ESCOLA DE GUERRA NAVAL

CMG (FN) LUIZ ARTUR RODRIGUES NUNES

GUERRA CIBERNÉTICA: ESTÁ A MB PREPARADA PARA ENFRENTÁ-LA?

Rio de Janeiro

2010

CMG (FN) LUIZ ARTUR RODRIGUES NUNES

GUERRA CIBERNÉTICA: ESTÁ A MB PREPARADA PARA ENFRENTÁ-LA?

Monografia apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso de Política e Estratégia Marítimas.

Orientador: CMG (RM1) Luiz Carlos de Carvalho Roth

Rio de Janeiro
Escola de Guerra Naval
2010

AGRADECIMENTOS

Inicio agradecendo ao meu orientador, CMG (RM1) Luiz Carlos de Carvalho Roth que, além de prover uma orientação precisa e oportuna, que me permitiu lapidar este trabalho, demonstrou total envolvimento, motivando-me ainda mais em sua elaboração.

E termino com um agradecimento especial pela compreensão, apoio e tolerância de minha família em face do prolongado período que dediquei a esta monografia. Sem o amor incondicional de minha esposa Fernanda e de meus filhos este trabalho não seria possível.

RESUMO

O mundo digital de hoje, capaz de reunir, distribuir ou compartilhar informações em quantidades cada vez maiores e tempos menores, encurtou distâncias e permitiu maior fluidez nas relações pessoais, bem como nas relações entre diversas organizações. Os grandes sistemas que gerenciam uma miríade de dados e transações das mais diversas formas de interação eletrônica disponíveis ao homem moderno estão, de algum modo, ao alcance de todos por meio da Internet. O avanço tecnológico que gerou oportunidade de crescimento e desenvolvimento se apresentou, ao mesmo tempo, como uma vulnerabilidade nos tempos atuais. A sociedade, que se tornou cada vez mais dependente desse mundo “on-line”, passou a viver diuturnamente sob a ameaça de um ataque cibernético, que pode se dar com os mais diversos fins, como o roubo de dados ou a corrupção de sistemas, entre outros. Para trazer mais incerteza a este cenário, as formas e métodos de ataque cibernético evoluem em ritmo acelerado, na mesma razão em que evolui a tecnologia de sistemas digitais. Infelizmente, essa vulnerabilidade foi vislumbrada por outros grupos como uma janela de oportunidade. Hoje já não se vive apenas sob ameaça do cibercrime. Grupos de menor poder militar, sejam Estados ou outros organismos, compreenderam o grande valor assimétrico proporcionado por um ataque cibernético. O mundo passa a conviver com a sombra do ciberterrorismo e, no caso dos Estados, com a possibilidade de hostilidades no ciberespaço, ou seja, uma Guerra Cibernética, a qual lança desafios e impõe transformações. A Marinha do Brasil, como uma das primeiras instituições nacionais a fazer uso da Tecnologia da Informação, possui diversos sistemas, tanto administrativos quanto operativos, que podem ser alvo de um ataque cibernético. Destarte, o presente trabalho realiza uma análise sobre a Guerra Cibernética e propõe uma base doutrinária para seu emprego operacional. Ademais, realiza uma análise de como a Marinha do Brasil está estruturada para enfrentá-la e sugere uma série de medidas para aperfeiçoar sua capacidade em relação às novas ameaças e oportunidades oferecidas pelo ciberespaço.

Palavras-chave: Guerra Cibernética, ciberespaço, ataque cibernético, Marinha do Brasil.

ABSTRACT

Today's digital world, able to gather, distribute or share information in increasing quantities and faster, shortened distances and allowed fluidity in personal relationships, as well as in various organizations affairs. The large information systems that manage a myriad of data and transactions from the most diverse forms of electronic interaction available to modern man are somehow at the reach of everyone via the Internet. The technological progress that generated growth and development opportunity presented itself, at the same time, as vulnerability. Society, which has become increasingly dependent on this online world, has continuously lived under the threat of a cyber attack, which can be executed with different purposes, such as data theft or systems corruption, among others. To bring more uncertainty in this scenario, the forms and methods of cyber attack evolve at a good pace, in the same ratio as technology of digital systems does. Unfortunately, this vulnerability was envisioned by other groups as a window of opportunity. Today we no longer live under the threat of cybercrime. Groups of smaller military power, whether States or other bodies, understood the great asymmetric value proportioned by a cyber attack. The world now lives in the shadow of cyberterrorism and, in the case of nation States, with the possibility of hostilities in cyberspace, i.e. a cyberwar, which imposes challenges and requires transformations. The Brazilian Navy, as one of the first national institutions using the Information Technology, has various systems, both administrative and operational, which can be the target of a cyber attack. Hence this monograph performs an analysis about cyberwar and proposes a doctrinal basis for its operational employment. In addition, performs an analysis of how the Brazilian Navy is structured to face it and suggests a series of measures to improve its capacity in respect of the new threats and opportunities posed by the cyberspace.

Keywords: Cyberwar, cyberspace, cyber attack, Brazilian Navy.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

APF –	Administração Pública Federal
CASNAV –	Centro de Análise de Sistemas Navais
CDN –	Conselho de Defesa Nacional
CENTCOM –	U. S. Central Command
CNO –	Comando de Operações Navais Norte-Americano
COC –	Centro de Operações de Combate
CREDEN –	Comissão de Relações Exteriores e Defesa Nacional
CSRECIM –	Centro de Suporte da Rede de Comunicações Integradas da Marinha
CTIM –	Centro de Tecnologia da Informação da Marinha
CYBERFOR –	Força Cibernética da Marinha Norte-Americana
DBM –	Doutrina Básica da Marinha
DCTIM –	Diretoria de Comunicações e Tecnologia da Informação da Marinha
DHS –	Departamento de Segurança Interna Norte-Americano
DISA –	Agencia de Sistemas de Informação de Defesa Norte-Americana
DoD –	Departamento de Defesa Norte-Americano
DSIC –	Departamento de Segurança da Informação e Comunicações
EUA –	Estados Unidos da América
FLTCYBERCOM –	Comando Cibernético da Esquadra da Marinha Norte-Americana
GC –	Guerra Cibernética
GSI-PR –	Gabinete de Segurança Institucional da Presidência da República
IP –	Internet Protocol
JFCC NW –	Joint Functional Component Command for Network Warfare
JTF GNO –	Joint Task Force for Global Network Operations

