

# DEFESA CIBERNÉTICA NA MARINHA DO BRASIL – Os desafios à Segurança Nacional

LEONARDO DA SILVA PIMENTA\*  
Suboficial (CN)

---

## SUMÁRIO

Histórico da cibernética no mundo e no Brasil  
Segurança para os sistemas ciberfísicos dos meios operativos de superfície  
Guerra cibernética – Operação Baluarte (Exercício)  
Jogos Olímpicos e Paralímpicos Rio 2016 – Caso de sucesso

## HISTÓRICO DA CIBERNÉTICA NO MUNDO E NO BRASIL

A cibernética<sup>1</sup>, assim como as descobertas nucleares e espaciais, está entre os grandes eventos da esfera científica e tecnológica ocorridos após a Segunda Guerra Mundial. Os avanços advindos com o desenvolvimento das novas tec-

nologias de informação<sup>2</sup> e comunicação, posteriormente potencializados pelo surgimento da internet, apresentaram efeitos mais tardios, mas não com menor magnitude, do que os decorrentes dos progressos ocorridos naqueles outros dois campos da ciência. Entretanto, ao contrário deles, não recebeu o mesmo tratamento em termos de mecanismos

---

\*Consultor de Segurança. Bacharel em Informática pela Universidade Estácio de Sá. Pós-Graduado em Perícia e Investigação Criminal Militar pelo Exército Brasileiro. MBA em Engenharia de Redes de Computadores pelas Faculdades Integradas Simonsen. Especialista em Gestão de Segurança da Informação pelo Gabinete de Segurança Institucional da Presidência da República – GSI-PR/UNB. Pós-graduado em Política e Estratégia pela Faculdade La Salle.

1 Termo que se refere à comunicação e ao controle relacionados aos ativos de informação, como uso de computadores, sistemas computacionais, redes de computadores e de comunicações e suas interações.

2 Meios de armazenamento, transmissão e processamento de dados e informação; os equipamentos necessários a isso (computadores, equipamentos de comunicações e de interconexão); os sistemas utilizados para tal, os sistemas de informação de um modo geral, os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

de fiscalização e controle em níveis internacionais.

Trata-se de fenômeno que implica desenvolvimento rápido, de difícil acompanhamento e difuso diante de suas aparências mutáveis, tornando mais complexa a identificação dos componentes que podem se converter em ameaças, mormente os desdobramentos dos efeitos sobre os indivíduos, as sociedades e os estados. Também traz à baila o desafio que se impõe entre a liberdade individual e as necessidades da segurança e defesa, ou, por outro viés, entre privacidade e controle de ameaças.

Nos últimos anos, tem-se observado o aumento do risco de perpetração de ataques cibernéticos<sup>3</sup> por estados, organizações e, até mesmo, pequenos grupos, com as mais diversas motivações.

As nações estão em processo de adequação para lidar com a cibernética em todos os campos do conhecimento. Por outro lado, o uso indevido deste conhecimento pode levar a danos de dimensões imprevisíveis para todo o mundo.

Diante desse quadro, podem-se elencar algumas das principais características do domínio cibernético:

- não possui limitações físicas de distância e espaço, nem fronteiras geograficamente definidas;
- é mutável e dependente das condições ambientais e da criatividade do ser humano, podendo os efeitos colaterais ser incontroláveis;

- há facilidade de acesso a ferramentas similares de Tecnologia de Informação (TI), tanto para os administradores de sistemas como para os oponentes; e

- não existe sistema computacional totalmente seguro.

O espaço cibernético<sup>4</sup> é *sui generis* e dual, visto que, normalmente, há dificuldade de se identificar a atribuição dos ataques, desconhecendo se sua proveniência vem de ações militares. Ademais, há uma infinidade de flancos cibernéticos sobre os quais não se tem controle. Entre as

principais ameaças, podem ser elencados: o crime cibernético, o terrorismo cibernético, a espionagem cibernética, a atuação de *hackers* (mais especificamente *crackers*) e organizações de estados.

A sociedade brasileira, em particular a expressão militar do Poder Nacional, deverá estar permanentemente preparada, considerando os atuais e futuros contenciosos internacionais. Para tal, medidas deverão ser adotadas de forma a capacitá-la a responder oportuna e adequadamente, antecipando os possíveis cenários adversos à defesa nacional.

