ESCOLA DE GUERRA NAVAL

CC WAGNER GUEDES ABRANTES

IMPLICAÇÕES DO DOMÍNIO CIBERNÉTICO NAS ESTRATÉGIAS MILITARES

Rio de Janeiro

2016

CC WAGNER GUEDES ABRANTES

IMPLICAÇÕES DO DOMÍNIO CIBERNÉTICO NAS ESTRATÉGIAS MILITARES

Dissertação apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso de Estado-Maior para Oficiais Superiores.

Orientador: CF PAULO OZÓRIO

Rio de Janeiro
Escola de Guerra Naval
2016

AGRADECIMENTO

À minha esposa Rosane pelo apoio e compreensão dispensados em todos os momentos.

Ao Capitão de Fragata Paulo Ozório, meu orientador, pelos ensinamentos e conselhos que balizaram o andamento deste trabalho.

RESUMO

O propósito da pesquisa é analisar quais as influências do domínio cibernético nas estratégias militares. Em vista dos avanços tecnológicos e da informatização das estruturas de comunicação entre os países e sociedades, ocorreu uma progressiva dependência dos países de tais estruturas de comunicação. Porém, os sistemas de Tecnologia da Informação (TI) apresentam vulnerabilidades, o que implica em perigos às estruturas em virtude das ameaças existentes no mundo virtual. A relevância do tema contribuirá para a compreensão da importância da guerra cibernética na preparação dos Estados nos novos conflitos e como os países devem atuar no novo domínio. Para a compreensão desse novo domínio, foram abordados os principais conceitos utilizados a fim de se chegar a compreensão do que é o espaço cibernético e o que é a guerra cibernética, bem como as principais vulnerabilidades das estruturas de TI e as ameaças no domínio virtual. Para alcançar esse objetivo foram abordados as principais características dos domínios terrestre, marítimo, aéreo e espacial, a fim de se realizar uma comparação com os princípios e características do domínio cibernético. Observando-se alguns conflitos recentes, em que ocorreram ataques cibernéticos contra redes privadas e públicas de Estados, verifica-se a necessidade de estruturação dos países para se contraporem a tais ameaças. Foi abordada a estrutura adotada pelos Estados Unidos da América como forma de preparo de um Estado no combate às ameaças no mundo virtual, verificando-se, assim, quais as impactos do domínio cibernético nas estratégias militares de um país.

Palavras-chave: Cibernética. Ciberespaço. Guerra Cibernética. Defesa Cibernética.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

Com o surgimento e evolução das tecnologias da informação (TI), a era industrial foi dando lugar à era da informação. Com tal evolução, a quantidade e velocidade de transferência de informações entre pessoas e Estados cresceu, alcançando grande penetração no cotidiano das sociedades. Essas novas tecnologias têm facilitado a interação das sociedades mas, tem criado uma dependência dos Estados que possuem maior grau de informatização de suas estruturas. Tal dependência à informatização tem tornado estes atores mais vulneráveis às novas ameaças surgidas no novo ambiente.

Em vista disso, a força física dos atores mundiais foi sendo complementada, e em alguns casos suplementada, por informações e *softwares* de computadores, os quais podem influenciar as esferas militares, econômicas, políticas e sociais quase simultânea e instantaneamente. Tais mudanças criaram um meio de troca e movimentação de informações, o qual chama-se de ciberespaço, que passa a desempenhar o papel de quinto domínio de guerra. A preocupação diante da dependência e vulnerabilidade existentes no ciberespaço passou ser mais um componente nos planejamentos e nas ações militares.

A possibilidade de utilização dessas tecnologias da informação e comunicação (TIC) nos últimos anos, em ações de ataque contra objetivos militares e não militares dos Estados, deu origem a uma nova forma de guerra, a Guerra Cibernética (GC).

Diante do exposto, o presente trabalho busca esclarecer quais são as implicações da guerra cibernética nas estratégias militares em um novo domínio de guerra. Para isso, buscará responder as seguintes questões: qual a definição de guerra cibernética?; quais são as semelhanças e diferenças com os domínios terrestre, marítimo, aéreo e espacial?; e quais as influências no planejamento estratégico nos conflitos atuais?

O propósito deste trabalho é identificar as implicações da concepção de um novo domínio no planejamento das estratégias militares.

A relevância do tema fundamenta-se na oportunidade de contribuir para a compreensão da importância da guerra cibernética na preparação e atuação nos novos conflitos e sua importância no planejamento das estratégias militares.

Para atingir o objetivo, a metodologia empregada nesta monografia é descritiva e analítica, fundamentada em pesquisa bibliográfica e documental. O estudo está baseado em publicações de órgãos de defesa do Brasil, dos Estados Unidos da América, bem como em estudos de pesquisadores da área de segurança e defesa cibernética. Serão adotados os conceitos descritos por Coutau-Bégarie para comparação com os demais domínios.

Esta dissertação está organizada em cinco capítulos, distribuídos conforme a seguir. O primeiro trata-se desta introdução, o segundo capítulo abordará os Fundamentos da Guerra Cibernética, que servirá para apresentar os principais conceitos envolvidos no domínio cibernético, os princípios do domínio cibernético, além das principais ameaças e vulnerabilidades do ambiente, a fim de subsidiar uma comparação com os demais domínios. O capítulo três apresentará características dos domínios terrestre, marítimo, aéreo e espacial, segundo a obra “Tratado de Estratégia” de Coutau-Bégarie, a fim de se realizar uma comparação com as características do domínio cibernético.

No quarto capítulo serão abordados eventos em que foram observadas ações cibernéticas em recentes conflitos entre Estados e quais as ações tomadas pelos Estados para se contrapor às ameaças desse novo domínio. Será abordada a estrutura criada pelos Estados Unidos da América, a fim de se contrapor a tais ameaças, como modelo de defesa às ameaças cibernéticas. Por fim, o último capítulo apresentará as conclusões do trabalho.

Inicia-se o estudo com a apresentação dos principais fundamentos do ambiente cibernético.

2 FUNDAMENTOS DA GUERRA CIBERNÉTICA

O presente capítulo se propõe a introduzir os conceitos básicos utilizados no ambiente cibernético, apresentando definições de termos utilizados ao se abordar o assunto, a fim de se ter subsídios para se definir o conceito de "Guerra Cibernética". Serão apresentadas as principais ameaças presentes no domínio cibernético, as quais colocam em risco conteúdos e estruturas das sociedades e Estados, como também as vulnerabilidades dos sistemas.

2.1 Os principais conceitos utilizados

Inicialmente, discorrer-se-á sobre a origem dos termos utilizados no ambiente cibernético, começando pela origem do termo "Cibernética". Derivada do grego *kubernetes,* este foi utilizado pelo pesquisador estadunidense Norbert Wiener[1], em 1948, para descrever o conjunto formado pela Teoria de Controle e a Teoria de Comunicação (WIENER, 1973).

No Brasil, segundo a Doutrina Militar de Defesa Cibernética, o termo Cibernética se refere à comunicação e controle, atualmente relacionado ao uso de computadores, sistemas computacionais, redes de computadores e de comunicações e sua interação. No campo da Defesa Nacional, inclui os recursos de tecnologia da informação e comunicações de cunho estratégico, tais como aqueles que compõem o Sistema Militar de Comando e Controle (SISMC[2]), os sistemas de armas e vigilância, e os sistemas administrativos que possam afetar as atividades operacionais (BRASIL, 2014).

Observa-se um conjunto de equipamentos e sistemas que fazem parte de um novo ambiente, os quais são integrados para permitirem a comunicação entre pessoas, órgãos e empresas. Tais componentes são denominados de Ativos de Informação, que, segundo Mandarino Jr.[2], são definidos em seu trabalho "Um estudo sobre a Segurança e Defesa do

1 Norbert Wiener serviu no Departamento de Matemática do Massachussets Institute of Technology (MIT) de 1919 até a sua morte em 1964. Em 1963, ele foi agraciado com a Medalha Nacional de Ciência dos Estados Unidos da América por suas contribuições nos campos da matemática, engenharia e ciências biológicas.

2 Raphael Mandarino Júnior - Matemático, Especialista em Gestão da Segurança da Informação pela UNB,

Espaço Cibernético Brasileiro" como os "meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso (computadores, equipamentos de comunicação e de interconexão), os sistemas utilizados para tal, os sistemas de informação de modo geral, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso" (MANDARINO, 2011).

Esses ativos também são definidos, segundo o Estado-Maior da Armada, como "as bases de dados, os arquivos, a documentação de sistemas, os manuais de usuário, o material de treinamento, os procedimentos de suporte, de desenvolvimento, de manutenção ou de operação, os planos de continuidade e todos os meios digitais onde as informações trafegam, são processadas ou encontram-se armazenadas" (BRASIL, 2007).

Esses dados e informações gerados nos meios públicos e privados, sejam militares ou civis, devem ser preservados das ameaças que possam ter acesso indevido aos mesmos. O acesso aos dados e informações pode-se dar por meio da interconexão pelas redes de dados, ou por meio de dispositivos que tenham acesso a um ponto de entrada de uma rede isolada, como um simples *pen-drive*.

Deve-se então proteger as fontes cibernéticas, que segundo a Doutrina Militar de Defesa Cibernética, são os recursos por intermédio dos quais se pode obter dados no Espaço Cibernético utilizando-se ações de busca ou coleta, normalmente realizadas com auxílio de ferramentas computacionais. A fonte cibernética poderá ser integrada a outras fontes (humanas, imagens e sinais) para produção de conhecimento de Inteligência (BRASIL, 2014).

O conjunto de todos esses equipamentos e sistemas interconectados vêm a compor um novo ambiente de interação entre os homens. Esse novo ambiente é definido por muitos como o Espaço Cibernético (Eciber).

Com as informações apresentadas, passa-se a buscar a definição do que é o

---

Mestrando de Ciência da Computação na UFPE, atua há 39 anos na área de Segurança da Informação.

Espaço Cibernético nas doutrinas dos Estados e acadêmicas. Como primeira definição, segundo Pierre Lévy, o Espaço Cibernético ou ciberespaço “é o novo meio de comunicação que surge da interconexão mundial dos computadores. O termo especifica não apenas a infraestrutura material da comunicação digital, mas também o universo oceânico de informações que ela abriga, assim como os seres humanos que navegam e alimentam esse universo” (LÉVY, 1999). Já segundo Carvalho, o Espaço Cibernético (Eciber) é descrito como o “espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas” (CARVALHO, 2011). No glossário do Departamento de Defesa dos Estados Unidos da América (EUA, 2016), o Espaço cibernético é definido como “Um domínio global dentro do ambiente da informação, consistindo de redes interdependentes de infraestruturas de dados residentes, incluindo a internet, redes de telecomunicações, sistemas computacionais, e processadores e controladores embarcados” (EUA, 2016, tradução nossa).

Diante do exposto, verifica-se que o ECiber é composto por todas as redes de computadores do mundo e por tudo que a elas se conectam, mesmo aquelas que não estão acessíveis a partir da Internet. Trata-se de um ambiente que integra praticamente todos os Estados através de conexões lógicas e que pode ser acessado a partir de todos os locais que ofereçam conexão no mundo. Essa característica traz inúmeras facilidades, porém, apresenta também diversas ameaças.

