataques cibernéticos envolvendo MAE visando prejudicar a obtenção de informações táticas, mas sem o propósito de manipular diretamente sistemas físicos (ataque na Operação Orchard).

Uma análise mais profunda dessas ofensivas sugere a possibilidade de serem desenvolvidos ataques cibernéticos envolvendo MAE, capazes de afetar diretamente sistemas físicos. Em sistemas navais, mais especificamente, tal possibilidade decorre da crescente integração entre sistemas computacionais, plantas físicas, sistemas de comunicação e sensores que fazem uso do espectro eletromagnético (BOYES; ISBELL, 2017; LAGOUVARDOU, 2018; BHATTI; HUMPHREYS, 2017). Desse modo, o foco da discussão deste trabalho se concentra em ações ofensivas que transitam entre os domínios cibernético, eletrônico e cinético, com possíveis impactos no ambiente naval.

TAXONOMIA

A adição de tecnologias às ferramentas e técnicas de combate por muitas vezes provocou, ao longo do tempo, a revisão da taxonomia militar. Tais revisões taxonômicas visam apoiar a discussão e o estudo da guerra, bem como estabelecer conceitos que promovam o desenvolvimento de capacidades de defesa. Nesse viés, esta seção apresenta uma taxonomia

que reúne terminologias existentes na literatura e estabelece novos termos e conceitos atinentes a ataques que explorem os domínios cibernético, eletrônico e cinético. Primeiramente, é necessário observar as definições das guerras cibernética, eletrônica e cinética:

— **Guerra cibernética,** segundo Parks e Duggan (PARKS; DUGGAN, 2011), é uma combinação de ataques, defesas e operações técnicas especiais em redes de computadores. O ambiente em que tais ações ocorrem é referido como mundo cibernético, cujo conceito, segundo Parks e Duggan, corresponde a "

> *... qualquer realidade virtual contida em um conjunto de computadores e redes.* (PARKS; DUGGAN, 2011, p. 1, tradução nossa).

Note que a definição admite a existência de diversos mundos cibernéticos, uma vez que diferentes realidades virtuais, contidas em diferentes conjuntos de computadores e redes, não interconectadas, podem coexistir. Ainda segundo Parks e Duggan (2011), dentre os diversos mundos cibernéticos existentes, a Internet seria o mais relevante.

O conceito de domínio cibernético adotado no presente artigo agrega a definição de mundo cibernético apresentada por Parks e Duggan (2011). Nesse contexto, o domínio cibernético corresponde ao ambiente composto por todos os mundos cibernéticos existentes.

— **Guerra eletrônica**, segundo (SHELTON, 1998), corresponde a:

> "*... qualquer ação militar envolvendo o uso de energia eletromagnética, dirigida para controlar o espectro eletromagnético ou atacar o inimigo,*"Shelton (1998) p.II-5, tradução nossa).

Em consonância com tal definição, a Política de Guerra Eletrônica de Defesa (MINISTÉRIO DA DEFESA, 2004) estabelece que as atividades de guerra eletrônica nas Forças Armadas visam, de uma forma geral, assegurar o uso do espectro eletromagnético e impedir, reduzir ou prevenir seu uso contra os interesses do país. O domínio da guerra eletrônica, portanto, reside no espectro eletromagnético, mais especificamente nas

faixas de frequência em que operam sensores – por exemplo sistemas radar –, equipamentos de guerra eletrônica e sistemas de comunicação por ondas eletromagnéticas.

— **Guerra cinética,** de acordo com (PARKS; DUGGAN, 2011), é definida como:

> "*...a guerra praticada em terra, mar, ar e espaço. Todos os tanques, navios, aviões e soldados tradicionais são os protagonistas da guerra cinética.*" (PARKS; DUGGAN, 2011, p.1, tradução nossa)

Note que, a definição de guerra cinética apresentada por (Parks; Duggan, (2011) não permite uma caracterização clara do domínio deste tipo de guerra, visto que ações de guerra cibernética e eletrônica também podem ser praticadas em terra, mar, ar e espaço. Por esse motivo, para caracterizar o domínio da guerra cinética, recorremos ao significado de cinética. Considerando que a cinética é a parte da física que estuda as mudanças de movimento produzidas pela força, podemos estabelecer que o domínio da guerra cinética reside no mundo real – isto é não virtual – sujeito a mudanças mediante a aplicação de forças.

Os exemplos de ofensivas digitais discutidas previamente neste artigo demonstram a existência de ataques cibernéticos híbridos que, para produzir o efeito cinético desejado, exploram também os domínios eletrônico e cinético. No diagrama da Figura 1 destacamos três classes de ataques híbridos, que podem derivar da exploração conjunta do domínio cibernético com os domínios eletrônico e/ou cinético:

— **Ciber-Cinéticos:** a classe de ataques ciber-cinéticos engloba ofensivas originadas no domínio cibernético, com o objetivo de causar impactos diretos no domínio cinético. Seus alvos são sistemas em que computadores e redes de comunicação são utilizados para acionar ou controlar processos físicos. Em outras palavras, nesse tipo de ofensiva, medidas de ataque digitais são empregadas para produzir forças físicas capazes de modificar diretamente o mundo real.

— **Ciber-Eletrônicos**: ataques ciber-eletrônicos são ataques compostos em parte por ações de guerra eletrônica contendo também elementos de guerra cibernética. De acordo com Yasar, (2012), pode-se

dizer que o conceito de ataque ciber-eletrônico corresponde a uma nova e aprimorada forma de ataque eletrônico. Em uma guerra eletrônica tradicional, uma MAE – por exemplo uma ação de jamming – pode ser usada, por exemplo, para negar o uso do espectro eletromagnético ao radar inimigo. Por outro lado, em um ataque ciber-eletrônico, o uso do espectro eletromagnético não é essencialmente negado ao sistema alvo. Nesse caso, o espectro eletromagnético é utilizado pelo atacante para enviar um fluxo de dados ao processador do sistema alvo de forma a manipular seu processo computacional, comprometendo assim o seu funcionamento. Para tal, um ataque ciber-eletrônico explora, como porta de entrada, os mesmos dispositivos de captação de ondas eletromagnéticas que o sistema alvo usa para cumprir sua função tática/operacional.

— **Multidomínio**: os ataques multidomínio correspondem a ofensivas que permeiam os três domínios: cibernético, eletrônico e cinético. Têm como alvo sistemas que de alguma forma interconectam plantas físicas, sistemas computacionais de automação e controle, e dispositivos/sensores que exploram o espectro eletromagnético. Nesses sistemas, computadores e redes são utilizados para acionar ou controlar processos físicos, possuindo também interligação – e, eventualmente, interação – com sistemas que operam no domínio da guerra eletrônica. Conceitualmente, em ataques se iniciam no espectro eletromagnético e utilizam como porta de entrada os dispositivos de captação de ondas eletromagnéticas – por exemplo a antena de um radar. Têm como objetivo manipular ou causar danos físicos diretos à planta física. Para tal, utilizam uma componente cibernética como pivô entre os domínios das guerras eletrônica e cinética. Tal componente cibernética, mecanismo digital implantado em software e/ou hardware, se encarrega de transformar informações recebidas a partir do espectro eletromagnético em ações cinéticas maliciosas na planta controlada.

