CIBERNÉTICA: A GUERRA EM CURSO

GLADYS MACHADO PEREIRA SANTOS LIMA*
Capitão de Fragata (T)

SUMÁRIO

---

* Engenheira eletricista formada pela Universidade Federal de Juiz de Fora (UFJF), com mestrado em Engenharia de Sistemas e Computação pela Universidade Federal do Rio de Janeiro (UFRJ). MBA em Gestão do Conhecimento e Inteligência Empresarial. Superintendente de Sistemas da Coordenadoria do Programa de Reaparelhamento da Marinha da Diretoria-Geral do Material da Marinha (DGMM).

INTRODUÇÃO

A garantia de condições para considerar que o Brasil não corre risco de uma agressão externa está inserida no conceito de Defesa Nacional, assim como a importância para a sociedade e o povo brasileiro em alcançar seus objetivos, sem pressões ou imposições, sendo capaz de dedicar-se ao desenvolvimento e ao progresso.

A Política Nacional de Defesa traça objetivos para prover a defesa do território, da soberania e dos interesses nacionais, explicitando a ênfase na expressão militar para sua consecução, sem ingerência externa de outros Estados. O posicionamento do Brasil no cenário internacional é o de partícipe de ações na defesa da paz, engajado na solução pacífica dos conflitos e na cooperação entre os povos.

Esses anseios nacionais não podem, entretanto, ofuscar a visão do mundo contemporâneo, caracterizado atualmente por uma ordem multipolar, com novos agentes influenciando o ambiente internacional, relacionados às tensões decorrentes da escassez de recursos, de atos terroristas, da grande integração e dependência tecnológica. Observa-se uma reestruturação de relação de poder entre Estados, engajada também na predominância de relações não conflituosas, mostrando a necessidade de preparo da defesa em novos cenários.

À luz de uma solução não beligerante, embora, até o presente momento, nenhum Estado tenha declarado ter sofrido um ataque cibernético, alguns Estados começaram a pensar (e atuar) em como armas cibernéticas poderiam ser usadas contra as infraestruturas críticas[1] de outros Estados. Tendo em vista a interdependência destas da integração tecnológica, principalmente da internet, pode-se inferir possíveis vulnerabilidades quanto à proteção e à segurança da informação digital, tanto no que tange à obtenção de informações privilegiadas como no ataque direto a outros alvos cinéticos, além dos impactos decorrentes.

Destarte, o entendimento moderno sobre a magnitude das mudanças promovidas pela Tecnologia da Informação e Comunicações (TIC) e as decorrentes mudanças de doutrina no plano militar, sendo considerada a RAM[2] dos tempos atuais, possibilitam identificar um novo domínio da guerra: o cibernético. A percepção da guerra cibernética (GC) em curso far-se-á notar, neste trabalho, por meio do entendimento dos conceitos das ações desta nova guerra como alternativa de poder/força sobre o adversário e suas consequências nas infraestruturas críticas, bem como pela explanação sobre alguns ataques cibernéticos ocorridos recentemente no cenário mundial, como fator agregador para a conscientização desta realidade.

Ao explicitar o andamento desta guerra assimétrica, com foco nos princípios doutrinários da guerra, buscou-se também ressaltar a importância das ações estruturantes promovidas por Estados visando atuar na defesa do seu espaço cibernético[3], mostrando alguma similaridade com o Brasil, no que tange ao Setor Estratégico Cibernético,

1 Infraestruturas Críticas (IC) – Instalações, serviços, bens e sistemas que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional e à segurança do Estado e da sociedade.

2 RAM – Revolução nos Assuntos Militares – Uma RAM ocorre quando a aplicação de novas tecnologias em um número significativo de sistemas é combinada com conceitos operacionais inovadores e adaptações organizacionais de modo a alterar a condução do conflito, produzindo um grande aumento do potencial de combate e da eficiência militar das Forças Armadas.

3 Espaço cibernético – Ambiente intangível formado por ativos de Tecnologia da Informação (TI), onde dados e informações digitais são criados, armazenados, modificados, trafegados e processados. Possui as seguintes características: alcance global, ausência de fronteiras e dinamismo.

como contribuição para Defesa Nacional, previsto na Estratégia Nacional de Defesa (END).

