CONTRAMEDIDAS CIBERNÉTICAS EM SISTEMAS OPERATIVOS*

KAISER **MAGALDE** COSTA MAGALHÃES**
Capitão de Corveta (EN)

SUMÁRIO

Introdução
Evidenciando vulnerabilidades e ameaças em sistemas digitais operativos
Identificação de metodologias de segurança cibernética
Proposta de um modelo de contramedidas cibernéticas
Conclusão

INTRODUÇÃO

Existe uma farta quantidade de artigos e publicações relacionados à segurança cibernética de sistemas comerciais e corporativos, mas, devido provavelmente ao sigilo militar, identificaram-se para consulta poucos trabalhos disponíveis voltados ao estudo de métodos de segurança cibernética a sistemas militares operativos, sobretudo no que diz respeito a aspectos relacionados a sistemas militares embarcados, em especial sistemas de combate de navios.

As ameaças a sistemas digitais operativos são similares a sistemas comerciais. A materialização das ameaças ocorre com a implantação de vírus, *malwares* ou demais pragas eletrônicas, de forma intencional ou não, por agentes que operam ou mantêm tais sistemas. Os desenvolvedores desses sistemas também devem ser alvo de constantes auditorias de segurança digital, pois podem implantar brechas em *softwares* ou *firmwares* desde a fase de concepção, mas que só serão efetivamente danosos em um futuro bem distante. *Softwares* de sistemas operacionais e até antivírus são outros

* Título original: "Um modelo de contramedidas cibernéticas para emprego em sistemas digitais operativos".

** Subchefe de Sistemas de Combate do Centro de Desenvolvimento de Submarinos (CDS). Engenheiro de Computação e mestre em Engenharia Elétrica – Inteligência Artificial. Possui cursos de Projeto Preliminar e Detalhado de Submarinos de Ataque.

tipos de ameaças que merecem especial atenção, devido à necessidade de constante atualização de *patches*[1]. Conforme será discutido, os *hardwares* maliciosos têm que ser considerados pelos engenheiros de segurança de sistemas como uma ameaça crível e de difícil combate.

O impacto de ações de guerra cibernética adversárias em sistemas operativos é tão importante que pode inviabilizar os lançamentos de armas e contramedidas ou mesmo comprometer a permanência do meio militar em combate, sem ter sido alvo de um engajamento por armas convencionais desferidas pelo adversário. A nova dimensão da guerra, a guerra cibernética, tem recebido especial atenção de muitos Estados e até de grupos hostis, pois tais ações são significativamente menos custosas do que especificar, desenvolver, produzir, qualificar, testar e lançar armas ou contramedidas convencionais contra inimigos (BELLOVIN *et al*, 2017).

EVIDENCIANDO VULNERABILIDADES E AMEAÇAS EM SISTEMAS DIGITAIS OPERATIVOS

Ataques a sistemas não-militares

Os sistemas digitais ganharam mais versatilidade com o aumento da integração em rede de equipamentos. Essa característica proporcionou o compartilhamento de dados e processamento, aumentando a eficiência dos sistemas computacionais. O incremento das tecnologias de redes e interfaces também proporcionou o acesso remoto a sistemas antes isolados em prédios e áreas específicas de empresas ou instituições, dando origem a novas soluções de conectividade entre estas e seus clientes. Por outro lado, esta abertura também proporcionou o acesso de agentes e códigos maliciosos a essas bases de dados, impactando a segurança destes e até a imagem da empresa/instituição e de seus clientes.

Os atacantes cibernéticos estudam e exploram vulnerabilidades presentes nos sistemas-alvo de forma a preparar códigos maliciosos os mais adaptados possíveis para atingir o efeito desejado, podendo ser principalmente: a negação de serviço (*denial of service*), o dano ao sistema de arquivos ou a destruição física de equipamentos. Existe uma grande quantidade de ataques conhecidos e alguns já documentados, mas focaremos em apenas três ataques mais relevantes ao escopo deste trabalho.

O famoso caso conhecido como Stuxnet baseou-se em código malicioso que se espalhou de máquina em máquina de controle das centrífugas de urânio em Natanz, Irã. Segundo Bellovin *et al*, "o Stuxnet carregava um *payload* como código malicioso – mas, primeiramente, existiram atividades de inteligência para determinar quais sistemas o Stuxnet deveria atacar e quais eram as suas características precisas". Ele descreveu ainda que este e o caso do ataque à Sony foram casos típicos de ataques cibernéticos e que:

> O Stuxnet utilizou de várias vulnerabilidades conhecidas como "zero-day vulnerabilities"[2] para se conseguir penetrar em um sistema não conectado à Internet. Em seguida, mais dados dos

1 *Patches*: atualizações de *softwares* de sistemas operacionais ou aplicativos produzidas pelos proprietários. Normalmente, estão relacionadas às correções de segurança.

2 *Zero-day vulnerabilities*: São vulnerabilidades descobertas e exploradas antes mesmo de serem reveladas aos vendedores do produto ou, de alguma maneira, ainda não publicamente reveladas. (BELLOVIN *et al*, 2017, p. 60) (tradução nossa).

> equipamentos alvos foram, de alguma maneira, coletados e novos códigos foram atualizados para preparação do *payload*[3] final. Esse código malicioso final foi provavelmente inserido por portas de *pen drive*. (BELLOVIN *et al*, 2017, p. 61) (tradução nossa).

Após esse ataque às usinas de enriquecimento de urânio, supõe-se que houve retaliação. Bellovin *et al*, citando o *New York Times*, descreve:

> É atribuído ao Irã (nesse meio as provas são muito difíceis de serem descobertas e, quando o são, evita-se ser publicamente enfático ou convicto) o ataque à companhia de óleo saudita Aramco. Essa arma, denominada Shamoon, apagou os discos rígidos dos computadores infectados. A arma foi programada para ser acionada às 11h08 da manhã de 15 de agosto de 2012. O código malicioso foi provavelmente inserido por um funcionário da própria companhia na rede corporativa e não na rede de produção (*New York Times apud* BELLOVIN *et al*, 2017, p. 62) (tradução nossa).

O ataque da (ou atribuído à) Coreia do Norte à empresa sul-coreana Sony utilizou-se de técnicas padrões para a penetração inicial e para as atividades de destruição. Bellovin *et al*, citando o *site* Ars Technica, comenta:

> A penetração deu-se via um *spear-phishing*, uma técnica que envolve o envio de um *e-mail* bem convincente a um alvo de forma a induzi-lo a abrir e clicar em um *link* específico. A partir desse *link*, um *malware* é instalado. Os atacantes passaram então meses explorando e investigando a rede da Sony, aprendendo onde estavam os arquivos de interesse e planejando como destruir o sistema de arquivos. A destruição final de discos da Sony deu-se por um *worm*. Pelo menos algumas partes do *software* de destruição usaram ferramentas comerciais de forma a "bypassar" as proteções do sistema operacional. (ARS TECHNICA *apud* BELLOVIN, 2017, p. 66) (tradução nossa).

Percebe-se que as técnicas de ataque vão de complexas às mais simples, de forma a explorar informações dos elementos-alvos, confirmar ou refutar técnicas e, finalmente, empregar algum meio de ataque efetivo.

Ameaças e vulnerabilidades em sistemas digitais operativos

Diferentemente de sistemas digitais administrativos que apenas apoiam atividades administrativas na MB e, por conseguinte, não são considerados críticos às operações navais, os equipamentos ou armas que executam sistemas digitais operativos, conceituados na Doutrina de Tecnologia da Informação da Marinha (BRASIL, 2007, p. 1-1) como "sistemas de informação digital projetados para o emprego em operações navais ou em benefício delas", são o foco efetivo de guerras cibernéticas contra alvos navais. Ainda de acordo com esta publicação, guerra cibernética "são ações ofensivas e defensivas destinadas a explorar, danificar ou destruir informações digitais, ou negar o acesso às suas informações. Tais ações utilizam-se de sistemas de informação e de redes de computadores" (BRASIL, 2007, p. 1-3).