NSA –	Agencia de Segurança Nacional Norte-Americana
OCDE –	Organização para Cooperação e Desenvolvimento Econômico
OODA –	(Ciclo) Observação – Orientação – Decisão – Ação.
OTAN –	Organização do Tratado do Atlântico Norte
PI –	Possibilidade do Inimigo
RECIM –	Rede de Comunicações Integradas da Marinha
RBN –	Russian Business Network
TI –	Tecnologia da Informação
TO –	Teatro de Operações
TYCOM –	Comando Tipo
USCYBERCOM –	Comando Cibernético dos EUA
USSTRATCOM –	Comando Estratégico dos EUA
VANT –	Veículo aéreo não tripulado

SUMÁRIO

1 INTRODUÇÃO

O mundo, fruto da engenhosidade humana, encontra-se em constante evolução. Sua contínua transformação se processa em diversas áreas, interdependentes, tais como a social, a ambiental e, sobretudo, a tecnológica. Esta última ganha dimensão e se destaca por possuir a capacidade de influenciar e alavancar tanto as demais, como a si própria.

A área militar, uma ramificação da área social, visto que a guerra, em um conceito clausewitiziano, nada mais é do que o enfrentamento violento de vontades, tem, como todas as outras, sua evolução intimamente ligada à evolução tecnológica. Ocorre que, por vezes, as necessidades militares são as grandes fomentadoras da tecnologia, como no caso da criação do primeiro computador eletrônico digital da história – o ENIAC –, cujo projeto teve início em 1943, durante a Segunda Guerra Mundial, com a finalidade de auxiliar o exército norte-americano a realizar cálculos balísticos (TERRA, 2006). Era lançada a semente da era digital.

A partir do ENIAC, com o avanço da eletrônica e a revolução causada pelo uso de materiais semicondutores, permitindo inicialmente a invenção de transistores e, após, sua combinação em circuitos miniaturizados com as mais variadas funções – os famosos CI, ou circuitos integrados –, os computadores deixaram de ser “instalações” (o ENIAC pesava 30 toneladas e ocupava 180 metros quadrados) e passaram a ser equipamentos cada vez menores. Conforme suas dimensões eram reduzidas, sua capacidade computacional, medida por meio do número de operações matemáticas realizadas em um segundo, aumentava – hoje já se fala em cálculos efetuados em nanossegundos.

Evolução natural à sua criação, a ligação de vários computadores com a finalidade de compartilhamento de dados deu origem às redes. Nessa evolução, ocorre uma vez mais a influência do setor militar, com a criação da ARPANET, considerada a precursora da Internet, cujo desenvolvimento foi fomentado pelo Departamento de Defesa norte-americano, no auge

da Guerra Fria, com o propósito de prover um sistema de comunicações independente de uma central de controle e capaz de manter a ligação entre as instalações militares mesmo diante de um ataque localizado (MANDEL, SIMON, LYRA, 1997).

Testemunhou-se, assim, no século passado, o surgimento da era digital, cujo ápice se deu com a popularização dos computadores, que se tornaram pessoais, e o surgimento da Internet no início da década de 1980. A partir de então, o mundo passou por uma verdadeira revolução informacional. O mundo passou a ser digital.

Esse novo mundo digital, capaz de reunir, distribuir ou compartilhar informações em quantidades cada vez maiores e tempos menores, encurtou distâncias e permitiu maior fluidez nas relações pessoais, bem como nas relações entre diversas organizações estatais, paraestatais e privadas, não só no interior dos Estados, mas, principalmente, além-fronteiras. As distâncias físicas foram reduzidas. O mundo como um todo passou a estar a um "clique do mouse" de distância, em alusão à facilidade de acesso à informação. O mundo se tornou mais integrado e o planeta transformou-se em uma aldeia global. Intensifica-se o fenômeno da globalização.

Transações bancárias, comércio eletrônico, tráfego aéreo, relacionamentos institucionais, telefonia e o controle da infraestrutura básica, como luz e água, entre outros, passaram a depender diretamente de recursos computacionais interligados em rede e conectados ao mundo "on-line". Os grandes sistemas que gerenciam uma miríade de dados e transações das mais diversas formas de interação eletrônica disponíveis ao homem moderno estão, de algum modo, ao alcance de todos por meio da Internet. Dados de toda a sorte passam a trafegar pela grande rede, incluindo informações sigilosas pessoais e institucionais.

A facilidade de acesso à informação e aos sistemas que a gerenciam nos dias de hoje acarretou, também, novos riscos relacionados à exposição virtual a que todos se submetem e o homem, fruto de suas imperfeições ético-morais, logo descobriu uma forma de

perpetrar atos ilícitos nesse novo mundo digital. Várias foram as ameaças criadas, tanto à integridade dos diversos sistemas digitais, como à privacidade de indivíduos e corporações. Hoje, tal fato passou a fazer parte do cotidiano da sociedade, conforme nos apresenta Kramer:

> Ataques cibernéticos, em suas várias formas, são um fato da vida moderna. Estados, como a China, têm sido publicamente acusados de sua utilização com o propósito de espionagem e atores não estatais, tais como criminosos e terroristas, possuem, igualmente, capacidades substanciais. Na vida moderna, é condição normal a ocorrência de milhares de intrusões a cada dia, algumas com consequências consideráveis[1] (KRAMER, 2009, p.15, tradução nossa).

O avanço tecnológico que gerou oportunidade de crescimento e desenvolvimento se apresentou, ao mesmo tempo, como uma vulnerabilidade nos tempos atuais. A sociedade, que se tornou cada vez mais dependente desse mundo "on-line", passou a viver diuturnamente sob a ameaça de um ataque cibernético, que pode se dar com os mais diversos fins, como o roubo de dados ou a corrupção de sistemas, entre outros. Para trazer mais incerteza a este cenário, as formas e métodos de ataque cibernético evoluem em ritmo acelerado, na mesma razão em que evolui a tecnologia de sistemas digitais.