No contexto nacional, particularmente na área governamental, o tema foi tratado, inicialmente, como Segurança da Informação, o que se caracterizou com a criação do Gabinete de Segurança Institucional da Presidência da República

---



---

**Nos últimos anos, tem-se observado o aumento do risco de ataques cibernéticos por estados, organizações e pequenos grupos, com as mais diversas motivações**

---



---

3 Causa potencial de um incidente indesejado, que pode resultar em dano ao espaço cibernético de interesse.

4 Espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas.

(GSI/ PR), por meio da Medida Provisória (MP) nº 2.216-37, de 31 de agosto de 2001, que alterou dispositivos da Lei nº 9.649, de 27 de maio de 1998. Ao novo órgão, entre outras competências, coube a coordenação das atividades de Segurança da Informação (BRASIL, 2001).

Pelo Decreto nº 5.772, de 8 de maio de 2006, foi criado o Departamento de Segurança da Informação e Comunicações (DSIC), no GSI/PR, com a missão de planejar e coordenar a execução das atividades de Segurança da Informação e Comunicações (SIC) na Administração Pública Federal (APF) (BRASIL, 2006a). Em dezembro de 2008, o Decreto nº 6.703 aprovou a Estratégia Nacional de Defesa, definindo prioridades nos três setores estratégicos para a defesa nacional: Nuclear, Cibernético e Espacial (BRASIL, 2008a).

A Diretriz Ministerial nº 0014, do Ministério da Defesa, de 9 de novembro de 2009, definiu providências para o cumprimento da Estratégia Nacional de Defesa (END) nos setores estratégicos da defesa, estabelecendo as responsabilidades para cada Força Armada.

O Decreto nº 7.411, de 29 de dezembro de 2010, explicitou, nas atribuições do DSIC – Gabinete de Segurança Institucional da Presidência da República, a sua competência de planejar e coordenar a execução das atividades de Segurança Cibernética<sup>5</sup> e de Segurança da Informação e Comunicações na Administração Pública Federal. Em 20 de setembro de 2012, o Decreto Presidencial nº 7.809, entre outras medidas, incluiu,

na Estrutura Regimental do Comando do Exército, o Centro de Defesa Cibernética (BRASIL, 2010b).

Posteriormente, o Ministério da Defesa, por intermédio da Portaria nº 3.405/MD, de 21 de dezembro de 2012, atribuiu ao Centro de Defesa Cibernética, do Comando do Exército, a responsabilidade pela coordenação e integração das atividades de defesa cibernética<sup>6</sup>, no âmbito do Ministério da Defesa (MD), consoante o disposto no Decreto nº 6.703, de 2008 (BRASIL, 2008, 2012b).

Concomitantemente, a Portaria Normativa nº 3.389, do Ministério da Defesa, de 21 de dezembro de 2012, aprovou a Política Cibernética de Defesa. Entre seus objetivos, incluem-se os de desenvolver e de manter atualizada a doutrina de emprego do setor cibernético, cujos fundamentos estão consubstanciados naquela política (BRASIL, 2012c).

O Decreto Legislativo nº 373, de 12 de setembro de 2013, atualizou a Estratégia Nacional de Defesa e aprovou o Livro Branco de Defesa Nacional. Nas premissas sobre o setor cibernético, citadas no documento, evidencia-se a proteção do espaço cibernético, que abrange um grande número de áreas, como: capacitação; inteligência; pesquisa científica; doutrina; preparo e emprego operacional; e gestão de pessoal (BRASIL, 2013).

Em 27 de outubro de 2014, a Portaria Normativa nº 2.777, do MD, definiu responsabilidades sobre a implantação das medidas que visam à potencialização da defesa cibernética nacional, nas quais figura a instituição do Comando de

5 Garantia da confidencialidade, integridade e da disponibilidade de um espaço cibernético. Adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas.

6 Conjunto de ações ofensivas, defensivas e exploratórias realizadas no espaço cibernético, no contexto de um planejamento de nível estratégico, com as finalidades de proteger os interesses da Marinha e comprometer os sistemas de informação do oponente.