---

3 *Payload*, ou *payload component*, é o mecanismo que efetivamente cumpre o que a arma foi feita para fazer.

Bellovin *et al* definem armas cibernéticas como "artefatos ou ferramentas baseadas em *software* ou *hardware* que podem causar efeitos de destruição, dano ou degradação no sistema ou rede contra o qual se é dirigida a ação". Acrescenta ainda que "uma arma cibernética tem dois componentes: um de penetração e um de carga[4]" (BELLOVIN, 2017, p. 60) (tradução nossa).

Loureiro destaca que, "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" (LOUREIRO, 2017, p. 85). Alguns desses sistemas até podem receber atualização de dados por sistemas de *link* de dados táticos, mas eles têm a característica primordial de não estarem conectados a redes mundiais, embora possam fazer uso de redes internas operativas. Então, como penetrar nesses sistemas? Em que momento? Como fazer um ataque efetivo? Este é o foco dos "soldados cibernéticos": estudar os detalhes de equipamentos, processadores, tipos de interfaces e protocolos de comunicações, *software*s aplicativos e *software*s de sistemas operacionais visando implementar medidas de exploração de dados e ataques aos sistemas dos adversários. O estudo de vulnerabilidades digitais envolve um esforço de diferentes tipos de conhecimento, como especialistas em *hardware*, especialistas em sistemas operacionais, desenvolvedores de *software*s, especialistas em armas, além de especialistas em protocolos de comunicação e dispositivos de interface.

Caso se consiga estudar de forma detalhada o conjunto de *hardware* e *software* de uma arma ou sistema operativo, é possível encontrar vulnerabilidades importantes que podem ser exploradas. Assim, testes em laboratórios cibernéticos são realizados em protótipos procurando explorar dados dos quais a arma convencional deverá dispor para acionar mecanismos de disparo da carga útil ou simplesmente configurar mecanismos de desabilitação ou destruição da arma antes que ela alcance efetivamente o alvo. Para sistemas que lançam munições, erros em parâmetros de entrada de cálculos de tiro podem ser introduzidos.

Percebe-se uma via árdua de análise de caminhos críticos estudados pelo adversário para inviabilizar armas convencionais ou sistemas operativos quando eles já foram produzidos, mas, ainda assim, "este é um caminho menos custoso do que desenvolver, testar e qualificar armas convencionais contra o inimigo" (BELLOVIN *et al*, 2017, p. 65) (tradução nossa). Daí entende-se o crescente interesse dos Estados nessa quarta dimensão da guerra, a guerra cibernética, em complemento ao uso de armas convencionais.

Imagine agora se fosse possível vender esta arma ou este sistema operativo com mecanismos já pré-posicionados em *software*s ou placas de *hardware* (como processadores ou placas de rede). Isso diminuiria ainda mais os custos (tempo e recursos) dos atacantes em ter que explorar, caso a caso, os sistemas adquiridos pelo adversário diante da diversidade de configurações de *hardware* x *software* possíveis. A empresa de produtos de defesa ou agentes infiltrados poderiam incluir vulnerabilidades em produtos já prontas para serem ativadas, com todas as

4 De acordo com BELLOVIN *et al*, o *penetration component* é o mecanismo por meio do qual a arma ganha acesso ao sistema-alvo. Já o *payload component* é o mecanismo que efetivamente cumpre o que a arma foi feita para fazer. (BELLOVIN, 2017, p. 60) (tradução nossa)

brechas desenhadas para serem exploradas no tempo certo e ainda engenhosamente escondidas – quase uma "obra de arte"! Adee (2008)[5], citado por Koch e Golling (2008), relatou:

> "de acordo com um contratante de produtos de defesa para os Estados Unidos, que falou em condição de anonimato, um 'produtor de *chips* europeu' construiu recentemente, dentro de seus microprocessadores, um mecanismo de destruição (*kill switch*) que poderia ser acessado remotamente [...] Se, no futuro, o equipamento caísse em mãos hostis, 'a França queria um modo de desabilitar os circuitos', ele disse" (ADEE S. *apud* KOCH e GOLLING, 2008, p. 197) (tradução nossa).

Percebe-se que a alteração de *hardware* e a inserção de *kill switches* já são uma realidade, sob a alegação de proteção contra possíveis adversários. E se houver outras "chaves" como essas para monitorar ou simplesmente realizar testes de ataques a partir dos sistemas dos clientes? Quantas *back doors* como essas já estão presentes nos sistemas militares em uso? Koch e Golling relataram também o caso da incursão de caças israelenses em território da Síria sem serem detectados pelos radares sírios de última geração, ao que se atribuem possíveis *back doors* em *chips* desses radares de forma a cegá-los. Entretanto, ainda mais relevante foram as sérias reflexões sobre a descoberta do Departamento de Defesa dos Estados Unidos da América (DoD) sobre uma grande quantidade de armas, incluindo mísseis, em que foi identificada a utilização de "*chips* falsificados" advindos de compras com fornecedores que tinham sido selecionados por possuírem os melhores preços (KOCH e GOLLING, 2008, p. 192).

Para sistemas comerciais que funcionam conectados entre si, brechas em sistemas podem ser exploradas de forma lenta, mas contínua, pelos *hackers*, e possíveis instabilidades em tais sistemas ou reinicializações podem ser toleráveis. Por outro lado, para os sistemas digitais operativos, que não se espera que funcionem conectados a redes externas ao meio militar, é mais efetivo ao atacante implantar mecanismos preliminarmente à saída do meio militar para o combate de forma a paralisar totalmente a arma ou seu sistema de controle durante as operações. Bellovin *et al* descrevem casos em que " 'mecanismos de disparo' de ações cibernéticas podem ser baseados num calendário de datas específico, num contador regressivo ou em condições ambientais detectadas por outros sistemas que 'alimentam' o sistema de armas, levando este último a iniciar processos de instabilidade ou paralização total". (BELLOVIN *et al*, 2017, p. 62) (tradução nossa)

King *et al* (2007) apresentam dois estudos de casos de implantação de brechas em sistemas a partir do *hardware*. Nesses casos, realizados em laboratório, os pesquisadores inserem um conjunto de portas lógicas adicionais que fazem parte de um processador malicioso especialmente desenvolvido[6] para os experimentos, chamado *Illinois Malicious Processors* (IMP). Os códigos maliciosos efetivos (*payload*) estão armazenados e atualizados externamente ao equipamento-alvo. O mecanismo de disparo para inicialização

5 ADEE S., "The hunt for the kill switch", *Spectrum*, IEEE, vol. 45, nº 5, p. 34-39, 2008.

6 A modificação é baseada na mudança do código fonte VHDL do processador Leon3 Sinthesizable Processor (http://www.gaisler.com), um projeto *open source* Sparc.

desses códigos maliciosos é executado a partir da leitura de um conjunto específico de códigos binários recebidos por uma porta de rede ou dispositivo externo (*pen drive*). A simples leitura de pacotes da rede para posterior descarte do pacote ativa mecanismos no processador para que outras portas sejam abertas, ainda que esse dispositivo não seja o endereçado do pacote de rede. Algo semelhante ocorre com a simples leitura de dispositivos externos, mesmo que o usuário não explore arquivos na mídia. Uma vez aberta essa nova porta, sem qualquer bloqueio do sistema operacional da máquina, seguem-se a cópia e a inicialização de ações maliciosas de ataque final a partir dos pacotes externos enviados por essa porta. Os pesquisadores conseguiram inclusive realizar o ataque e apagar os poucos vestígios deixados, de forma a inviabilizar sua descoberta. Casos como esses são muito difíceis de descobrir ou de se tomarem contramedidas efetivas contra eles, pois são muito rápidos e ficam escondidos em camadas muito baixas do sistema. Os denominados "circuitos maliciosos" podem "bypassar" as técnicas defensivas tradicionais. Os autores reforçam que essa é uma área com grande capacidade de expansão e oportunidades de ataques. E destacam: "Existem muitas oportunidades para inserir ataques baseados em *hardware*, incluindo as fases de projeto, de fabricação, de empacotamento, de testes e estágios de integração – por exemplo, em uma planta de montagem de dispositivos". (KING *et al*, 2007, p. 2) (tradução nossa)