Infelizmente, essa vulnerabilidade foi vislumbrada por outros grupos como uma janela de oportunidade. Hoje já não se vive apenas sob a ameaça do cibercrime. Grupos de menor poder militar, sejam Estados ou outros organismos, compreenderam o grande valor assimétrico proporcionado por um ataque cibernético. O mundo passa a conviver com a sombra do ciberterrorismo e, no caso dos Estados, com a possibilidade de hostilidades no ciberespaço, ou seja, uma Guerra Cibernética.

A assimetria reportada acima remete, instintivamente, à ideia de guerra assimétrica, na qual um oponente obtém resultados muito superiores em relação aos meios empregados, sugerindo haver relação entre as guerras cibernética e assimétrica.

A criatura voltou-se contra seu criador. A tecnologia, desta feita, pauta o campo

---

[1] Cyber attacks – hacking of various kinds – are a fact of modern life. Nation-states, such as China, have been publicly accused of hacking for espionage purposes, and nonstate actors, such as criminals and terrorists, likewise have substantial capabilities. The steady state of modern life is that thousands of intrusions occur each day, some with important consequences.

militar que, atento às transformações do mundo hodierno, começa a buscar adaptar-se às modernas ameaças que configuram um novo ambiente de enfrentamento: o espaço cibernético ou ciberespaço.

A Guerra Cibernética lança desafios e impõe transformações. A Marinha do Brasil, como uma das primeiras instituições nacionais a fazer uso da Tecnologia da Informação (TI), possui diversos sistemas, tanto administrativos quanto operativos, que podem ser alvo de um ataque cibernético. Assim, faz-se mister analisar e compreender este novo tipo de embate, cujas consequências poderão facilmente ultrapassar os limites dos sistemas militares, com implicações que poderão afetar toda a sociedade. Destarte, o propósito do presente trabalho é realizar uma análise sobre a Guerra Cibernética e de como a Marinha do Brasil está estruturada para enfrentá-la, de modo a propor medidas para aperfeiçoar sua capacidade em relação às novas ameaças e oportunidades oferecidas pelo ciberespaço.

Portanto, o segundo capítulo abordará os conceitos e fundamentos teóricos ligados ao tema, de modo a prover uma melhor compreensão do que venha a ser Guerra Cibernética. Buscará não só defini-la, mas analisar suas características e as principais ameaças do ciberespaço. O terceiro capítulo complementará os conceitos apresentados, aprofundando o tema com relação ao nível de condução operacional da Guerra Cibernética. Ambos os capítulos têm como função servir de arcabouço teórico doutrinário, de modo a subsidiar a futura construção de uma Doutrina de Guerra Cibernética para a Marinha do Brasil. Complementando-os, o Apêndice A apresenta um breve relato sobre o emprego real da Guerra Cibernética em operações militares.

No quarto capítulo serão apresentadas outras considerações sobre a Guerra Cibernética, de modo a conhecer alguns modelos de organização, políticas e fundamentos doutrinários, mormente as dificuldades enfrentadas para adoção e eventuais deficiências existentes nesses modelos, além de aspectos jurídicos pertinentes ao tema e sua interação com

as Relações Internacionais, cujo conhecimento contribuirá para uma percepção global sobre a Guerra Cibernética e à implementação de uma estrutura para a Marinha do Brasil.

Em sequência, ao longo do quinto capítulo, utilizando-se dos conceitos e conhecimentos obtidos nos capítulos precedentes, será realizada uma análise sobre a situação atual da Marinha do Brasil com relação à Guerra Cibernética, em que serão abordados o preparo de pessoal, a identificação de vulnerabilidades, a estrutura organizacional e a identificação de estruturas nacionais enquadrantes. Terá como meta apresentar as propostas do autor visando à correção de possíveis vulnerabilidades identificadas ao longo do trabalho e ao aperfeiçoamento da capacidade da Marinha do Brasil no que diz respeito à Guerra Cibernética.

Por fim, será apresentada uma breve conclusão com o fito de sintetizar os aspectos mais importantes do presente estudo, de forma a consolidar a contribuição do autor para a conscientização das ameaças apresentadas pela Guerra Cibernética e para o aperfeiçoamento da estrutura de Guerra Cibernética da Marinha do Brasil.

2 ELEMENTOS CONCEITUAIS DE GUERRA CIBERNÉTICA

2.1 Definição de Guerra Cibernética

Atualmente, muito se fala em Guerra Cibernética. A par das ameaças existentes no ciberespaço e da consequência dos atos de diversos atores, particularmente o aumento da ocorrência de ataques cibernéticos, o termo tende a se vulgarizar. A crescente presença dos Estados no espaço cibernético e as atividades dos atores não estatais, incluindo entidades comerciais, criminosos cibernéticos e grupos terroristas, tornam o ciberespaço um ambiente cada vez mais complexo. Tais ações combinam crime, espionagem e ações militares de modo que, frequentemente, para o usuário do ciberespaço, esses elementos são indistinguíveis. Todo e qualquer incidente de ordem digital ocorrido em um computador, uma rede de computadores e/ou nos sistemas de Tecnologia da Informação (TI) nela residentes tem sido tratado, equivocadamente no entender deste autor, como Guerra Cibernética.

Em verdade, o único ponto em que há concordância entre vários autores e peritos no assunto, é que não existe uniformidade de conceito acerca do que vem a ser Guerra Cibernética, o mesmo ocorrendo com o termo ciberespaço.

> O aumento da dependência mundial na tecnologia da informação aliada à crescente sofisticação dos ataques cibernéticos tem motivado especialistas a examinar a noção de Guerra Cibernética. Ainda não existe concordância entre especialistas de segurança cibernética, tecnologia e relações internacionais sobre que tipo de ações, se é que há algum, constitui a guerra no ciberespaço[2] (MCAFEE, 2009, p. 8, tradução nossa).

Assim, como marco para o presente trabalho, deve-se entender Guerra Cibernética como sendo o conflito travado entre dois ou mais Estados no ciberespaço. Destarte, as demais atividades desenvolvidas por atores não estatais, com potencial de dano à informação no

---

[2]The world's increasing reliance on information technology coupled with the growing sophistication of cyber attackers has prompted experts to examine the notion of "cyber war." Yet there is disagreement among cyber security, technology and international relations experts as to what kind of actions, if any, constitute warfare in cyberspace.

ciberespaço, devem ser tratadas como incidentes cibernéticos ou, usando um termo também já generalizado, como ataques cibernéticos.