AS AÇÕES DA GUERRA CIBERNÉTICA

É presumível a intenção de um governo, controlador das armas, quando deflagradas as ações bélicas no domínio militar tradicional. Entretanto, no domínio cibernético, a confiabilidade das intenções de um ataque é reduzida, tendo em vista as dificuldades inerentes à identificação de sua autoria e de seus delimitadores geográficos (sem fronteiras).

Estudar o alvo ao qual foi direcionado o ataque, pesquisar os possíveis patrocinadores, os interesses envolvidos e os padrões de comportamento, ainda que apoiado em ações de Inteligência, pode não resultar em certeza sobre a identificação da fonte com o grau de certeza necessário. Esta característica é propositalmente explorada pelo adversário, por não viabilizar o processo de tomada de decisão pelo Estado atacado, relativo às contramedidas cibernéticas, tampouco em relação ao direito internacional. Observando os ataques cibernéticos ocorridos durante a guerra na Geórgia, é possível constatar os benefícios advindos destas ações nas redes georgianas. Não se pode estabelecer evidência clara do patrocínio dessas ações, nem permitir atribuição direta ao governo russo, apesar do sucesso do ataque convencional russo (cinético) ocorrido.

A percepção da dimensão das ações cibernéticas pode ser alcançada com o conhecimento de que as interfaces (anteriormente manuais) entre os mundos físico (cinético) e digital foram delegadas a controladores computadorizados, conhecidos como sistemas Scada[4]. O comando e o controle do espaço cibernético representam, em última forma, o domínio sobre outros sistemas interligados à infraestrutura. Esta percepção é conceitualmente conhecida como *poder no espaço cibernético*, ou seja, a habilidade de usar o espaço cibernético para gerar vantagens e influenciar eventos em outros ambientes operacionais.

> ***Poder no espaço cibernético*** **é a habilidade de usar esse espaço para gerar vantagens e influenciar eventos em outros ambientes operacionais**

No contexto deste artigo, a Guerra Cibernética é entendida como ações militares, no espaço cibernético, conduzidas com o propósito de negar, explorar, destruir ou comprometer a integridade de ativos do adversário baseados em informações, sistemas de informações e redes de computadores. Assim, sua inserção no Planejamento Estratégico Militar[5], principalmente no que tange às medidas de dissuasão, é possível por meio da classificação das ações cibernéticas. Alguns autores as dividem em três tipos: de exploração, de ataque e de proteção cibernéticas.

---

4 Scada – Sistemas de Supervisão e Aquisição de Dados, proveniente da abreviatura do nome em inglês *Supervisory Control and Data Acquisition*, são sistemas que utilizam *software* para supervisionar e monitorar variáveis e dispositivos de sistemas de controle conectados por meio de controladores específicos.

5 Planejamento Estratégico Militar – Tem o propósito de definir e organizar funcionalmente as atividades relacionadas com o preparo e o emprego do poder militar para atender às demandas da defesa do país.

Ações de exploração cibernética

Entre os pensamentos de Sun Tzu, encontramos aquele que remete à "necessidade de conhecer o inimigo". No ambiente cibernético, é essencial mapear as redes computacionais e os sistemas empregados pelo adversário, como parte do processo de planejamento, preferencialmente sem alertar o adversário, antes de um ataque propriamente dito.

A penetrabilidade da internet em diversas esferas da atividade humana promoveu uma mudança cultural de comportamento da sociedade

Uma das maneiras de explorar conhecimentos protegidos em redes e em sistemas digitais é acessar uma credencial digital lícita, explorando a falta de mentalidade de segurança, que ocorre com o relaxamento, pelos usuários, das medidas recomendadas para criar e manter protegidas suas credenciais. Ou seja, obtendo uma identificação de usuário (*login*) e sua senha, quer por meio de ações de engenharia social[6] ou por meio de *software* para quebra de senhas, conhecido por "algoritmo de força bruta".