Na Figura 1, podemos verificar ainda um quarto subconjunto de ataques que, por definição, agem simultaneamente – e exclusivamente – nos domínios eletrônico e cinético. Tais ataques, que não agem no domínio cibernético, não estão no enfoque deste trabalho (que se concentra no encontro da guerra cibernética com as guerras eletrônica e cinética). Porém, por uma questão de completude da presente taxonomia, os definimos como ataques eletro-cinéticos.

A título de exemplo, podemos enquadrar nesta classe de ataques

eventuais ofensivas eletromagnéticas lançadas contra espoletas de proximidade utilizadas na Segunda Guerra Mundial (BONNER, 1947; BROWN, 1993). As espoletas de proximidade, embutidas em projéteis, eram basicamente constituídas por um transmissor de ondas eletromagnéticas e um receptor conectado diretamente a uma cadeia de explosivos (Bonner(1947) Brown, (1993). Para deflagrar a cadeia de explosivos, bastava que o receptor do projétil captasse as ondas eletromagnéticas refletidas pelo alvo, as quais deveriam atender a um determinado padrão de amplitude e frequência Doppler. O processo de detonação não passava pelo domínio cibernético. Com base na arquitetura de espoleta apresentada em (BONNER, 1947; BROWN, 1993), é possível dizer que o lançamento de interferências eletromagnéticas específicas contra este tipo de espoleta seria capaz de eventualmente induzir a detonação do projétil, causando efeitos diretos no domínio cinético. Note que um ataque desse tipo contra as referidas espoletas age, conjuntamente, nos domínios eletrônico e cinético sem fazer uso, em nenhum momento, do domínio cibernético. Por esse motivo, o classificamos como um ataque eletro-cinético.

Cabe ressaltar que, na taxonomia ora proposta, as classes de ataques ciber-cinéticos, ciber-eletrônicos e multidomínio visam apenas especificar os domínios que são explorados durante a execução de uma dada ofensiva. Entretanto, as nomenclaturas adotadas e os exemplos discutidos neste artigo não restringem todos os possíveis caminhos que um ataque pode percorrer ao transitar entre os domínios de sua respectiva classe.

DISCUSSÃO

Uma vez estabelecida uma taxonomia abrangendo ataques ciber-cinéticos, ciber-eletrônicos e multidomínio, apresentamos nesta seção uma discussão quanto ao emprego dessas classes de ataque contra alvos pertencentes ao Poder Marítimo. Primeiramente, discutimos de forma sucinta os ataques ciber-cinéticos, ciber-eletrônicos e multidomínio, e caracterizamos alguns de seus possíveis alvos. Em seguida, discutimos políticas que podem contribuir de forma ampla para a mitigação desses tipos de ameaça.

Pelos exemplos de ataque já reportados neste artigo, é possível observar que seus alvos não são exclusivamente militares. Enquanto o ataque ciber-eletrônico da Operação Orchard tinha como alvo um sistema militar de vigilância aérea, os ataques à Estônia e à Geórgia tinham – em grande parte – alvos civis, assim como o ataque ciber-cinético ao gasoduto transiberiano. Sendo assim, na presente discussão, é necessário

considerar tanto alvos civis quanto militares. Ainda que, por vezes, existam diferenças notórias entre esses dois tipos de alvo, é comum que os mesmos compartilhem das mesmas tecnologias – muitas vezes duais. Além disso, um ataque a qualquer um dos dois tipos de alvo pode trazer impactos significativos ao Poder Naval, ao Poder Marítimo e à nação.

ATAQUES CIBER-CINÉTICOS

De acordo com a taxonomia apresentada, um ataque ciber-cinético busca causar impactos diretos em uma planta física, por meio de manipulações digitais no domínio cibernético. Nesse tipo de ataque, o alvo é composto tipicamente por plantas físicas, sistemas computacionais, sensores, atuadores e sistemas de comunicação (DE SÁ; CARMO; MACHADO, 2017; LANGNER, 2011). Os sensores têm o papel de medir o comportamento físico da planta, ao passo que os atuadores cumprem a função transformar sinais de controle em ações físicas capazes de alterar o estado dele. Os sinais de controle são calculados por computadores convencionais, microcontroladores, ou computadores projetados especificamente para o controle de processos físicos, como os Controladores Programáveis (CP) ou Controladores Lógicos Programáveis (CLP[15]) . Sendo os dois últimos (i.e. CPs e CLPs) empregados em grande parte dos sistemas de automação e controle de plantas físicas.

De forma ampla, podemos dizer que o conjunto de potenciais alvos para um ataque ciber-cinético compreende dispositivos de Internet das Coisas (ou *Internet of Things* – IoT) (GUBBI et al., 2013), sistemas da Indústria 4.0 (LEE; BAGHERI; KAO, 2015; LASI et al., 2014) e outros sistemas de controle e automação de plantas não necessariamente industriais. De forma mais estrita, no que tange ao Poder Marítimo, os alvos podem ser, por exemplo:

- Sistemas de automação e controle de navios o que inclui, por exemplo, sistemas de propulsão (HART, 2004) e sistemas de geração de energia (ZIVI, 2005) tanto em meios da marinha mercante quanto do Poder

[15] CLPs e CPs são sistemas computacionais projetados especificamente para executar o controle/automação de plantas físicas. Em geral, são dispositivos de prateleira, genéricos, que podem ser utilizados para o controle de diversos tipos de sistemas bastando, para tal, programá-lo em função das características da planta. São compostos por microprocessadores, memórias, interfaces de programação/comunicação, e interfaces de entrada e saída de sinais. As interfaces de entrada de sinais são utilizadas para receber sinais medidos por sensores na planta. As interfaces de saída de sinais transmitem os sinais de controle para os atuadores da planta.

Naval. No caso de ataques a sistemas geradores de energia, citamos como prova de conceito o experimento de ataque *Aurora* realizado pelo *Idaho National Laboratory,* subordinado ao *Department of Homeland Security* dos EUA. No experimento, os atacantes causam a destruição de um gerador de energia a diesel de 2,25MW por meio de 20 linhas de código de um vírus (AYALA, 2016);

— Sistemas de combate navais, em que sensores e armas são conectados a computadores e redes – ainda que locais –, conforme os exemplos discutidos em (Norcutt, (2001;) Janer; Proum (; 2014);

— Diques flutuantes cujo controle de estabilidade e flutuabilidade é feito via sistemas SCADA (TOPALOV; KOZLOV; KONDRATENKO, 2016);

— Sistemas *offshore* de exploração, produção e transporte de óleo e gás (WADHAWAN; NEUMAN, 2015; ERICKSON et al., 2003), frequentemente controlados por sistemas SCADA;

— Sistema de automação de canais e controle de eclusas (AMIN et al., 2010; AMIN et al. 2013; SMITH, 2015);

— Usinas de geração de energia elétrica a partir de fonte maremotriz, controladas por CLPs e sistemas SCADA (KUMAR; MAJUMDAR; BABU, 2012);

— Parques *eólicos offshore*[16] automatizados (SUN; HUANG; WU, 2012; FLEMING et al. 2017);

— Estaleiros que empreguem sistemas de automação e controle típicos da Indústria 4.0, tanto nos seus processos industriais quanto em suas infraestruturas (ARAKAKI, 2009).