Apesar de simples, a definição apresentada acima é suficiente para diferenciar a Guerra Cibernética dos demais incidentes que diuturnamente ocorrem no ciberespaço e estabelecer uma linguagem de uso comum. No entanto, visando à formação de um arcabouço teórico doutrinário, faz-se mister aprofundar tal conceito.

Ao observar, inicialmente, as definições disponíveis em publicações militares brasileiras, obtém-se diferentes definições para Guerra Cibernética. Para o Ministério da Defesa:

> Guerra Cibernética é o conjunto de ações para uso ofensivo e defensivo de informações e sistemas de informações para negar, explorar, corromper ou destruir valores do adversário baseados em informações, sistemas de informação e redes de computadores. Estas ações são elaboradas para obtenção de vantagens tanto na área militar quanto na área civil (BRASIL, 2007b, p. 123).

Já a Marinha do Brasil oferece dois conceitos referentes ao tema em estudo. O primeiro, encontrado na Doutrina Básica da Marinha (DBM), diz respeito às Ações de Guerra da Informação[3], assim conceituadas:

> São aquelas que envolvem as ferramentas disponíveis no nível da informática e telemática para desestabilizar os sistemas operacionais e de comunicações do inimigo e, também, para possibilitar a defesa dos referidos sistemas amigos. Essas ações visam, principalmente, destruir, desativar, retardar ou confundir os sistemas de comando e controle pelo ataque deliberado à lógica operacional do sistema inimigo ou, no caso de sistema amigo, garantir a sua operacionalidade e confiabilidade (BRASIL, 2002, p. 4-21).

A segunda definição de interesse encontra-se em uma publicação de caráter doutrinário, porém com enfoque mais técnico do que operacional, a Doutrina de Tecnologia da Informação da Marinha, que, por ser mais atual que a DBM, faz referência direta à Guerra Cibernética, assim definida:

> São ações ofensivas e defensivas destinadas a explorar, danificar ou destruir informações digitais, ou negar o acesso às suas informações. Tais ações utilizam-se de sistemas de informação e de redes de computadores (BRASIL, 2007a, p. 1-3).

---

[3] Há autores que consideram que as Operações de Informação constituem algo maior, englobando a Guerra Cibernética. Contudo, como se pode depreender da definição apresentada, não é o caso.

Ao analisar as definições apresentadas acima, pode-se dizer que são similares: ambas incluem ações ofensivas e defensivas; possuem propósitos comuns; e incluem o ciberespaço como seu ambiente operacional. Entretanto, essas definições não cobrem efetivamente todo o escopo necessário ao perfeito entendimento. Inicialmente, a **exploração**, que não é citada no conceito expresso pela DBM, é colocada como um fim, enquanto, na verdade, trata-se de uma ação de caráter preparatório ligada intimamente à atividade de inteligência:

> [...] a noção de que um guerreiro cibernético pode ser designado a atacar um alvo qualquer imediatamente pode não ser plenamente viável. Os sistemas informatizados são os mesmos em todo o mundo, assim, a habilidade para invadi-lo adquirida em um lugar deveria funcionar em outro. Entretanto, esse princípio subestima a quantidade de inteligência necessária para a preparação de um ataque bem sucedido. O sucesso na Guerra Cibernética operacional dependerá, em larga escala, do conhecimento sobre as vulnerabilidades do alvo [4] (LIBICKI, 2009a, p. 154, tradução nossa).

Deve ser considerado, também, que a exploração será utilizada em apoio ao esforço de inteligência como um todo, não estando ligada apenas às ações preparatórias do ataque cibernético. Ademais, diferentemente do que ocorre com as ações ofensivas, o entendimento atual com respeito às ações de inteligência no ciberespaço não as classifica como um ato de agressão (ESTADOS UNIDOS DA AMÉRICA, 2010d; LEWIS, 2010).

Outro ponto a destacar nas definições em lide diz respeito à falta de alusão ao propósito das ações defensivas. Assim, de modo a cobrir as lacunas apontadas, este autor apresenta as seguintes definições[5]:

a) Ações Ofensivas de Guerra Cibernética: 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;

---

[4][…] (the) notion that cyberwarriors can be assigned to any target on the fly may not be entirely the case. Computer systems are the same the world over, so hacking skills learned in one place should work just as well in another. But this tenet understates how much intelligence preparation is required for a successful attack. Success at operational cyberwar depends to a great extent on knowing where the target is vulnerable.

[5] Tais definições foram apresentadas pelo autor no curso dos trabalhos do I Workshop de Guerra Cibernética da Marinha do Brasil.

b) Ações Defensivas de Guerra Cibernética: 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;

c) Ações de Exploração de Guerra Cibernética: 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.

Ao sintetizar os conceitos acima elencados, chega-se, por fim, à definição que se propõe para Guerra Cibernética: *são as ações ofensivas, defensivas e de exploração realizadas por meio de sistemas de informação e de redes de computadores, destinadas a interromper, negar, corromper, destruir ou acessar as informações contidas nos sistemas de TI inimigos e, ao mesmo tempo, garantir o uso continuado e a inviolabilidade dos nossos sistemas de TI.*

2.2 Ciberespaço – o ambiente operacional da Guerra Cibernética

Recorrendo à mais simples definição de Guerra Cibernética – guerra travada no espaço cibernético – percebe-se o vínculo intrínseco desta com o ciberespaço, que se caracteriza como seu ambiente operacional, somando-se aos domínios[6] marítimo, terrestre, aéreo e espacial. Tal assertiva vem ganhando força entre as principais forças militares mundiais e estudiosos no assunto, como Kuehl (2009) e Rattray (2009). Impende, pois, buscar compreender o que vem a ser esse ambiente de grande complexidade.

