ATAQUES CIBERNÉTICOS: AMEAÇAS REAIS AO PODER NAVAL*

MARCUS VINICIUS DE **CASTRO LOUREIRO****
Capitão de Mar e Guerra

SUMÁRIO

INTRODUÇÃO

Não se pode ignorar que a nossa crescente dependência de sistemas, equipamentos e serviços conectados a uma rede tem aumentado a nossa exposição e consequente risco aos incidentes e ataques cibernéticos. A constante evolução tecnológica nos equipamentos militares, nem sempre acompanhada do nível de segurança cibernética necessária, permite inferir que a ação de um único *hacker* pode ser decisiva para burlar e/ou abalar as defesas de um adversário. Em virtude disso, as grandes

*N.R.: 1º colocado no Concurso da Revista Passadiço de 2016.

** Adjunto do Estado-Maior Conjunto do Comando de Defesa Cibernética – Comando do 7º Distrito Naval.

potências militares e, também, países com dificuldades para manter os custos de Forças Armadas convencionais estão se aprofundando na guerra cibernética.

As forças navais não se encontram alheias a este cenário, pois a proteção contra ataques maliciosos aos sistemas computadorizados, a bordo dos navios, está atingindo o topo da agenda das principais Marinhas do mundo. Renomados exercícios combinados, como o *Joint Warrior*, já contemplam a ameaça e execução de ações cibernéticas.

Os desafios, atualmente, estão em aprimorar a doutrina de defesa cibernética, encontrar a melhor estratégia para a capacitação dos recursos humanos frente a esta nova ameaça, e a mitigação dos riscos, já que a evolução desses sistemas torna imperativo que os ativos de informação[1], a bordo dos navios, estejam seguros contra todas as formas de incidentes cibernéticos. Entretanto, a ação de proteção passa por um conjunto complexo de questões, e não apenas sobre o funcionamento de um *firewall,* ou a instalação de um antivírus nos computadores. É necessário reforçar as capacidades de segurança cibernética com foco na gestão de riscos e analisar, conjuntamente, as vulnerabilidades de todos os sistemas controlados e monitorados por *softwares*.

É necessário reforçar as capacidades de segurança cibernética com foco na gestão de riscos e analisar as vulnerabilidades de todos os sistemas controlados e monitorados por *softwares*

O SETOR CIBERNÉTICO

A conectividade global, a existência de vulnerabilidades e o anonimato são características que favorecem a utilização do espaço cibernético. É um setor que cresce em complexidade e em que se observa, ainda, um déficit de conhecimento especializado. É quase uma regra esperar que a atividade dos *hackers* supere a tecnologia de prevenção.

Os ataques cibernéticos, cada vez mais sofisticados, vêm sendo considerados uma ameaça emergente em face de serem uma alternativa de baixo custo e não necessitarem de logística (recursos tecnológicos complexos). As motivações dos ataques são imprecisas e variam entre ganho pes-

1 Ativos de informação – meios de armazenamento, transmissão e processamento de dados e informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os sistemas de informação de um modo geral, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

soal, cunho político, roubo de informações, *hacktivismo*[2], sabotagem, negação ou degradação do acesso ao espaço cibernético e o mapeamento das redes.

Ressalta-se, ainda, que os impactos sobre o pessoal militar e a população civil, hoje, influem de forma crucial nos planejamentos, nas decisões e no andamento dos conflitos. Essa perspectiva leva a se vislumbrar a priorização da ação cibernética, quando comparada à cinética[3]. De acordo com Richard Clarke (2010), "o espaço cibernético é vital para os conflitos atuais e para a vantagem militar futura".

Os ataques cibernéticos representam uma ameaça tão grande quanto os mísseis e os torpedos

SETOR MILITAR NAVAL

As Marinhas necessitam de acesso e uso irrestrito do seu espaço cibernético de interesse (por ex: segurança nas comunicações, manutenção do C2, aquisição de informações de inteligência) para bem executar as suas tarefas militares.