Percebe-se que a diversidade de ataques cibernéticos tem aumentado. Em contraponto a isso, diversos estudos da área de segurança de sistemas têm proposto metodologias com o propósito de minimizar os impactos dos ataques cibernéticos (PIÈTRE-CAMBACÉDÈS e BOUISSOU, 2013). Um ponto comum entre eles é que as vulnerabilidades e possíveis ameaças aos sistemas devem ser estudadas e listadas de forma a implementar medidas de proteção. De acordo com Bellovin *et al*:

> Ataques como o Stuxnet simplesmente não ocorreriam se não houvesse alguma porta de aceso aos sistemas de controle usados pelas cascatas de centrífugas em Natanz, Irã. Foi necessário um trabalho minucioso e atento dos agentes cibernéticos para obter informações atualizadas de tudo o que estava conectado e se certificar de que o novo *firmware* a ser implantado funcionaria exatamente como o planejado. (BELLOVIN *et al*, 2017, p. 63) (tradução nossa)

Portas de acesso como *pen drives* ou discos, além de redes de comunicações, são os canais necessários para atualização ou até funcionamento de sistemas, mas eles também são as portas de acesso para escrutínios e ataques.

Ameaças ou vulnerabilidades a sistemas digitais operativos

A pergunta principal que se deve responder quando se quer identificar ameaças é: de onde vem o perigo? Adotou-se aqui o conceito de "vulnerabilidade" restringindo-o a vulnerabilidades do *software*, *firmware* ou *hardware*. Sendo assim, uma pessoa, ao realizar interações com o sistema na condição de usuário ou desenvolvedor, não é considerada um agente vulnerável, mas sim parte de uma ameaça, de tal maneira que esse agente atua intencionalmente ou não para atingir vulnerabilidades presentes no sistema. Algumas ameaças mais comuns aplicáveis aos sistemas digitais operativos são discutidas a seguir.

– Ameaças de usuários ou desenvolvedores

Os operadores e mantenedores dos sistemas estão incluídos nesta classe. Ameaças de usuários de sistemas ocorrem principalmente pelo uso de senhas de cadastro fracas ou com baixa frequência de renovação. O uso de senhas em sistemas digitais operativos para todos os tipos de usuários é pouco prático, uma vez que a operação de tais sistemas deve ser ágil e apropriada para a condição de postos de combate. Portanto, sugere-se o uso de senhas apenas para usuários especiais, como mantenedores e supervisores de sistemas, que podem alterar, atualizar ou instalar programas e bibliotecas operativas. Sempre que possível, procedimentos de testes de segurança cibernética devem ser realizados após a necessária atualização de dados.

Furnell *et al* (2018) descrevem como variações de métricas de senhas e comentários de retorno ao usuário podem afetar positivamente os resultados na escolha de senhas e o consequente aumento à segurança digital. O artigo demonstrou, por meio de dois casos de estudos, que, ao se associar textos, imagens *emoji*[7] ou alertas aos usuários no momento em que eles estão para criar ou alterar senhas, é estatisticamente relevante o impacto no estabelecimento de senhas fortes por esses métodos, levando ao consequente aumento da segurança digital. De maneira geral, uma melhora no comportamento de segurança dos usuários como um resultado de esforços de aumento da consciência de segurança foi percebida. Os autores concluem, por fim, que, *"*levando isso ao extremo, podemos arguir que organizações não necessitam se preocupar se seus colaboradores entendem, de fato, o que é segurança digital, desde que eles façam continuamente as coisas certas*"*. (FURNELL *et al*, 2018, p. 8).

Uma vez que os sistemas digitais operativos dependerão, em algum momento, de usuários com elevado nível de segurança, seja para realizar manutenções ou atualizar dados de bibliotecas operativas, é relevante que tais sistemas sempre disponham de menus contextualizados sobre o quanto a senha que está sendo proposta pelo usuário é segura, fornecendo-lhes indicativos contextualizados de nível de segurança. Isso pode ser estabelecido em contratos com fornecedores de sistemas digitais operativos de forma que eles incluam tais menus para direcionar os usuários a sempre estabelecerem senhas consideradas fortes.

Uma brecha inserida na fase inicial de desenvolvimento de sistemas digitais operativos pode inviabilizar o uso efetivo de armas em um futuro bem distante

Em relação aos desenvolvedores de sistemas, é esperado que suas ações sejam muito mais danosas do que as ações de simples usuários de tais sistemas. Os desenvolvedores de *software*, ao realizarem suas tarefas, podem incluir rotinas especiais (não contratadas ou não necessárias) que podem ser a porta de entrada para explorar ou paralisar sistemas ou armas. Uma brecha inserida nessa fase inicial de desenvolvimento de sistemas digitais operativos pode inviabilizar o uso efetivo de armas em um futuro bem distante.

7 *Emoji* são figuras reduzidas que procuram expressar sentimentos humanos como alegria, tristeza, raiva etc.

Bellovin *et al* (2017) enfatizaram essa possibilidade de destruição programada quando descreveram:

> [...] aplicáveis a armas cibernéticas, que algumas vezes são chamadas de bombas lógicas. Tais armas são implantadas em computadores de adversários antes de hostilidades, e com elas se pretende causar danos não na implantação, mas em algum tempo mais à frente, quando alguma condição é atingida. A condição do mecanismo de disparo pode ser um acúmulo de tempo decorrido, uma data/hora específica, a recepção de uma mensagem do produtor ou operador da arma ou a percepção de determinada condição no ambiente na qual a arma é preposicionada (BELLOVIN *et al*, 2017, p. 66) (tradução nossa).

O adestramento constante de usuários de sistemas por meio de ações de aumento da consciência de segurança digital é fundamental

Sendo assim, empresas de desenvolvimento devem ter políticas e práticas de segurança cibernética efetivas e auditáveis. Caso a decisão seja por desenvolvimentos autóctones dentro da Força, devem-se contratar empresas de desenvolvimento de *software* para rotinas ou métodos bem específicos e com acesso total aos códigos-fonte, além de se preverem cláusulas contratuais específicas de acordos de sigilo e segurança cibernética.

Outro tipo de ameaça relacionada a usuários e desenvolvedores é quanto à corrupção destes agentes por meio da engenharia social ou demais técnicas realizadas por agentes adversários que visam captar dados sigilosos ou demandar ações danosas a sistemas digitais operativos, incluindo a destruição física de dispositivos ou equipamentos. Para casos como esses, o adestramento constante de usuários de sistemas por meio de ações de aumento da consciência de segurança digital é fundamental, além de manter uma forma de tornar o relato de incidentes mais fácil e expedito.

– Ameaças de dispositivos de *hardware* maliciosos

Conforme exposto anteriormente, Koch e Golling (2016) descrevem uma preocupação crescente de governos com relação a aquisição e uso de dispositivos de *hardware* de fabricantes não nacionais em seus produtos de defesa. Processadores, placas de redes e outros dispositivos de interface já podem vir com "mecanismos de destruição" desde as fábricas de fornecedores ou implementados durante o processo de empacotamento ou finalização industrial. Adams e Kurzer (2013) fizeram um extenso trabalho sobre vulnerabilidades e riscos de produtos de defesa e na base industrial de defesa dos Estados Unidos.

– Vulnerabilidade de programas desatualizados, notadamente sistemas operacionais

Uma grande quantidade de ataques cibernéticos explora as vulnerabilidades de sistemas operacionais desatualizados. *Hackers* estudam os sistemas operacionais em uso pelos seus alvos de forma a encontrar brechas para explorar dados ou iniciar efetivamente um ataque. São recorrentes as manchetes em *sites* de segurança ou alertas dos próprios sistemas operacionais e aplicativos sobre novos *patches* para corrigir problemas de segurança detectados. Devido à dinâmica de

softwares aplicativos e a novas interfaces que surgem no meio computacional, há necessidade de se realizarem constantes atualizações de *softwares* de sistemas operacionais das máquinas.