Lugar comum em relação às definições relacionadas ao adjetivo “cibernético”, o

[6] O termo “domínio” é usado com a mesma conotação de “ambiente”, sendo empregado pelo autor de modo a evitar a repetição excessiva do termo original ao longo do texto.

ciberespaço – espaço cibernético – carece de unanimidade em relação ao seu significado. Kramer (2009) relata a existência de vinte e oito diferentes definições para o termo. Tal indefinição acarreta problemas, sendo o maior deles a incapacidade de se comunicar efetivamente:

> A dificuldade do estabelecimento de uma comunicação efetiva é manifestada em debates sobre os mais simples termos, como, por exemplo, ciberespaço, nos quais as definições chave são controversas. Coerentemente à natureza complexa do problema, não é surpresa que os esforços no sentido de caracterizar o espaço cibernético foram infrutíferos. Atualmente, não existe consenso sobre uma taxonomia que possibilite uma teoria abrangente sobre o tema[7] (STARR, 2009, p. 45, tradução nossa).

Destarte, torna-se necessário o uso de uma linguagem comum, não só no âmbito da Marinha do Brasil, como no seio de todo o Ministério da Defesa. Como visto na seção anterior, a definição apresentada por aquele ministério carece de aperfeiçoamento, fato este que oferece oportunidade à Marinha do Brasil, credenciada por seu pioneirismo na área cibernética, para apresentar sugestões e pautar o tema, reforçando ainda mais sua posição como detentora da expertise cibernética. Tem-se, pois, que buscar uma definição ao termo.

Como ponto de partida, tem-se ciberespaço definido como:

> [...] um domínio global que faz parte do ambiente da informação, cujo traço único e distintivo é formado pelo uso dos espectros eletrônico e eletromagnético para criar, armazenar, modificar, permutar e explorar a informação em redes interconectadas e interdependentes por meio do uso de tecnologias da informação e comunicações[8] (KUEHL, 2009, p. 28, tradução nossa).

Em que pese ser a mais completa e atual entre as definições pesquisadas, ela carece de um aspecto que este autor considera como fundamental para diferenciar o ciberespaço do domínio eletromagnético, como a própria definição pode sugerir. Para tanto, há que se recorrer à noção de que "o melhor marco referencial para sua definição é que o

---

[7] This difficulty (for the stakeholders to communicate effectively) is manifested in debates about the most basic of terms (for example, cyberspace) where key definitions are still contentious. Consistent with the heterogeneous nature of the problem, it is not surprising that prior efforts to characterize this space have not been successful. At present, there is no agreed taxonomy to support a comprehensive theory.

[8] Cyberspace is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies.

ciberespaço está relacionado à operação em rede, à transferência bidirecional de informações ao invés de sua transmissão, na qual a informação é transferida em apenas um sentido[9]" (LIBICKI, 2009b, p. 276, tradução nossa). Ou seja, a interatividade é critério *sine qua non*, sem a qual não há ciberespaço.

Segundo Libicki (2009b), é a interatividade do ciberespaço que permite maior agilidade e capacidade de comando e controle, possibilitando, entre outras vantagens, aumentar o ritmo de execução do ciclo OODA[10], efeito esse que não seria possível caso o único resultado do uso militar do ciberespaço fosse o recebimento de maior quantidade de informação em um menor período de tempo.

Dessa forma, chega-se a uma proposta de definição, onde *ciberespaço é a parcela integrante do ambiente da informação caracterizada pelo uso interativo dos espectros eletrônico e eletromagnético para criar, armazenar, modificar, trocar e explorar a informação, por meio de tecnologias da informação e comunicações em redes interdependentes e interconectadas*.

Deve-se observar, entretanto, que, conforme observado por diversos autores – Kramer (2009); Rattray (2009); Kuehl (2009); Parks e Duggan (2001); Boleng, Schweitzer e Gibson (2008); entre outros – o ciberespaço é um ambiente artificial, construído pelo homem e sujeito a constantes modificações, sendo, portanto, imperfeito.

O ciberespaço é, assim, um ambiente onde novas capacidades e habilidades são desenvolvidas, as quais são por ele incorporadas e assim por diante, como em um moto contínuo, em que sua retroalimentação o regenera tornando-o algo novo em sua composição. Logo, o ciberespaço não se trata de um domínio coerente e encontra-se em constante evolução, por meio da contribuição independente e descentralizada de diversos atores, cada

---

[9] The best defining marker is that cyberspace is about networking, the two-way transfer of information, in contrast to broadcasting, in which information is transferred only one way.
[10] Ver glossário.

qual com sua própria capacidade e motivação.

Daí resulta que, segundo Parks e Duggan (2001), tal artificialidade confere uma dose de instabilidade ao ciberespaço: software e hardware falham e programas geram resultados inesperados. Como consequência, na Guerra Cibernética, deve-se observar que os resultados dos ataques nem sempre serão os mesmos e que haverá a possibilidade de alteração de desempenho dos meios cibernéticos, além de que a "geografia" do próprio ambiente estará em mutação, como alerta Rattray (2009).

Ao se caracterizar o ciberespaço como um ambiente operacional, vêm à mente, instintivamente, comparações com os demais ambientes operacionais. A esse respeito, a de mais fácil compreensão relaciona-se aos pontos focais, locais geográficos que apresentam determinada restrição, possibilitando seu controle e favorecendo àquele que o efetivamente controla, de acordo com as teorias geopolíticas do poder. Rattray (2009) considera que os ativos da infraestrutura física que permitem a comunicação no ciberespaço, portanto pontos de passagem obrigatória ao fluxo de dados, são os novos pontos focais do século XXI. Destacam-se entre esses ativos a infraestrutura de cabos óticos submarinos, os satélites de comunicações e os principais pontos de interconexão das grandes redes globais. Entretanto, deve-se observar que, enquanto no mundo físico os pontos focais tendem a ser imutáveis, eles podem mudar com rapidez no ciberespaço, como, por exemplo, a localização de centros de dados (STARR, 2009).

O ciberespaço possui duas características próprias que, unidas, o diferenciam de todos os outros ambientes operacionais. A primeira diz respeito à inexistência de fronteiras no ciberespaço, o que vale dizer que não existem distâncias, ou seja, uma ação executada no Brasil pode ter consequências em qualquer parte do globo. Sendo assim, não há necessidade de contiguidade física entre oponentes para execução de ações de Guerra Cibernética. A segunda refere-se ao fato de que sempre haverá um usuário conectado ao ciberespaço.