Tais vulnerabilidades e ameaças, que são causa potencial de incidentes indesejados por Estados, empresas e pessoas, em vários setores, podem resultar em violação, acesso ou dano aos conteúdos e redes pertencentes ao Espaço Cibernético de interesse. As ameaças, dentro do espaço cibernético, visam provocar danos, interromper serviços ou subtrair informações. Para isso, é preciso garantir a segurança, principalmente, das chamadas Infraestruturas Críticas (IC), que, segundo Mandarino Júnior, são descritas como “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" (MANDARINO, 2011). Dentro desse conceito de IC, temos as Infraestruturas Críticas da Informação (ICI), que segundo o mesmo autor, é descrita como o "Subconjunto dos ativos de informação que afeta diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade" (MANDARINO, 2011).

Essas infraestruturas críticas devem compor a principal preocupação de proteção por parte dos Estados, visto que a sua inoperância gera graves transtornos no seu interior. Diante disso, deve-se estabelecer barreiras que minimizem os problemas causados por interferências externas indesejadas nas estruturas vitais de um país. Num contexto militar e estatal, trata-se das defesas Cibernéticas.

Segundo a Doutrina Militar de Defesa Cibernética, a defesa cibernética se refere ao "conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente" (BRASIL, 2014).

Esse conjunto de ações deve ser implementado de forma a proteger o Estado das ameaças antes ou durante um conflito. A Defesa Cibernética exige ações que provejam uma segurança no trâmite e operações no Eciber. Essas medidas podem ser descritas como a segurança cibernética.

O termo segurança cibernética é descrito no JP 1-02 (EUA, 2016), como "prevenção, proteção, e restauração de computadores, sistemas de comunicação eletrônicos, serviços de comunicação eletrônicos, comunicações com fio, e comunicações eletrônicas, incluindo informações nele contidas, para garantir a sua disponibilidade, integridade,

autenticação, confidencialidade e não repúdio" (EUA, 2016). Já na Doutrina Militar de Defesa Cibernética é descrito como a "arte de assegurar a existência e a continuidade da sociedade da informação de uma nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas" (BRASIL, 2014).

Das definições acima, podemos verificar que a segurança cibernética é composta das medidas necessárias a prevenção e repressão de interferências no espaço cibernético, assegurando a sua utilização pelo Estado de forma confiável. Enquanto isso, a defesa cibernética se reveste de ações ofensivas e defensivas por parte do Estado na prevenção de conflitos ou no seu decorrer.

Ao abordar as operações no espaço cibernético, tem-se a seguinte definição dessas ações: "o emprego de capacidades do ciberespaço onde o propósito principal é assegurar objetivos no ciberespaço" (EUA, 2016).

Dentro dessas operações, segundo NUNES (2010), pode-se ter as ações ofensivas, defensivas e de exploração de guerra cibernética, conforme descritas abaixo:

- Ofensivas: ações realizadas por meio de redes de computadores para interromper, negar, degradar/corromper ou destruir a informação contida em computadores, redes e/ou sistemas de TI inimigos;

- Defensivas: ações realizadas por meio de redes de computadores para proteger, monitorar, analisar, detectar e responder à atividade não autorizada em computadores e/ou redes, de modo a garantir o uso continuado e a inviolabilidade dos nossos sistemas de TI; e

- Exploração: ações realizadas por meio de redes de computadores para a obtenção de informações sobre as vulnerabilidades dos sistemas de TI inimigo ou para a coleta de dados contidos nesses sistemas.

Diante dos conceitos expostos, passa-se à busca da definição do que é a Guerra

Cibernética (GC). Inicialmente, segundo Parks e Duggan (2001), no artigo *Principles or Cyber-warfare*, temos que:

> A Guerra Cibernética envolve ações realizadas no mundo cibernético. O espaço cibernético é qualquer realidade virtual compreendida numa coleção de computadores e redes. Existem diversos mundos cibernéticos, mas o mais relevante para a Guerra Cibernética é a internet e as redes a ela relacionadas, as quais compartilham mídias com a internet. A definição militar mais próxima para o nosso termo é uma combinação de ataque a redes de comutadores e defesa de redes de computadores, e possivelmente, operações especiais de informação. Nós definimos guerra cibernética como sendo a guerra praticada no "mundo real". Todos os tanques e navios e aviões e soldados tradicionais são os protagonistas da guerra cibernética (PARKS e DUGGAN, 2001, tradução nossa)

Dessa definição observa-se que o campo de atuação da guerra cibernética pode envolver os equipamentos físicos empregados em combate, interligados por meio das redes de computadores. Como os países têm implementado diversas redes informatizadas em apoio às Forças Armadas, os seus meios podem se tornar alvos de ataques antes mesmo de se confrontarem fisicamente.

Ao observar as definições disponíveis em publicações militares brasileiras, obtêm-se diferentes conceitos para guerra cibernética. Inicialmente, segundo a Doutrina Militar de Defesa Cibernética (BRASIL, 2014), a guerra cibernética "corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de Comando e Controle (C^2) do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. A guerra cibernética compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle ($STIC^2$) do oponente e defender os próprios $STIC^2$. A GC abrange, essencialmente, as Ações Cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente

em relação à TIC" (BRASIL, 2014).

Do exposto, tem-se que a guerra cibernética corresponde às ações no nível operacional e tático desenvolvidas no espaço cibernético a fim de garantir a utilização de forma confiável do espaço cibernético, bem como negar o uso pelos oponentes dos conteúdos e redes num conflito entre Estados.

2.2 As principais ameaças no domínio cibernético

Ameaças podem se apresentar de forma estatal ou não estatal, como ativistas isolados (hackers) ou terroristas, ou mesmo atores internos das instituições/empresas, bem como por desastres naturais. As ameaças cibernéticas aproveitam as vulnerabilidades dos sistemas para acesso aos ativos. Podendo causar perdas ou danos de diferentes graus. Sendo assim, a vulnerabilidade é um fator interno ao sistema e a sua existência permite a ação de ameaças externas. Para impedir ou mitigar as vulnerabilidades deve-se aplicar as salvaguardas (O'HANLEY et al., 2013)

Conforme Egger (2014), as ameaças são agentes ou ações, que podem atuar de modo espontâneo ou proposital, aproveitando das vulnerabilidades de um sistema para conseguir seu intento. A ameaça é um fator externo ao sistema (EGGER, 2014).

As ameaças virtuais no ciberespaço passaram daqueles agentes que eram, inicialmente, simples curiosos do mundo da computação, os quais invadiam sistemas de tecnologia da informação em busca de desafios, conhecimento ou mesmo do reconhecimento dos seus feitos no grupo, os chamados de *hackers*, para, atualmente, oponentes com interesses bem mais amplos e perigosos.

Nos dias atuais há os criminosos, os terroristas e mesmo outros Estados competidores. Tais oponentes são motivados por interesses políticos, ideológicos e financeiros

muito mais abrangentes e dispõem de estruturas mais poderosas para realizarem ataques no espaço cibernético.

Temos como possíveis ameaças o bloqueio e desinformação em recursos de informação e telecomunicação; ações de guerra ou terrorista contra fluxos de informação em estruturas vitais; a desestabilização da sociedade por meio da manipulação da consciência da população; a adoção de doutrinas e políticas, individualmente, pelas nações, com respeito à segurança das informações, provocando uma corrida armamentista; o uso de recursos de TI em detrimento dos direitos humanos e da liberdade de acesso à informação; a disseminação generalizada de informação, violando os princípios e as normas da legislação internacional; e o desenvolvimento de conceitos e meios por países membros, visando à guerra cibernética. (ALMEIDA, 2011).

Podemos apresentar cinco principais atores que representam as ameaças no mundo cibernético, quais sejam: os Estados, o terrorismo cibernético, o ativismo cibernético, os *hackers* e os elementos internos (NUNES, 2010). Seguem as descrições de tais ameaças:

O Estado figura como principal ator presente no espaço cibernético em função de sua insuperável capacidade de recursos, com relação aos demais atores. É, atualmente, o único ator com capacidade de desenvolver ferramentas para ataques com elevado grau de sofisticação, em função dos elevados custos envolvidos para desenvolvimento. A principal ameaça apresentada pelos Estados é a Guerra Cibernética que envolveria o uso de ataques cibernéticos com uma motivação política.

Hoje figuram como os principais Estados no domínio cibernético: Estados Unidos da América, Rússia, China, Coreia do Norte e Israel (CLARKE, 2015).

O terrorismo cibernético pode ser definido como um ataque baseado em computador ou ameaça de ataque a intenção de intimidar ou coagir governos ou sociedades na busca de objetivos que são políticos, religiosos ou ideológicos. O ataque deve ser

suficientemente destrutivo ou perturbador para gerar medo comparável ao de atos físicos de terrorismo. Ataques que levam à morte ou lesão corporal, falta de energia prolongada, acidentes de avião, a contaminação da água, ou grandes perdas econômicas seriam exemplos (LACHOW, 2009).

Segundo Lachow (2009) o ativismo cibernético ou *Hacktivismo* é geralmente entendido como a manipulação da informação digital para promover uma ideologia política. Em geral, os atos de hacktivismo visam alavancar o uso de código para ter "efeitos semelhantes ao ativismo regular ou desobediência civil". Ao contrário de terrorismo cibernético, o ativismo cibernético não é focado na criação de um sentimento de medo ou terror. Os ativistas cibernéticos muitas vezes atacam alvos decisores diretamente para expressar sua insatisfação com várias políticas, ao passo que os terroristas geralmente têm como alvo vítimas inocentes ou de terceiros.

Segundo Clarke, *Hacker* é o indivíduo capaz de alterar determinadas instruções nos códigos dos programas com a finalidade de fazer com que o sistema realize novas tarefas para os quais não estava programado (CLARKE, 2010). Porém, existem diferenças deste com os criminosos cibernéticos e os guerreiros cibernéticos. Criminosos cibernéticos são os que realizam intrusões, por meio de computadores, em locais não autorizados. Guerreiros cibernéticos são os que trabalham para o Governo e realizam todas essas tarefas.

O elemento interno recai na categoria de introdução de uma vulnerabilidade operacionalmente por meio de ação humana direta, ou seja, por meio físico (CSIS, 2008). O acesso pode se dar durante o projeto, desenvolvimento, teste, empacotamento, distribuição, operação ou manutenção de componentes do sistema.

As ameaças, conforme exposto, apresentam diversas fontes e motivações, porém, todas podem proporcionar danos significativos aos Estados e sociedades. Diante disso, mostra-se necessária uma estrutura robusta para proteção dos interesses comuns.

2.3 Vulnerabilidades e ataques cibernéticos

Segundo Fred Shreier[3], os ciberataques e a exploração cibernética só são possíveis devido ao fato de que os sistemas de tecnologia da informação são vulneráveis. A maioria das vulnerabilidades existentes são introduzidas acidentalmente por meio de falhas de *design* ou implementação (SCHREIER, 2015). No Quadro 1 do Anexo estão apresentadas as possíveis falhas dos sistemas de TI, segundo o mesmo autor. Também segundo Schreier, "os ataques cibernéticos e a exploração cibernética exigem vulnerabilidades, o acesso a essa vulnerabilidade e uma carga útil a ser executada. A diferença técnica principal entre ataque cibernético e exploração cibernética é da natureza da carga útil a ser executada. A carga útil do ataque cibernético é destrutiva ao passo que uma carga útil de exploração cibernética adquire informações ou dados de inteligência de forma não destrutiva" (SCHREIER, 2015).

A carga útil deve ser implantada nos alvos que são os objetivos de ataques e podem fazer uso das vulnerabilidades dos oponentes. Pode ser realizada, como exemplo, com a implantação de um vírus na rede do oponente, ou simplesmente em dispositivo de armazenamento que possa vir a ter contato com um dos pontos de acesso a tais redes. Na medida em que consegue se inserir no sistema, ele pode reproduzir, retransmitir, destruir ou alterar dados no sistema invadido.