Evidentemente, estes exemplos não esgotam as possibilidades de alvo em um eventual ataque ciber-cinético no Poder Marítimo. No entanto, ajudam a retratar o amplo espectro de sistemas sujeitos a este tipo de ameaça.

Note que em muitos dos exemplos acima mencionados, os controladores (e.g. CLPs e CPs) também são conectados a sistemas supervisórios (SCADA) por meio de redes de comunicação. Além disso, dependendo do propósito da planta física, pode haver ainda a conexão física entre os sistemas SCADA e outras redes – o que eventualmente inclui um caminho físico até a Internet.

[16] Embora ainda esteja começando a ser explorada no Brasil (LUNA, 2018), um estudo do Instituto Nacional de Pesquisas Espaciais (INPE) aponta que "o potencial energético *offshore* na ZEE brasileira é cerca de 12 vezes maior que na área continental do país, sendo capaz de alavancar o desenvolvimento sustentável do Brasil em longo prazo." (ORTIZ; KAMPEL, 2011)

Nos casos em que há a necessidade de uma conexão física entre a rede de controle e outras redes, a literatura recomenda a adoção de soluções de segurança envolvendo, por exemplo, firewalls, zonas desmilitarizadas (ou demilitarized zones – DMZ), sistemas de detecção de intrusão (ou Intrusion Detection System – IDS) e arquiteturas de rede específicas (STOUFFER; FALCO; SCARFONE, 2011). Evidentemente, uma medida de segurança simples e eficiente para minimizar a probabilidade de ataques a estes tipos de sistema consiste em manter a rede de controle isolada de outros tipos de rede – i.e. sem conectividade física entre as mesmas. Esta estratégia, também conhecida como *air-gapping*[17] , é comumente adotada em sistemas críticos como, por exemplo, sistemas nucleares, militares, etc. No entanto, é importante grifar que o uso de *air-gapping* não garante a segurança plena dos sistemas cibernéticos. Um malware pode, por exemplo, vencer o *air-gap* por meio do uso de mídias removíveis, como no caso do Stuxnet (FALLIERE; MURCHU; CHIEN, 2011); ou mesmo ser implantado no sistema antes ou durante o seu comissionamento, como no caso do ataque ao gasoduto transiberiano (CLARK; KNAKE, 2010). Isto sugere a necessidade de adoção de outras medidas de segurança – além das medidas técnicas acima exemplificadas – capazes de mitigar eventuais ataques a estes tipos de sistema, isolados ou não por *air-gap*.

ATAQUES CIBER-ELETRÔNICOS

O conceito de ataque ciber-eletrônico ora apresentado estabelece que este tipo de ofensiva reúne elementos da guerra eletrônica e da guerra cibernética. Evidentemente, portanto, os potenciais alvos para este tipo de ataque têm por característica uma arquitetura que interconecta dispositivos que atuam nos domínios eletrônico e cibernético. Tipicamente estes alvos são compostos por equipamentos de transmissão/recepção de ondas eletromagnéticas e sistemas computacionais que se encarregam de processar as informações recebidas via espectro eletromagnético.

Para facilitar a compreensão de como este tipo de ataque pode ocorrer, trazemos, como exemplo, uma descrição sucinta do funcionamento de um radar de busca com vídeo sintético. Neste tipo de radar, os ecos

[17] *Air-gapping* é uma medida de segurança de rede utilizada para garantir que a rede de computadores a ser protegida esteja fisicamente isolada de redes desprotegidas, como a Internet ou uma rede local insegura. Neste tipo de medida, como não há conectividade física entre as redes, diz-se que elas estão isoladas por uma barreira conceitual de ar (air-gap).

recebidos por sua antena na forma de ondas eletromagnéticas são tratados eletronicamente, convertidos para valores binários e armazenados em uma memória para posterior processamento. Enquanto o radar varre o espaço de busca, todos os ecos válidos recebidos são armazenados na memória formando, assim, um retrato da situação da área monitorada. Para reproduzir a informação armazenada, um processo computacional iterativamente lê os dados contidos na memória e os converte em imagem para o operador do radar (BOLE; DINELEY; WALL, 2005).

Observe que, assim como os ecos reais do ambiente são convertidos em bits e armazenados na memória, os ecos sintéticos, eventualmente transmitidos por um atacante, também serão convertidos em bits e armazenados na mesma memória. Dessa forma, é possível que um atacante transmita comandos codificados em sequências de ecos sintéticos, os quais, ao serem recebidos pelo radar alvo, serão armazenados na memória do sistema como se fossem ecos do ambiente monitorado. Evidentemente, este processo – por ora caracterizado apenas como MAE – por si só não tem a capacidade de alterar o funcionamento normal do radar. Se o sistema não estiver comprometido por um processo computacional mal intencionado, esta informação falsa (inserida por meio de ecos sintéticos) será tratada pelo sistema e pelo operador como dados de alvo ou clutter (BOLE; DINELEY; WALL, 2005). Ainda que esta MAE possa atrapalhar a interpretação do que ocorre no ambiente, ou ainda influencie o processo decisório do usuário, o sistema continuará operando da mesma forma em que foi projetado. Contudo, se o sistema estiver comprometido por um processo computacional malicioso, é possível fazer com que as informações introduzidas na memória do radar por meio de ecos sintéticos (transmitidos pelo atacante) sejam interpretadas como comandos. Neste caso, a componente cibernética do ataque ciber-eletrônico se encarrega de interpretar tais comandos podendo, em função destes, acionar rotinas maliciosas que alterem o processo computacional normal do sistema. Tais rotinas maliciosas podem, por exemplo, causar o desligamento do sistema, interromper a atualização das imagens para o operador, ou mesmo reproduzir imagens previamente gravadas de uma operação normal – como supostamente ocorreu no caso da operação Orchard (CLARK; KNAKE, 2010).

De forma similar ao exemplo acima descrito, outros sistemas que processem informações recebidas via espectro eletromagnético também estão sujeitos a ataques ciber-eletrônicos. Sem a pretensão de esgotar

os potenciais alvos deste tipo de ataque, são apresentados aqui alguns exemplos:

- Sistemas Radar e ARPA (Automatic Radar Plotting Aids) que, de forma geral, façam uso de sinais de vídeo digitalizados (BOLE; DINELEY; WALL, 2005). Isto inclui, por exemplo, radares de navegação, de busca aérea e de busca combinada, utilizados por embarcações e instalações civis e militares;

- Sistemas de Exibição de Cartas Eletrônicas e Informação (Eletronic Chart Display and Information Systems – ECDIS) (WARD; ROBERTS; FURNESS, 2000) que integram às cartas eletrônicas informações obtidas de outros sistemas como radar, gps, etc.;

- Sistemas Integrados do Passadiço (Integrated Bridge System – IBS), que interconectam sistemas radar/ARPA, GPS, etc. a Sistemas de Exibição de Cartas Eletrônicas e Informação (ECDIS), bem como a sistemas de controle de leme e propulsão de navios (BHATTI; HUMPHREYS, 2017);

- Sistemas de Medida de Apoio à Guerra Eletrônica (MAGE), composto tipicamente por antenas, receptores de micro-ondas e sistemas computacionais responsáveis por processar, classificar e identificar as emissões eletromagnéticas presentes no ambiente (MATUSZEWSKI, 2008).