Parece ser improvável que os sistemas operativos atuais voltem a utilizar sistemas operacionais dedicados ou produzidos especialmente para certos produtos de defesa, pois a utilização de sistemas operacionais comerciais tem a grande vantagem de baratear custos de desenvolvimento e ajuda a empresa a focar no desenvolvimento de solução para o problema efetivamente demandado pelo cliente. Por conseguinte, a maioria dos sistemas digitais operativos atuais executa suas aplicações baseada em sistemas operacionais comerciais. Bellovin *et al* (2017, p. 66) descrevem que a grande maioria dos ataques aproveitam as vulnerabilidades 'bem conhecidas' de *patches* de correções liberadas pelos fornecedores. Entretanto, como descrito melhor abaixo, a necessidade de realizar constantes atualizações de tais sistemas operacionais em meios militares acaba aumentando a insegurança geral dos sistemas operativos de bordo e deve ser evitada.

O ganho de segurança por *softwares* antivírus pode ser menor por promover a abertura de portas para combatentes cibernéticos que já estejam escrutinando vulnerabilidades

– Vulnerabilidade devido a programas de antivírus

Os programas de antivírus têm a missão de proteger os sistemas contra vírus, *malwares* e outras pragas eletrônicas. Entretanto, para executar suas tarefas, exigem sua própria execução em modo privilegiado em nível de segurança do Sistema Operacional em que atuam. Sendo assim, eles podem identificar ameaças, fechar portas e executar rotinas de inclusão de arquivos suspeitos em quarentena. Paradoxalmente, programas antivírus também podem abrir portas que não deveriam ser abertas e perscrutar áreas de dados privativas dos aplicativos ou do sistema operacional. Aliado a essas características e à necessidade premente de manter os antivírus atualizados, aumenta-se, por fim, a insegurança geral do sistema, pois, para se atualizar o antivírus, certamente será necessário o carregamento de novos arquivos (*patches*) no sistema por vias ou mídias externas, o que conduz a possíveis explorações de vulnerabilidades do sistema-alvo. Desta forma, o uso de *softwares* de antivírus em sistemas digitais operativos é desaconselhado, uma vez que o desejado ganho de segurança pode ser muito menor do que a abertura de portas para combatentes cibernéticos que já estejam escrutinando vulnerabilidades desses sistemas. *Softwares* militares embarcados devem ter sua instalação ou renovação realizados com a mínima frequência possível e de forma completa ou modular, sem a necessidade de *patches* constantes de atualização.

Algumas consequências para as armas, para o meio militar e o tráfego de dados militares

Essas ameaças descritas anteriormente foram listadas por serem consideradas as mais relevantes e aplicáveis aos sistemas digitais operativos; entretanto, muitas

outras ameaças podem ser identificadas após um estudo mais detalhado de sistemas. Ações inimigas baseadas nessas categorias de ameaças podem explorar vulnerabilidades existentes em sistemas digitais operativos e, por fim, usar tais informações para preparar ações de ataque para se paralisar ou induzir os sistemas a erros de cálculos. Essas medidas podem, por fim, inviabilizar o uso efetivo de armas ou do próprio meio militar, tornando impossível a realização de missões, antes mesmo de se iniciar o combate.

Um sistema de *link* de dados táticos que contenha erros de posicionamento ou de classificação de alvos pode confundir sistemas de designação de alvos de outros meios militares, ou mesmo indicar como alvo um meio anteriormente considerado como aliado.

Sistemas antigos de acompanhamento de alvos e controle de armas baseados em circuitos analógicos ou sistemas digitais discretos eram mais imunes a essa manipulação de dados. Nos sistemas atuais que fazem uso maciço de dados digitais, ao final, cada informação coletada pelos sensores ou informada pelos operadores de bordo tornar-se-á um dado digital que pode ser manipulado de forma a inserir erros de cálculos ou paralisar sistemas de armas, se corrompidos por agentes adversários. Por conseguinte, é necessário identificar uma metodologia adequada aos sistemas digitais operativos, de forma a maximizar sua proteção cibernética.

IDENTIFICAÇÃO DE METODOLOGIAS DE SEGURANÇA CIBERNÉTICA

De acordo com Stallings e Brown, aspectos como confidencialidade, integridade e disponibilidade de dados devem ser minuciosamente avaliados e priorizados pelos desenvolvedores, em decorrência das análises de ataques possíveis. Eles reforçam a ideia de se produzir "*softwares* defensáveis", em que a arquitetura do *software* prevê uma forma de "falhar de forma elegante" e dentro dos padrões de segurança, em decorrência de eventos que levam a falhas (STALLINGS e BROWN, 2014, p. 333).

Piètre-Cambacédès e Bouissou (2013) apresentaram diversos métodos de análise de segurança em sistemas digitais. Chegou-se a quatro deles, que, devido a suas características e propostas de análise de ataques e ou defesa, são apropriados aos estudos de caso discutidos anteriormente. A seguir, apresenta-se um resumo sobre cada método. Os métodos selecionados foram: tolerância a intrusões, defesa em profundidade, injeção de falhas e árvores de ataque.

O método de tolerância a intrusões é derivado do método de tolerância a falhas aplicado a sistemas críticos de segurança, como aos setores espacial e nuclear. É baseado nos conceitos de redundância, diversificação e separação de equipamentos ou funções de forma a que o sistema continue a prover suas funções ou serviços a despeito de falhas. Outros conceitos importantes deste método são os de *survivability* (sobrevivência) e *resilience* (resiliência) tratados por Ellison *et al* (1997), reafirmando que os sistemas devem ser dotados de funções de segurança que lhes garantam continuar fornecendo as funcionalidades principais ou críticas, ainda que tenham sido invadidos.

O método de defesa em profundidade utiliza conceitos já empregados pelo meio militar e que atualmente têm sido muito estudados e implementados para setores de segurança de sistemas críticos no meio civil, como o nuclear. O conceito principal é considerar que o sistema é vulnerável;

então, devem ser providas barreiras de segurança independentes que impeçam a sequência de eventos críticos ou ameaças atuando no sistema, de forma a não permitir o colapso de seu núcleo crítico. Essas barreiras funcionariam como camadas de segurança, completamente independentes, de forma a estatisticamente minimizar a probabilidade de que todas as camadas de segurança sejam quebradas. Assim, um sistema computacional deveria ser detalhadamente especificado com algumas dessas camadas de proteção em sua arquitetura, independente das seguranças externas, geralmente disponíveis comercialmente. Pièrre-Cambacédès e Bouissou comentam que:

> "Embora esses conceitos de defesa em profundidade sejam usados no campo da segurança digital, eles não são ainda tão consolidados como nas aplicações de segurança industriais. Em particular, a independência das barreiras e a necessidade de se cobrir tanto aspectos de projeto quanto operacionais são frequentemente esquecidos [...]. Para ambos, segurança industrial ou segurança digital, independência e diversidade exercem um papel-chave para garantir a eficiência do método de defesa em profundidade". (PIÈTRE-CAMBACÉDÈS e BOUISSOU, 2013, p. 117-118) (tradução nossa)

O método de injeção de falhas utiliza técnicas de análise de *software* em domínios não necessariamente previstos, como entradas ou comportamentos normais do programa projetado. Assim, são adicionadas entradas incomuns (ou denominadas *bad inputs*) ao padrão de entradas esperado pelos programas, tais como erros do operador humano ou falha de dispositvos de *hardware*. A partir desses dados, analisa-se o comportamento final do *software* quanto a sua resposta e estabilidade (VOAS, 1996, p. 4-7). O método não se utiliza ou necessita de uma lista de códigos de teste como os modelos de testes de *software*, em que são apresentadas as diversas saídas esperadas para um domínio de entradas possíveis, o que é uma vantagem no tempo de preparação ou modelagem de testes. Segundo o autor, o método de injeção de falhas é caracterizado como um método empírico. Outra importante fonte sobre esses conceitos pode ser consultada em (DU e MATHUR, 1998). Um dos problemas desse método é a necessidade de acesso aos códigos-fonte mais básicos do *software*, códigos de baixo nível, *assembler*, de forma a simular às *bad inputs*.