São apresentadas no Quadro 2 do Anexo, segundo SCHREIER (2015), as principais formas de ataques com as respectivas descrições.

2.4 Princípios e Características da Guerra Cibernética

A guerra cibernética possui alguns diferentes princípios de guerra em se

3 Fred Schreier, é consultor do Centro de Genebra para o Controle Democrático de Forças Armadas – DCAF.

comparando aos princípios da guerra cinética[4]. Alguns princípios tradicionais da guerra cinética se aplicam à guerra cibernética, porém, outros não tem significado neste domínio.

Em seus estudos, Raymond C. Parks e David P. Duggan desenvolveram experiências com guerra cibernética limitada, resultando na apresentação de oito princípios para este novo domínio, quais sejam:

1. Guerra Cibernética deve produzir efeitos no mundo cinético;

2. Medidas ativas podem ser adotadas para se dissimular no mundo cibernético, mas qualquer coisa que alguém faça é visível;

3. Não existem leis de comportamento imutáveis no mundo cibernético, excetuando-se aquelas que necessitam de uma ação no mundo real;

4. Alguma entidade no mundo cibernético possui a autoridade, acesso, ou habilidade necessários para pôr em prática qualquer ação que um atacante deseje realizar; o objetivo do atacante é assumir a identidade dessa entidade, de alguma forma;

5. As ferramentas, ou armamentos, da Guerra Cibernética são de natureza dual;

6. Tanto o atacante, como o defensor de um sistema, controlam uma pequena parcela do ciberespaço que utilizam;

7. O ciberespaço não é consistente, nem confiável; e

8. Limitações físicas de distância e espaço não se aplicam ao mundo cibernético.

Em estudos apresentados por CAHILL, ROSINOV e MULÉ (2003), sintetizados por DUTRA (2007), a tais princípios foram apresentadas denominações conforme descrito a seguir. O sexto princípio foi dividido em dois outros (usurpação e compartimentação) por sugestão destes autores em virtude de apresentarem duas situações diferentes:

- O **Princípio do Efeito Cinético** diz que a guerra cibernética deve produzir efeitos no mundo cinético, ou seja, ações no mundo cibernético devem implicar em algum

4 Termo adotado para descrever as ações bélicas realizadas nos domínios físicos.

dano real a um Estado ou diversão de autoridades que coordenem um país.

- O **Princípio da Dissimulação e Visibilidade** afirma que medidas ativas podem ser adotadas para se dissimular no mundo cibernético, mas qualquer coisa que alguém faça no mundo cibernético é visível. A questão é se alguém está observando. Qualquer ação realizada nesse domínio envolve a movimentação ou manipulação de dados. Porém, a alteração de dados pode ser detectada, não podendo ser camuflada. Cabe à defesa cibernética conseguir detectar tais ações que permeiam todo o fluxo de dados no domínio cibernético.

- O **Princípio da Mutabilidade** diz que não existem leis de comportamento imutáveis no mundo cibernético, excetuando-se aquelas que necessitam de uma ação no mundo real. No "mundo real" há a previsibilidade de determinados comportamento pois este é regido pelas leis da física. No mundo cibernético, que é um ambiente criado pelo homem, não existem quaisquer leis que permitam prever esse tipo de comportamento, pois sempre poderão ocorrer falhas em softwares, programas, equipamentos etc. Porém, como exceção, há mudanças no comportamento de sistemas quando ocorrem melhorias nos equipamentos e infraestrutura, como por exemplo a substituição de processadores por modelos mais avançados, a troca de tecnologias como a implementação de redes de fibra ótica etc.

- Pelo **Princípio do Disfarce,** se alguma entidade no mundo cibernético possui a autoridade, acesso, ou habilidade necessários para pôr em prática qualquer ação que um atacante deseje realizar, o objetivo do atacante é assumir a identidade dessa entidade, de alguma forma. Como o mundo cibernético é um ambiente construído e gerenciado integralmente pelo homem ou suas ferramentas, sempre é possível que um atacante se faça passar pela imagem da entidade detentora de determinado site ou serviço e realizar ações se fazendo passar por esta, conseguindo ataques bem-sucedidos sem a ciência da entidade.

- O **Princípio da Dualidade do Armamento** diz que as ferramentas ou armamentos da Guerra Cibernética são de natureza dual. No combate convencional, as

ferramentas, equipamentos e armamentos possuem um uso único e bem definido. No combate cibernético, as mesmas ferramentas são usadas por atacantes e administradores de sistemas com finalidades distintas: uma ferramenta que busque as vulnerabilidades do sistema, por exemplo, pode ser usada por atacantes para encontrar pontos que representem oportunidades de ataque em seus sistemas alvos, e por administradores para descobrir as fraquezas de equipamentos e redes.

- No Princípio da Compartimentação, tanto o atacante como o defensor de um sistema controlam uma pequena parcela do ciberespaço que utilizam. Como todo o ciberespaço está contido em equipamentos, programas e fluxo de dados, todos subprodutos do trabalho humano, um ciber grupo raramente controla algo além dos limites da sua infraestrutura de comunicações. A parcela de ciberespaço controlada está compreendida entre seus equipamentos e programas, até a interface com a infraestrutura de comunicações na maioria dos casos.

- O **Princípio da Usurpação diz que** quem controlar a parte do ciberespaço que o oponente utiliza, pode controlar o oponente.

- O **Princípio da Incerteza** diz que o ciberespaço não é consistente, nem confiável. Este princípio está relacionado com o princípio da mutabilidade. Devido à natureza artificial do ciberespaço, nem sempre os equipamentos, e principalmente os softwares, irão trabalhar conforme esperado. Assim, não é possível saber, com plena certeza, se o próximo passo numa ação cibernética funcionará.

- O **Princípio da Proximidade** tráz que as limitações físicas de distância e espaço não se aplicam ao mundo cibernético. No mundo cibernético, ações desencadeadas do outro lado do mundo, ou da sala ao lado, são executadas com igual grau de eficácia; dessa forma, distâncias físicas não constituem um obstáculo na condução dos ataques, ao passo que as ações no mundo cinético tem que atravessar, quase sempre, grandes distâncias.

Neste capítulo foram apresentados os principais termos utilizados no ambiente do quinto domínio, o domínio cibernético. Nesse ambiente de inúmeras ameaças, pode-se perceber as necessidades de uma estrutura de defesa cibernética que minimize as vulnerabilidades que permeiam praticamente todos os sistemas. As ameaças, que se multiplicam cada vez mais, são representadas por diversos atores, com inúmeros objetivos.

Verificando a definição de guerra cibernética, podemos perceber que ela permeia diversos segmentos que fazem uso da *internet* e, que não há como deixar de perceber e reconhecer a necessidade de estruturas para defesa deste domínio.

No capítulo seguinte serão tratadas algumas características dos domínios tradicionais de guerra, realizando-se uma comparação com o domínio cibernético.

3 DOMÍNIOS NA GUERRA

Neste capítulo será realizada uma abordagem das geoestratégias terrestre, marítima, aérea e espacial, de modo a apresentar um posicionamento de estratégias do ciberespaço[5] a fim de se realizar uma comparação entre o domínio cibernético e os demais domínios existentes. Pretende-se com isso permitir a visualização do novo domínio virtual com as características observadas nos domínios do mundo real.

3.1 Domínio Terrestre

Para descrever as características do domínio terrestre, segundo Coutau-Bégarie, integra-se os fatores geográficos de distância, topografia, condições climáticas, vias de comunicação e fortificações numa classificação dividida em fatores estáticos e dinâmicos (COUTAU-BÉGARIE, 2010).

3.1.1 Fatores Estáticos

Segundo Coutau-Bégarie, o os fatores estáticos abrangem os elementos que se classificam como de longa duração, não modificáveis no curto prazo pela ação humana. São eles os elementos duráveis da estratégia. Subdividem-se em: topoestratégia, morfoestratégia, fisioestratégia e meteoestratégia (COUTAU-BÉGARIE, 2010)

Na topoestratégia, de acordo com Coutau-Bégarie, o objeto de estudo e atenção dos teóricos militares é o terreno. É ele que define a manobra, apontando o posicionamento decisivo. Para Clausewitz, o defensor tem a vantagem do terreno, o atacante, a da surpresa. Após as concepções geométricas de Dietrich von Bullow, adotadas no século XVIII,

5 Serão levantados aspectos e características abordados na obra “Tratado de Estratégia”, de Coutau-Bégarie (2010)

Clausewitz confere ao terreno ampla relevância:

> Esta conexão (entre a guerra e o terreno) é permanente, de modo que é absolutamente impossível conceber uma operação de guerra, realizada por um exército organizado, que se desenvolva em algo que não seja em um espaço determinado; em segundo lugar, ela tem uma importância decisiva, já que modifica e vai por vezes até mesmo transformar totalmente os efeitos de todas as forças; em terceiro, ela envolve tanto os detalhes mínimos de uma localidade quanto as mais vastas extensões de um país (CLAUSEWITZ, apud COUTAU-BÉGARIE, 2010).

O terreno passa a ser aliado da defesa com os seus diversos obstáculos naturais inerentes, tais como relevo, vegetação, hidráulicos, desertos quentes ou gelados etc. Tais obstáculos aplicam retardamento, isolamento e/ou canalização dos avanços dos inimigos. Ao passo que os defensores devem se valer desses benefícios do terreno, o atacante deve aplicar tropas especializadas ou meios de transposição adequados a fim de minimizar as desvantagens impostas. Assim como algumas características do terreno podem facilitar a defesa, algumas vias naturais de invasão, como vales e rios entre montanhas favorecem atacantes, o que determina as estratégias de cada um.

O terreno no domínio cibernético é o ciberespaço. Um ambiente virtual composto por conexões lógicas e físicas de cabos, fios, fibras óticas, roteadores, enlaces satelitais etc., construído pelo ser humano para se comunicar. Nesse ambiente, as distâncias e composições geométricas aplicadas ao domínio terrestre não se aplicam, são todas planificadas e reduzidas às conexões existentes. Porém, como no terreno físico, a conexão entre o ambiente e a guerra é constante. Apesar disso, o combate cibernético é desenvolvido num espaço não determinado, visto a característica inerente ao mundo virtual. Ou seja, o combatente inimigo pode se encontrar a pouquíssimos metros de distância ou milhares de quilômetros, mas poderá atingir seus alvos cibernéticos da mesma forma.

Um dos objetivos principais de conquista é o local de concentração de população e riquezas. As cidades, principalmente as capitais de Estados, são, portanto, objetivos sempre

perseguidos por apresentarem grande representação simbólica de concentração do poder do Estado, como por concentrarem grande capacidade de convergência e propagação de informações, além de proporcionarem a possibilidade de diversos pontos de apoio e de defesa.

O terreno pode ser utilizado por ambos os contendores, de acordo com o princípio da dualidade do armamento, as ferramentas de ataque e defesa podem ser aplicadas por qualquer das partes.

Os alvos de ataques, assim como no domínio terrestre, podem ser as grandes cidades as quais apresentam grandes concentrações de população. Nessas localidades, onde há grande infraestrutura digital instalada, que implica em grande número de serviços e estruturas conectadas, ocorre uma maior dependência da interconectividade, o que leva a maiores vulnerabilidades aos ataques.

Nos estudos da Morfoestratégia, segundo Coutau-Bégarie, os geógrafos do fim do século XIX fizeram uso por vezes excessivo da forma do Estado, dos quais pretendiam extrair extrapolações em todos os domínios. Porém, atualmente, esse gênero não tem mais valia. Mas a forma permanece como uma componente da geostratégia. A forma, compacta, longilínea ou fragmentada de um Estado ou grupo de Estados determina a extensão das frentes a defender ou das bases de ataque (COUTAU-BÉGARIE, 2010).