Defesa Cibernética (ComDCiber) e da Escola Nacional de Defesa Cibernética (ENaDCiber). E, em 18 de novembro de 2014, a Portaria Normativa nº 3.010, do MD, aprovou a Doutrina Militar de Defesa Cibernética (BRASIL, 2014b, 2014c).

Em 2 de janeiro de 2015, o comandante do Exército criou o ComDCiber e a ENaDCiber, subordinados, inicialmente, ao CDCiber, e ativou seus núcleos, a contar de 1º de janeiro de 2015.

Em 13 de julho de 2015, a presidente da República, pelo Decreto nº 8.491, alterou a Estrutura Regimental do Comando do Exército e a subordinação do CDCiber, definindo sua competência, caracterizada pelas seguintes ações:

- assessorar o comandante do Exército e o ministro da Defesa nas atividades do setor cibernético, formular doutrina e obter e empregar tecnologias;
- planejar, orientar e controlar as atividades operacionais, doutrinárias e de desenvolvimento das capacidades cibernéticas; e
- executar atividades de exploração cibernética, em conformidade com as políticas e diretrizes do Ministério da Defesa (BRASIL, 2015a).

Em 3 de março de 2016, o Estado-Maior do Exército emitiu a Portaria nº 61, que aprovou a diretriz para a implantação do Comando de Defesa Cibernética (ComDCiber) (BRASIL, 2016c).

Na Marinha do Brasil (MB), a Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM) tem

como propósito assegurar a eficiência e a eficácia do sistema de comunicações da Marinha, garantir a defesa do espaço cibernético de interesse da MB e contribuir para a supervisão das atividades relativas à Governança de Tecnologia da Informação e ao Sistema de Inteligência da Marinha (Simar).

A Agência de Inteligência de Ameaças Cibernéticas da Marinha (AgIntA-Ciber-MB), ativada pela Diretoria de Comunicações e Tecnologia da Informação da Marinha, em 27 de fevereiro de 2018, produzirá conhecimentos de inteligência sobre as ameaças ao Espaço Cibernético da Marinha (ECiber-MB)<sup>7</sup>, analisará as suas vulnerabilidades e

proproará medidas de mitigação, prevenção e correção, a fim de contribuir para a manutenção de uma consciência situacional cibernética visando à defesa e segurança do ECiber-MB, com sede na cidade do Rio de Janeiro

(Bono nº 292, de 16 de abril de 2018).

### **A Diretoria de Comunicações e Tecnologia da Informação da Marinha tem como propósito garantir a defesa do espaço cibernético de interesse da MB**

### **SEGURANCA PARA OS SISTEMAS CIBERFÍSICOS DOS MEIOS OPERATIVOS DE SUPERFÍCIE**

Sistemas Ciberfísicos (SCF) são sistemas em que ocorre a integração de computação e processos físicos (LEE, 2008). Em termos gerais, são sistemas que atuam na tarefa de controle de um processo físico e, de acordo com a teoria de controle, esses sistemas devem escolher as ações ao longo

<sup>7</sup> Espaço cibernético composto pelos ativos de informação da MB.

do tempo para influenciar o processo sob seu controle. Se a escolha dessas ações depende do processo a ser controlado, um SCF observa esse processo por meio de sensores de aquisição de dados, perfaz o controle empregando computadores para escolher as ações e, por meio de atuadores, efetiva as ações de controle sobre esse processo físico.

O uso de SCF é crescente, devido aos ganhos e ao desempenho que ele pode prover, ou pela possibilidade de redução de pessoal necessário para a execução de um conjunto de tarefas. Na Marinha do Brasil, o uso de SCF se dá na utilização dos sistemas de armas empregados em navios de superfície, como os das fragatas da classe *Niterói* e da Corveta *Barroso*. Em adição a esses, outros sistemas podem ser listados, como o Sistema de Controle e Monitoração da Propulsão e Auxiliares (SCMPA) das fragatas da classe *Niterói*, desenvolvido pelo Centro Tecnológico da Marinha em São Paulo (CTMSP), e o Sistema de Controle e Monitoração (SCM) das corvetas da classe *Inhaúma*, desenvolvido pelo Instituto de Pesquisas da Marinha (IPqM). Adicionalmente, cito os sistemas de comunicação satelital, detecção, auxílio à navegação e apoio à saúde (raio X e mamógrafo), utilizados pelos navios de assistência hospitalar da classe *Oswaldo Cruz*, empregados nas operações de assistência à saúde e ações humanitárias

**Ao longo de seu ciclo de vida, o sistema ciberfísico tem um aumento na probabilidade de apresentar alguma vulnerabilidade**

(inclusão digital e emissão de seguro social, entre outras) para populações ribeirinhas da Amazônia.