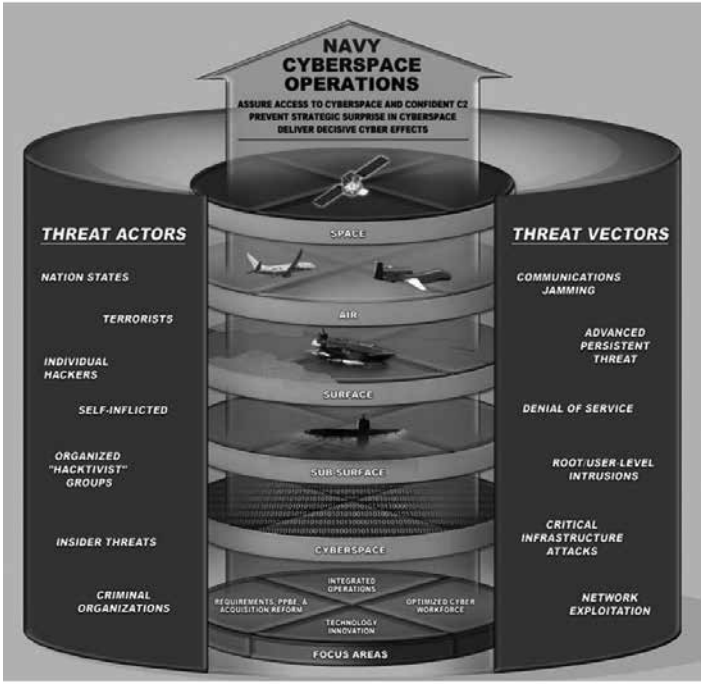
Cabe destacar que os sistemas empregados nos novos navios vêm se tornando cada vez mais dependentes de uma rede de computadores. Enquanto a conectividade fornece às Marinhas plataformas e sistemas de armas com precisão, agilidade e velocidade sem precedentes, também abre vários vetores de ataque para os *hackers*. O sistema de arma dos *Tomahawk*, por exemplo, utiliza o espaço cibernético para receber dados em voo dos centros de comando operacionais.

Fruto disso, a preocupação com a ameaça cibernética só aumenta, a ponto do incremento do nível de proteção dos sistemas computadorizados e automatizados tornar-se foco na construção naval dos navios militares. Para o especialista em defesa Ben Farmer (2015), os ataques cibernéticos representam uma ameaça tão grande quanto os mísseis e os torpedos. Novos navios, como o *Litoral Combat Ship*, da Marinha dos Estados Unidos da América (US Navy), e o futuro *Type-26* (*Global Combat Ship*), da Marinha do Reino Unido (RN), já foram projetados com proteção cibernética integrada para os seus equipamentos e sistemas.

Os navios mais antigos, em que a preocupação com sistemas e *softwares* é menor e nem sempre é fácil substituir sis-

2 *Hacktivismo* – Junção de *hacking* com o ativismo político (bloqueios virtuais, bombardeios de *e-mail*, invasões de computadores e do uso de vírus e *worms*, para infectar redes computacionais).

3 Cinética – envolve equipamentos, armamento e/ou forças militares.



temas antiquados, ou já sem atualizações pelos fabricantes, também demandam significativa atenção. Essas características os convertem nos alvos mais frágeis para ações dos *hackers*.

IDENTIFICAÇÃO DE VULNERABILIDADES

Dentre as possibilidades das ações cibernéticas sobre os meios do Poder Naval, encontram-se:

a) alterações no AIS (*Automatic Identification System*), sistema de monitoração de curto alcance utilizado em navios e Serviços de Tráfego de Embarcações. Segundo Bartlett (2015), testes já foram efetuados no sistema AIS e fizeram, por exemplo, com que navios inteiros desaparecessem dos sistemas de rastreamento e embarcações não existentes aparecessem, bem como surgissem falsos alertas de socorro, colisão e informações alteradas do curso dos navios;

b) interceptações nas comunicações via Inmarsat (telecomunicações via satélite), a ponto de a empresa Trustwave, braço de segurança cibernética da Singtel (Singapore Telecommunications Limited), ter sido contratada para fornecer o serviço UTM (*Unified Threat Management* – *firewall* avançado, antivírus, prevenção de intrusão e filtros *web*, com suporte global 24 horas), baseado em *software* e integrado com o *hardware* da Inmarsat a bordo de navios, para proteger os dados e reduzir o risco cibernético de companhias da Marinha Mercante;

c) alterações em informações de satélites, do GPS (*Global Positioning System*) e do ECDIS (*Electronic Chart Display and Information System*), sendo possível a modificação de rota dos navios. Em decorrência, afirma Mollman (2015), algumas academias de formação militar naval estão recrudescendo e enfatizando o ensino da navegação astronômica e a navegação pelo sistema Loran[4];

d) comprometimento da malha de redes de comunicação, seja de voz, dados ou vídeo, que trazem consigo vulnerabilidades

4 Loran – sistema terrestre de radionavegação, baseado na utilização de emissões coordenadas de impulsos radioelétricos de ondas MF e LF.