Essas formas são minimizadas pelas distâncias hoje em vista do avanço das tecnologias.

A morfologia do “terreno” cibernético não teria grandes influências nos ataques. A formação das redes podem dificultar em termos de velocidade e/ou dificuldade de acesso, mas não geram grandes barreiras que impeçam os ataques. A conectividade de redes *intranet* à rede *internet* facilita acessos.

Segundo Coutau-Bégarie, o objetivo da Fisioestratégia é compreender o espaço em relação à totalidade do sistema, levando-se em consideração as distâncias e a posição, num

enfoque dinâmico (COUTAU-BÉRGARIE, 2010).

Tem-se a construção do pensamento do esgotamento da ofensiva pela distância. Clausewitz propõe como regra que “quanto mais estendida a esfera das operações que ele deva atravessar, mais o exército assaltante é enfraquecido”, afirmando que “todo avanço ao longo do ataque estratégico enfraquece aquele que o lança, por sua simples existência ou porque uma divisão de forças torna-se necessária”. O alongamento das frentes atacantes é muito dependente da capacidade de manutenção de uma linha de apoio logístico ao longo do avanço (CLAUSEWITZ, apud COUTAU-BÉGARIE, 2010).

As distâncias teóricas, simples métricas, não refletem a real distância entre objetivos visto que o terreno apresenta inúmeras adversidades a serem transpostas. Possuir ou deter uma posição ou zona estratégica pode conferir grande vantagem num conflito. Esta vantagem pode se configurar por interesse político, econômico ou estratégico, dependendo das facilidades de suas linhas de comunicação ou existências de obstáculos que impeçam a sua conquista, das fontes de matérias-primas necessárias ao abastecimento, da influência do seu posicionamento no controle de determinada região etc.

Num enfoque fisiológico do espaço cibernético, a composição deste não impediria o avanço das frentes de atacantes cibernéticos nem implicariam na necessidade de pontos de apoio logístico assim como no domínio terrestre. A conexão lógica pode-se fazer a curtíssimas ou extremas distâncias, não sendo relevantes a posição. Os objetivos políticos, econômico ou estratégicos do domínio do espaço cibernético podem ser conquistados por meio de ataques a partir do interior do Estado atacado ou a longas distâncias deste.

A Meteoroestratégia trata das influências climáticas nas batalhas. Segundo Coutau-Bégarie, a influência das condições meteorológicas é mais fortemente sentida nas regiões frias e quentes (COUTAU-BÉGARIE, 2010). Dessa forma, há que se levar em conta tais fatores nas estratégias no terreno. Porém, com o avanço da tecnologia nos materiais, tais

fatores são minimizados em sua influência.

As mudanças climáticas não representam grandes ameaças às operações dentro das estruturas do espaço cibernético, a exceção de redes dependentes de comunicações satelitais ou em HF, as quais sofrem perturbações no meio de propagação dependendo da variação das condições na propagação no campo eletromagnético. Isso possibilita a operação virtual mesmos em tempos adversos.

3.1.2 Fatores Dinâmicos

Segundo Coutau-Bégarie, tem-se os fatores dinâmicos, que são aqueles sensíveis à ação imediata do homem. São divididos em fatores ofensivos: os recursos, as vias e infraestruturas de comunicação e as bases; e defensivos: os obstáculos políticos e o estado das fortificações e outros meios de defesa (COUTAU-BÉGARIE, 2010).

- Fatores Ofensivos

Segundo Coutau-Bégarie, “a geoestratégia dos recursos explora os recursos potenciais, não tanto como objetivos, mas por sua contribuição imediata à condução das operações tanto em tempo de paz quanto em tempo de guerra” (COUTAU-BÉGARIE, 2010).

Os recursos disponíveis numa região de conflito despertam interesse pelo potencial de apoio às ações desses, como fonte de suprimentos. A disponibilidade imediata de recursos como petróleo, mantimentos, munição, etc., põe em vantagem aqueles que os detêm ou os conquistam. Porém, isso pode variar de acordo com as potencialidades de cada região, com o grau de colaboração ou resistência da população local, dentre outros fatores.

A mecanização, segundo Coutau-Bégarie, “deu uma importância crescente ao estado das vias de comunicação. Um exército moderno necessita de infraestruturas que devem avançar ao mesmo tempo que ele” (COUTAU-BÉGARIE, 2010).

As vias e infraestruturas de comunicação são vitais para os deslocamentos de

tropas, bem como de via de suprimento das forças combatentes. No domínio terrestre, temos as ferrovias e estradas que permitem o avanço e o apoio de forma mais eficaz e rápida.

Segundo Coutau-Bégarie, “a dilatação das distâncias e a complexidade crescente dos exércitos modernos, que necessitam de uma logística muito aperfeiçoada, somam-se para dar uma importância decisiva às bases, que podemos definir sumariamente como áreas organizadas e protegidas permitindo abrigar, comandar, reabastecer, preparar e recuperar forças ou meios militares de qualquer natureza” (LEPOTIER apud COUTAU-BÉGARIE, 2010).

Em relação aos fatores dinâmicos, ainda na comparação com os fatores geoestratégicos, os atacantes cibernéticos podem se beneficiar dos recursos de rede infectados, tais como bombas lógicas, para poderem tomar vantagem de ação em momento oportuno. A resistência a tais infecções depende em muito das barreiras impostas pelos defensores. Como as redes interconectadas da internet foram projetadas segundo parâmetros de velocidade e interconexão, em detrimento da segurança, tem-se a possibilidade de utilização de inúmeros pontos de ataque.

- Fatores Defensivos

Segundo Coutau-Bégarie, “os obstáculos estudados pela geografia militar e a geoestratégia são, em princípio, obstáculos naturais, que se distinguem por sua permanência e que o analista pode facilmente marcar a decênios ou séculos de distância. Mas os obstáculos políticos são, no momento, no mínimo, também temíveis (COUTAU-BÉGARIE, 2010).

Os obstáculos políticos, representados por países neutros, tem sua relevância ao passo que transpô-los, sem a devida anuência, pode acarretar a entrada de terceiros indesejáveis no conflito. O papel de países neutros, vizinhos às áreas de instabilidade, se revestem de maior importância com as alterações do direito internacional.

A utilização do princípio do disfarce e da dissimulação e visibilidade pode levar à

falsa impressão de ataques por terceiros que não estão envolvidos nos conflitos, porém, por vezes, devido às fragilidades de suas estruturas cibernéticas, permitem a camuflagem de ataques, omitindo a real fonte dos ataques. Isso pode levar à distração em prol de ações dos verdadeiros atacantes. Por isso, é necessária a implementação de estruturas cibernéticas mais robustas e confiáveis, e que a monitoração de suas redes seja efetiva e constante.

As fortificações foram originadas com a finalidade de reforçar a proteção no terreno. Podem ser planejadas e erguidas em tempos de paz, impondo uma linha de barreiras contínua, concentradas ou dispersas, ao longo de uma fronteira.

As fortificações de campanha são implementadas com os conflitos já instalados e seguem o movimento das forças em combate. Como descrito por Napoleão, em suas notas da arte da guerra, "As praças fortes são úteis para a guerra defensiva como para a ofensiva. Sem dúvida, elas não podem por si só ocupar o lugar de um exército, mas são o único meio que se tem para retardar, entravar, enfraquecer, inquietar um inimigo vencedor"[6](NAPOLEÃO, apud COUTAU-BÉGARIE, 2010).

A construção de barreiras às ameaças cibernéticas também podem ser erguidas em tempos de paz ou durante conflitos. Tais fortificações erguidas em tempos de paz fazem com que a possibilidade de detecção de invasões em períodos de conflitos futuros seja mais provável. Já com o conflito em curso, a sua implementação tende a obter resultados menos favoráveis.

3.2 O domínio marítimo

Devido à necessidade de comunicação e transporte entre os continentes, com o incremento das relações comerciais entre Estados, o mar é a via natural de ligação entre estes.

6 *Commentaires de Napoléon 1er*, tomo VI, *Notes sur l´art de la guerre*, Paris, Imprimerie inpériale, 1867, p. 181.

Notadamente, pela superfície de 71% do planeta, não se pode deixar de reconhecer a sua importância nos diversos aspectos políticos, econômicos, militares etc.

Conforme descrito por Coutau-Bégarie, como primeira característica do mar, pode-se constatar que não o habitamos e que "o mar não tem interesse a não ser por sua relação com a terra, residência habitual do homem" (COUTAU-BÉGARIE, 2010).

A sua importância se dá pelas relações de transporte, fonte de alimento e barreiras naturais entre nações. Diante disso, o mar apresenta funções negativas e positivas.

O domínio cibernético, assim como o domínio marítimo, não é habitado, sendo um campo para a atividade humana. Funciona como meio de comunicação entre pessoas, empresas, organizações e Estados. Por meio dele também são gerados negócios virtuais, que em muito tem crescido a oferta e demanda de serviços virtuais.

- Funções Negativas

Consoante Coutau-Bégarie, "O mar é um obstáculo, ao mesmo tempo político e militar" (COUTAU-BÉGARIE, 2010).

Desde os primórdios da humanidade, os oceanos fizeram a função de separador dos povos, isolando diversas áreas devido às dificuldades de locomoção impostas pelo meio. Os contatos entre sociedades se fazem facilitados pela ligação contínua em terra.

Segundo Coutau-Bégarie, as "sociedades separadas por um elemento líquido um pouco extenso têm menos contato do que os povos com continuidade territorial. Esta regra sofre exceções apenas quando obstáculos tornam as comunicações quase impraticáveis." Os impérios ultramarinos seriam mais difíceis de manter unidos em relação aos impérios continentais, segundo a "teoria da água salgada", cujo pai é o britânico lord Curzon[7]

7 George Nathaniel Curzon, afirmava que "é por causa da interposição do mar que a Inglaterra perdeu a América, que os holandeses e os portugueses perderam o essencial de seus impérios nas Índias; que Napoleão enfrentou, como Roma, tantas dificuldades mo Egito; que a aventura mexicana da França e da Áustria terminou em fiasco". (PANNIKAR apud COUTAU-BÉGARIE , 2010). Descreve a "Teoria da água salgada": um império ultramarino teria mais chances de ser exposto à fragmentação do que um império constituído por extensão contínua a partir de um centro (COUTAU-BÉGARIE, 2010).

(COUTAU-BÉGARIE, 2010).

Como o isolamento insular constitui uma excelente barreira contra as invasões, muitas nações tentaram expandir os seus territórios pela conquista de novas ilhas espalhadas pelos oceanos.

Segundo Coutau-Bégarie, deve-se levar em consideração três complementos em relação à superioridade do mar, num plano defensivo: ela não é absoluta, sendo condicionada pela distância e pela relação de forças; a vantagem defensiva tem por corolário obrigatório uma dificuldade da potência insular de se projetar sobre o continente; e a vantagem defensiva diminuiu na época contemporânea (COUTAU-BÉGARIE, 2010)

Em virtude do progresso dos armamentos e, principalmente, pelo surgimento da arma aérea, essas vantagens defensivas são minimizadas.

Como o ambiente marítimo, o cibernético também abrange diversos Estados de todo o planeta, tendo a capacidade adicional de atingir inclusive os Estados interiores. O espaço cibernético, então, ao contrário de atuar como um obstáculo, funciona então como uma via expressa que interliga os Estados e sociedades. Dessa forma, analogamente para este ambiente, a teoria da "água salgada" do lord Curzon não teria validade.