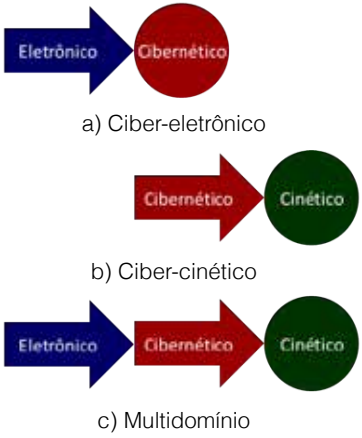
Em geral, estes sistemas são mantidos isolados de outras redes de comunicação (e da Internet). Isto significa que, em grande parte dos casos, a componente cibernética do ataque ciber-eletrônico deve ser capaz de vencer o *air-gap* para se instalar no ambiente computacional do alvo. Contudo, apesar da dificuldade imposta pelo *air-gap*, estes sistemas não podem ser considerados integralmente seguros do ponto de vista cibernético. Assim como relatamos no caso de ataques ciber-cinéticos, um malware pode, por exemplo, vencer o *air-gap* através de mídias removíveis. Além disso, um gatilho lógico pode ser implantado no alvo durante a sua fabricação ou comissionamento.

ATAQUES MULTIDOMÍNIO

Na taxonomia apresentada descrevemos os ataques multidomínio como aqueles cuja execução permeia os três domínios ora em discussão: cibernético, eletrônico e cinético. Já tratamos conceitualmente neste artigo como um ataque cibe-eletrônico pode manipular um sistema

computacional – e acionar processos mal intencionados – a partir de comandos/informações sintéticas recebidas do domínio da guerra eletrônica. Tal conceito de ataque é representado e exemplificado na Figura 2a. Discutimos conceitualmente, também, como manipulações digitais mal intencionadas no domínio cibernético podem produzir efeitos cinéticos diretos em uma planta física, através de ataques ciber-cinéticos. Para comparação, este conceito de ataque também é representado na Figura 2b. Em ataques multidomínio, a componente cibernética do ataque atua como um pivô entre os domínios das guerras eletrônica e cinética. Conforme ilustrado na Figura 2c, a componente cibernética pode ser implantada para permitir, por exemplo, que comandos originados no domínio da guerra eletrônica sejam interpretados e convertidos em efeitos cinéticos diretos em uma planta física.

Figura 2 –Fluxos de acionamento dos ataques.



Portanto, os potenciais alvos para este tipo de ataque são sistemas que integram equipamentos de transmissão/recepção de ondas eletromagnéticas e sistemas computacionais que controlam plantas físicas. Um exemplo de potencial alvo para ataques multidomínio são os Sistemas Integrados do Passadiço (Integrated Bridge System – IBS), ou ainda sistemas Smartship (FULLERTON et al., 2004). Dentre os dispositivos de transmissão/recepção de ondas eletromagnéticas conectados à um IBS há sistemas radar/ARPA, receptores GPS, e receptores AIS (Automatic Identification System). Tipicamente, os IBSs reúnem em um único local informações oriundas destes sistemas, plotando em uma carta náutica digital as informações do navio e de

outras embarcações – detectadas pelos radares de navegação. A interligação do IBS com os sistemas de controle da propulsão e do leme permite a realização de funções de piloto automático, eliminando a necessidade de atuação contínua de um timoneiro (FULLERTON et al., 2004; BHATTI; HUMPHREYS, 2017). O uso de IBSs em meios navais proporciona como vantagens a redução das tripulações, o aumento da prontidão dos navios, a redução do tempo necessário para treinamento, o aumento da consciência situacional, e a redução da carga administrativa sobre o pessoal (FULLERTON et al., 2004). Estes benefícios têm motivado o aumento do uso destes sistemas tanto em navios mercantes quanto em navios de guerra (FULLERTON et al., 2004).

Ao mesmo tempo em que sistemas do tipo IBS trazem uma série de vantagens, também podem expor os meios navais a novos tipos de ameaça, como os ataques multidomínio. Do mesmo modo que a componente cibernética de um ataque ciber-eletrônico pode acionar processos computacionais maliciosos a partir da interpretação de comandos oriundos do espectro eletromagnético, isto também pode ocorrer em um ataque multidomínio. No entanto, em um ataque multidomínio, o processo computacional malicioso, ao ser acionado, estende suas ações e atinge os processos físicos controlados. Em um IBS, por exemplo, isto significa que o controle da propulsão pode ser afetado por comandos recebidos por uma antena (e.g. a antena de um radar), se o sistema estiver infectado por um código malicioso capaz de interpretar/converter as informações recebidas em comandos para a máquina do navio.

Note que, mesmo que o alvo esteja protegido pelo *air-gap*, a componente cibernética do ataque pode ser injetada no sistema mor meio de mídias removíveis. Além disso, conforme já discutido anteriormente, este tipo de gatilho lógico também pode ser implantado no alvo durante a sua fabricação ou comissionamento. A motivação de um ataque deste tipo está na capacidade de o atacante acionar remotamente rotinas maliciosas que impactem fisicamente o funcionamento dos meios, sem a necessidade de ter acesso direto ao ambiente cibernético do alvo.

POLITICAS PARA MITIGAÇÃO DE ATAQUES

Nesta seção são discutidas algumas políticas para a segurança do poder marítimo em relação às três classes de ataque em questão. Considerando que o domínio cibernético é a parcela comum aos referidos ataques, o foco da discussão se concentra em políticas voltadas para a segurança deste domínio. Mais especificamente, são abordadas políticas visando a qualificação de pessoal e a homologação e certificação de produtos.

QUALIFICAÇÃO DE PESSOAL

Em 2003, o governo dos EUA publicou a sua estratégia nacional para segurança do ciberespaço (WHITE HOUSE, 2003), onde declara como propósito:

> "*... envolver e capacitar os Americanos para proteger as parcelas do ciberespaço que possuem, operam, controlam ou com as quais interagem." (WHITE HOUSE, 2003, p.vii,* tradução nossa)

Ao mesmo tempo em que a referida estratégia traça este objetivo, a mesma reconhece que:

> *"Proteger o ciberespaço é um desafio estratégico difícil, que requer esforço coordenado e concentrado de toda a nossa sociedade - o governo federal, os governos estaduais e locais, o setor privado e o povo Americano."* (WHITE HOUSE, 2003, p.vii, tradução nossa).

De fato, proteger o ciberespaço é um desafio estratégico complexo, a começar – no caso específico daquela Estratégia – pelo objetivo de envolver e capacitar o povo Americano na proteção de suas parcelas do ciberespaço. Algo difícil de ser alcançado de forma plena, se considerarmos todos os elementos e setores da sociedade previstos em (WHITE HOUSE, 2003). No entanto, apesar das dificuldades impostas pela abrangência, é indiscutível a necessidade de uma nação perseguir o objetivo de envolver e capacitar a sua sociedade na segurança do ambiente cibernético.