Os ataques cibernéticos almejam interromper, negar, degradar, corromper ou destruir informações no espaço cibernético de interesse

A penetrabilidade da internet em diversas esferas da atividade humana promoveu uma mudança cultural de comportamento da sociedade, estabelecendo oportunidades para exposição de informações de indivíduos ou grupos. Redes sociais – Facebook, Orkut, Twitter – *blogs* estão sendo empregados como fontes abertas de informação, a fim de obter vantagens em prol das ações de exploração, tendo em vista seu alto grau de oportunidade e o seu baixo custo.

Cabe mencionar que as ações de exploração podem ser interpretadas como ações de ataque propriamente ditas, quando descobertas, tendo em vista seu caráter não autorizado. Assim, as ações de exploração precisam ser definidas no escopo do Planejamento Militar, sendo sua execução condicionada às autorizações previstas.

Ações de ataque cibernético

Os ataques cibernéticos almejam interromper, negar, degradar, corromper ou destruir informações no espaço cibernético de interesse. Todavia, quando empregadas na guerra, estas ações também devem estar inseridas em um Planejamento Militar, pois visam contribuir para o cumprimento de uma missão e possuem características efetivamente ofensivas. São direcionadas às redes e aos sistemas que suportam o(s) alvos(s) que compõe(m), geralmente, as infraestruturas críticas do Estado. A versatilidade técnica deste domínio (ciberné-

6 Engenharia Social – É a arte de manobrar seres humanos visando a ações sobre algum aspecto de suas vidas, aplicada em setores da segurança da informação, independentemente da tecnologia utilizada.

tico)[7] permite estabelecer ações de ataque que não se baseiam em acesso direto ao sistema alvo.

Na prática, um *malware*[8], por exemplo, poderá atingir diversos computadores ligados na internet (sem estabelecimento da fronteira geográfica), criando uma rede de computadores, infectados e dominados, conhecidos como zumbis (*botnet*). Esses computadores "sequestrados", durante as ações de exploração, poderão ser empregados em uma ação de ataque distribuído por negação de serviços (*Distributed Denial of Service*, DDoS).

Um ataque de negação de serviços foi empregado na Geórgia, com grande impacto psicológico e de informação, isolando-a da comunidade internacional, representando um caso real de comprometimento, impedindo o uso legítimo de recursos por aquele Estado. Os computadores que hospedavam os sítios eletrônicos do Governo e da mídia local receberam (dos zumbis) volume de dados maior do que suas capacidades de atender aos pedidos enviados, esgotando seus recursos de comando e controle e tornando os serviços indisponíveis (DDoS). Os ataques tiveram seu escopo ampliado, posteriormente, para outros sítios eletrônicos, alcançando novos alvos, como bancos, empresas privadas e instituições de ensino, entre outros.

As ações de proteção cibernética visam minimizar as possibilidades de sucesso dos ataques ou de explorações contra o espaço cibernético a ser protegido

Ações de proteção cibernética

As ações de proteção cibernética visam minimizar as possibilidades de sucesso dos ataques ou de explorações contra o espaço cibernético a ser protegido. Partindo do princípio que não é possível predizer a forma dessas ações ou o momento em que elas ocorrerão, fica, assim, estabelecida a necessidade de uma defesa holística e permanente.

Segundo Sun Tzu, é tão importante conhecer o inimigo como a si mesmo. Este princípio também faz-se presente no caso da guerra cibernética. É preciso explorar o próprio espaço cibernético (consciência situacional) em busca de vulnerabilidades (fraquezas) que possam ser empregadas pelos adversários. Todavia, as medidas e os esforços de proteção devem ser empregados coerentemente, sob pena de não serem adotados, caso planejados de forma majorada, se tornando inexequíveis do ponto de vista financeiro.

Simulações de ações de ataque em sistemas ou redes de computadores, realizadas em exercícios operativos, promovem a sinergia entre os diversos setores da estrutura, propiciando condições de aperfeiçoamento deste aparato. Neste contexto, adotar uma escala progressiva dos níveis de alarmes cibernéticos também contribuirá para escalar as ações reativas a serem executadas com o proporcional dispêndio de esforço

7 Domínio cibernético – Entendido como o "campo de batalha" onde se desenvolve a guerra. Historicamente, a terra e o mar foram os primeiros domínios estabelecidos. Entretanto, com o desenvolvimento tecnológico, novas armas surgiram e novos domínios foram estabelecidos, como, por exemplo, o ar e o espaço.

