Guerra Cibernética no Âmbito do Poder Marítimo

Alan Oliveira de Sá¹, Raphael Carlos Santos Machado^{2,3}, Nival Nunes de Almeida⁴

¹ Centro de Instrução Almirante Wandenkolk (CIAW) – Marinha do Brasil
Ilha das Enxadas, Baía de Guanabara, Rio de Janeiro, RJ, Brasil.

² Instituto Nacional de Metrologia, Qualidade e Tecnologia (Inmetro)
Av. Nossa Senhora das Graças, 50, Xerém, Duque de Caxias, RJ, Brasil.

³ Centro Federal de Educação Tecnológica Celso Suckow da Fonseca (CEFET/RJ)
Av. Maracanã, 229, Maracanã, Rio de Janeiro, RJ, Brasil.

⁴ Escola de Guerra Naval (EGN) – Marinha do Brasil
Av. Pasteur, 480, Urca, Rio de Janeiro, RJ, Brasil.

alan.olivera.sa@gmail.com, rcmachado@inmetro.gov.br,
nivalnunes@yahoo.com.br

Abstract. *This paper presents a taxonomy that encompasses new classes of attack that exploit the cybernetic domain together with the electronic and kinetic domains. The analysis of these possible attacks in the scope of the Sea Power indicates the need for policies capable of promoting the cybersecurity of its systems. In this sense, this paper proposes the use of policies for certification of cyber products that belong to the Sea Power.*

Resumo. *Este artigo apresenta uma taxonomia que abarca novas classes de ataque que exploram o domínio cibernético em conjunto com os domínios eletrônico e cinético. A análise destes possíveis ataques no âmbito do Poder Marítimo aponta para a necessidade de políticas capazes de promover a segurança cibernética dos seus sistemas. Neste viés, este artigo propõe o uso de políticas para certificação dos produtos cibernéticos pertencentes ao Poder Marítimo.*

1. Introdução

A inclusão do domínio cibernético [Parks e Duggan 2011] 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 conceitos e princípios da guerra erguidos com base em milênios de guerras cinéticas [Parks e Duggan 2011].

Neste contexto, o presente artigo discute algumas formas pelas quais ataques com componentes cibernéticas podem afetar um combate naval, a navegação, ou mesmo a exploração e uso do mar e de águas interiores. Mais especificamente, são discutidos os possíveis impactos decorrentes do encontro da guerra cibernética com 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: o domínio cibernético, o domínio eletrônico, e o domínio cinético. Mais estritamente, o foco 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 e impacto.

O restante deste artigo está organizado da seguinte forma. Primeiramente, é apresentada uma taxonomia que abrange ataques que exploram os domínios cibernético, eletrônico e cinético, caracterizando por meio de exemplos seus possíveis alvos no Poder Marítimo. Em seguida, é discutido o uso de políticas de certificação de produtos cibernéticos para a segurança do Poder Marítimo. Por fim, são apresentadas as conclusões.

2. Taxonomia

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 e 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 e Duggan 2011, p. 1, tradução nossa]. O conceito de domínio cibernético adotado no presente artigo agrega a definição de mundo cibernético de Parks e Duggan [Parks e Duggan 2011]. Neste 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]. O domínio da guerra eletrônica, portanto, reside no espectro eletromagnético, mais especificamente nas faixas de frequência em que operam sensores – e.g., sistemas radar –, equipamentos de guerra eletrônica e sistemas de comunicação por ondas eletromagnéticas.
- **Guerra cinética**, segundo Parks e Duggan, 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 e Duggan 2011, p.1, tradução nossa]. Note que a definição de guerra cinética apresentada por [Parks e 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 este motivo, para caracterizar o domínio da guerra cinética, recorreremos 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 – i.e., não virtual – sujeito a mudanças mediante a aplicação de forças.

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 onde computadores e redes de comunicação são utilizados para acionar ou controlar processos físicos. Em outras palavras, neste tipo de ofensiva, medidas de ataque digitais são empregadas para produzir forças físicas capazes de modificar diretamente o mundo real. De forma 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]; sistemas de combate navais, onde sensores e armas são conectados a computadores e redes [Janer e Proum 2014]; sistemas offshore de exploração, produção e transporte de óleo e gás [Wadhawan e Neuman 2015], frequentemente controlados por sistemas SCADA; ou mesmo estaleiros que empreguem sistemas de automação e controle típicos da Indústria 4.0 [Arakaki 2009].