Da mesma forma, inspirados no propósito de White House (2003), consideramos imprescindível envolver e capacitar os atores do Poder Marítimo quanto à proteção de suas parcelas do ciberespaço. Embora o Poder Marítimo represente público menor do que o visado por White House (2003), trata-se ainda de um público abrangente. Por este motivo, qualificar o pessoal do Poder Marítimo quanto à segurança de suas parcelas do ciberespaço é uma tarefa desafiadora, que sugere o emprego de políticas de conscientização e capacitação de pessoal. Estas políticas devem abranger não só os recursos humanos do Poder Naval e da Marinha Mercante, mas também de setores industriais e infraestruturas pertencentes ao Poder Marítimo.

No Brasil, os recursos humanos do Poder Naval e da Marinha

Mercante, são formados pelo Sistema de Ensino Naval e pelo Sistema de Ensino Profissional Marítimo, ambos de responsabilidade da Marinha do Brasil (BRASIL, 2006). É desejável, portanto, que os currículos dos referidos Sistemas de Ensino contenham disciplinas que abarquem conceitos sobre o funcionamento e a segurança do domínio cibernético e de sistemas híbridos (onde o domínio cibernético interage diretamente com os domínios eletrônico e/ou cinético).

A exemplo da discussão apresentada em (SCHNEIDER, 2013; CONKLIN; CLINE; ROOSA, 2014) - onde a educação sobre segurança cibernética visa um público mais abrangente do que nos casos do Poder Naval e da Marinha Mercante - o desafio maior está em promover a qualificação dos recursos humanos dos setores industriais e de infraestruturas pertencentes ao Poder Marítimo, no que concerne à segurança cibernética e de sistemas híbridos. Isto porque a formação técnico-profissional de seu pessoal conta com a participação de um grande número de instituições e estabelecimentos de ensino, públicos e privados. Deste modo, e com base na discussão apresentada em (SCHNEIDER, 2013), é razoável concluir não ser trivial solucionar a questão através de um processo amplo de aprimoramento curricular - ainda que necessário. Neste caso, soa ser adequado apoiar estes setores através de programas de treinamento e conscientização promovidos, a priori, pelos órgãos do Estado responsáveis pela Segurança e Defesa cibernética no Brasil – i.e. o Gabinete de Segurança Institucional e o Comando do Exército, respectivamente.

Iniciativa similar a essa é praticada, por exemplo, pelo Department of Homeland Security, dos EUA, por meio dos programas de treinamento conduzidos pelo Industrial Control Systems Cyber Emergency Readiness Team (ICS-CERT). O ICS-CERT oferece continuamente cursos de segurança cibernética de sistemas de controle industrial para o pessoal da indústria e de infraestruturas críticas daquele país, bem como para desenvolvedores/fornecedores de dispositivos e softwares. É importante ressaltar que os programas de treinamento do ICS-CERT não se restringem à indústria do Poder Marítimo dos EUA, abrangendo também outros setores da indústria. No modelo do ICS-CERT, o referido órgão federal apoia de forma centralizada a qualificação do pessoal da indústria no assunto. No caso do Poder Marítimo brasileiro, guardadas as devidas proporções, um modelo similar de apoio centralizado à capacitação parece ser adequado para suprir a necessidade da sua indústria e infraestruturas, no que concerne à segurança dos tipos de sistema discutidos neste artigo.

HOMOLOGAÇÃO E CERTIFICAÇÃO DE PRODUTOS

Discutiu-se neste artigo uma possível estratégia de qualificação de pessoal para promover a segurança de sistemas cibernéticos e híbridos do Poder Marítimo. Contudo, ainda que tal qualificação seja de extrema importância, ela não é, por si só, suficiente para maximizar a segurança dos sistemas (BAARS et al.; 2015). Para uma maior segurança, as políticas de qualificação de pessoal devem ser complementadas por políticas que combatam possíveis vulnerabilidades tecnológicas nos *hardwares e softwares.*

As vulnerabilidades de um sistema podem surgir de forma não intencional (DU; MATHUR, 1998; GROVER; CUMMINGS; JANICKI, 2016), por falhas de projeto, implementação ou configuração, ou podem ser intencionalmente introduzidas por agentes maliciosos (ADEE, 2008; ROBERTSON; RILEY, 2018) durante o projeto, fabricação, distribuição, comissionamento, operação e manutenção do sistema. Uma forma de combater vulnerabilidades – intencionais ou não – é por meio da adoção de um conjunto de requisitos de segurança, estabelecidos de acordo com a criticidade do sistema, os quais devem ser rigorosamente atendidos (HERRMANN, 2002).

Chega-se, então, à seguinte pergunta: como garantir que um equipamento em uso pelo Poder Marítimo atende a um determinado conjunto de requisitos de segurança, permitindo afastar ou mitigar determinado conjunto de riscos de segurança cibernética? Tal pergunta traz uma série de desafios, sobre os quais passamos a dissertar, a seguir.

Considere a complexidade da cadeia de produção dos produtos de hardware e software usados pelo Poder Naval, pela Marinha Mercante, pelas indústrias e infraestruturas pertencentes ao Poder Marítimo. A indústria responsável pela produção de equipamentos civis, militares ou duais do Poder Marítimo brasileiro não apenas opera distante do monitoramento dos órgãos de Segurança e Defesa cibernética do Brasil como também, por pertencer à cadeia global de valores de eletrônicos, muitas vezes depende de intricadas cadeias de produção que incluem a subcontratação de empresas baseadas em outros países (PINTO, 2016) – o que dificulta ainda mais o monitoramento da produção. Dessa forma, mesmo que se tenha um entendimento pleno a respeito dos requisitos

de segurança cibernética a serem atendidos pelos hardwares/softwares, pouca confiança pode ser trazida por um processo de avaliação baseado tão-somente em testes "funcionais" – i.e. testes que caracterizem o comportamento do hardware/software em condições típicas de operação. De fato, conforme os exemplos apresentados em (ZETTER, 2014; ADEE, 2008; CLARK; KNAKE, 2010), caso um equipamento viesse a ser objeto de manipulação com vistas à implantação de um comportamento malicioso por parte de uma nação hostil, certamente tal comportamento malicioso seria ativado por meio de operações não triviais, dificilmente identificados através de testes meramente associados às condições típicas de uso do equipamento.