As conquistas de ilhas para servirem como bases de apoio e expansão de domínios físicos e estabelecimento de presença contínua em todas as regiões, na analogia com o domínio cibernético, não teria grande validade. A expansão de domínios lógicos se faz a distância, bastando, em alguns casos, a implantação de agentes virtuais maliciosos nos domínios de interesse dentro dos domínios do oponente.

No domínio cibernético não ocorre a superioridade absoluta num plano defensivo. Há sempre a possibilidade de ataques de fontes assimétricas, que necessitam de relativamente poucos recursos para infringir danos consideráveis às infraestruturas críticas de adversários, mesmo distantes. A vantagem defensiva diminui com os ataques cibernéticos.

- Funções Positivas

São identificadas três funções positivas do elemento marinho: fonte de riquezas, via de comunicação e teatro de conflitos (COUTAU-BÉGARIE, 2010).

A atividade pesqueira é há muito tempo explorada no meio marítimo em busca de proteína pelo homem. Com o desenvolvimento e expansão da capacidade de explotação de petróleo no mar, a partir do século XX, foram desenvolvidas também capacidades de explotação de outros recursos minerais do fundo do mar, o que elevou consideravelmente a sua importância como fonte de riquezas. O uso como via de comunicação é reconhecidamente mais barato, seguro e mais veloz do que em muitas vias terrestres, principalmente com grandes distâncias envolvidas e quando os relevos terrestres são mais inóspitos. Os volumes transportados nas vias marítimas crescem muito no século XX.

Analogamente, a dependência do ambiente cibernético permeia diversos segmentos como financeiros, de comércio, de serviços de infraestrutura de energia elétrica, de transportes, de entretenimento, e mesmo militares, o que faz gerar uma grande gama de transações diárias, consequentemente, gerando grandes movimentações financeiras. O Eciber se tornou grande fonte de geração de riquezas.

Segundo Coutau-Bégarie, a alteração decisiva nas batalhas navais se situa no século XII a.C. com o surgimento do *trirreme*[8], em que Beaufre afirma que “com ela, o combate deixa de opor homens contra homens para tornar-se o combate entre seres animados que são os navios”. A guerra no mar tornou-se em seguida um fato quase permanente, tanto na Europa quanto no extremo Oriente. Três pontos, entretanto, precisam ser sublinhados: primeiro, a guerra naval foi por muito tempo costeira; segundo, a guerra naval é muito dependente da técnica; e terceiro, por ser o mar simultaneamente meio de comunicação e teatro de conflitos, a guerra naval não se limita estritamente a um enfrentamento puramente

8 Primeiro navio especificamente concebido para o combate.

militar" (COUTAU-BÉGARIE, 2010).

Pelo exposto, observa-se que: em virtude das necessidades logísticas, das dificuldades de comunicação a longa distância e da incapacidade de detectar o inimigo no meio do oceano, não era possível o afastamento a grandes distâncias da costa; o papel de importância que tem o navio numa batalha é significantemente superior ao do papel do homem num conflito e o combate será normalmente recusado sempre que a parte não se considere em condições de igualdade; e que a guerra naval envolve também os meios mercantes que fazem o comércio entre beligerantes e não beligerantes, de forma a atingir a economia e comércio do inimigo.

Comparando com o domínio cibernético, o conflito não se limita a poucos estados margeados pelo mar ou canais fluviais, mas exerce maior influência nos Estados que possuem um maior índice de conectividade e apresentam maior dependência do Eciber. Por sua vez, o papel do homem exerce significativa maior influência do que os equipamentos utilizados numa guerra cibernética. E, como no domínio marítimo, o espaço cibernético é utilizado para diversos fins, inclusive militares.

Segundo Coutau-Bégarie, "pode-se dizer que toda sociedade que atinge um certo grau de potência ou de desenvolvimento é necessariamente conduzida a se aventurar no mar (COUTAU-BÉGARIE, 2010).

Assim como as nações que chegaram ao patamar de grandes potências e se voltaram para o mar, a fim de manter e expandir seus domínios, hoje não há como ignorar a necessidade de desenvolver as capacidades cibernéticas defensivas e ofensivas no Eciber. É um caminho sem volta, reforçado pelas capacidades de pequenos Estados, ou grupos independentes, de realizarem ataques mesmo às grandes potências.

- A dilatação do elemento marinho

O mar não é somente líquido, mas também fluido, com uma tendência a se dilatar

sem nenhuma comparação com o que se passa sobre a terra (COUTAU-BÉGARIE, 2010).

Inicialmente, reinava a teoria de que o mar não pertencia a ninguém. Com o passar do tempo e com o aumento dos interesses no poder econômico que o mar pode oferecer, iniciaram-se as disputas pelo domínio dele e a busca da delimitação dos limites pertencentes a cada Estado, bem como a definição das áreas comuns a todos.

A dilatação do espaço cibernético é uma constante. A sua criação se fez, inicialmente, para apoio às pesquisas entre cientistas de universidades estadunidenses, mas logo que foi se expandindo para outras universidades, ganhou o campo aberto para as populações do mundo. O acesso passou a ser irrestrito pela expansão de pontos de conexão. Os Estados tentam se precaver tentando criar estruturas cibernéticas mais seguras, valendo-se do princípio da compartimentação, mas, ainda assim, não são imunes ao acesso indevido de atacantes, que se utilizam dos mais diversos artifícios para conseguirem invadir as estruturas de interesse. Como no ambiente marítimo, são inúmeras as consequências estratégicas devido a essa capacidade de acessibilidade, e segundo o princípio da usurpação, uma vez que se controla parte do ciberespaço que o oponente utiliza, pode-se controlar o oponente.

- Especificidades da guerra no mar

Conforme Coutau-Bégarie, enquanto o raciocínio estratégico integre distâncias de dezenas, no máximo centenas de quilômetros quando se trata da terra, deve-se considerar no mar distâncias que se enumeram em centenas de quilômetros , por vezes com mais frequência, em milhares de quilômetros (COUTAU-BÉGARIE, 2010).

As distâncias envolvidas no domínio marítimo tendem a ser cada vez maiores em função da capacidade de locomoção dos meios cada vez mais elevada. O espaço estratégico dilatado aliado à flexibilidade e mobilidade do instrumento naval permite a realização de ataques em múltiplos lugares.

Segundo Coutau-Bégarie, devido aos progressos técnicos, os combates se

desenvolvem a partir de então a distâncias cada vez maiores (COUTAU-BÉGARIE, 2010).

Os canhões ficaram em segundo plano, dando lugar a outros armamentos de maior alcance, aos aviões e aos mísseis.

Comparando-se com o domínio marítimo, o domínio cibernético não sofre influências das distâncias físicas, desde que se estabeleçam as conexões lógicas.

Segundo Coutau-Bégarie, apesar da propulsão nuclear ou do reabastecimento no mar, as bases permanecem indispensáveis: o descanso das tripulações e a manutenção do material cada dia mais complexo o exigem de maneira imperativa (COUTAU-BÉGARIE, 2010).

Conforme exposto, as bases de apoio continuam sendo necessárias para a projeção e o prolongamento da permanência em áreas distantes.

Segundo Coutau-Bégarie, “o meio marítimo se caracteriza pela homogeneidade: não existe obstáculo sobre o qual o defensor possa se apoiar, de modo que não pode haver aí uma frente” e “o controle do mar não se divide, salvo a rigor no Pacífico” (COUTAU-BÉGARIE, 2010).

O espaço cibernético pode apresentar pontos de apoio virtual, pela implantação de bombas lógicas ativáveis remotamente ou por utilização do princípio da Dissimulação e da Visibilidade, operando a partir de equipamentos remotos de terceiros.

Segundo Coutau-Bégarie, “a surpresa e a proteção no mar não são dadas pelo ambiente, mas construídas pela manobra (COUTAU-BÉGARIE, 2010).

A flexibilidade do instrumento cibernético permite a realização de inúmeros ataques a um único alvo ou a vários espalhados nos diversos continentes. A capacidade de permanência também pode ser muito elevada, o que se faz uma ameaça constante. A manobra também pode ser utilizada pelos combatentes no espaço cibernético.

3.3 O domínio Aéreo

Segundo Coutau-Bégarie, mais ainda do que o meio marinho, onde encontramos ilhas e estreitos, e o oceano finda sempre pro se chocar com as costas, meio aéreo é homogêneo e contínuo. Não há a presença de obstáculos a grandes altitudes que interdite a nevegação em todas as direções (COUTAU-BÉGARIE, 2010).

Em vez de relevos, observa-se apenas a presença de correntes de ventos, que muito se assemelham às correntes marinhas, mas que não imprimem barreiras intransponíveis à navegação aérea. Observa-se uma estratificação vertical, a qual varia suas características de acordo com a altitude.

Observa-se no domínio cibernético uma análoga homogeneidade como no domínio aéreo. As estratificações apresentadas no Eciber são as barreiras implantadas nas redes particulares (*intranets*) como os *firewall*, mas que se conectam à internet.

Conforme Coutau-Bégarie, o argumento topográfico somente se manifesta verdadeiramente de três maneiras, todas relativas ao substrato e não ao meio aéreo propriamente dito: o voo acima da terra ou do mar não obedece às mesmas regras; o poder aéreo é a soma de aviões e bases; e a topografia reencontra toda a sua força na dimensão de apoio no solo (COUTAU-BÉGARIE, 2010).

Os voos sobre diferentes terrenos apresentam diferentes graus de dificuldades para os pilotos, demandando diferentes adaptações ao terreno que sobrevoam.

A projeção do poder aéreo depende do conjugado avião e base. Com a evolução dos meios aéreos, que passaram de centenas de quilos a algumas dezenas de toneladas, houve a necessidade de ampliar e modernizar as estruturas das bases de apoio, que passaram a exigir uma maior complexidade nas estruturas, como maiores e mais elaboradas pistas. A disponibilidade desses pontos de apoio estratégicos passam a ser determinantes para o emprego de aeronaves em distâncias mais elevadas.

E a topografia do terreno influi diretamente na precisão dos ataques a objetivos terrestres. A configuração do terreno dos objetivos em terra pode dificultar as ações de reconhecimento e ataque pelas alas aéreas.

Os tipos de conexões e dispositivos de proteção entre redes no Eciber pode dificultar as explorações e ataques, exigindo também maiores habilidades dos invasores. Podem ser necessários diferentes tipos de dispositivos cibernéticos para acessar ou invadir nas diferentes redes interconectadas.

Segundo Coutau-Bégarie, o avião é, por excelência, o instrumento de combate a grande distância. Apresenta, em muitos casos, uma limitação devido à resistência física dos pilotos (COUTAU-BÉGARIE, 2010).

Já no domínio cibernético, os ataques não dependem do componente da distância e podem ser programados via software para se multiplicarem por diversos lugares à diferentes alvos, não sendo exigidos grandes esforços físicos dos atacantes.

O impacto da arma aérea sobre as operações terrestres ou marítimas é comparativamente maior do que o efeito da defesa antiaérea sobre as operações aéreas. Bem como, a arma aérea confere vantagem à ofensiva em virtude das capacidades de intervir ou atacar a longas distâncias e de forma rápida. (COUTAU-BÉGARIE, 2010).

Enquanto o instrumento naval é reconhecido pela capacidade de permanência, o meio aéreo tem a possibilidade da instantaneidade das ações. São forças complementares e não concorrentes. O surgimento da aviação possibilitou a projeção de ataques sobre alvos terrestres bem como a ampliação da capacidade de defesa de ataques vindos do mar. O surgimento do porta-aviões e do bombardeiro intercontinental vem ampliar a capacidade de projeção de poder.