Num SCF, o espaço cibernético em questão pode conter as conexões internas e externas deste, bem como seu mecanismo de aquisição de dados, controle e respectivos atuadores. Um ataque a um SCF pode resultar em efeitos no respectivo processo físico. Segundo Loukas (2015, p. 12), “um ataque ciberfísico é uma brecha de segurança no espaço cibernético que afeta um espaço físico de modo adverso”. O ataque a um SCF envolve uma ação não autorizada no espaço cibernético, aproveitando-se de uma vulnerabilidade, que terá como consequência um efeito no espaço físico.

Ao longo de seu ciclo de vida, o SCF tem um aumento na probabilidade de apresentar alguma vulnerabilidade, e esse aumento decorre, principalmente,

dos aspectos listados abaixo:

- emprego de tecnologias cada vez mais difundidas no mercado, sejam *softwares* ou *hardwares*;
- o *software* que permeia esses sistemas pode ser derivado de uma linha de produto de *software*<sup>8</sup>;
- ao longo de seu ciclo de vida, um meio de superfície pode ter alguns sistemas removidos, outros substituídos ou mesmo receber novos sistemas. Uma substituição ou um recebimento de novo sistema pode trazer consigo novas vulnerabilidades decorrentes das tecnologias

8 Conjunto de sistemas que usam *software* intensivamente, compartilhando um conjunto de características comuns e gerenciadas, que satisfazem às necessidades de um segmento particular de mercado ou missão e que são desenvolvidos a partir de um conjunto comum de ativos (CLEMETS; NORTHROP, 2001).

que compõem esse sistema, ou de como ele seja instalado. Usando como exemplo uma antena de comunicação por satélite das estações móveis navais nas bandas Ku, Ka e X<sup>9</sup>, observam-se algumas funcionalidades providas para facilitar a sua operação, e o sistema tem excelente *software* remoto, permitindo que a antena seja monitorada e controlada por meio do protocolo de internet a partir de qualquer computador da rede do navio, ou mesmo, se necessário, a partir de um computador com acesso à rede do navio em organizações da MB em terra. Pela interface homem-máquina a partir do *software*, por meio do protocolo de internet, aumentam o espaço cibernético e o risco de este equipamento sofrer ações maliciosas; e

– devido à crescente necessidade de informações para a tomada de decisão, ao crescente emprego de sistemas de informação e SCF e à convergência tecnológica entre eles, tem-se o aumento da interconectividade entre esses sistemas. Essas interconexões formam redes e permitem a transferência de dados e o acesso de usuários. Assim, o espaço cibernético onde os SCF e os Sistemas de Tecnologia da Informação estão contidos é alargado com o passar do tempo.

Atualmente, no âmbito da Marinha do Brasil, os SCF não possuem uma política dedicada à sua segurança. As medidas de segurança em vigor na MB têm como principal norma a Doutrina

de Tecnologia da Informação da Marinha (EMA-416). Esta norma trata dos objetivos da segurança da informação, com aplicação direta nos sistemas de TI, e deixa de considerar os seus efeitos nos processos físicos relacionados aos sistemas ciberfísicos.

Um outro aspecto interessante a destacar é o efeito desejado de ações no domínio cibernético definido tanto na Doutrina Militar de Defesa Cibernética (MD31-7) quanto na Doutrina Básica da Marinha (EMA-305), e, em ambas as normas, as ações de guerra cibernética têm efeito no nível informacional e nos respectivos sistemas de informação. Essas normas não consideram que as referidas ações também poderiam ter efeito direto no nível de processos físicos. Vê-se que, no domínio cibernético, ainda não está amadurecida a visão de possíveis efeitos cinéticos e, conseqüentemente, isso afeta a percepção de que os SCF também devem ser protegidos.