que podem ser exploradas por um inimigo ou oponente, que pode atacar as redes de comando e controle de uma imensa variedade de sistemas militares, buscando a desestabilização ou a degradação da capacidade militar;

e) afetar os sistemas mecânicos, como os de energia e de controle de propulsão. Um navio poderia perder o controle sobre a alimentação dos equipamentos, encalhar, mudar de direção etc.; e

f) comprometimento dos sistemas de combate. A perda ou a degradação do poder combatente. Um radar, hoje, é uma porta aberta em um computador. A mesma frequência poderia ser utilizada para transmitir um pacote de dados de volta ao computador e alterar o funcionamento do sistema de defesa antiaérea, por exemplo. Especialistas militares da Airforce-Technology (2008) e o escritor Richard Clarke (2010) garantem que o sistema de ataque cibernético dos EUA, chamado de *Senior Suter*, possui esta capacidade. Afirmam que essa tecnologia, inicialmente testada pelos EUA nas guerras do Iraque e do Afeganistão, foi utilizada por Israel num ataque sobre uma instalação de armas nucleares na Síria, em 2007.

A PROTEÇÃO

Os países com maior tradição e cultura de defesa já sinalizam medidas para reduzir as vulnerabilidades e os riscos neste importante flanco estratégico.

A US Navy está desenvolvendo o sistema Rhimes (*Resilient Hull, Mechanical, and Electrical Security*). Trata-se de um sistema de proteção cibernética projetado para tornar seus sistemas de controle mecânicos e elétricos (controle de danos/combate a incêndios, máquinas de suspender e fundear, geração de energia, hidráulicas, máquina do leme e controle da propulsão) resistentes a ataques cibernéticos. O Rhimes se baseia em técnicas avançadas de resiliência cibernética para se defender desses ataques. A maioria dos controladores físicos possui *backups* redundantes (cópias de segurança) que permitem que o sistema permaneça operacional em caso de falha.

Em caráter geral, a mitigação de riscos de um ataque cibernético, no mínimo, deve identificar as ameaças, elaborar um programa de conscientização da tripulação e desenvolver padrões e diretrizes a fim de resolver as questões de segurança cibernética. O caminho passa pelo incremento de inspeções para minimizar falhas, implementar controle de acesso de usuários e soluções de segurança adequadas para os sistemas de bordo, instituir planos de contingência e também estar preparado para gerenciar incidentes que possam vir a acontecer. Além disso, é preciso manter os sistemas atualizados e aperfeiçoados ao longo de toda sua vida útil e trocar informações com o setor privado (fornecedores), para o desenvolvimento de melhores práticas.

CONSIDERAÇÕES FINAIS

No âmbito da cibernética, quanto maior o grau tecnológico e a dependência da interconexão por redes de comunicação de dados, maior será a vulnerabilidade dos equipamentos e sistemas. Os ataques estão cada vez mais sofisticados, e nota-se o crescimento no universo de atores e alvos.

A preparação para garantir a utilização com segurança do espaço cibernético pelas forças navais trata-se de uma tendência mundial. É imperativo organizar e treinar equipes de profissionais em defesa cibernética para êxito contra os possíveis adversários no espaço cibernético, e que se desenvolvam ações destinadas a aumentar as capacidades de prevenção, defesa, detecção, exploração, análise, recuperação e resposta diante dessa nova ameaça no ambiente marítimo.

A proteção dos navios passa pela elaboração de ações de conscientização e sensibilização neste domínio específico, bem como por ações preventivas e redução das vulnerabilidades, a fim de garantir que os ativos de comunicação e informação existentes a bordo possuam a adequada segurança e resiliência cibernética[5]. Em médio prazo, todas as Marinhas necessitarão ser capazes de mitigar o impacto dos ataques por ações de proteção e, se necessário, de defesa ativa.

Sob o ponto de vista doutrinário, pode-se dizer que as operações das Marinhas no espaço cibernético enfrentam hoje os desafios típicos de outras disciplinas emergentes na História, tais como foram a Guerra Antiaérea e a Guerra Antissubmarino

Sob o ponto de vista doutrinário, pode-se dizer que as operações das Marinhas no espaço cibernético enfrentam hoje os desafios típicos de outras disciplinas emergentes na História, tais como foram a Guerra Antiaérea e a Guerra Antissubmarino.

🗁 CLASSIFICAÇÃO PARA ÍNDICE REMISSIVO:
<GUERRAS>; Guerra cibernética;

REFERÊNCIAS

Ameaça cibernética em alto mar. 2013. Disponível em: <http://www.decisionreport. com.br/publique/cgi/cgilua.exe/sys/start.htm?infoid=14987&sid=42&tpl=printerview>. Acesso em 10 abr. 2016.

A New Defense for Navy Ships: Protection from Cyber Attacks. 2015. Disponível em: <http://www.navy.mil/submit/display.asp?storyid=91131>. Acesso em 10 abr. 2016.