Note que a literatura tem reportado casos com indícios/evidências de implantações maliciosas em sistemas cibernéticos críticos, embora muitas vezes careçam de detalhes em virtude do sigilo. Um exemplo é o caso do ataque ao sistema de vigilância aéreo sírio ocorrido durante a operação Orchard, já discutido neste artigo. Conforme relatado em (ADEE, 2008), especula-se que os microprocessadores comerciais no radar sírio possam ter sido propositalmente fabricados com um backdoor escondido. Ao enviar um código pré-programado para esses chips, um atacante desconhecido teria a capacidade de bloquear temporariamente o radar. Sobre a prática de implantar vulnerabilidades em hardwares, Adee afirma ainda que:

> *"De acordo com um fornecedor do setor de defesa dos EUA que falou sob condição de anonimato, um "fabricante europeu de chips" recentemente embutiu em seus microprocessadores uma chave de desligamento que pode ser acessada remotamente."*
> (ADEE, 2008, p.1, tradução nossa)

Um exemplo mais recente de implantação de chips maliciosos em hardwares de sistemas críticos é relatado em (ROBERTSON; RILEY, 2018). Trata-se de um ataque à cadeia de produção – ou supply chain attack – reportado pela Amazon.com Inc. às autoridades dos EUA. Neste caso, especialistas identificaram um minúsculo microship, "não muito maior do que um grão de arroz" (ROBERTSON; RILEY, 2018), escondido em placas-mãe de servidores. Tal microship não fazia parte do projeto original das placas. Segundo Robertson e Riley, investigadores concluíram que os referidos chips permitem que invasores criem uma entrada furtiva em

qualquer rede que contenha as máquinas com as placas alteradas. Além disso, segundo Robertson e Riley, investigadores relatam que os chips foram inseridos em fábricas controladas por empresas subcontratadas na China (ROBERTSON; RILEY, 2018). Dentre os sistemas críticos comprometidos pelo supply chain attack estão centros de dados do Departamento de Defesa dos EUA, sistemas de operação de drones da CIA e as redes a bordo de navios de guerra da Marinha dos EUA (ROBERTSON; RILEY, 2018).

Sendo assim, com o objetivo de mapear e mitigar os riscos associados ao uso de softwares e hardwares produzidos em ambientes não monitorados, algumas nações ao redor do mundo têm implantado sistemas de homologação de produtos cibernéticos (FNCA, 2018; DSD, 2015; NIST, 2011; DISA, 2017). Trata-se de metodologias que permitem atestar, com um grau mínimo de confiança, e por meio de testes e ensaios sistemáticos, que um produto de software ou hardware atende a um conjunto de requisitos de segurança – mesmo que o seu processo de produção não esteja completamente sob controle/supervisão dos órgãos de segurança e defesa cibernética do país. Dentre os sistemas deste tipo existentes pelo mundo citamos Certification de Sécurité de Premier Niveau (CSPN) (FNCA, 2018) utilizado na França, o Australasian Information Security Evaluation Program (AISEP) (DSD, 2015) implementado na Autrália e Nova Zelândia (DSD, 2015), o Department of Defense Information Network Approved Products List (DoDIN/APL) dos EUA e o Federal Information Processing Standard 140-2 (FIPS 140-2) (NIST, 2011) adotado tanto nos EUA quanto no Canadá.

O Brasil vem ocupando uma posição de relativo pioneirismo nessa área, ao estabelecer o chamado Sistema de Homologação e Certificação de Produtos de Defesa Cibernética (SHCDCiber). O SHCDCiber foi concebido em 2015 e tem por objetivo estabelecer um sistema de avaliação de segurança cibernético objetivo e baseado nas principais normas internacionais, garantindo o rigor científico nas avaliações de segurança e o reconhecimento internacional por parte dos fabricantes que submeterem seus produtos à avaliação.

A exemplo dos sistemas CSPN, AISEP, DoDIN/APL e FIPS 140-2, o SHCDCiber consiste num sistema voltado para o uso de mecanismos de avaliação da conformidade com o objetivo de avaliar a segurança de ativos de tecnologia e equipamentos com software embarcado. Trata-se, portanto, de um sistema com potencial de contribuir para o aumento da segurança dos sistemas cibernéticos e híbridos do Poder Marítimo. O SHCDCiber segue uma abordagem de avaliação da conformidade composta de três

etapas:

1 - Análise de riscos da aplicação. Cada aplicação apresenta um conjunto de riscos específicos e que deve ser levando em consideração na construção de mecanismos de avaliação.

2 - Especificação de requisitos. Os requisitos exatos de segurança a serem atendidos por uma aplicação serão determinados pelos riscos apresentados por aquela aplicação.

3 - Ensaios de segurança. O atendimento a um conjunto de requisitos de segurança é realizado por meio da execução de ensaios que correspondem a procedimentos sistemáticos de validação.

As três etapas acima, realizadas conjuntamente, contemplam o que se pode denominar como um Programa de Avaliação da Conformidade. Na área de segurança da informação, tais programas são particularmente desafiadores, na medida em que o comportamento de um ativo de Tecnologia de Informação e Comunicação (TIC) depende de seu software embarcado. Dessa forma, pesquisas vêm sendo desenvolvidas no sentido de aumentar a confiança em avaliações de segurança nas áreas de criptografia (MACHADO et al., 2016; KOWADA; MACHADO; 2017), aleatoriedade (RIBEIRO et al. 2018), protocolos de segurança (MACHADO et al., 2015), análise de software (BENTO, 2017, no prelo) e testes caixa-preta (TELES; MACHADO, 2017).

Cabe observar que a aprovação em um programa de avaliação da conformidade não significa uma confiança total na segurança do objeto aprovado. Afinal, os requisitos são especificados em consistência com os riscos de aplicação – e variações no cenário de riscos podem levar a eventuais mudanças na condição de segurança de um produto ou sistema.

Análise crítica. Mesmo após o sucesso nas etapas anteriores, dependendo da criticidade, cabe ainda observar aspectos adicionais que podem levar à decisão pela não adoção de uma tecnologia. Tais aspectos incluem, tipicamente, as características do desenvolvedor e do seu processo produtivo. Como exemplo, listamos algumas perguntas a serem respondidas antes da adoção de uma tecnologia – mesmo que a mesma tenha superado adequadamente as etapas 1 a 3:

- O fornecedor da tecnologia tem condições de atender aos pedidos na escala demandada?

- O fornecedor da tecnologia possui um sistema de gestão

de segurança da informação implantado?

- Mais especificamente nos sistemas do Poder Naval, dependendo da criticidade do sistema, os desenvolvedores e produtores – pessoas a serviço de entidades públicas ou privadas – possuem a devida credencial de segurança para lidar com o produto ou tecnologia em questão?

- O fornecedor da tecnologia cumpre processos adequados de proteção e descarte de dados sensíveis?

- O fornecedor da tecnologia mantém o núcleo de sua produção (conhecimento crítico para a produção) no país?

CONCLUSÕES

Neste artigo discutimos como o encontro da guerra cibernética com as guerras eletrônica e cinética pode impactar diretamente o Poder Marítimo. Visando dar suporte à discussão sobre as novas vertentes da guerra cibernética que decorrem deste encontro, apresentamos uma taxonomia que estabelece classes de ataques híbridos que, além de explorar o domínio cibernético, exploram também os domínios eletrônico e cinético. Desta taxonomia, emergem três classes de ataque – ciber-cinético, ciber-eletrônico e multidomínio – que ampliam o espectro das formas de manifestação do princípio dos efeitos cinéticos. Discutimos estas três classes de ataque e caracterizamos, por meio de exemplos, seus potenciais alvos dentro do Poder Marítimo. A discussão, pautada em casos conhecidos, evidências e deduções tecnológicas, indicam ser factível a ocorrência de estes tipos de ataque no referido Poder. Sendo assim, o estudo aponta para a necessidade de desenvolver políticas capazes de promover a segurança dos sistemas cibernéticos e híbridos do Poder Marítimo.