Inicialmente, os SCF tinham pouca semelhança com os sistemas de TI tradicionais, pois, em geral, os SCF eram sistemas isolados<sup>10</sup> que executavam protocolos de controle e comunicação proprietários, utilizando *hardware* e *software* especializados. Fisicamente, os componentes dos SCF eram posicionados em áreas com segurança física e não eram conectados a redes ou sistemas de TI.

Atualmente há uma ampla disponibilidade de dispositivos de baixo custo

9 Faixas de frequência utilizadas nas comunicações com satélites. Nessas frequências, o sinal se propaga em linha reta e é afetado por mudanças climáticas na atmosfera. A banda Ka (mais nova) e a banda Ku (tradicional) utilizam satélites comerciais, enquanto a banda X opera com satélite militar. Na comparação Ka/Ku, a banda Ka tem mais espectro disponível (2.500 MHz/750 MHz); o dobro de ganho de polarização; reutiliza seis vezes mais a frequência; e a eficiência espectral do enlace total (ida e vinda ao satélite) é 20 vezes maior. Em suma, a banda Ka oferece muito mais capacidade, o que sinaliza um custo menor para o usuário. Os navios da Marinha do Brasil fazem uso da banda Ku e da banda X.

10 São sistemas desenvolvidos por um certo fabricante que não funcionam com equipamentos de outro fabricante. Não trocam informações com o ambiente externo, sendo restritivos à troca de informações.

empregando o Protocolo de Internet (IP)<sup>11</sup> e que agora estão substituindo as soluções proprietárias antes utilizadas em SCF, o que aumenta a possibilidade de vulnerabilidades de segurança cibernética e incidentes. Além disso, os SCF estão adotando soluções de TI para permitir a conexão aos sistemas de negócios corporativos e o acesso remoto, sendo projetados e implementados utilizando-se de computadores, sistemas operacionais e protocolos de rede padrão da indústria. Dessa forma, os SCF estão começando a possuir similaridades com os sistemas de TI. Essa integração provê novos recursos aos sistemas de TI, mas leva a um decréscimo significativo no isolamento de um SCF do mundo exterior, criando maior necessidade de proteger esses sistemas.

Aliado a esse quadro, há um crescente uso das redes sem fio, colocando alguns SCF em maior risco, pois permite que adversários possam acessá-los a alguma distância, sem ter acesso físico direto ao equipamento.

Para sistemas de TI, a segurança é entendida como a união de três macroatividades: prevenção, detecção e resposta (CONKLIN; WHITE, 2014). Cada técnica de segurança ou tecnologia aplicada à segurança pode ser vista em uma ou mais dessas atividades, e os objetivos da segurança são a confidencialidade, a integridade e a disponibilidade dos dados nos sistemas. Segundo Coklin e White (2014), por muito tempo o foco da

segurança foi na prevenção, assumindo que, se é possível prevenir que alguém tenha acesso a um sistema, então ele está seguro. Entretanto, com o passar do tempo, foi visto que não importa o quanto se consiga prevenir o acesso a um sistema, basta haver uma violação ao mesmo que esta hipótese assumida se torna falsa. Assim, é preciso agregar aos métodos de prevenção os mecanismos que indiquem quando eles falharem, ou seja, a detecção de modo a permitir que os meios para se resolver o problema possam ser adequadamente empregados, isto é, que a resposta seja executada.

Um SCF controla o mundo físico, enquanto sistemas de TI gerenciam dados.

As características que os diferem incluem os riscos e as prioridades.

Em geral, SCF possuem requisitos de desempenho e são sistemas de tempo real críticos, isto é, quando o prazo para execução de

uma tarefa não pode ser violado. Em geral, esses sistemas requerem respostas determinísticas, confiáveis e nem sempre com alta taxa de transferência. Em contraste, sistemas de TI requerem alta taxa de transferência e são mais resistentes a algum nível de atraso.

Muitos dos processos controlados por SCF são de natureza contínua ao longo do tempo, e interrupções inesperadas não são aceitáveis. Os requisitos de disponibilidade em SCF são elevados, e sua parada e sua reinicialização comprometem o meio físi-

### **As preocupações primárias dos dados em sistemas de TI são confidencialidade, integridade e disponibilidade**

<sup>11</sup> Internet Protocol, ou o acrônimo IP, é um protocolo de comunicação usado entre todas as máquinas em rede para encaminhamento dos dados. Tanto no Modelo TCP/IP quanto no Modelo OSI, o importante protocolo da internet IP está na camada chamada “camada de rede”.

co em que atuam. Por isso, nesses sistemas são encontrados componentes redundantes, em geral em execução paralela, para prover continuidade de funcionamento mesmo na falha do componente principal.