Árvores de ataque é uma metodologia derivada da engenharia de segurança de instalações críticas *default-tree,* como instalações nucleares, e que foi inicialmente proposta por Salter (1998) como aplicação para a área de engenharia de segurança de sistemas computacionais (SALTER, 1998, p. 2-10). "Ela se baseia em uma representação gráfica de ataques em uma estrutura lógica, em que o objetivo dos atacantes está na raiz da árvore, e os diferentes meios de alcançar este objetivo são as folhas da árvore, conectados por meio de portas lógicas AND ("e") ou OR ("ou")" (PIÈTRE-CAMBACÉDÈS e BOUISSOU, 2013, p. 113) (tradução nossa). Segundo os autores, esse é um dos métodos que têm sido largamente usado fora do meio acadêmico, sendo a base para estudo de ataques a sistemas concebidos ou a serem concebidos. Como exemplos, eles comentam seu uso em sistemas SCADA (*Supervisory Control and Data Acquisition*), *software on-line* de bancos, sistema de votação *on-line*, sistemas para redes de celulares, sistemas inteligentes de

métricas e medidas, além de ser utilizado em vários métodos de análise de riscos.

A metodologia denominada Morda (*Mission-Oriented Risk and Design Analysis*), desenvolvida pela NSA (*US National Security Agency*) (IEEE, 2004), apresenta um modelo para que desenvolvedores ou analistas de sistemas consigam identificar o melhor custo-benefício entre o nível pretendido de funcionalidade dos sistemas e sua segurança. Ele é baseado em uma tabela de riscos que relaciona uma lista de ataques preferenciais de adversários e seus impactos nas funcionalidades do sistema-alvo. Baseia-se, ainda, no método de árvores de ataque (SALTER, 1998, p. 2-10) para caracterizar e pontuar os possíveis ataques ao sistema.

O modelo possui as seguintes etapas listadas pelos autores (IEEE, 2004, p. 2): 1) desenvolva uma análise focada na descrição do sistema; 2) defina as ameaças ao sistema e modele o adversário; 3) identifique missões e impactos relevantes; 4) identifique objetivos de ataque dos adversários; 5) derive ataques para encontrar objetivos de ataques adversários; 6) caracterize passos de ataques em termos de parâmetros que influenciam a estratégia de ataque dos adversários; 7) calcule a prioridade de ataques com base nas características de preferências dos adversários e impactos da missão; 8) avalie os riscos do sistema com base em ponderações calculadas (*scores*); 9) avalie a sensibilidade de dados de entrada; e 10) desenvolva uma arquitetura de segurança baseada nos resultados da análise de riscos.

O modelo recebe como dados de entrada uma descrição funcional pormenorizada do sistema, a modelagem dos adversários e missões de usuários do sistema. A partir deste momento, o Morda identifica objetivos de ataque, ataques de sistema e características de ataques, buscando produzir uma proposta de arquitetura de riscos com uma lista de prioridades caracterizada pelo modelo de preferências de ataques do adversário e o consequente impacto em missões de uso do sistema pelo cliente. Essa avaliação de riscos alimenta o processo de engenharia de segurança de sistemas e influencia as futuras arquiteturas de segurança. Por fim, o processo reinicia pela avaliação de riscos das novas arquiteturas de sistemas encontradas. A análise de ataques no Morda é baseada apenas na técnica *attack-tree* – árvore de ataque.

Existe outro aspecto também importante a ser considerado. Ao tratar-se de guerras convencionais, os tratados e acordos internacionais estabelecem um ambiente de guerra com regras e delimitações de forma a minimizar efeitos colaterais aos não combatentes ou, ainda, a propriedades públicas e ou privadas não designadas como alvos militares (BRASIL, 1993). O manual TALLINN (SCHMITT, 2017) é uma fonte útil que descreve os diversos casos do ambiente das guerras convencionais e suas regras com aplicação ao ambiente da guerra cibernética. Bellovin *et al* (2017, p. 61), ao apresentarem o conceito de armas cibernéticas, explorando ainda a diferença entre armas indiscriminadas e armas direcionais (*target weapons*), examinam os requisitos técnicos necessários para garantir que armas cibernéticas não sejam indiscriminadas, além de apresentar algumas direções de políticas para garantir essa classificação. Sendo assim, eles propõem a aplicação de regras, já normalmente usadas para armas convencionais, para as armas cibernéticas, de forma a delimitar seu uso e alcance. Apresentam duas condições básicas para que armas cibernéticas sejam consideradas direcionais:

> Condição 1: a arma cibernética deve ser capaz de ser dirigida explicitamente

contra alvos designados; isto é, a arma cibernética deve ser direcional.

Condição 2: quando direcionada a uma entidade explicitamente designada, a arma deve minimizar a formação de efeitos negativos significativos em outras entidades que o atacante não tem explicitamente designado como alvo. (BELLOVIN *et al*, 2017, p. 61) (tradução nossa)

É reforçada ainda a ideia de que, para um ataque ser efetivo e preciso, ele deve ser muito bem estudado e, em alguns casos, as brechas já devem estar preliminarmente presentes na máquina-alvo. A questão da inteligência da arma é descrita, ainda, levando-se em conta que o mecanismo possa vir a progredir ou evoluir de forma autônoma, uma vez carregada em sistemas desconectados da internet. Novamente o autor analisa os impactos colaterais adversos que devem ser levados em conta pelo projetista da arma, sob aspectos legais e éticos. Uma das justificativas importantes é que efeitos colaterais de ataques levam analistas da parte atacada a perceber e estudar o ataque, podendo inclusive diminuir seus efeitos ou produzir semelhantes armas por meio de engenharia reversa. Muitos ataques podem ser baseados em portas IP específicas ou números de série específicos de equipamentos. Sendo assim, o uso de itens COTS (*Commercial Off The Shelf*) realmente genéricos é um fator que dificulta o projetista de ataque cibernético em construir mecanismos muito direcionais, pois há grande probabilidade de o mesmo efeito acontecer em equipamentos não diretamente relacionados ao inimigo ou ao alvo específico pretendido, facilitando o estudo de contramedidas ou proteções. Ainda assim, o Departamento de Defesa americano (2005), citado por King *et al* (2007), indica que "a aquisição e a produção global de dispositivos COTS conduzem a uma 'enorme e incrível' oportunidade para ataques (indiscriminados), afinal de contas, nem todo mundo está preocupado com questões éticas em meio à essa 'guerra'". (KING, 2008, p. 1) (tradução nossa)

As discussões anteriores concentraram-se em apresentar modelos e técnicas que basicamente analisam as vulnerabilidades de sistemas digitais e propõem medidas de correções em *softwares,* considerando a possibilidade de reescrever os códigos-fonte ou efetuar mudanças em suas arquiteturas. Mas o que ocorre na prática de sistemas das Forças Armadas é que muitos sistemas estão em uso e, em sua maioria, são resultado de aquisições (de que geralmente não se dispõe) dos códigos fontes e da possibilidade de alterar sua arquitetura. Sendo assim, há duas categorias de sistemas: os sistemas em uso e aqueles em processo de especificação ou desenvolvimento (ainda que em planejamento).

Pode-se também inferir que existem medidas classificadas como estritamente técnicas, simplesmente operacionais ou uma combinação de ambas, a depender do grau de acesso a códigos-fonte e recursos de atualização desses sistemas (compiladores, plataformas de desenvolvimento, bibliotecas etc). As medidas de atuação estritamente técnicas em sistemas digitais, em contraposição às ameaças cibernéticas, demandam o acesso aos códigos-fonte e demais recursos de produção ou modificação desses sistemas. As medidas operacionais atuam de forma mais preventiva, educacional ou emergencial, de forma a minimizar os efeitos de ataques cibernéticos sem, contudo, poder alterar os sistemas. De fato, há sistemas adquiridos que possibilitam algum grau

de reconfiguração ou recompilação de *software* sem, contudo, possibilitar mudanças de arquitetura do sistema. Nesse caso, medidas técnicas e operacionais são possíveis de serem propostas e aplicáveis.