O instrumento cibernético consegue reunir as características de permanência do instrumento marítimo e a de instantaneidade do instrumento aéreo além de também apresentar

vantagem ofensiva nas ações.

3.4 O domínio espacial

A dimensão espacial está limitada às funções de comunicação e observação, que se resumem frequentemente à tríade Ver-Escutar-Comunicar (COUTAU-BÉGARIE, 2010)

Em virtude das limitações tecnológicas e econômicas, a chamada “guerra nas estrelas” continua como uma ficção científica.

Segundo Coutau-Bégarie, é graças ao uso dos satélites que a Terra tornou-se, pela primeira vez, um teatro verdadeiramente unificado, no qual um comando centralizado pode controlar em tempo real e contínuo das ações a distâncias elevadas – a dilatação do espaço e a contração do tempo (COUTAU-BÉGARIE, 2010)

Recente como a dimensão espacial, a dimensão cibernética tem cada vez mais avançado no alcance de suas capacidades de ataque. Enquanto as limitações tecnológicas impedem o uso pleno do meio espacial, limitando-se basicamente à tríade “ver-escutar-comunicar”, de característica eminentemente defensiva, a capacidade de realização de ataques no espaço cibernético já é uma realidade.

O número de países que detêm a capacidade de operar no ambiente espacial é limitado. Não há como esconder as posições dos satélites existentes, por ser um ambiente transparente. Porém, a possibilidade de serem atingidos é remota devido às dificuldades tecnológicas existentes no ambiente espacial.

Analogamente à transparência do ambiente espacial, segundo o princípio da visibilidade, as ações no domínio cibernético deixam marcados os seus passos, sendo possível a visualização por terceiros.

Contrariamente ao ambiente espacial, o número de Estados com capacidade de atuar no ambiente cibernético é elevado, com tendências a crescer ainda mais as ações de grupos não estatais.

O ciberespaço é um meio virtual, e como tal muito menos tangível do que terra, mar, ar e espaço, ou o Espectro de Radiofrequência (SCHREIER, 2015). Não se trata de um "habitat" do homem.

Como visto acima, o ciberespaço é um domínio bem particular, com características próprias e que implica em desafios às novas estratégias dos Estados. Para operar com sucesso neste novo domínio, deve-se pensar de forma integrada com todos os demais domínios. Por estar interconectado com diversos recursos que permeiam os domínios tradicionais, praticamente em tempo integral, este domínio requer comando e ações de defesa cibernética em tempo real. A guerra cibernética é mais um componente que reforça o poder combatente das forças contemporâneas.

Com os subsídios abordados até então, passa-se a apresentar, no próximo capítulo, situações de emprego de ataques cibernéticos já observados e a verificar quais as suas influências no planejamento das estratégias dos Estados diante de ações cibernéticas desenvolvidas e/ou esperadas pelos diversos atores do espaço cibernético.

4 INFLUÊNCIAS NO PLANEJAMENTO ESTRATÉGICO

Neste capítulo estudaremos quais as influências da guerra cibernética no planejamento estratégico dos Estados. Para isso, serão vistas, inicialmente, algumas situações observadas em conflitos recentes, aonde foram observadas as primeiras ações cibernéticas no mundo virtual ocorridas em conflitos entre Estados ou a partir de agentes não estatais. Para entender as repercussões e resultados decorrentes de tais ações serão abordadas as estratégias de defesa cibernéticas adotadas pelos Estados Unidos da América, verificando-se a composição e funções dos seus principais órgãos envolvidos na defesa cibernética, bem como os seus objetivos estratégicos.

4.1 O despertar para ações cibernéticas em conflitos

Em abril de 2007, após ações de retiradas de estátuas que representavam os combatentes mortos do Exército Vermelho de praças da Estônia, houve grande indignação de nacionalistas, com protestos na mídia de Moscou e no Legislativo da Federação Russa. A Estônia, que segundo Clarke e Knake (2015), "é um dos países mais conectados do mundo, competindo com a Coreia do Sul, e bem a frente dos Estados Unidos, na utilização de aplicativos de internet e na penetração da banda larga cotidiana", teve vários sites governamentais e privados inundados com inúmeros pedidos de acesso, o que levou ao colapso e à parada de funcionamento deles. A população do país ficou impedida de acessar os seus bancos, mídias e serviços do governo. Observou-se um Ataque Distribuído de Negação de Serviço (DdoS), que foi o maior já visto até então, e que perdurou por semanas. A Estônia atribuiu a origem dos ataques a máquinas localizadas em solo russo. O governo russo negou qualquer ligação com o ataque porém, também não realizou nenhuma cooperação para que os ataques cessassem (CLARKE e KNAKE, 2015).

Tal acontecimento levou a OTAN a criar, em 2008, um centro de defesa cibernética[9] na Estônia (OTAN, 2008).

Em julho de 2008, rebeldes da Ossétia do Sul e Abkházia iniciaram um conflito com a Geórgia, promovendo ataques de mísseis contra aldeias georgianas. A Geórgia reagiu atacando a capital da Ossétia do Sul. Foram iniciados bombardeios à capital da Ossétia do Sul e em 07 de agosto a Geórgia invadiu a região. Tal ação fez com que o exército russo entrasse no conflito e expulsasse o exército georgiano da região. Ao mesmo tempo, guerreiros cibernéticos realizavam ações em alvos na Geórgia a fim de mascarar as ações cinéticas do exército russo, bloqueando acessos de sites do governo, canais de comunicação e sites de notícias internacionais.

O mundo passou a ver um ataque cinético em ação conjunta com o cibernético pela primeira vez.

Mesmo com estruturas sem conectividade à internet ou qualquer outra rede, as instalações para enriquecimento nuclear de urânio de Natanz, no Irã, foram alvo de ataques cibernéticos. Vários governos e organizações no mundo temiam o desenvolvimento de armas nucleares pelo Irã, e a conquista do enriquecimento da matéria-prima seria um passo para atingir tal capacidade. Israel era um dos países mais preocupados com o desenvolvimento da tecnologia bélica nuclear do seu adversário e ensaiava ações para bombardeios às instalações em Natanz. Porém, o que se realizou foi um bombardeio com "*bytes*". Um *worm*[10] de nome *Stuxnet* foi implantado nas instalações daquele país. Tal *worm* tinha como alvo o software do

9 O Centro de Defesa Cibernética Cooperativa de Excelência é uma organização militar internacional OTAN acreditada, com a função de melhorar as capacidades de defesa cibernética cooperativas de países da OTAN e da própria OTAN, melhorando assim a interoperabilidade da Aliança no domínio da defesa cibernética cooperativa. O centro foi criado por sete países: Estónia, Alemanha, Itália, Lituânia, Letónia, República Eslovaca e Espanha, que assinaram o Memorando de Entendimento no dia 14 de Maio de 2008. A Estônia serviu como "start" para a OTAN aprovar a sua primeira política de defesa cibernética em janeiro de 2008, justificada pelo ataques cibernético aos estonianos. Após o ocorrido, a Estônia em conjunto com a OTAN criaram o Centro de Defesa Cibernético Cooperativo OTAN de Excelência (CoE CCD) em Tallinn. (OTAN, 2016)

10 Conforme Quadro 2 do Anexo.

sistema de controle das centrífugas iranianas. Tratou-se de um ataque "zero-day[11]", o qual empregava quatro técnicas diferentes e inovadoras, até então nunca observadas. Foi o ataque mais elaborado realizado no domínio cibernético até aquele momento. Conseguiu-se com isso a quebra de quase mil centrífugas de enriquecimento de urânio iranianas (CLARKE e KNAKE, 2015).

Os três fatos citados acima demonstram grandes acontecimentos que marcaram o modo de operação de defesa em crises, conflitos e guerras. O elemento cibernético passa a ser empregado contra Estados e isto faz com que se torne evidente a necessidade de implementação de medidas e estruturas para se contrapor a isso. O quinto domínio, que foi desenvolvido pelo homem, passa a desempenhar papel significativo na condução das operações militares contra ataques de origem estatal ou não estatal. As estratégias militares devem se readequar a esta nova realidade de forma a prover defesas seguras para os Estados.

4.2 Mudanças no planejamento estratégico

Diante das ameaças cibernéticas, a segurança cibernética deve ter a capacidade de prover a proteção tanto para o setor público estatal como para o setor privado em virtude da dependência do Estado e da sociedade dos serviços disponibilizados nas redes.

Em vista dos ataques cibernéticos contra Estados, observa-se o princípio do efeito cinético descrito por PARKS e DUGGAN (2001), conforme tratado no capítulo 02. Tanto na Estônia como na Geórgia, pode-se observar que as ações cibernéticas geraram efeitos no mundo real. Ao passo que tais ataques não foram dirigidos à destruição física de instalações, mas a sua execução afetou a vontade do inimigo e o seu processo de tomada de decisão, tais ações passaram a desempenhar papel importante nos planejamentos estratégicos dos Estados.

11 Designação atribuída à situação na qual há uma ameaça capaz de explorar uma vulnerabilidade de segurança descoberta em sistemas computacionais e que não teve, ainda, correção disponibilizada pelo desenvolvedor ou fabricante (MD31-M-07, 2014)

Já no ataque às centrífugas de enriquecimento de urânio iranianas, o ataque cibernético gerou destruição de equipamentos daquele país, retardando a capacidade de desenvolvimento de artefatos nucleares.

Conforme descrito no estudo do Centro de Pesquisas Cibernéticas – Sistemas de Controles Industriais (CRC-ICS[12], 2016), "O ciberespaço tornou-se uma zona de guerra orientada pelos governos em todo o confronto do globo pela supremacia digital de um novo e, principalmente, invisível teatro de operações. Inicialmente limitado a criminosos oportunistas, os ataques cibernéticos estão se tornando uma nova arma para os governos que procuram defender a soberania nacional e projetar poder nacional" (CRC-ISC, 2016, tradução nossa).

A segurança no espaço cibernético passou a ser uma das metas da estratégia de segurança nacional a ser atingida pelos Estados, de forma a garantir a segurança do trâmite de mensagens e resguardar o conteúdo sensível de suas organizações. As ameaças de ciberataques às estruturas de bancos, geração e distribuição de energia elétrica, transportes, defesa, etc., põem em risco inúmeros habitantes de um país que se tornou dependente das integrações de tais sistemas.

Diante da necessidade de se estabelecer uma estratégia para atuação no novo domínio, observa-se a posição adotada pelos Estados Unidos da América quanto ao assunto, a fim de se verificar as ações estabelecidas pelo país, tido como um dos melhores preparados no ambiente cibernético.

Segundo LYNN (2010), ficou evidente a escalada crescente das ameaças de guerra cibernéticas para a segurança nacional e economia estadunidenses, "o Pentágono construiu

12 O CRC-ICS é uma organização independente, não para participação nos lucros, pesquisa e informação, centro especializado que trabalha sobre o estado futuro da Física e defesa cibernética e Resiliência. As metas do CRC-ICS são informar indústrias/infraestruturas críticas sobre as rápida evolução das ameaças que enfrentam e as medidas, controles e técnicas que podem ser implementadas para estar preparado para lidar com essas ameaças cibernéticas. Está localizado na Holanda (www.crc-ics.net).

defesas robustas e em camadas ao redor das redes militares. O Pentágono está trabalhando com o Departamento de Segurança Interna para proteger redes governamentais e estruturas críticas e com os mais próximos dos Estados Unidos da América para expandir essas defesas internacionalmente" (LYNN, 2010, tradução nossa).