As preocupações primárias dos dados em sistemas de TI são confidencialidade, integridade e disponibilidade. Para os SCF, as preocupações são a segurança da vida humana, as perdas de equipamento, produtos e produção, a tolerância a falhas para prevenir dados e a aderência às normas de segurança. Desse modo, os requisitos para o gerenciamento de riscos são diferentes, e o pessoal que opera, mantém e protege um SCF deve entender a relação entre proteção do sistema e a segurança do meio físico.

O sistema operacional e as redes de controle de um SCF são bem diferentes dos respectivos componentes no âmbito da TI, requerendo outras habilidades, experiência e maturidade para a sua operação. A característica de trabalhar em tempo real e com dispositivos de capacidade de processamento variável torna os SCF um sistema de recursos restritos, sem que se possam incorporar algumas capacidades de segurança existentes em sistemas de TI, como incitação e registro de erros (*logging*).

A gerência de mudanças é importante para manter a integridade de um sistema, seja ele de TI ou SCF, pois um *software* desatualizado representa uma das maiores vulnerabilidades. Para um sistema de TI, as atualizações são aplicadas em tempo hábil e seguindo alguma política e procedimento de segurança. Para os SCF, essas atualizações nem sempre podem ser feitas em tempo hábil, e um agendamento de uma atualização pode precisar ser realizado com antecedência, a fim de não comprometer o processo físico devido a uma parada. Uma outra particularidade

é que alguns produtos podem utilizar um *software* sem manutenção do fabricante, por ter sido descontinuado, ficando, por isso, sem a possibilidade de atualização, como é o caso dos sistemas de comunicação (rádio VHF/ HF + *modem* + RTD *software*), detecção (Saete *software* + equipamento Radar) e auxílio à navegação (GPS/AIS + OZI Explorer - GPS *mapping software*) de alguns navios de superfície.

A assistência técnica em sistemas de TI permite diversas modalidades de prestação de serviço. Para SCF em geral, a assistência técnica é feita por apenas um provedor, e soluções de segurança de terceiros podem não ser permitidas devido à licença de uso, ou por causa da perda da assistência devido à utilização de um produto de terceiros.

O tempo de vida de um componente de TI típico é da ordem de três a cinco anos, podendo ser menor devido à rápida evolução tecnológica. Para os SCF, em que a tecnologia é desenvolvida para atender a requisitos bem específicos de uso e implementação, o tempo de vida dos itens pode ser de dez a 15 anos.

Um produto de segurança ou uma tecnologia não podem proteger adequadamente um SCF. A proteção deste tipo de sistema é calcada na combinação de políticas de segurança nas respectivas implementações, nas quais estarão incluídos os produtos e tecnologias.

Considerando o estado atual da Marinha, os SCF são fundamentais para emprego e desempenho de meios de combate, porém, ao longo do tempo, esses sistemas tendem a ser mais vulneráveis. Por meio de um gerenciamento de riscos, alguns questionamentos poderiam ser feitos, como:

– Como iniciar um programa numa organização militar que ainda não trata a segurança desse tipo de sistema?

– Como alinhar o nível do sistema de informação com um nível superior?

– Quais contramedidas são mais apropriadas para mitigar os riscos em sistemas já em produção e sem capacidade de mudança?

– Dado que a quantidade de riscos é enorme, como priorizá-los?

Como resultados futuros, pode-se considerar que os riscos serão utilizados em simuladores ora existentes, permitindo aos operadores vivenciarem os efeitos de uma ação maliciosa e o treinamento dos componentes de monitoração e resposta.