8 *Malware* – *Software* malicioso, destinado a se infiltrar em um sistema de computador alheio de forma ilícita, com intuito de causar algum dano ou roubo de informações (classificadas ou não).

e, consequentemente, de custo compatíveis com os riscos identificados, em exercícios ou em situações reais, para minimizar ou neutralizar o efeito indesejável do ataque sofrido.

Princípios da Guerra e a Guerra Cibernética

As atividades no domínio cibernético podem estabelecer condições adequadas, exequíveis e aceitáveis para ações em outros domínios ou vice-versa. Este entendimento facilita explorar o emprego das ações cibernéticas e sua aplicação nas operações militares, à luz dos tradicionais princípios de guerra.

Aplicando os Princípios na Guerra Cibernética

Os princípios mapeados e explorados na guerra, até o momento, são comentados sob o ponto de vista das características e dos recursos tecnológicos do ambiente cibernético e, em alguns casos, destacando a vantagem de sua adoção quanto ao efeito no ambiente cinético (físico).

a) **Economia de Recursos** – As ações cibernéticas de exploração são empregadas para conhecer as vulnerabilidades do espaço cibernético do adversário, contribuindo, assim, para o desenvolvimento de uma ação de ataque que permita economia das forças, visando à obtenção do esforço máximo, muitas vezes em ocasiões decisivas. Um ataque cibernético pode despender menos recursos ou causar menor dano político do que um ataque cinético. Lançar um *malware*, por exemplo, pode ser menos custoso do que o esforço para lançar um míssil. Considerando apenas o ambiente cibernético, é possível escolher tecnicamente, entre possíveis ataques cibernéticos, aquele que envidará menor esforço.

b) **Exploração** – Indica a necessidade da intensificação das ações ofensivas ou de exploração cibernética, quando ocorrer um êxito em qualquer dos níveis de condução da guerra ou uma mudança favorável na situação. No contexto tecnológico, o sucesso no acesso a um sistema de informação pode ser fator motivador e validar esforços em galgar outro nível de acesso (com direitos maiores), visando alcançar informações mais protegidas.

A exploração de vulnerabilidades cibernéticas conquistadas pode ser mais bem empregada quando associada a informações da Inteligência. A aplicação deste princípio dependerá, em grande parte, de um julgamento pautado em boas informações, de uma experiência amadurecida e de um elevado grau de controle sobre a situação.

c) **Manobra** – Doutrinariamente, este princípio representa a exploração das características básicas das forças e pela adequada aplicação do poder de combate, visando estabelecer uma situação favorável que possibilite conquistar ou lograr a realização de um objetivo. No ambiente cibernético, este princípio pode ser entendido pela exploração de vulnerabilidades críticas do adversário, ou seja, direcionada à sua infraestrutura crítica. Quando é possível executar um ataque cibernético sem identificação do ponto de origem, ou mesmo dificultando seu rastreamento, o que é conhecido por incerteza da autoria, vê-se a caracterização de uma manobra.

d) **Massa** – O ataque distribuído de negação de serviço (DDoS) aplica o princípio da massa, concentrando forças no ponto decisivo (o serviço negado) no tempo devido e a capacidade de sustentar esse esforço, enquanto necessário, o que dependerá do grau de engajamento de equipamentos *zombies* ou *hackers* mobilizados.

e) **Moral** – A alteração do conteúdo de sítios eletrônicos na internet do adversário,

expondo uma vulnerabilidade, pode reduzir a crença do oponente na sua própria capacidade de defesa, inclusive na defesa de outros sistemas. O estado de espírito ou a atitude mental de um indivíduo ou de um grupo de indivíduos se reflete em sua conduta. A não conservação de um moral elevado pode contribuir no comprometimento da missão, no caso a própria defesa cibernética do adversário.

f) **Objetivo** – Diz respeito à obtenção dos efeitos desejados. A finalidade da definição dos efeitos é permitir que todas as ações militares decorrentes concorram para um único fim, somando esforços e evitando desperdícios de forças em ações que não contribuam para o cumprimento da missão. Ao evitar ataques que implicassem danos diretos às redes georgianas e às estações componentes da infraestrutura crítica, como usinas, oleodutos ou refinarias, por exemplo, pode-se perceber a intenção de não prejudicar estes sistemas, limitando-se ao objetivo de somente "isolar e silenciar", sem danos à conexão física da Geórgia à internet.