Considerando que o domínio cibernético é a parcela comum entre as três classes de ataque analisadas neste artigo, concentramos a nossa discussão em políticas voltadas para a segurança deste domínio, abordando tanto a questão de qualificação de pessoal, quanto o combate às vulnerabilidades em produtos cibernéticos. No que concerne à qualificação de pessoal, encorajamos a adoção de um modelo apoiado nos sistemas de ensino naval e profissional marítimo, já existentes, complementado pela atuação de um órgão centralizado de capacitação sobre segurança cibernética. O Sistema de Ensino Naval e o Sistema de Ensino Profissional Marítimo, com currículos continuamente atualizados

quanto ao assunto, se encarregariam da capacitação do pessoal do Poder Naval e da Marinha Mercante, respectivamente (como já é previsto). Já um órgão centralizado de capacitação sobre segurança cibernética se encarregaria de promover a qualificação dos recursos humanos dos setores industriais e de infraestruturas pertencentes ao Poder Marítimo. No que tange a mitigação de vulnerabilidades em produtos cibernéticos em uso no Poder Marítimo, o estudo aponta para a solução por meio de um sistema de homologação e certificação de produtos cibernéticos, o que já vem sendo adotado de alguma forma por países como a França, Austrália, Nova Zelândia, EUA e Canada. Cabe ressaltar, que as políticas de qualificação de pessoal, homologação e certificação de produtos aqui discutidas não têm a pretensão de assegurar, de forma plena, a segurança dos sistemas cibernéticos e híbridos do Poder Marítimo. No entanto, têm o potencial de contribuir, de forma positiva e abrangente, para a segurança destes sistemas.

THE MEETING OF CYBER WARFARE WITH THE ELECTRONIC AND KINETIC WARFARES IN THE SCOPE OF THE SEA POWER

ABSTRACT

The search for better operational and management capacities in the Sea Power has motivated the increase of the use of hybrid systems, where cybernetic components interact with physical plants and with sensors/devices that explore the electromagnetic spectrum. However, at the same time as this integration brings benefits, it also exposes such systems to new threats that result from the meeting of cyber warfare with the electronic and kinetic warfares. The present paper analyzes how these new threats can affect the Sea Power, characterizing, through examples, their possible targets. To support this discussion, it is proposed a taxonomy that encompasses new classes of attack that exploit the cybernetic, electronic, and kinetic domains. The analysis indicates the need for policies capable of promoting the cybersecurity of the Sea Power. In this sense, policies regarding personnel training and certification of cyber products are discussed, both with the potential to contribute comprehensively to the security of the Sea Power.

Key-words: Cyberwarfare; Electronic Warfare; Kinetic Warfare; Sea Power.

REFERÊNCIAS

ADEE, Sally. The hunt for the kill switch. IEEE Spectrum, v. 45, n. 5, p. 34-39, 2008.

AMIN, Saurabh et al. Cyber security of water SCADA systems—Part I: Analysis and experimentation of stealthy deception attacks. IEEE Transactions on Control Systems Technology, v. 21, n. 5, p. 1963-1970, 2013.

AMIN, Saurabh et al. Stealthy deception attacks on water SCADA systems. In: Proceedings of the 13th ACM international conference on Hybrid systems: computation and control. ACM, 2010. p. 161-170.

ARAKAKI, Glenn T. Yokosuka Naval Base Prepares for Nuclear Aircraft Carrier. Army Engineer School Fort Leonard Wood MO, 2009.

AYALA, Luis. Prevent Hackers from Destroying a Backup Generator. In: Cyber-Physical Attack Recovery Procedures. Apress, Berkeley, CA, 2016. p. 41-42.

BENTO, Lucila MS et al. Dijkstra graphs. Discrete Applied Mathematics, 2017. No prelo.

BHATTI, Jahshan; HUMPHREYS, Todd E. Hostile control of ships via false GPS signals: Demonstration and detection. NAVIGATION: Journal of the Institute of Navigation, v. 64, n. 1, p. 51-66, 2017.

BOLE, Alan G.; DINELEY, William O.; WALL, Alan. Radar and ARPA manual. 2. ed. Oxford: Elsevier Butterworth Heinemann, 2005.

BONNER, Henry M. The radio proximity fuse. Electrical Engineering, v. 66, n. 9, p. 888-893, 1947.

BOYES, Hugh; ISBELL, Roy. Code of Practice: Cyber Security for Ships. 2017.

BRASIL. Lei nº 11.279, de 9 de fevereiro de 2006. Dispõe sobre o ensino na

Marinha. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2006/Lei/L11 279.htm>. Acesso em: 29 out. 2018.

BROWN, Louis. The proximity fuze. IEEE Aerospace and Electronic Systems Magazine, v. 8, n. 7, p. 3-10, 1993.

CLARK, Richard A.; KNAKE, Robert K. Cyber War: The next threat to national security and what to do about it. New York: Ecco, 2010.

DE SÁ, Alan Oliveira; DA COSTA CARMO, Luiz F. Rust; MACHADO, Raphael CS. Covert attacks in cyber-physical control systems. IEEE Transactions on Industrial Informatics, v. 13, n. 4, p. 1641-1651, 2017.

DIPERT, Randall R. Other-than-Internet (OTI) cyberwarfare: challenges for ethics, law, and policy. Journal of Military Ethics, v. 12, n. 1, p. 34-53, 2013.

DISA. Department of Defense Information Network (DoDIN) Approved Products List (APL) Process Guide. Defense Information Systems Agency (DISA). 2017. Disponível em: <https://aplits.disa.mil/docs/aplprocessguide.pdf> Acesso em: 28 out. 2018.

DSD. Australian government information and communications technology security manual. Defence Signals Directorate (DSD) Auditing, v. 3, p. 31, 2005.

ERICKSON, Kelvin T. et al. Reliability of S CADA Systems in Offshore Oil and Gas Platforms. In: Stability and Control of Dynamical Systems with Applications. Birkhäuser, Boston, MA, 2003. p. 395-404.

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

FLEMING, Paul et al. Field test of wake steering at an offshore wind farm. Wind Energy Science, v. 2, n. 1, p. 229-239, 2017.

FNCA. Catalogue of the Qualified Solutions. French National

Cybersecurity Agency (FNCA). 2018. Disponível em: <https://www.ssi.gouv.fr/uploads/2018/01/catalogue_ qualified_solutions_anssi.pdf> Acesso em: 28 out. 2018.

FULLERTON, Jeff et al. Operational Impacts of the Aegis Cruiser Smartship System. NAVAL SEA SYSTEMS COMMAND WASHINGTON DC, 2004.

GUBBI, Jayavardhana et al. Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems, v. 29, n. 7, p. 1645-1660, 2013.

HART, Dennis. An approach to vulnerability assessment for Navy Supervisory Control and Data Acquisition (SCADA) system. 2004. Tese de Mestrado. Monterey, California. Naval Postgraduate School.