PROPOSTA DE UM MODELO DE CONTRAMEDIDAS CIBERNÉTICAS

O modelo proposto é baseado na Norma ABNT NBR ISO/IEC 27005 (2011), estabelecendo medidas e procedimentos que devem ser observados pelos agentes envolvidos em especificação, desenvolvimento, testes, aquisição e manutenção de sistemas digitais operativos. Utilizou-se um acrônimo para facilitar a memorização das etapas: ALERT-N (A = Analise ameaças e vulnerabilidades, monte a tabela de riscos e prepare planos de contramedidas; L = "pLaneje" e execute exercícios de guerra cibernética e ações de auditoria; E = Evidencie e documente todos os eventos externos e internos detectados; R = Reaja imediatamente em caso de ataque ou ataque iminente; T = Treine uma ou mais equipes especializadas em defesa cibernética; N = utilize algoritmos e dispositivos Nacionais para itens críticos).

Essas medidas estão coerentes com a Doutrina de Tecnologia da Informação da Marinha (BRASIL, 2007, p. 5-1), em que ações básicas de proteção dos sistemas de informação digital são estabelecidas, enumerando as seguintes principais atividades: planejamento, histórico, análise, correção e adestramento. Entretanto, nesta análise, foi incluída a importante ação de se iniciar o uso efetivo de itens nacionais para algoritmos e dispositivos críticos. Os especificadores, desenvolvedores e até mantenedores de sistemas digitais operativos (ao realizar atividades de Modtec) devem priorizar o uso de algoritmos e dispositivos nacionais, em detrimento a soluções com itens importados. Cláusulas contratuais específicas devem ser claras quanto ao favorecimento de empresas nacionais para itens considerados críticos aos sistemas digitais operativos. Segue-se um resumo dessas etapas.

– Analise ameaças e vulnerabilidades, monte a tabela de riscos e prepare planos de contramedidas

A análise deve começar pela modelagem do sistema estudado, identificando suas funcionalidades (esta é a etapa de identificação de ativos primários constante na Norma ABNT NBR ISO/IEC 27005, 2011) e quais os principais recursos (*hardware*, *software*, *firmware)* que se quer proteger (ativos de suporte da Norma). O método Morda, explicado anteriormente, é adequado quando se tem condições de modificar a arquitetura dos sistemas. No entanto, para os casos em que isso não é possível, devem-se identificar métodos aplicados também a *hardware* e que possibilitem estabelecer contramedidas adequadas.

À etapa "Derive ataques para encontrar objetivos de ataques adversários" do Morda foi adicionado o método de injeção de falhas, motivado por suas características de incluir falhas aleatórias de *hardwares* ou *software*. Isso aumentará as possibilidades de possíveis ataques, incluindo "falhas" que poderiam ser ataques. Na Figura 1, o processo "Aplique Métodos II" do fluxograma é composto pelo Morda modificado, para o qual acrescentou-se o método de injeção de falhas.

Para o caso de "Dispositivos Críticos" (placas diversas de *hardware*, mídias de armazenamento, equipamentos), foi decidido pelas técnicas de tolerância à intrusão e defesa em profundidade para análise da arquitetura do sistema, envolvendo *software* e *hardware*. Essas técnicas

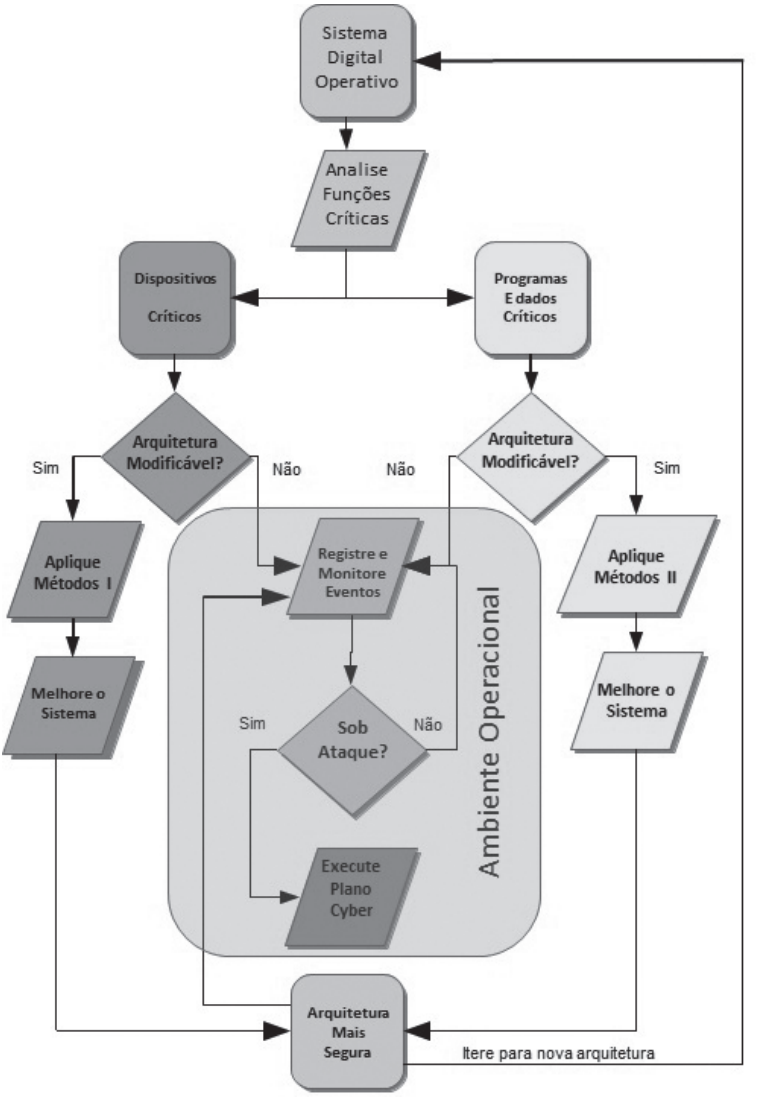

Figura 1 – Modelo ALERT-N

compõem o processo "Aplique Métodos I" do fluxograma citado. Os conceitos de redundância, diversificação e separação de equipamentos ou funções de forma a que o sistema continue a prover suas funções ou serviços a despeito de falhas (o modo sobrevivência), utilizados pelo método de tolerância a intrusão, são essenciais para manter as funcionalidades de sistemas críticos, como os sistemas digitais operativos. Um sistema de navegação, por exemplo, deve ter condições de prover outros meios de dispor de dados de navegação confiáveis, em redundância ao principal. Já o método de defesa em profundidade, caracterizado por barreiras que funcionariam como camadas de segurança completamente independentes (*software*

ou *hardware*), de forma a minimizar a probabilidade de que todas as camadas de segurança sejam quebradas, é também aplicável aos sistemas digitais operativos quando se proveem camadas físicas, como chaves (físicas ou eletrônicas) em equipamentos ou o controle de acesso a dispositivos críticos, como mídias que contenham bibliotecas operativas.

Após essas análises, são delimitadas funções ou recursos críticos, priorizando-os diante da grande quantidade de funções exercidas pelo sistema.