BARTLETT, Charlie. A segurança cibernética e por que é necessário preocupar-se com o transporte. 2015. Disponível em: <http://www.ubmbrazil.com.br/ pt/responsabilidade-social/51-noticias/marintec/668-a-seguranca-cibernetica-e-por-que-e-necessario-preocupar-se-com-o-transporte>. Acesso em 10 abr. 2016.

5 Resiliência Cibernética – capacidade de manter as infraestruturas críticas de tecnologia da informação e comunicações operando em condições de ataque cibernético ou de restabelecê-las após uma ação adversa.

BRASIL. Ministério da Defesa. MD 31-M-08 - Doutrina Militar de Defesa Cibernética. Brasília, 2014.

CLARKE, Richard. Guerra *Cibernética: A próxima ameaça à segurança e o que fazer a respeito*. Brasport. Tijuca, cap. 1, p. 11, set. 2010.

Cyber threat to ships–real but manageable. 2013. Disponível em: <https://library. e.abb.com/public/b9d267b4767c582f85257ca1003280e9/106_Cyber_threat_to_ships_real_but_manageable.pdf>. Acesso em 10 abr. 2016.

Cyber-warfare at sea? Royal Navy vessels must be hacker-proofed, says designer. 2015. Disponível em: <https://www.rt.com/uk/311752-cyber-warfare-british-navy/>. Acesso em 10 abr. 2016.

ESPANHA. Gobierno de España. Estrategia de Seguridad Marítima Nacional da Espanha. Madri, 2013.

EUA. Navy Ciber Power 2020. Washington, 2012.

FARMER, Ben. Cyber attacks 'as big a threat to new warships as missiles and torpedoes'. 2015. Disponível em: <http://www.telegraph.co.uk/news/uknews/defence /11786558/Cyber-attacks--as-big-a-threat-to-new-warships-as-missiles-and-torpedoes. html>. Acesso em 10 abr. 2016.

Guidelines on Cyber Security onboard Ships. 2016. Disponível em: <http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on -cyber-security--onboard-ships.pdf?sfvrsn=12>. Acesso em 10 abr. 2016.

Hacking threat to new £250m warships. 2015. Disponível em: <http://www.thetimes. co.uk/tto/news/uk/defence/article4518482.ece>. Acesso em 10 abr. 2016.

LCS: Novos navios de guerra não fazem frente a "um ataque modesto". 2016. Disponível em: <http://www.defesaaereanaval.com.br/tag/pentagono?print=print-search>. Acesso em 10 abr. 2016.

MACHADO, Gladys. "Cibernética: a guerra em curso". *Revista Marítima Brasileira*, p.178, set. 2013.

MOLLMAN, Steve. US Navy Revives Ancient Navigation as Cyber Threats Grow. 2015. Disponível em: <http://www.defenseone.com/technology/2015/10/navy-navigation-sextant-cyber-threats/122853/>. Acesso em 10 abr. 2016.

Navy Battles Cyber Threats: Thumb Drives, Wireless Hacking, & China. 2013. Disponível em: <http://breakingdefense.com/2013/04/navy-cyber-threats-thumb-drives-wireless-hacking-china/>. Acesso em 10 abr. 2016.

Navy takes cyber threat seriously. 2015. Disponível em: <http://www.marsecreview. com / 2015 / 08/navy-takes-cyber-threat-seriously/>. Acesso em 10 abr. 2016.

Navy Warships Brace For Cyber Attacks. 2012. Disponível em: <http:// breakingdefense.com/2012/01/navy-warships-brace-for-cyber-attacks/>. Acesso em 10 abr. 2016.

PORTUGAL. Revista da Armada de Portugal. Lisboa, Nº 498, ano XLVI, julho. 2015.

RHIMES-Cyber-Attack. 2015. Disponível em: <http://www.onr.navy.mil/Media-Center/ Press--Releases/2015/RHIMES-Cyber-Attack-Protection.aspx>. Acesso em 10 abr. 2016.

Royal Navy under threat from cyber-attacks. 2015. Disponível em: <http://www. scmagazineuk.com/royal-navy-under-threat-from-cyber-attacks/article/398225/>. Acesso em 10 abr. 2016.

The Israeli 'E-tack' on Syria – Part I e II. 2008. Disponível em: <http://www.airforce-technology.com/features/feature1625/>. Acesso em 10 abr. 2016.

US Navy Developing Cyber Protection System to Protect Ships from Cyberattacks. 2015. Disponível em: < https://www.hackread.com/us-navy-cyber-attack-protection-system/>. Acesso em 10 abr. 2016.