g) **Ofensiva** – Princípio que se caracteriza por levar a ação bélica ao inimigo, de forma a se obter e manter a iniciativa das ações, estabelecendo o ritmo das operações e determinando o curso do combate. No domínio cibernético, este princípio também representa a imposição ao adversário da sua vontade. O propósito dos ataques cibernéticos à Geórgia era "isolar e silenciar", em que o efeito de silenciar era direcionado à mídia georgiana e o efeito de isolar representava o objetivo de isolar a Geórgia da comunidade internacional.

h) **Prontidão** – Subentende-se que as forças estão providas dos meios essenciais e organizadas para operações de combate. Isto envolve o preparo antes das hostilidades e continuamente, no decorrer da guerra. Estender este princípio ao domínio cibernético implica estabelecer condições de monitoramento do espaço cibernético do adversário, identificando suas vulnerabilidades e das armas cibernéticas associadas às respectivas vulnerabilidades exploradas. Na guerra da Geórgia, é possível perceber indícios da existência prévia de listas de alvos e de ferramentas (ações de exploração) para ampliar o ataque, tendo em vista a velocidade das ações das *botnets*. Estes indícios ficam mais fortes considerando os ataques a servidores da Geórgia, em julho de 2008, como ensaio às ações de agosto.

i) **Segurança** – Requer adequada análise das possibilidades do inimigo, visando à própria defesa, com o propósito de reduzir vulnerabilidades e de preservar a liberdade de ação. Prover segurança implica, pois, proporcionar as condições que neutralizem os efeitos de ameaças, sem a eliminação do risco de forma total.

j) **Simplicidade** – Indica que o melhor plano é aquele que, sem prejudicar a propriedade de ser completo, evita uma desnecessária complexidade em sua concepção, disseminação e execução. Na guerra cibernética, o emprego de um *malware* pode atingir o espaço cibernético adversário e ser tecnicamente de implementação simples.

k) **Surpresa** – Princípio que consiste em atingir o inimigo onde, quando ou de forma tal que ele não esteja preparado, reduzindo sua capacidade de reação. O emprego de um *malware* que explore uma vulnerabilidade desconhecida de uma rede ou de um sistema em um ataque exemplifica o princípio no âmbito cibernético, dada sua originalidade no contexto tecnológico, tendo em vista a não adoção de medidas de proteção para a vulnerabilidade explorada. A capacidade de inovação tecnológica tem sido explorada como vantagem de ações cibernéticas, juntamente com a certeza da insegurança latente do ambiente tecnológico, tornando impossível garantir a inexistência de vulnerabilidades.

l) **Unidade de Comando** – Caracterizado pela atribuição da autoridade a uma só pessoa. A adoção de nível de alarme cibernético, como medida de proteção, busca unificar e assegurar relações de comando apropriadas às tarefas necessárias ou desejáveis para manutenção do controle que permita o exercício pleno do comando.

O ambiente tecnológico e sua influência na Guerra Cibernética

A tecnologia, no contexto da Guerra Cibernética, se torna um paradoxo, pois quanto mais complexa e desenvolvida, maior a dependência dos serviços ofertados no espaço cibernético, mas, simultaneamente, este fica mais propenso a vulnerabilidades, aumentando a diversidade e o grau de dificuldade das ações de proteção.

Outro aspecto tecnológico a ser observado em um ataque é a dificuldade de controlar ou restringir os efeitos decorrentes do emprego de arma cibernética. No caso de um *malware*, por exemplo, não há garantia de que sua atuação não tenha efeito no próprio espaço cibernético, tendo em vista que este pode adotar redes ou sistemas com vulnerabilidades semelhantes àquelas visadas no espaço alvo. Deste modo, os Estados vêm buscando estabelecer procedimentos e regras para engajamento em ações cibernéticas, comentadas a seguir.