A partir desses estudos de vulnerabilidade e ameaças, crie a tabela de riscos de forma a identificar e ponderar quais os casos mais críticos para os quais devem ser estabelecidas contramedidas ou ações mitigatórias, em detrimento de outros casos menos importantes (à semelhança do que ocorre no Morda). Essas ações mitigatórias serão, ao final, os requisitos de segurança cibernética para aquele dado sistema. Essas medidas podem ser usadas no processo "Melhore o sistema" descrito no fluxograma do Apêndice. Em seguida, crie e mantenha atualizado o plano de contramedidas cibernéticas (Plano Cyber): Quais as correções a aplicar e onde? Como e quando agir em cada caso? Reinstalação de *software*s ou *firmwares*? Substituição por outro equipamento? Redundância a bordo? Sugere-se que esse plano faça parte efetiva do Plano de Apoio Logístico Integrado (Pali) do meio. Como uma parte dessas contramedidas, estabeleça cláusulas específicas de segurança cibernéticas para contratos com fornecedores e demais empresas envolvidas com sistemas digitais operativos a serem adquiridos ou desenvolvidos para a Marinha do Brasil (MB).

Retomando o fluxograma da Figura 1, caso não se consiga alterar a arquitetura dos sistemas, segue-se apenas à fase de monitoração e registro de eventos e execução do Plano Cyber. Essas alterações podem ser classificadas como uma Modtec ou apenas para implementação em projetos futuros. A nova arquitetura do sistema é então novamente submetida à análise, reiniciando o ciclo no fluxograma proposto.

– "pLaneje" e execute exercícios de guerra cibernética e ações de auditoria

Estabeleça um plano de adestramento constante para os agentes envolvidos no processo. Além de realizar visitas técnicas em organizações militares que mantêm sistemas digitais operativos, equipes cibernéticas deverão analisar registros de eventos em tais sistemas, dos mais simples aos mais relevantes, de forma a identificar possíveis ataques ou ações de exploração de dados realizados ou em curso. O uso de *smartphones* em ambientes de operação, desenvolvimento e manutenção de *software*s digitais operativos deve ser terminantemente proibido. Esses equipamentos têm a capacidade de receber atualizações de aplicativos que podem ser direcionados a gravar, fotografar ou filmar os ambientes onde estão, inclusive com base na localização geográfica, sem que isso seja necessariamente habilitado pelo usuário. Esta pode ser uma ferramenta útil para explorar ou simplesmente estudar sistemas e pessoas envolvidos nos processos.

Execute planos e exercícios de testes de sistemas digitais operativos antes de missões relevantes. O custo envolvido em se preparar um meio militar para uma missão é muito elevado. Às medidas previstas nos planos logísticos para a prontidão do meio devem ser acrescidos testes preliminares de segurança cibernética para os sistemas operativos e sua integração com as armas.

Devido ao alto custo de se verificar a segurança cibernética de cada arma a ser embarcada, testes ainda mais preliminares podem ser realizados e caracterizados por lotes de armas que possuem exatamente

as mesmas configurações de *hardware*, *software* e *firmware*. Essas configurações devem ser gerenciadas com total segurança, de forma a se manter elevado grau de confiabilidade para uso daquelas armas ou de sistemas já testados.

– Evidencie e documente todos os eventos externos e internos detectados

A mensagem é "registre tudo!". Se os planos e simulações de ataque forem bem planejados e os sistemas especificados atenderem aos requisitos de projeto de segurança dos sistemas elaborados, é esperado que atacantes sigam os caminhos delineados anteriormente para explorar os sistemas. Assim, é importante que suspeitas e eventos detectados sejam sempre registrados em sistema próprio e de fácil acesso pelos envolvidos no processo. Essa base de dados funcionará como *feedback* para ataques tentativos ou executados, podendo realimentar e reforçar contramedidas a serem implementadas futuramente nos sistemas digitais operativos. Com a evolução na segurança de sistemas, é esperado que eles próprios sejam capazes de alertar o pessoal de bordo sobre tentativas de violações de segurança e combatam ou suspendam ações em curso de forma segura.

– Reaja imediatamente em caso de ataque ou ataque iminente

É prudente inicializar medidas de proteção estabelecidas em caso de suspeitas ou efetividade de um ataque em sistemas de bordo. A velocidade das máquinas é incomparavelmente maior do que o tempo de reação humano; portanto, agir em caso de suspeitas pode ser crucial. Paralelamente ao acionamento de contramedidas cibernéticas, o comandante tem que iniciar a comunicação do caso às equipes de defesa cibernética da Força, de tal maneira que sejam iniciadas as simulações em laboratório a partir de cenários semelhantes e sejam preparadas medidas adicionais a serem aplicadas a todos os meios militares que utilizem os mesmos sistemas e dispositivos afetados.

– Treine uma ou mais equipes especializadas em defesa cibernética

Crie e mantenha atualizada uma equipe cibernética de defesa e auditoria de sistemas. Ações de treinamento desses agentes, incluindo participação em congressos da área de segurança digital, e a constante divulgação de práticas de segurança digital são necessárias para mantê-los em estado de alerta. Eles têm que participar dos planos de treinamento citados anteriormente como responsáveis pela preparação e execução das atividades. Adicionalmente, eles serão os responsáveis em manter atualizados os modelos e procedimentos de medidas de combate à guerra cibernética de sistemas digitais operativos dentro da Força, implementando as correções necessárias.

– Utilize algoritmos e dispositivos Nacionais para itens considerados críticos

Priorize o uso de algoritmos e dispositivos críticos (como processadores e placas de interface) de empresas nacionais para serem aplicados em armas e sistemas digitais operativos. Essa é uma medida de difícil implementação em um país com pouca tradição tecnológica na área de *chips* de computadores, mas é essencial diante da evolução da engenhosidade de mecanismos de destruição (*kill switches*) disseminados em diversos itens COTS e em produtos de empresas de defesa sob a alegação de ter como agir em caso de um dispositivo seu cair em mãos adversárias (KOCH R. e GOLLING M, 2016, p. 197). Conforme mencionado anteriormente, essa medida tem se tornado imprescindível para o aumento da segurança cibernética de armas e sistemas digitais operativos. A produção desses itens tem ainda a

vantagem de ser completamente dual, podendo ser empregados tanto no meio militar quanto no meio civil, facilitando a obtenção de recursos governamentais e privados para projetos de tecnologia em parceria. No momento tecnológico atual, é posível a utilização de métodos, linguagens de programação e equipamentos de prototipação de circuitos complexos como esses em solo nacional. Isso está ainda em consonância com o Decreto 6.703 de 18 de dezembro de 2008 (BRASIL, 2008), que lista algumas características para seleção de projetos estratégicos: "[...] os projetos a serem apoiados serão selecionados e avaliados de acordo com ações estratégicas [...], a possibilidade de uso comum pelas Forças, o uso dual – militar e civil – das tecnologias, subprodutos tecnológicos de emprego civil, o índice de nacionalização [...]".

O uso de trilhos em benefício do transporte de tropas e materiais a longas distâncias foi vislumbrado por Friedrich List e utilizado pela Prússia nas guerras dos anos de 1860. Mais adiante, outros líderes europeus também incrementaram o uso de vias férreas, cientes de seu valor estratégico e tático. Entretanto, perceberam que o inimigo também poderia fazer uso desses trilhos, conectando-os às suas malhas ferroviárias. Como resultado, cada país passou a usar diferentes bitolas de trilhos, impossibilitando que outros trafegassem por suas vias (RAILWAYS THROUGH EUROPE, 2016). Pretende-se usar similar analogia para algoritmos e dispositivos computacionais críticos. Use os seus!

CONCLUSÃO

As ações de guerra cibernética podem afetar não apenas alvos como empresas e instituições civis, mas também equipamentos militares, como armas, sistemas de controle de armas, radares, sonares ou sistemas de contramedidas, tornando-os vulneráveis. O acesso a dispositivos e sistemas mais baratos, como os COTS, conduziu empresas militares a incorporar tais itens em seus sistemas e armas. Entretanto, algumas empresas de defesa têm implantado mecanismos de destruição (*kill switch*) em seus produtos sob a alegação de dispor de uma medida de desativação futura, caso isso seja necessário. Esses aspectos são relevantes, e seus impactos foram avaliados para os sistemas digitais operativos.