## **GUERRA CIBERNÉTICA – OPERAÇÃO BALUARTE (EXERCÍCIO)**

O espaço cibernético é um novo domínio operacional, assim como o marítimo, o terrestre, o aéreo e o espacial. Ao mesmo tempo em que cresce exponencialmente a exploração econômica deste ambiente, a ameaça cibernética tornou-se uma das maiores preocupações mundiais, ao lado do terrorismo e do tráfico de todos os gêneros. O computador é hoje uma arma perigosa, discreta, eficiente, eficaz e lucrativa, quer seja utilizada por adolescentes ou por grandes atores internacionais, estatais ou não. Portanto, a tecnologia *hacker* transformou-se num

poderoso instrumento bélico, principalmente no contexto da guerra irrestrita, ao alcance de todos. O emprego da TI nos meios operativos, na administração naval e na infraestrutura nacional é intensivo, ampliando dia a dia os ativos informacionais a defender. A Marinha do Brasil, anualmente, executa o Exercício de Guerra Cibernética, a Operação Baluarte, conduzido pelo Comando de Operações Navais (ComOpNav), em coordenação com a DCTIM. O exercício tem como propósitos principais: incrementar a mentalidade de segurança<sup>12</sup> das informações digitais da MB, exercitar a doutrina de guerra cibernética e contribuir para o aprimoramento contínuo das medidas de defesa cibernética adotadas no dia a dia e por ocasião de grandes eventos, bem como a utilização de fontes de inteligência cibernéticas (EMA-416 – Doutrina de Tecnologia da Informação na MB).

## **JOGOS OLÍMPICOS E PARALÍMPICOS RIO 2016 – CASO DE SUCESSO**

As atividades relativas à preparação para os Jogos Olímpicos e Paralímpicos Rio 2016 envolveu ações diversas, como conscientização dos usuários dos ativos de informação<sup>13</sup>, adoção de boas práticas previstas nas normas de Segurança da Infor-

12 O esforço para as atividades de SIC deve ser de todos e não somente do pessoal diretamente envolvido com o setor de Informática. O fator mais importante para a SIC é a existência de uma mentalidade de segurança inculcada em todo o pessoal. Pouco adiantará o estabelecimento de rigorosas medidas de segurança se o pessoal responsável pela sua aplicação não tiver delas perfeita consciência. Todos devem, portanto, envidar esforços para desenvolver e manter um alto nível de conscientização do pessoal quanto à SIC. Isto pode ser feito, por exemplo, por meio de cartilhas e de palestras, adestramentos, exercícios internos e outras atividades cabíveis, englobando publicações, normas e procedimentos afetos ao assunto. Além disso, dentro do Programa de Adestramento de cada OM, devem ser formalmente estabelecidos e continuamente cumpridos adestramentos que aborem todos os aspectos de SIC.

13 Meios de armazenamento, transmissão e processamento de dados e informação; os equipamentos necessários a isso (computadores, equipamentos de comunicações e de interconexão); os sistemas utilizados para tal; os sistemas de informação de um modo geral; os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

mação e Comunicações, maior colaboração e fiscalização das empresas terceirizadas que prestam serviços de TIC e aquisição de novas soluções para aumentar a proteção cibernética e a consciência situacional.

Como pontos fortes da atuação do Centro de Defesa Cibernética (CDCiber) em grandes eventos, podem-se citar: trabalho preventivo, atuação conjunta, articulação em Destacamentos Conjuntos de Defesa Cibernética (DstCjDefCiberRmt) e o trabalho colaborativo em ambiente interagências.

As principais operações técnicas realizadas nos jogos incluíram: avaliação de riscos; detecção automática de incidentes; pesquisa e análise; análise de incidentes de segurança; tratamento de incidentes de segurança; assistência e recuperação a incidentes; coordenação da resposta a incidentes<sup>14</sup>; distribuição de alertas, recomendações e estatísticas.

## CONCLUSÃO

No cenário atual, no que tange à defesa nacional, o Estado brasileiro deve dispor de capacidades cibernéticas para identificar e se contrapor às ameaças orientadas aos ativos de informação estratégicos do país ou às infraestruturas críticas de interesse.

Como foi visto ao longo do presente artigo, ações concretas visando à potencialização da defesa cibernética nacional estão sendo implementadas, e novas capacidades geradas no âmbito da Defesa, de forma a tornar as Forças Armadas aptas

a combater no domínio cibernético, com efetividade operativa, no amplo espectro dos conflitos, agregando valor à segurança cibernética brasileira.