Do exposto acima, pode-se observar que a estratégia de defesa cibernética dos Estados Unidos da América é pautada em dois pilares: o incremento de estrutura de segurança nas redes militares e de infraestruturas críticas, bem como o desenvolvimento de trabalhos de segurança com outros países para que as defesas sejam incrementadas. A estrutura em camada permite a criação de mais barreiras contra ameaças cibernéticas, o que dificulta o acesso de oponentes às redes que controlam as estruturas vitais do país.

Por uma questão doutrinária, o Pentágono reconheceu formalmente o ciberespaço como um novo domínio de guerra, como os tradicionais terra, mar, ar e espaço (LYNN, 2010).

A necessidade de operar num ambiente construído pelo homem, mas que se tornou extremamente relevante com a evolução tecnológica, levou à busca dos militares por capacitação para poder operar no ciberespaço, tanto na defesa como no ataque e exploração. Isso requer uma estrutura apropriada para que as ações sejam integradas e que os procedimentos sejam padronizados e difundidos.

Como parte do Comando Estratégico estadunidense, o *U.S. Cyber Command* (USCYBERCOM) foi criado em 2009 para concentrar os esforços das demais forças em proteger o espaço cibernético sob um único comando.

A missão do USCYBERCOM é: "planejar, coordenar, integrar, sincronizar e conduzir atividades para: dirigir as operações e defesa de redes específicas do Departamento de Defesa de informação e; prepare-se para, e quando dirigido, conduzir operações militares em todo espectro do ciberespaço de modo a permitir ações em todos os domínios, assegurar a liberdade de ação dos EUA e dos aliados no ciberespaço e negar o mesmo aos nossos

adversários" (EUA, 2015, tradução nossa).

Inicialmente, as Forças Armadas dos EUA possuíam, cada uma, em suas estruturas, unidades de Defesa Cibernética posicionadas em diferentes pontos do território estadunidense. Com a unificação do Comando Cibernético dos EUA as ações de defesa passam a ser ligadas com informações de inteligência necessárias, de forma a antecipar invasões e ataques, tanto de ameaças externas como de ameaças internas. Com o estabelecimento dessa ligação, o Comando Cibernético garante a capacidade de prover segurança nas estruturas internas das forças de uma forma mais dinâmica e com respostas mais ágeis às ameaças, e, consequentemente, implementando maior segurança das estruturas críticas do país.

Segundo OLIVEIRA (2011), a estrutura de coordenação e operação dos órgãos ligados à segurança cibernética dos Estados Unidos da América é composta, dentre outras, das seguintes entidades:

- Conselho Nacional de Segurança (*National Security Council*), no nível político, com as funções de planejar e coordenar atividades ligadas à segurança cibernética;

- Departamento de Defesa (Department of Defense – DoD), no nível estratégico, com as funções de promoção da capacitação e adestramento profissional em segurança e defesa cibernética.

- O Comando Cibernético (*Cyber Command*), chefiado por um general de quatro estrelas, no nível estratégico-operacional, tem como funções, além das já descritas, a coordenar as ações de segurança cibernética entre os órgãos de segurança, dentre eles: os comandos cibernéticos das Forças Armadas, a Agência de Inteligência de Defesa, Agência do Sistema de Informações de Defesa, a Agência de Segurança Nacional, etc.;

- A Agência do Sistema de Informações de Defesa (*Defense Information System Agency*), é encarregada de planejar, instalar, operar e manter, com segurança, a estrutura de

tecnologia da informação e comunicações necessária para apoiar as operações conjuntas das Forças Armadas, líderes nacionais e outras missões envolvendo parcerias nacionais, em todo o espectro de ações militares;

- A Agência de Segurança Nacional (*National Security Agency*-NSA) é a responsável pelas ações de inteligência de sinais dos EUA, tais como coleta, avaliação, integração, e interpretação de dados relativos às emissões eletromagnéticas;

- O Departamento de Segurança Interna (*Department of Homeland Security*) tem como função prover um estado de prontidão nacional diante das ameaças cibernéticas às infraestruturas críticas;

- O Departamento de Educação e o Escritório de Ciência e Tecnologia (*Department of Education* e *Office of Science and Tecnology*) devem promover uma conscientização do cidadão a respeito da ameaça cibernética, em todos os níveis e com diferentes graus de intensidade; e

- O Escritório de Gestão de Pessoal (*Office of Personal Management*) tem como função a promoção da conscientização dos servidores públicos federais, no que tange ao seu papel no combate às ameaças cibernéticas.

Pode-se observar que a preocupação com a segurança e defesa cibernéticas permeia vários níveis de decisão no governo dos EUA. Diante das ameaças impostas pelos diferentes atores no mundo cibernético, é necessária uma verdadeira mobilização do governo e de diversos setores que o compõe na prevenção a tais ameaças.

Em estudos apresentados pelo CRC-ICS (2016) a respeito do quinto domínio de guerra, foram apresentados alguns fatores principais a serem considerados nas Estratégias Nacionais dos países em relação às ameaças cibernéticas existentes, quais sejam: Interrupção de infraestruturas críticas nacionais; Defesa cibernética ou guerra cibernética; e Novos atores e novas tecnologias.

Conforme apresentado por CLARKE e KNAKE (2015), como não é possível a defesa de todos os computadores e sistemas internos dos EUA, a estratégia de defesa cibernética é baseada numa “Tríade Defensiva”, a qual teria três pilares de infraestrutura:

O primeiro pilar é o *backbone* da internet, no qual trafegam grande parte dos dados por fibra ótica através de todo o país e se conectam a outros continentes por cabos submarinos. Porém, o controle de tráfego deste meio implica em dois grandes problemas, um de ordem técnica e outro de ordem política. O de ordem técnica se dá em virtude do retardo causado pelo monitoramento de todo o volume de tráfego que passa pelo tronco em busca de *malwares* ou *scripts* de ataque; o de ordem política é em virtude da privacidade dos dados que passam pelo *backbone* os quais seriam monitorados pelo governo.

O segundo pilar é a rede elétrica segura. Uma falha gerada por ataques cibernéticos às redes de controle de energia elétrica deixaria o país sem acesso à maioria dos serviços de hoje. Os sistemas de backup não atenderiam a todos por muito tempo. Tal problema poderia ser minimizado com a desconexão dos sistemas de controle das redes de geração, transmissão e distribuição de energia elétricas da *internet* e implantação de acesso com necessidade de autenticações. Porém, tais medidas necessitam de regulamentação federal e esbarram na resistência das centenas de empresas do setor em aumentar os seus gastos.

O terceiro pilar é a defesa (Departamento de Defesa). Certamente será alvo de ataques em caso de conflito com o intuito de minimizar e/ou atrasar as reações cinéticas estadunidenses. São necessárias redes seguras, com *softwares* e *hardwares* confiáveis.

Segundo CLARKE e KNAKE (2015), “A parte principal da tríade é a nossa postura declarativa para nações que poderiam pensar em nos atacar por meio do espaço cibernético. Uma postura declarativa é uma afirmação da política e da intenção do governo articulada formalmente”.

O reforço na segurança das estruturas destes três pilares da infraestrutura não

impede a ocorrência dos ataques cibernéticos por outros Estados ou demais agentes, mas impõem dúvidas nos oponentes quanto ao sucesso de tais ataques.

Ainda no ano de 2015, o Pentágono estabeleceu cinco objetivos estratégicos para as missões de defesa cibernética (BARBOSA, 2015):

- criar e manter preparadas forças e capacitações para conduzir operações no espaço cibernético;

- defender a rede de informação do Departamento de Defesa, tornando seguros seus dados e mitigando os riscos nas missões do Pentágono;

- estar preparado para defender o território e os interesses vitais norte-americanos contra ataques cibernéticos de consequência significativa;

- montar e manter opções viáveis de operações de cibernética e planos para utilizar essas opções a fim de controlar escaladas de conflitos e controlar o ambiente de conflito em todas as etapas;

- construir alianças e parcerias internacionais para conter ameaças comuns e para aumentar a segurança e a estabilidade internacionais.

Diante do exposto, tomando-se como base o posicionamento dos Estados Unidos da América, observa-se a necessidade de uma postura estratégica de fortalecer as estruturas internas e capacitar o pessoal envolvido na defesa cibernética para combater as ameaças cibernéticas, tanto numa postura defensiva como ofensiva, bem como ampliar o número de parcerias com outros Estados a fim de incrementar a segurança dos interesses dos Estados.

As ações de defesa no espaço cibernético ocorrem de forma contínua e devem ser sempre levadas em conta, tanto na proteção das infraestruturas críticas como na negação de dados aos oponentes. A necessidade de estruturação dos Estados para se contrapor às ameaças cibernéticas não pode mais ser desconsiderada por qualquer país.

5 CONCLUSÃO

Neste trabalho buscamos identificar as implicações do quinto domínio de guerra, o domínio cibernético, no planejamento das estratégias militares dos Estados nos dias atuais.

Para cumprir tal propósito, buscamos responder as questões apresentadas inicialmente com a pesquisa bibliográfica e documental a respeito desse novo ambiente.

Para isso, iniciamos, com a apresentação dos principais fundamentos do ambiente cibernético, buscando a origem do termo cibernética e os seus desdobramentos, como fontes cibernéticas, espaço cibernético, defesa e segurança cibernética, dentre outros, a fim de se chegar ao conceito do que é a guerra cibernética. Chegamos ao conceito de que GC corresponde às ações no nível operacional e tático desenvolvidas no espaço cibernético a fim de garantir a utilização de forma confiável do espaço cibernético, bem como negar o uso pelos oponentes dos conteúdos e redes num conflito entre Estados. Além disso, verificamos quais as ameaças existentes nesse novo domínio e quais as principais vulnerabilidades apresentadas no mesmo, a fim de se chegar aos principais perigos no Eciber.

Verificamos que os princípios do domínio cibernético são bem específicos, mas podem-se fazer comparações com algumas características observadas nos demais domínios. Com o levantamento desses dados, foi realizada uma comparação com os domínios terrestre, marítimo, aéreo e espacial, tendo como base o "Tratado de Estratégia" de Coutau-Bégarie. Tal comparação se fez por analogias de características de cada domínio, levando-se em conta os princípios do domínio cibernético. Verificamos que o ciberespaço é um meio virtual, e como tal muito menos tangível do que terra, mar, ar e espaço. Não se trata de um habitat do homem, mas, hoje, está presente no cotidiano dele.

Como visto, para operar com sucesso no novo domínio, deve-se pensar de forma integrada com todos os demais domínios. Por estar interconectado com diversos recursos que

permeiam os domínios tradicionais, praticamente em tempo integral, este domínio requer comando e ações de defesa cibernética em tempo real. A guerra cibernética é mais um componente que reforça o poder combatente das forças contemporâneas. Vê-se que não se pode separar a atuação isoladamente por domínios de guerra e que estes devem ser tratados de forma complementar num conflito nos dias atuais.

Diante das ameaças surgidas, faz-se necessária uma nova estruturação dos Estados para se assegurar um mínimo de segurança no espaço cibernético dos Estados. Vê-se que quanto mais aderente às novas tecnologias, ou seja, quanto maior a dependência da informatização, maiores as vulnerabilidades às ameaças do Eciber. No capítulo quatro apresentou-se parte da estrutura de defesa cibernética organizada pelos Estados Unidos da América de forma a minimizar as vulnerabilidades e se contrapor às ameaças cibernéticas. Mas além de fortalecer as estruturas internas, verificamos que se deve capacitar o pessoal envolvido na defesa cibernética de forma a prover maior eficiência no combate a tais ameaças, de forma defensiva e ofensiva, bem como se faz necessária a ampliação do número de parcerias com outros Estados a fim de incrementar a segurança dos interesses dos Estados.