Ao conceito de prontidão do navio para suas missões no mar deve estar associada sua capacidade total de usar seus sistemas e armas em um ambiente de guerras cibernéticas

Diante da diversidade de vulnerabilidades e ameaças identificadas, foi vislumbrada a necessidade de encontrar modelos para se defender de ações cibernéticas contra sistemas digitais operativos. O modelo Morda, da IEEE Computer Society, avalia as vulnerabilidades e ameaças a sistemas computacionais e propõe contramedidas a ataques cibernéticos, considerando os custos e benefícios associados. Partindo-se deste modelo e adicionando-se outros métodos de segurança, como Injeção de Falhas, Defesa em Profundidade e Tolerância a Intrusões, foi proposto um novo modelo, denominado ALERT-N, que aprofunda a análise tanto de "Programas e Dados Críticos" quanto de "Dispositivos Críticos". Adicionalmente, concluiu-se que a nacionalização de

algoritmos e dispositivos mais críticos é essencial para se maximizar a proteção de sistemas digitais operativos, pois foi observado que é grande a possibilidade de que os sistemas digitais operativos incorporem dispositivos ou sistemas vulneráveis. Por fim, listaram-se várias contramedidas que os envolvidos em especificação, desenvolvimento, aquisição e manutenção de sistemas digitais operativos devam seguir, de forma a minimizar os impactos de ações de guerra cibernética.

É esperado que a aplicação das contramedidas aqui descritas, como resultado de um estudo sobre vulnerabilidades, ameaças e métodos aplicáveis a sistemas digitais operativos, venha a reduzir o risco de ataques cibernéticos adversários bem-sucedidos. Em especial, vislumbra-se que ao conceito de prontidão do navio para suas missões no mar esteja também associada sua capacidade total de usar seus sistemas e armas em um ambiente de guerras cibernéticas.

Este trabalho tem seu enfoque em sistemas navais, mas é também aplicável aos sistemas digitais operativos de outras Forças, ou até mesmo a outras instituições e empresas que utilizam sistemas críticos à segurança de seus dados digitais. No entanto, adpatações ao modelo podem ser necessárias.

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

REFERÊNCIAS

ABNT NBR ISO/IEC 27005. Tecnologia da Informação – Técnicas de Segurança – Gestão de Riscos de Segurança da Informação. Segunda edição, 2011.

ADAMS, J.; KURZER, P. *Remaking American Security: Supply chain vulnerabilities & national security risks across the US defense industrial base.* Alliance for American Manufacturing, 2013.

ARS TECHNICA. *Inside the wiper malware that brought Sony Pictures to its knees*. http://arstechnica.com/security/2014/12/inside-the-wiper-malware-that-brought-sony-pictures-to-its-knees. Acessado em 26/06/2016, *apud* BELLOVIN, Steven M.; LANDAU, Susan; e LIN, Herbert S. "Limiting the undesired impact of cyber weapons: technical requirements and policy implications". *Journal of Cybersecurity*, 3(1), p. 66, 2017.

BELLOVIN, Steven M.; LANDAU, Susan; LIN, Herbert S. "Limiting the undesired impact of cyber weapons: technical requirements and policy implications". *Journal of Cybersecurity*, 3(1), p. 59-68, 2017.

BRASIL. Decreto nº 849, de 25 de junho de 1993. Promulga os Protocolos I e II de 1977, adicionais às Convenções de Genebra de 1949, adotados em 10 de junho de 1977 pela Conferência Diplomática sobre Reafirmação e o Desenvolvimento do Direito Internacional Humanitário aplicável aos Conflitos Armados. Disponível em: <http://www2.camara.leg.br/legin/fed/decret/1993/decreto-849-25-junho-1993-449220-norma-pe.html>. Acesso em: 5 ago 2018.

BRASIL. Decreto nº 6.703, de 18 de dezembro de 2008. Aprova a Estratégia Nacional de Defesa e dá outras providências. Disponível em: <http://www.planalto.gov.br/ ccivil_03/_Ato2007-2010/2008/Decreto/D >. Acesso em: 3 jul 2018.

BRASIL. Estado-Maior da Armada. EMA-416: *Doutrina de Tecnologia da Informação da Marinha*. 1ª rev. Brasília, 2007.

BRASIL. Estado-Maior da Armada. EMA-420: *Normas para Logística de Material*. 2ª rev. Brasília, 2002.

DEPARTAMENTO DE DEFESA DOS ESTADOS UNIDOS. *Defense science board task force on high performance microchip supply*. http://www.acq.osd.mil/dsb/reports/2005-02-HPMS_Report_Final.pdf. Fevereiro, 2005 *apud* KING, S. T. *et al*. *Designing and implementing malicious hardware*. LEET, vol. 8, p. 1-8, 2008.

DU, Wenliang; MATHUR, Aditya P. *Vulnerability Testing of Software System Using Fault Injection.* Purdue University, W. Lafayette, Abril de 1998.

ELLISON, R. *et al*. "Survivable network systems: an emerging discipline". *Technical Report* CMU/SEI-97-TR-013. Carnegie Mellon University: Maio, 1997.

FURNELL, Steven *et al*. "Enhancing security behavior by supporting the user". *Computers & Security Journal*, Nº 75, 2018.

IEEE COMPUTER SOCIETY. *Risk-based systems security engineering: stopping attacks with intention*. IEEE Security & Privacy, volume 2, issue 6, p. 59-62. Dezembro, 2004.

KING, Samuel T. *et al*. "Designing and implementing malicious hardware". *Leet*, vol 8, p. 1-8, 2008.

KOCH, Robert; GOLLING, Mario. *Weapons Systems and Cyber Security – A Challenging Union.* 8th International Conference on Cyber Conflict – Cyber Power. Nato CCD COE Publications, Tallinn, p. 191-203, 2016.

LOUREIRO, Marcos Vinicius de Castro. "Ataques cibernéticos: ameaças reais ao poder naval". *Revista Marítima Brasileira*. v. 137, n. 01/03, p. 80-85, 2017.

NEW YORK TIMES. "Cyberattack on Saudi firm, US sees Iran firing back". http://nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html. Accessado em 26/6/2016, *apud* BELLOVIN, Steven M.; LANDAU, Susan; e LIN, Herbert S. "Limiting the undesired impact of cyber weapons: technical requirements and policy implications". *Journal of Cybersecurity*, 3(1), p. 59-68, 2017.

PIÈTRE-CAMBACÉDÈS, L.; BOUISSOU, M. "Cross-fertilization between safety and security engineering". *Reliability Engineering and System Safety*, v. 110, p. 110-126, 2013.

RAILWAYS THROUGH EUROPE. *Maps and facts on European interoperability issues.* Disponível em: <http://www.bueker.net/trainspotting/voltage_map_europe.php>. Acesso em 04/04/2016 *apud* Escola de Guerra Naval, C-SUP, II-S-4 Logística, Videoaula 1 – UE1.1, 2018. Videoaula.

SALTER, C. *et al*. "Toward a secure system engineering methodology". In: *Proceedings of the 1998 workshop on new security paradigms* (NSPW '98), Charlottesville, VA, United States, 1998, p. 2-10.

SCHMITT, Michael N. (general editor). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. United Kingdom: Cambridge University Press (www.cambridge.org), 2017.

SHIREY, R. Request For Comments: 2828. Disponível em: <https://www.rfc-editor.org/rfc/pdfrfc/rfc2828.txt.pdf>. Acesso em: 7 jul 2018.

STALLINGS, William; BROWN, Lawrie. *Segurança de Computadores: princípios e práticas*. 2 ed. Rio de Janeiro: Elsevier, 2014.

STONEBURNER, Gary; GOGUEN, Alice; FERINGA, Alexis. *Risk Management Guide for Information Techn-ology Systems – recommendations of National Institute of Standards and Technology* (NIST 800-30). Julho, 2002.

VOAS, Jeffrey. "Testing Software for Characteristics Other than Correctness: Safety, Failure Tolerance, and Security". In: *Proceedings of the 10th international conference on testing computer software*. Washington DC, USA, 1996.