Dentre as principais iniciativas em curso, destacam-se: o Programa Estratégico Defesa Cibernética na Defesa Nacional, o Projeto Estratégico Defesa Cibernética, o emprego da Defesa Cibernética nos Jogos Olímpicos e Paralímpicos Rio 2016, a concepção do Sistema Militar de Defesa Cibernética, o emprego da Defesa Cibernética nas Operações Conjuntas e a atuação colaborativa com outros atores civis e militares da sociedade brasileira, representada pelos segmentos governamentais, acadêmicos e empresariais.

Segundo diretriz da Estratégia Nacional de Defesa, para se alcançarem a efetividade, a eficácia e a eficiência nessas ações, é preciso que se intensifiquem a interação e a colaboração entre o Ministério da Defesa e os demais atores envolvidos com o setor cibernético, nos níveis nacional e internacional.

Por último, mas não menos importante, deve ser destacado que todas essas iniciativas relacionadas ao desenvolvimento da defesa cibernética trazem benefícios não só às Forças Armadas, mas ao país como um todo. A criação de capacidades nesse setor propicia a projeção do Brasil no cenário internacional, bem como proporciona melhores possibilidades de solução de problemas relacionados ao trato de informações digitais.

No que tange à Marinha, na utilização e no emprego de sistemas de TI e SCF,

---

14 Quando sua organização sofre um ciberataque, o tempo de resposta é determinante para minimizar as consequências e proteger as informações críticas. O Computer Security Incident Response Team (CSIRT), ou Grupo de Resposta a Incidentes de Segurança, é o time responsável por analisar e responder, com máximo de precisão, os incidentes de segurança de uma rede computacional. Quando ocorre um incidente de segurança, o CSIRT deve ser acionado imediatamente para efetuar as verificações necessárias, pois o tempo de resposta é determinante para minimizar as consequências e proteger as informações críticas, seja de uma empresa, de um órgão governamental ou de um país.

considerando as suas singularidades, sugere-se o emprego de uma Sistemática de Avaliação Operacional, como forma de:

- iniciar pelo nível da missão, em alinhamento com o nível da informação;
- permitir a priorização dos riscos que mais afetem a execução das tarefas dos meios;

- avaliar riscos decorrentes da interligação de sistemas e subsistemas; e

- trazer uma sistemática de avaliação já em curso e madura na MB para ser empregada numa nova atividade da organização, com o intuito de diminuir o risco da implantação dessa nova atividade.

Para a MB, os reflexos da implantação de um processo de gerenciamento nesse nível permitirão compreender como os riscos, nos sistemas que compõem um meio, afetam a execução das suas tarefas, permi-

tindo ao comando do meio ou mesmo de escalões mais elevados ter conhecimento do grau de vulnerabilidade de um conjunto de meios e, conseqüentemente, dos riscos ao cumprimento de alguma missão.

A longo prazo, um programa sistemático de gerenciamento de riscos permitirá avaliar os custos de sua manutenção e respectivo retorno e, num futuro, gerar uma base de conhecimento para a especificação de requisitos de segurança para novos meios, considerando a segurança desde a fase de projeto. Isso permitirá que se empregue um maior número de soluções voltadas para a segurança, bem como integrar futuros meios na arquitetura de gerenciamento de riscos já utilizada, que aumentará seu escopo e incluirá outros meios, como submarinos, aeronaves e unidades de fuzileiros navais.

#### 📁 CLASSIFICAÇÃO PARA ÍNDICE REMISSIVO:

<INFORMÁTICA>; Administração de Informática; Análise de Sistemas; Cibernética; Computação; Sistema de Informática; Tecnologia da Informação;

<FORÇAS ARMADAS>; Defesa, Exercício; Exercício Militar; Marinha do Brasil; Ministério da Defesa;

### BIBLIOGRAFIA

MARINHA DO BRASIL. *Revista Marítima Brasileira* – v. 138, n. 04/06 (abril/ junho. 2017). Brasil. Serviço de Documentação da Marinha, 2017.

ESCOLA SUPERIOR DE GUERRA. “Ciberdefesa e cibersegurança: novas ameaças à segurança nacional”. Organizador José Cimar Rodrigues Pinto. Rio de Janeiro: ESG, 2016.