Parks e Duggan (2001) defendem que, em face de seu caráter artificial, o ciberespaço é construído e controlado pelo homem e suas ferramentas, não existindo, portanto, parte do ciberespaço que não esteja sob o controle de alguém. Tal conceito é corroborado por Lewis (2009), que considera que o ciberespaço não é o alto-mar, existindo um controle soberano sobre cada uma das redes que poderão ser utilizadas por uma arma cibernética para atingir seu alvo – mesmo que esse controle ocorra por apenas alguns milissegundos. Segundo Lewis, "não existe momento em que um conjunto de bits que se move de um computador a outro não esteja situado em uma rede que pertença a alguém e que esteja fisicamente localizada em um Estado soberano[11]" (LEWIS, 2009, tradução nossa).

Entretanto, há limites a esse controle, não se aplicando, portanto, aos conceitos militares de supremacia e de superioridade, pois, conforme expressado por Rattray (2009), não se pode controlar o ciberespaço no mesmo nível em que se controlam os ambientes terrestre, marítimo, aéreo e, até mesmo, espacial. Tal assertiva é confirmada por Kramer (2009), o qual sugere que se tal capacidade fosse possível os Estados Unidos já teriam se livrado dos ataques cibernéticos a que estão sujeitos diuturnamente.

Tomando-se em conta que, em termos militares, o ciberespaço é um ambiente operacional, deve-se ter em mente que vários aspectos de uma força serão diretamente influenciados, como a organização, o adestramento e o equipamento de combatentes cibernéticos (STARR, 2009) e sua importância às operações navais pode ser traduzida nas palavras do Almirante Gary Roughead, atual Comandante de Operações Navais da Marinha norte-americana:

> O ciberespaço é um domínio único, que possui um conjunto de desafios totalmente diferente. Para operar com sucesso nesse novo domínio a Marinha deve, em primeiro lugar, pensar diferente sobre operações no ciberespaço. Esse mundo viaja à velocidade da luz e requer ações de comando e controle em tempo real. Nós

[11] There is no moment when a collection of bits moving from one computer to another is not actually on a network that someone owns and that is physically located in a sovereign state.

> devemos assegurar alinhamento e integração perfeitos com as operações da Esquadra[12] (ESTADOS UNIDOS DA AMÉRICA, 2010c, tradução nossa).

2.3 As ameaças no ciberespaço

As ameaças atuais no ciberespaço não são provenientes apenas dos entusiastas da computação que invadem sistemas de TI em busca do conhecimento ou da notoriedade, que são genericamente chamados de *hackers*, mas de oponentes muito mais dedicados. Hoje, as ameaças mais perigosas vêm de criminosos, terroristas e Estados competidores. Estes oponentes não estão interessados em fama ou em satisfazer o ego, em vez disso, são motivados por interesses políticos, ideológicos e financeiros muito mais poderosos (BOLENG; SCHWEITZER; GIBSON, 2008).

Portanto, faz-se necessário conhecer os principais atores que habitam o ciberespaço, de modo a compreender o grau de ameaça apresentado por cada um deles: os Estados, o terrorismo cibernético, o ativismo cibernético, o hacker e o elemento interno.

O **Estado** é o principal ator presente no espaço cibernético em função de sua insuperável capacidade de recursos, com relação aos demais atores analisados, que lhe propiciará grande capacidade de atuar nesse ambiente. É, atualmente, o único ator com capacidade de desenvolver ferramentas para ataques com elevado grau de sofisticação, em função dos elevados custos envolvidos para tal. A principal ameaça apresentada pelos Estados é a Guerra Cibernética que, em uma concepção clausewitiziana, envolveria o uso de ataques cibernéticos com uma motivação política. Entretanto, a maior incidência de atuação dos Estados nos dias de hoje são as ações de exploração, havendo vários indícios de que China e

---

[12] Cyberspace is a unique domain with a totally different set of challenges. To operate successfully in this newly defined domain the Navy must first think differently about cyberspace operations. This world travels at the speed of light and requires real time command and control. We must ensure seamless alignment and integration with fleet operations.

Rússia têm se aproveitado do anonimato possibilitado pelo ciberespaço para executar tais ações, que são usualmente tratadas como espionagem cibernética.

Um exemplo típico é a rede de espionagem chamada *GhostNet*, que se infiltrou em 1.295 computadores, de 103 diferentes países, dos quais aproximadamente 30% pertenciam a setores diplomáticos, políticos, econômicos e militares considerados como alvos de alto valor. As sofisticadas técnicas utilizadas por aqueles que controlavam a *GhostNet* levam a crer no envolvimento de um Estado. Em que pese a análise forense computacional[13] realizada indicar como ponto de controle alguns endereços IP[14] localizados na Ilha de Hainan, sede das instalações de inteligência de sinais chinesa Lingshui e do Terceiro Departamento Técnico do Exército chinês, não há como apontar o envolvimento do governo chinês com absoluta certeza (INFORMATION WARFARE MONITOR, 2009).

Segundo dados constantes do relatório elaborado pela Comissão de Segurança Cibernética para o presidente norte-americano Barack Obama, em 2007 foi reportada a existência de 108 países com organizações dedicadas ao ataque cibernético e em busca de segredos industriais (CSIS, 2008).

Outra presença no ciberespaço e fonte de grande preocupação aos Estados, o **terrorismo cibernético** pode ser definido como o ataque cibernético, ou sua ameaça, com o fim de intimidar ou coagir governos ou sociedades de modo a alcançar objetivos políticos, religiosos ou ideológicos (LACHOW, 2009). Entretanto, como alertado por Denning (2006), para alcançar sua finalidade, tais ataques deverão possuir efeitos que provoquem medo e caos comparáveis aos produzidos pelos ataques físicos do terrorismo. Lachow (2009) observa, ainda, que o terrorismo cibernético se refere ao meio utilizado para a execução dos ataques e não à natureza dos alvos.

Segundo Lewis (2010), não há ocorrência de terrorismo produzido por meio de

---

[13] Ver glossário.
[14] Internet Protocol. Ver glossário.

ataques cibernéticos, pois seriam necessários ataques com elevado grau de dificuldade e sofisticação, cuja capacidade somente poucos Estados possuem. Contudo, conforme os grupos terroristas crescem em termos de sofisticação, eles estarão se aperfeiçoando em suas habilidades para utilizar o ataque cibernético (CSIS, 2008), o que remete à ameaça de que poderá chegar o dia em que o terrorismo cibernético se torne uma realidade. O problema é definir quando isso ocorrerá.