A CONDUÇÃO DA GUERRA CIBERNÉTICA NO CENÁRIO MUNDIAL

O colapso das centrífugas do complexo de Natanz, em 2008, ponto forte do programa nuclear iraniano, não foi o único sucesso conquistado pelo *Stuxnet*, a arma cibernética empregada pelos governos israelense e norte-americano para assumir o controle dos computadores que coordenavam aquela planta nuclear. A eficiência e a eficácia deste ataque cibernético, em detrimento de uma ofensiva cinética, comprovaram a validade dos esforços de estruturação deste novo domínio (cibernético) da guerra.

No cenário mundial, essas preocupações foram sendo inseridas em pautas de discussões, como ocorrido no encontro dos chefes de Estado e de Governo dos países integrantes da Organização do Tratado do Atlântico Norte (Otan), durante a Conferência de Lisboa (em novembro de 2010). A percepção da importância do domínio cibernético para a Segurança Nacional foi concretizada por meio do entendimento da Guerra Cibernética como ameaça aos Estados.

O posicionamento norte-americano sobre a possibilidade de emprego das ações cibernéticas somente foi externado, por meio de publicações, mais recentemente. Em maio de 2011, na Estratégia Internacional de Defesa – Prosperidade, Segurança e Abertura em um mundo em rede, a Presidência dos Estados Unidos da América, com base na relevância das tecnologias em rede (internet) para a sociedade e a economia, estabeleceu princípios fundamentais para sua operacionalização livre e segura: *vis-à-vis* "reserva-se ao direito de defender os ativos nacionais vitais como necessário e apropriado".

Reforçando essa postura, em julho de 2011 o Departamento de Defesa norte-americano (DoD) divulgou sua Estratégia de Operação no Ciberespaço, composta de cinco iniciativas estratégicas: estabelecer o ciberespaço como um novo domínio operacional no contexto da segurança nacional; prever a necessidade de empregar novos conceitos operacionais para proteção de redes e sistemas, contemplando uma ampla conscientização da mentalidade de segurança das informações digitais; buscar parceiros governamentais e privados para o desenvolvimento de novas capacidades;

buscar parceiros no âmbito internacional, robustecendo a capacidade de defesa coletiva; e preparar continuamente os recursos humanos (cooptar novos talentos).

A estruturação dos Estados, comentada a seguir, demonstra a materialização das políticas e doutrinas de guerra cibernética, alinhadas com as orientações da Conferência da Otan.

A Estruturação do Setor Cibernético nos Estados Unidos da América (EUA)

A estruturação norte-americana é anterior à divulgação da Estratégia de Defesa Cibernética. A Agência de Segurança Nacional (NSA[9]), vinculada ao Departamento de Defesa, conduz operações de segurança para garantir vantagens no espaço cibernético. Estas ações militares estão inseridas, doutrinariamente, no contexto da segurança das informações, visando à manutenção dos requisitos básicos de disponibilidade, integridade, sigilo e autenticidade das informações.

Também pertencente ao DoD, foi criado, em 2009, o US Cyber Command (USCybercom), com a atribuição de realizar ações cibernéticas em proveito dessas operações, colocando a inteligência, a defesa e o ataque, no âmbito militar, sob uma única coordenação. O USCybercom também é responsável pela integração em operações conjuntas das demais estruturas militares: Fleet Cyber Command/Tenth Fleet (Marinha), Air Force Space Command/Fourth Air Force (Força Aérea), Army Cyber Command/Second Army (Exército) e United States Marine Corps Forces Cyberspace Command (Fuzileiros).

É oportuno citar que o Departamento de Segurança Interna dos EUA, comumente denominado Homeland Security, trabalha no âmbito civil, atuando na proteção (cibernética) contra ataques terroristas.

A Estruturação do Setor Cibernético no Reino Unido

As ações cibernéticas no Reino Unido são vinculadas ao Government Communications Headquarters (GCHQ), organismo ligado à Inteligência e que coordena ações não somente para promover a proteção dos ativos de Tecnologia da Informação do Governo, como também para incitar e apoiar o setor privado na prevenção de invasões em seus sistemas e suas redes. Destarte, por sua forte atuação em promover padrões de segurança e de capacitação de recursos humanos, o GCHQ tem autoridade para desencadear ataques cibernéticos inseridos no conceito de defesa ativa[10].