Dessa forma, ao passo que as inovações tecnológicas não param de evoluir, as ações de defesa no espaço cibernético devem ocorrer de forma contínua, desde os tempos de paz, para proverem segurança aos Estados e sociedades, que não podem ser negligenciadas, tanto na proteção das infraestruturas críticas como na negação de dados aos oponentes. A necessidade de estruturação dos Estados para se contrapor às ameaças cibernéticas não pode mais ser desconsiderada por qualquer país no planejamento das estratégias militares.

Diante da relevância do tema, o Brasil também deve contemplar, em suas estratégias, o domínio cibernético.

REFERÊNCIAS

ALMEIDA, José Eduardo Portella, O setor cibernético nas Forças Armadas brasileiras, Desafios Estratégicos para a Segurança e Defesa Cibernética, 1ª Edição, 2011.

BARBOSA, Rubens, EUA: cinco objetivos estratégicos para as missões de defesa cibernética, <http://www.defesanet.com.br/cyberwar/noticia/20151/EUA-cinco-objetivos-estrategicos-para-as-missoes-de-defesa-cibernetica/>, 2015, Acesso em 19 julho 2016.

BELLO, O. A. e Aderbigbe F. M., Cyberwar: The New Frontier of International Warfare, International Journal of Sustainable Development Research, 2015, <http://www.sciencdpublishinggroup.com/j/ijsdr>, Acesso em 20 Julho 2016.

BRASIL. Estado-Maior da Armada. EMA-416: Doutrina de Tecnologia da Informação da Marinha. Rev. 1 Mod. 2, Brasília, 2007.

BRASIL, Doutrina Militar de Defesa Cibernética (MD31_M_07), 2014.

CAHILL, T. P.; ROZINOV, K.; MULÉ, C. Cyber Warfare Peacekeeping. Proceedings of the IEEE Workshop on Information Assurance. West Point, NY, p 100 – 107, 2003. Trabalho apresentado no Seminário de Segurança da Informação da Academia Militar do Estados Unidos da América, 2003, West Point, NY.

CARVALHO, Paulo Sérgio Melo de, O setor cibernético nas Forças Armadas brasileiras, Desafios Estratégicos para a Segurança e Defesa Cibernética, 2011.

CLARKE, Richard A; KNAKE, Robert K. Cyber War: The Next Threat to National Security and What To Do About It. Nova Iorque, Ed. HarperCollins, 2010.

CLARKE, R e KNAKE, R., Guerra Cibernética. Brasport, 2015.

COUTAU-BÉGARIE, Hervé, Tratado de Estratégia, tradução de Brigitte Bentolila de Assis Manso et al. - Rio de Janeiro: Escola de Guerra Naval, 2010.

CROWELL, Richard M., Some Principles of Cyber Warfare, The United States Naval War College, NWC2160, 2014.

CRC-ICS, Cyberspace: the Fifth Domain of War!?, Cyber Research Center – Industrial Control Systems, Critical Infraestructure Protection & Resilience, 2016.

CSIS, Threat Working Group of the CSIS Commission on Cybersecurity for the 44th Presidency. Threats Posed by Internet. CSIS: EUA, 28 out. 2008. <http://csis.org/files/media/csis/pubs/081028_threats_working_group.pdf>. Acesso em: 10 jul 2016.

DUTRA, André Melo Carvalhais, Introdução à Guerra Cibernética: a necessidade de um despertar brasileiro para o assunto, 2007.

EGGER, Máximo Eduardo, A Guerra Cibernética no Nível Estratégico para uma Força Naval

no Mar, Escola de Guerra Naval, 2014.

ESTADOS UNIDOS DA AMÉRICA (EUA), Estratégia Cibernética do Departamento de Defesa para Web, 2015, <http://www.defense.gov/Portals/1/features/2015/0415_cyberstrategy /Final_2015 _DoD_CYBER_STRATEGY_for_web.pdf>. Acesso em: 04 jun 2016.

ESTADOS UNIDOS DA AMÉRICA (EUA), DoD Cyber Strategy, 2015, <http:// www.defense.gov/News/Special-Reports/0415_Cyber-Strategy>. Acesso em: 10 jun 2016.

ESTADOS UNIDOS DA AMÉRICA (EUA), United States Cyber Command, <https://www. Stratcom .mil/factsheets/2/Cyber_Command/> , 2015, Acesso em 26 julho 2016.

ESTADOS UNIDOS DA AMÉRICA (EUA), Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02 (JP 1-02), USA, Revisão 2016.

LACHOW, Irving. Cyber Terrorism: Menace or Myth? In: KRAMER, Franklin D.; STARR, Stuart H.; WENTZ, Larry K. Cyberpower and National Security. 1. ed. Dulles, EUA: National Defense University Press and Potomac Books, 2009. cap. 19, p. 437-464.

LÉVY, Pierre, Cibercultura, Editora 34, 1999.

LIBICKI, Martin C., Ciberspace Is Not a Warfighting Domain, Journal or Law and Policy for the Information Society, Vol. 8,:2, 2012.

LYNN, William, Defending a new domain – The Pentagon´s Ciberstrategy, Foreign Affairs, v. 89, n. 5, p. 97 – 108, Set. 2010.

MANDARINO JR., Raphael. Um estudo sobre a Segurança e Defesa do Espaço Cibernético Brasileiro. Brasília, 2009. p.19.

NUNES, Luiz Artur Rodrigues, Guerra Cibernética: Está a MB preparada para enfrentá-la?, Escola de Guerra Naval, 2010.

O' HANLEY, Richard. Information Security Management Handbook. 2013. ed. New York: Auerbach Publications.

O´HARA, Timothy F., Cyber warfare/Cyber terrorism, U.S. Army War College, 2004.

OLIVEIRA, José Roberto de, O setor cibernético nas Forças Armadas brasileiras, Desafios Estratégicos para a Segurança e Defesa Cibernética, 1ª Edição, 2011.

OTAN, Cooperative Cyber Defese Centre of Excellence, 2008 <https://ccdcoe.org/centre-first-international-military-organization-hosted-estonia. html>, Acesso em 26 julho 2016.

OTAN, OTAN2030-III SiGI, Dossiê República da Estônia, 2015, https://otan2030iiisigi. wordpress.com/2015/07/20/dossie-republica-da-estonia/, Acesso em 26 julho 2016.

PARKS, Raymond C. E DUGGAN, David P., Principles of Cyber-warfare. Proceedings of the

IEEE, Workshop on Information Assurance and Security, 2001.

SCHREIER, Fred, On Cyberwar, DCAF HORIZON 2015 WORKING PAPER No. 7, 2015.

WIENER, Norbert, Cibernética e sociedade – o uso humano dos seres humanos, 4. ed., Cultrix, 1973.

ANEXO

Quadro 1 – Principais vulnerabilidades

VULNERABILIDADES	DESCRIÇÃO
Software	Aplicativos ou software de sistemas podem ter, acidentalmente ou deliberadamente, introduzidas falhas cuja utilização pode subverter a finalidade para a qual o software é projetado.
Hardware	As vulnerabilidades podem ser encontradas no hardware, incluindo microprocessadores, microcontroladores, placas de circuitos, fontes de alimentação, periféricos (impressoras e *scanners)*, dispositivos de armazenamento e equipamentos de comunicação, tais como placas de rede. A adulteração de tais componentes pode secretamente alterar a funcionalidade pretendida do componente ou fornecer oportunidades para introduzir malware.
Linha de junção entre *Software* e *Hardware*	Um exemplo de uma linha pode ser a memória só de leitura de um computador reprogramável (*firmware*) que pode ser de forma abusiva e clandestinamente reprogramado.
Canais de comunicação	Os canais de comunicação entre um sistema ou rede e o mundo "de fora" podem ser usados por um adversário de muitas maneiras. Um adversário pode fingir ser um usuário autorizado do canal, bloqueá-lo, e, portanto, negar a sua utilidade para o seu adversário, ou espionar o canal para obter informações sigilosas do seu adversário.
Configurações	A maioria dos sistemas oferece uma variedade de opções de configuração que os usuários podem definir com base em suas próprias vantagens e desvantagens entre segurança e conveniência. Porque conveniência muitas vezes é mais valorizada do que a segurança, muitos sistemas são - na prática - configurados de forma insegura.
Usuários e operadores	Usuários e operadores autorizados de um sistema ou rede podem ser enganados ou chantageados de modo a cumprir uma ordem de um adversário, ou vender seus serviços.
Provedores de serviços	Muitas instalações de computadores dependem de terceiros para prestar serviços relacionados com a informática, como manutenção ou serviço de Internet. Um adversário pode ser capaz de convencer um provedor de serviços para tomar alguma ação especial em seu nome, como a instalação de software ataque em um computador de destino.

Fonte: SCHREIER (2015)

Quadro 2 – Categorias comuns e principais métodos de ataque cibernético

Ataque	Descrição
Ataques de negação de serviço	
Inundação (*Flooding*)	Envio de dados irrelevantes ou respostas para bloquear um serviço de acolhimento
Inundações sincronizadas/reset	Exploração do cache limitado na pilha de protocolo IP para bloquear conexões
Smurfing	Utilização do sistema de divulgação IP e a falsificação de IP para multiplicar ataques de inundação
Ataques fora de banda/fragmentados	Exploração de vulnerabilidades em implementações de núcleo de protocolo IP
Nurking	Uso de mensagens forjadas para redefinir conexões ativas
Negação de serviço específico	Geração de pedidos que bloqueiam um serviço vulnerável
Ataque de software malicioso	
Backdoor	Recurso do programa que permite a execução remota de comandos arbitrários
Verme (*worm*)	Programa que gera replica e se espalha num computador
Vírus	Código que se auto- reproduz em aplicações existentes
Cavalo de Tróia	Programa dentro de outro programa que executa comandos arbitrários
Exploração de Vulnerabilidades	
Permissão de acesso	Explorando acesso de leitura ou escrita a arquivos de sistema
Força bruta	Tentativas de combinações de senhas padrão ou fracas
Overflow	Transbordamento de dados ou estouro de *buffer*. Escrita de códigos arbitrários para causar falha na memória e ganhar acesso ao sistema
Condições de corrida	Exploração de condições temporárias inseguras em programas
Manipulação de pacote IP	
Falsificação de porta	Uso de portas de origem comummente utilizadas (pontos de entrada) para evitar as regras de filtragem
Fragmentos pequenos	Uso de pequenos pacotes para burlar verificações de protocolo/porta/tamanho de *firewalls*
Falsificação de IP cego	Modificação da fonte IP para acessar os serviços de senha sem uma senha
Falsificação de ID nome-servidor	*Spoofing* cego com números falsos de identificação calculados nome-servidor-caches
Adivinhação de sequência de números	Cálculo de sequência TCP / reconhecimento de número para falsificar um *host* (servidor) confiável
Sequestro de seção remota	Uso de falsificação para interceptar e redirecionar as conexões
Ataque de invasor	
Backdoor daemons	Abertura de porta para acesso remoto futuro

Manipulação de acesso	Remoção de vestígios de ataques ou acessos não autorizados
Cloaking (disfarce)	Substituição de arquivos de sistemas para encobrir acessos não autorizados
Sniffing (farejamento)	Monitoramento de dados de redes para encontrar dados sensíveis
Falsificação *nonblind*	Monitoramento de rede para seqüestrar ativos ou a fazer conexões esquecidas

Fonte: SCHREIER (2015)