Outro ponto que merece atenção diz respeito à utilização de mercenários para preencher a lacuna tecnológica dos grupos terroristas na atualidade.

> [...] ainda que os terroristas não possuam a capacidade de produzir essas habilidades, eles certamente podem comprá-las. Existe um número incontável de mercenários cibernéticos em todo o mundo – hackers sofisticados, com treinamento avançado e desejosos em oferecer seus serviços pelo preço certo[15] (HABIGER, 2010, p. 15, tradução nossa).

Em que pese esses mercenários não possuírem conhecimento e/ou recursos necessários aos ataques mais sofisticados, o patrocínio de grupos terroristas poderá abreviar o tempo necessário à aquisição das capacidades necessárias, tornando sua ameaça cada vez mais próxima.

Atualmente, as organizações terroristas têm usado o ciberespaço em atividades de apoio às suas ações, como recrutamento, levantamento de fundos, propaganda, treinamento e planejamento. Como exemplo, tem-se que o planejamento, a coordenação e o financiamento dos ataques terroristas de 11 de setembro de 2001 ao *World Trade Center*, conduzidos por membros da *AL-Qaeda*, foram realizados com o auxílio da Internet (KRAMER; STARR; WENTZ, 2009; WRONA, 2005).

Outro fato que se pôde observar é que as tecnologias da informação e comunicações permitiram que terroristas alcançassem sua audiência-alvo, mesmo ao estarem impedidos de usar outras mídias, como ocorrido quando as emissoras de televisão dos Estados

---

[15] [...] even if the world's terrorists are unable to breed these skills, they can certainly buy them. There are untold numbers of cybermercenaries around the world – sophisticated hackers with advanced training who would be willing to offer their services for the right price.

Unidos da América (EUA) não transmitiram as decapitações de reféns americanos e aliados durante a operação *Iraqi Freedom*, ocasião em que os terroristas garantiram a disponibilidade de tais vídeos para sua audiência em vários sítios da web (WRONA, 2005).

O **ativismo cibernético**, conhecido também por seu nome em inglês – *hacktivism*, é entendido como a manipulação da informação digital a fim de promover uma mudança política ou social. Segundo Lachow (2009), os atos de ativismo cibernético buscam resultados similares aos obtidos pelo ativismo regular ou atos de desobediência civil, por meio de ataques de negação de serviço[16] ou protestos efetuados via alteração de sítios da Internet.

As intrusões digitais destinadas a massagear o ego e a consolidar reputações de jovens aficionados pela computação são casos raros. Hoje, a Internet é uma máquina de gerar lucro para grupos criminosos organizados, dedicados e muito hábeis no uso da tecnologia da informação. Ela provê anonimato e alcance mundial, o que permite ao **cibercrime** operar em qualquer lugar no mundo e esconder seus rastros através de um labirinto de computadores comprometidos por malware[17].

Segundo Muttick (2008), nos últimos anos, a motivação financeira tem desempenhado um papel cada vez maior no aumento de produção de malware. Existem grupos de hackers mercenários vendendo suas habilidades e produtos na Internet.

De acordo com a Organização para Cooperação e Desenvolvimento Econômico (OCDE), um em cada três computadores está comprometido (controlado remotamente por outra pessoa que não seja seu usuário habitual). É muito importante compreender que os agentes das ameaças não precisam saber como construir seus programas para invasão de sistemas, assim como ninguém precisa saber como construir uma arma para usá-la. Hoje a Internet se transformou em um imenso bazar de armas onde qualquer pessoa pode adquirir

---

[16] Ver glossário.
[17] Ver glossário.

uma arma cibernética, ou baixá-la (download) gratuitamente e usá-la onde e como desejar (CSIS, 2008).

Uma das maiores redes de crime cibernético é a *Russian Business Network* (RBN). Ela oferece uma completa infraestrutura para atividades criminosas. É um serviço provedor de cibercrime que oferece ferramentas de ataque cibernético e serviços de cibermercenários. Estimativas dão conta de que a RBN e seus clientes foram responsáveis por 60% do cibercrime no ano de 2006 (CSIS, 2008). Chegou-se ao ponto em que, para causar algum dano a um sistema de TI ou à informação nele residente, o conhecimento deixou de ser necessário e bastará apenas possuir recursos financeiros.

Amplamente empregado para nomear a qualquer um que venha a perpetrar uma atividade ilícita no ciberespaço, o termo **hacker**, na verdade, está relacionado à invasão de sistemas, o que de certo modo ampara a assertiva inicial. Segundo Boyd (2009), o conceito do hacker moderno está ligado à exploração de erros e/ou brechas existentes no código do sistema operacional de um computador, de modo a permitir o acesso ao sistema e sua consequente manipulação. Como a invasão de sistemas, por si só, não se presta à caracterização do hacker, pois todos os atores já abordados a utilizam, o que irá distingui-lo dos demais atores será sua motivação, que está relacionada, na maioria das vezes, à satisfação de seu ego (LACHOW, 2009).

Boyd (2009) apresenta uma categorização realizada pelos próprios hackers, com base em seus propósitos. Aqueles cuja ação é voltada à realização de testes nos sistemas de modo a aprimorar a segurança se autodenominam de *White Hat Hackers*, enquanto os que realizam ações criminosas são chamados de *Black Hat Hackers*.

Última ameaça a ser analisada, o **elemento interno** recai na categoria de introdução de uma vulnerabilidade operacionalmente por meio de ação humana direta, ou seja, por meio físico. O acesso pode se dar durante o projeto, desenvolvimento, teste,

empacotamento, distribuição, operação ou manutenção de componentes do sistema (CSIS, 2008).

O mais sério ataque que se tem conhecimento a uma infraestrutura crítica já ocorrido até os dias de hoje foi realizado por um elemento interno. No caso, em 2000, um ex-funcionário de uma companhia de tratamento de esgotos na Austrália, insatisfeito por não ter conseguido a promoção almejada e munido do software e conhecimento do sistema que ele próprio instalou, invadiu o sistema de controle de bombas da companhia, causando o derramamento de milhões de litros de esgoto *in natura* (DENNING, 2006).