A capacidade de defesa britânica é resultante de sinergia das ações do Governo e do setor privado, conquistada por meio do entendimento de que a segurança econômica está interligada com a defesa nacional. Esta sensibilização foi amadurecida no esforço realizado para a segurança durante os Jogos Olímpicos de Londres, em 2012. O modelo adotado pelo Reino Unido também se apoia, no nível operacional, em duas unidades de Comando Conjunto para manter, operar e proteger sua rede operativa.

A ESTRUTURAÇÃO DA PROTEÇÃO CIBERNÉTICA NA MARINHA DO BRASIL

É possível observar a preocupação do Estado brasileiro em proteger os ativos e a capacidade de atuação em rede, a intero-

9 Agência de Segurança Nacional – *National Security Agency* (NSA), em inglês, é a agência de segurança dos Estados Unidos, responsável pela Inteligência, incluindo interceptação e criptoanálise.

10 Defesa ativa – Engloba ações de ataque em prol da defesa.

perabilidade dos sistemas e a obtenção dos níveis de segurança desejados dentro do seu espaço com o estabelecimento do Setor Cibernético como estratégico na END. Este eixo estruturante tem o propósito de conferir confidencialidade, disponibilidade, integridade e autenticidade aos dados e aos sistemas do espaço cibernético.

O Ministério da Defesa (MD), em dezembro de 2012, aprovou a Política Cibernética de Defesa para orientar as atividades de defesa cibernética, no nível estratégico, e de guerra cibernética, nos níveis operacional e tático, no âmbito das Forças Armadas. As ações cibernéticas emanadas do MD visam assegurar, de forma conjunta, o uso efetivo do espaço cibernético (preparo e emprego operacional) pelas Forças Armadas (FA), de forma a impedir ou dificultar seu uso contra os interesses da Segurança Nacional, garantindo a liberdade de ação.

À semelhança de outros modelos, a estruturação do Setor Cibernético objetiva, ainda, contribuir para a Segurança da Informação e Comunicações (SIC) e para a Segurança Cibernética realizada por outros órgãos do governo envolvidos, em especial o Gabinete de Segurança Institucional da Presidência da República (GSI/PR[11]), por meio da produção do conhecimento, oriundo de fonte cibernética. A partir de dezembro de 2012, foi atribuída a responsabilidade ao Centro de Defesa Cibernético do Exército Brasileiro (CDCiber) pela coordenação e integração das atividades de Defesa Cibernética no âmbito do MD.

No âmbito da Marinha do Brasil (MB), a atual estrutura de Governança de Tecnologia da Informação (GovTI da MB), implantada desde 2007, estabeleceu a Guerra Cibernética como um dos temas de interesse, estando inserida também no Plano de Tecnologia da Informação da Marinha (PTIM). Para execução das atividades de proteção cibernética, a MB é assistida pela Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM), pelo Centro de Tecnologia da Informação da Marinha (CTIM) e por outras estruturas distribuídas pelas diversas regiões do País, os Centros Locais de Tecnologia da Informação (CLTI), para apoiar as quase 400 organizações militares.

As atividades de proteção empregadas pela MB são monitoradas e avaliadas de forma contínua, em busca de novas ameaças, à luz dos princípios aplicados à guerra cibernética, em consonância com as normas específicas para o assunto. Nos últimos anos, foram realizados exercícios (simulações) no espaço cibernético da Marinha, visando explorar este novo domínio e sua importância para o Comando e Controle das Operações Militares, contando ainda, em algumas oportunidades, com a participação de especialistas das demais Forças, estreitando a integração e o compartilhamento do conhecimento.

CONSIDERAÇÕES FINAIS

Observando as ações em curso para estruturação do setor cibernético em diversos Estados, principalmente aqueles com avançado domínio tecnológico, é possível perceber que a guerra cibernética não é apenas mais um novo conceito doutrinário. As revelações de Edward Snowden, ex-colaborador da NSA, sobre detalhes da vigilância das comunicações e tráfego das informações, corroboram o senso da existência de ações de exploração e de

11 GSI/PR – É o órgão da Presidência da República encarregado da coordenação, no âmbito da Administração Pública Federal (APF), de alguns assuntos estratégicos que afetam a segurança da sociedade e do Estado, quais sejam: Segurança das Infraestruturas Críticas Nacionais, SIC e Segurança Cibernética.