JANER, Denis; PROUM, Chauk-Mean. Open Architecture for Naval Combat Direction System. In: Complex Systems Design & Management. Springer, Cham, 2014. p. 73-84.

KAISER, Robert. The birth of cyberwar. Political Geography, v. 46, p. 11-20, 2015.

KOWADA, L. ; MACHADO, R.C.S. . Esquema de Acordo de Chaves de Conferência Baseado em um Problema de Funções Quadráticas de Duas Variáveis. Anais do XVII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg), 2017, Brasília, 2017.

KUMAR, Nishant; MAJUMDAR, Sayan; BABU, G. Madhu. Automatic control of tidal power plant. In: Emerging Trends in Electrical Engineering and Energy Management (ICETEEEM), 2012 International Conference on. IEEE, 2012. p. 24-28.

LAGOUVARDOU, Sotiria. Maritime Cyber Security: concepts, problems and models. 2018.

LANGNER, Ralph. Stuxnet: Dissecting a cyberwarfare weapon. IEEE Security & Privacy, v. 9, n. 3, p. 49-51, 2011.

LASI, Heiner et al. Industry 4.0. Business & Information Systems Engineering, v. 6, n. 4, p. 239-242, 2014.

LEE, Jay; BAGHERI, Behrad; KAO, Hung-An. A cyber-physical systems architecture for industry 4.0-based manufacturing systems. Manufacturing Letters, v. 3, p. 18-23, 2015.

LUNA, D. Petrobrás vai gerar energia eólica no mar. O Estado de S.Paulo, São Paulo, 24 de julho de 2018. Disponível em: < https://economia.estadao.com.br/noticias/geral,petrobras-vai-gerar-energia-eolica-no-mar,70002412545> Acesso em: 17 out. 2018.

MACHADO, Raphael CS et al. Fair fingerprinting protocol for attesting software misuses. In: Availability, Reliability and Security (ARES), 2015 10th International Conference on. IEEE, 2015. p. 110-119.

MACHADO, Raphael CS et al. Software control and intellectual property protection in cyber-physical systems. EURASIP Journal on Information Security, v. 2016, n. 1, p. 8, 2016.

MANDARINO JUNIOR, Raphael; CANONGIA, Claudia. Livro verde: segurança cibernética no Brasil. Brasília: GSIPR/SE/DSIC, 2010.

MARINHA DO BRASIL. Doutrina Básica da Marinha. Rev. 2. Brasília 2014.

MATUSZEWSKI, Jan. Specific emitter identification. In: Radar Symposium, 2008 International. IEEE, 2008. p. 1-4.

MILLER, Bill; ROWE, Dale. A survey SCADA of and critical infrastructure incidents. In: Proceedings of the 1st Annual conference on Research in information technology. ACM, p. 51-56, 2012.

MINISTÉRIO DA DEFESA. Política de Guerra Eletrônica de Defesa – MD32-P-01, 1ª Edição, 2004.

MINISTÉRIO DA DEFESA. Manual de Doutrina Militar de Defesa – MD51-M-04, 2ª Edição, 2007.

MINISTRY OF DEFENSE. UK Defense Doctrine – Joint Doctrine Publication 0-01. 5 ª Edição, 2014.

NIST. FIPS 140-2: Security Requirements for Cryptographic Modules. National Institute of Standards and Technology (NIST) v. 25, 2001.

NORCUTT, L.S. Ship Self-Defense System Architecture. Johns Hopkins Apl Technical Digest, v.22, n.4, p. 536-546, 2001.

ORTIZ, G. P.; KAMPEL, M. Potencial de energia eólica offshore na margem do Brasil. Instituto Nacional de Pesquisas Espaciais. V simpósio Brasileiro de Oceanografia, Santos, 2011.

PARKS, Raymond C.; DUGGAN, David P. Principles of cyberwarfare. IEEE Security & Privacy, v. 9, n. 5, p. 30-35, 2011.

REED, Thomas C. At the abyss: an insider's history of the Cold War. Presidio Press, 2005.

RIBEIRO, Leonardo C. et al. True Random Number Generators for Batch Control Sampling in Smart Factories. In: 2018 Workshop on Metrology for Industry 4.0 and IoT. IEEE, 2018. p. 213-217.

ROBERTSON, Jordan.; RILEY, Michael. The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies. Bloomberg Businessweek,04 de outubro de 2018. Disponível em: <https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny -chip-to-infiltrate-america-s-top-companies> Acesso em: 27 out. 2018.

SHAKARIAN, Paulo. The 2008 Russian cyber campaign against Georgia. Military review, v. 91, n. 6, p. 63, 2011.

SHELTON, H. JP3-13: Joint Doctrine for Information Operations. 1998. http://www.c4i.org/jp3_13.pdf.

SMITH, Roy S. Covert misappropriation of networked control systems:

Presenting a feedback structure. IEEE Control Systems, v. 35, n. 1, p. 82-92, 2015.

STOUFFER, Keith; FALCO, Joe; SCARFONE, Karen. Guide to industrial control systems (ICS) security. NIST special publication, v. 800, n. 82, p. 16-16, 2011.

SUN, Xiaojing; HUANG, Diangui; WU, Guoqing. The current state of offshore wind energy technology development. Energy, v. 41, n. 1, p. 298-312, 2012.

TELES, C. ; MACHADO, R.C.S. . Testes de sobrecarga: uma avaliação sobre requisitos de Disponibilidade e Desempenho. Anais do XVII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, Workshop sobre Regulação, Avaliação da Conformidade, Testes e Padrões de Segurança (SBSeg/WRAC+), Brasília, 2017.

TOPALOV, Andriy; KOZLOV, Oleksiy; KONDRATENKO, Yuriy. Control processes of floating docks based on SCADA systems with wireless data transmission. In: Perspective Technologies and Methods in MEMS Design (MEMSTECH), 2016 XII International Conference on. IEEE, 2016. p. 57-61.

WADHAWAN, Yatin; NEUMAN, Clifford. Evaluating Resilience of Oil and Gas Cyber Physical Systems: A Roadmap. In: Annual Computer Security Application Conference (ACSAC) Industrial Control System Security (ICSS) Workshop. 2015.

WARD, Robert; ROBERTS, Chris; FURNESS, Ronald. Electronic chart display and information systems (ECDIS): State-of-the-art in nautical charting. Marine and Coastal Geographical Information Systems, p. 149-161, 2000.

WEIGLEY, Russell F. JP1 Doctrine for the Armed Forces of the United States. 2013.

WEISS, Gus W. The Farewell Dossier. Center for the Study of Intelligence, Central Intelligence Agency (CIA), Washington DC, 1996.

WHITE HOUSE. The national strategy to secure cyberspace. Washington, DC: White House, 2003.

YASAR, Nurgul; YASAR, Fatih Mustafa; TOPCU, Yucel. Operational advantages of using Cyber Electronic Warfare (CEW) in the battlefield. In: Cyber Sensing 2012. International Society for Optics and Photonics, 2012.

ZETTER, Kim. Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon. Broadway books, 2014.

ZIVI, Edwin. Design of robust shipboard power automation systems. Annual Reviews in Control, v. 29, n. 2, p. 261-272, 2005.