- **Ciber-Eletrônicos:** ataques ciber-eletrônicos são ataques compostos em parte por ações de guerra eletrônica contendo também elementos de guerra cibernética. Em uma guerra eletrônica tradicional, uma medida de ataque eletrônico (MAE) – *e.g.*, uma ação de *jamming* – pode ser usada para negar o uso do espectro eletromagnético ao radar inimigo. Já em um ataque ciber-eletrônico, o uso do espectro eletromagnético não é essencialmente negado ao sistema alvo. Neste 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 e operacional. Sem a pretensão de esgotar os potenciais alvos deste tipo de ataque, são apresentados aqui alguns exemplos: sistemas Radar que façam uso de sinais de vídeo digitalizados [Bole, Dineley e Wall 2005]; ou mesmo sistemas de Medida de Apoio à Guerra Eletrônica (MAGE), composto tipicamente por antenas e sistemas computacionais responsáveis por processar, classificar e identificar emissões eletromagnéticas [Matuszewski 2008].

- **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 ou sensores que exploram o espectro eletromagnético. Nestes 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, estes ataques se iniciam no espectro eletromagnético e utilizam como porta de entrada os dispositivos de captação de ondas eletromagnéticas – *e.g.*, a antena de um radar. Têm como objetivo manipular ou causar danos físicos diretos à planta física. Para tal, conforme ilustrado na Figura 2, utilizam uma componente cibernética como pivô entre os domínios das guerras eletrônica e cinética, transformando informações recebidas via espectro eletromagnético em ações cinéticas maliciosas na planta controlada. Um exemplo de potencial alvo para ataques multidomínio são os Sistemas Integrados do Passadiço (Integrated Bridge System – IBS). Dentre os dispositivos de transmissão e recepção de ondas eletromagnéticas conectados à um IBS há sistemas radar, ARPA, receptores GPS, e receptores AIS (Automatic Identification System). 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 [Bhatti e Humphreys 2017]. Dessa forma, em um IBS, é possível que o controle da propulsão seja 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 e converter as informações recebidas em comandos para a máquina do navio.

Figura 2 – Atuação de um ataque multidomínio em um IBS (Fonte: Adaptado de Bhatti e Humphreys 2017).

3. Políticas de Homologação e Certificação de Produtos Cibernéticos

As vulnerabilidades de um sistema podem surgir de forma não intencional, por falhas de projeto, implementação ou configuração, ou podem ser intencionalmente introduzidas por agentes maliciosos 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.

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, muitas vezes, depende de intrincadas cadeias de produção que incluem a subcontratação de empresas baseadas em outros países – 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* e *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* e do *software* em condições típicas de operação. De fato, 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 ou 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. 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 *hardware*, 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 e Riley, 2018]. Trata-se de um ataque à cadeia de produção – *supply chain attack* – reportado pela Amazon.com Inc. às autoridades dos EUA. Neste caso, especialistas identificaram um minúsculo *microchip*, “não muito maior do que um grão de arroz” [Robertson e Riley, 2018], escondido em placas-mãe de servidores. Tal *microchip* 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 e 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 e Riley, 2018].

Sendo assim, com o objetivo de mapear e mitigar os riscos associados ao uso de *softwares* e *hardwares*, algumas nações ao redor do mundo têm implantado sistemas de homologação de produtos cibernéticos [FNCA 2018; DSD 2015; 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 e 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 Austrália e Nova Zelândia [DSD 2015] e o Department of Defense Information Network Approved Products List (DoDIN/APL) [DISA 2017] dos EUA.

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 e DoDIN/APL, 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. 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.

4. Conclusões

Neste artigo 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. Conceituamos estas três classes de ataque e caracterizamos, por meio de exemplos, seus potenciais alvos dentro do Poder Marítimo. O estudo aponta para a necessidade de desenvolver políticas capazes de promover a segurança dos sistemas cibernéticos do Poder Marítimo. Para o combate às vulnerabilidades cibernéticas deste Poder, apresentamos o possível uso de políticas de homologação e certificação de produtos cibernéticos, o que já vem sendo adotado em um contexto mais amplo por países como a França, Austrália, Nova Zelândia, EUA e Canada. Concluímos que o uso de políticas de homologação e certificação de produtos cibernéticos pode contribuir, de forma positiva e abrangente, para a segurança dos sistemas do Poder Marítimo.

Agradecimentos

Este trabalho foi parcialmente apoiado pelo projeto SHCDCiber.

Referências

- ADEE, Sally. The hunt for the kill switch. IEEE Spectrum, v. 45, n. 5, p. 34-39, 2008.
- ARAKAKI, Glenn T. Yokosuka Naval Base Prepares for Nuclear Aircraft Carrier. Army Engineer School Fort Leonard Wood MO, 2009.
- 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.

- 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.
- 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.
- 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.
- MATUSZEWSKI, Jan. Specific emitter identification. In: Radar Symposium, 2008 International. IEEE, 2008. p. 1-4.
- PARKS, Raymond C.; DUGGAN, David P. Principles of cyberwarfare. IEEE Security & Privacy, v. 9, n. 5, p. 30-35, 2011.
- 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.
- SHELTON, H. JP3-13: Joint Doctrine for Information Operations. 1998. http://www.c4i.org/jp3_13.pdf.
- 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.