Inteligência desta nova guerra global em andamento.

Para o Estado atacante, a guerra no domínio cibernético pode ser menos onerosa, tanto do ponto de vista financeiro quanto político, quando não comprovado o ataque, se tornando uma alternativa exequível e adequada, conforme o cenário prospectivo. Do ponto de vista defensivo, a ameaça cibernética pode ser considerada de maior complexidade, dada a diversidade e as vulnerabilidades da própria tecnologia. Assim, a adaptação dos Estados para enfrentá-la deve ser abordada com responsabilidade, flexibilidade, rapidez e visão estratégica.

A adaptação dos Estados para enfrentar a ameaça cibernética deve ser abordada com responsabilidade, flexibilidade, rapidez e visão estratégica

Observamos que, no Brasil, a importância atribuída pelo Governo em relação ao setor cibernético está registrada na END. Além da estruturação militar no contexto do Ministério da Defesa, é possível perceber outras ações do Governo brasileiro em busca de uma sinergia com outros parceiros, por meio de normas específicas para compras, contratações e desenvolvimento de produtos e sistemas de defesa, demonstrando ainda o entendimento sobre a necessidade de estabelecer incentivos ao setor privado, nas áreas de informação e de Inteligência, conhecimentos fundamentais neste novo domínio operacional da guerra, o cibernético.

O desenvolvimento conjunto do Setor Cibernético, no cenário militar, aumentará a capacidade das Forças Armadas atuarem em rede. Neste sentido, sob a coordenação do Exército Brasileiro, o MD tem conquistado nos últimos anos avanços significativos para prover meios e métodos e implementar estruturas que colaborem para assegurar o uso efetivo do espaço cibernético pelas Forças Armadas e dificultar ou impedir seu emprego contra interesses da Defesa Nacional.

Todavia, estes esforços de desenvolvimento do Setor Cibernético, traduzidos pelos avanços tecnológicos, almejados em primeira instância pelas Forças Armadas, bem como pelo Governo brasileiro, em uma visão mais holística, são limitados pela disponibilidade orçamentária do próprio Governo Federal. A proximidade de grandes eventos, como a Copa do Mundo, em 2014, e os Jogos Olímpicos de 2016, impõe a necessidade de preparo imediato para fazer frente às ameaças cibernéticas, se traduzindo em um novo desafio para o País.

CLASSIFICAÇÃO PARA ÍNDICE REMISSIVO:
<GUERRAS>; Guerra Cibernética; Defesa;

REFERÊNCIAS BIBLIOGRÁFICAS

ANDRESS, Jason; WINTERFELD, Jason. *Cyber warfare: techniques, tactics and tools for security practioners*. Elsivier, Waltham, 2011.

BRASIL. Política Nacional de Defesa. Decreto Legislativo nº 373 de 25/09/2013.

BRASIL. *Desafios estratégicos para a segurança e defesa cibernética*, Presidência da República. 1ª edição. Brasília, 2011.

BRASIL. Livro Branco de Defesa Nacional. Ministério da Defesa. Brasília, 2012.

BRASIL. Política Cibernética de Defesa. Portaria Normativa nº 3.389/MD, de 21/12/2012.

CARR, Jeffrey. *Inside Cyber Warfare*. 2nd Edition. O'Reilly Media, USA, 2011.

CASTELLS, Manuel. *A sociedade em rede – a era da informação: economia, sociedade e cultura*. Volume 1. 6ª edição. São Paulo. Terra e Paz, 1999.

CLARKE, Richard e KNAKE, Robert k. *Cyber War*. HarperCollins Publishers, New York, 2010.

HADNAGY, Christopher. *Social Engineering: the art of human hacking*. Wiley Publishing. 2011.

MANDARINO JUNIOR, Raphael. *Segurança e defesa do espaço cibernético brasileiro*. Recife. Cubzac, 2010.

SANGER, David E. *Confront and Conceal*. Crown Publishers. New York, 2012.