Logo, a ameaça interna, origem da maioria dos ataques conhecidos, não pode ser ignorada. Sua existência deve ser considerada, pois um elemento interno está em uma posição particularmente favorável, uma vez que uma das fases mais difíceis de um ataque cibernético já foi superada: o acesso ao sistema, e medidas de segurança orgânica deverão ser implementadas de modo a negar a oportunidade ou, no mínimo, reduzir sua chance de sucesso.

2.4 A participação direta de civis em conflitos cibernéticos

O envolvimento de civis em conflitos contra Estados, seja em apoio a ações de seu país, seja de forma autônoma, tem sido um fenômeno frequente no ciberespaço. Muitas dessas participações não se enquadram no conceito de Guerra Cibernética, do mesmo modo que não existe guerra de um Estado contra um grupo não estatal ou vice-versa.

Algumas dessas ações consistem de ativismo cibernético e, considerando que ainda não houve a ocorrência de atos de terrorismo cibernético, os demais ataques empreendidos por grupos não militares a Estados carecem de uma definição.

Como exemplo, podem ser citados três casos que tiveram repercussão na mídia

mundial: o ataque cibernético à Estônia, em 2007; o conflito Rússia – Geórgia, em 2008; e por ocasião da ofensiva israelense na faixa de Gaza, em 2009. Em todos esses, os ataques cibernéticos foram realizados por elementos civis independentes, com o uso de *botnets*[18] controladas por hackers e coordenados por meio de fóruns civis na Internet. Os códigos para ataque utilizados por esses "exércitos" de hackers civis podem ter sido fornecidos por algum órgão do Estado, além de que há a possibilidade de que eles tenham recebido algum tipo de orientação estatal, mas não há evidência em documentos ostensivos que comprovem a tese de envolvimento de algum Estado nos incidentes citados acima. Atualmente, os Estados têm sido relutantes em assumir abertamente a participação em ataques cibernéticos, seja por questões políticas, seja para não confirmar a posse de capacidades cibernéticas. Tal atitude tem colocado esses grupos de hackers civis na linha de frente do conflito cibernético. Nesses três casos houve a participação de civis em ambos os lados da contenda (BOYD, 2009; INFORMATION WARFARE MONITOR, 2009).

Aparentemente, as campanhas cibernéticas desse gênero podem vir a tomar rumo próprio. Mesmo que um Estado venha a insuflar uma campanha por meio de influência direta ou por meio da leniência com relação à imposição de sanções e repressão às atividades ilícitas no ciberespaço, essas campanhas são inerentemente caóticas e seus resultados não podem ser previstos ou controlados. Entretanto, alguns governos aparentam se beneficiar desse tipo de situação e atuam como santuários. O benefício de que desfrutam é a possibilidade de uso de hackers e, até mesmo, de criminosos cibernéticos como uma força substituta, irregulares que podem se engajar em espionagem ou atacar oponentes por ordem do governo, enquanto proporcionam aos Estados um grau de negação de autoria dessas ações bastante plausível (INFORMATION WARFARE MONITOR, 2009; LEWIS, 2009).

O patrocínio de ações de hackers civis por Estados, mesmo que velado, embora

---

[18] Ver glossário.

permita uma grande capacidade de mobilização, possui deficiências. Inicialmente, seria por demais arriscado o Estado fornecer armas cibernéticas, uma vez que favoreceria a indicação de seu envolvimento, pois o desenvolvimento de armas mais sofisticadas é uma atividade que, normalmente, somente o Estado poderia executar. Haveria, também, a possibilidade de, no futuro, tais armas serem utilizadas contra o próprio Estado que as forneceu (a história está repleta de exemplos do fornecimento de armas convencionais a grupos de insurgentes que se voltaram contra seus patrocinadores iniciais, como no caso dos Mujahidin, no Afeganistão). Ademais, há o risco de infiltração do inimigo, que passaria a ter acesso às capacidades desenvolvidas e disponibilizadas aos voluntários. Logo, a melhor opção aos Estados recai sobre o simples fomento às ações, que deverão ser desencadeadas com as ferramentas que esses grupos já possuírem.

Outro ponto a ser considerado é que não há como os Estados controlarem as ações desses grupos, o que poderá levar a resultados inesperados e contrários aos interesses do Estado patrocinador. Logo, a mobilização de hackers requer a assunção de riscos, mesmo que seja realizada de forma pontual e em pequena escala, que demandará a adoção de medidas de segurança e de contrainteligência de modo a mitigá-los.

Cumpre salientar que cada país deve aceitar o fato de que seus cidadãos hackers podem causar incidentes internacionais contrários aos seus interesses. Durante o confronto que ficou conhecido como *Interfada*, em 2000, que representa o primeiro conflito político no qual ambos os lados combateram de modo organizado por meio da Internet, Israel foi arrastado para um conflito cibernético por ações de seus próprios hackers e não por uma decisão governamental. O primeiro ataque partiu de jovens israelenses que sabotaram a página do grupo *Hesbollah* na Internet. Em retaliação, vários sítios de grupos extremistas islâmicos incitaram seus usuários a atacar sítios israelenses e disponibilizaram as ferramentas (programas de computador) e instruções para a realização dos ataques. Hackers voluntários ao

movimento pró-Palestina atacaram sítios do governo, forças militares e de instituições financeiras de Israel, que, à época, não estava preparado para travar uma Guerra Cibernética e era mais vulnerável que seu adversário (ALLEN; DEMCHAK, 2004; WRONA, 2005).

Há um fato peculiar sobre a *Interfada* que reflete uma vulnerabilidade a que o Brasil pode ser exposto e conduzi-lo a um conflito semelhante: a participação de grupos de hackers brasileiros atuando em ambos os lados – palestino e israelense. A atuação brasileira também se fez presente, ao lado dos EUA, durante o conflito EUA x China, em 2000, em que hackers de ambos os países se confrontaram motivados pela colisão de uma aeronave americana EP-3 e uma aeronave comercial chinesa. Em ambos os casos a adesão dos grupos brasileiros foi voluntária e motivada, aparentemente, por questões político-ideológicas. Tal fato leva a crer que incidentes de igual natureza poderão ocorrer no futuro e envolver, de forma não intencional, o Estado brasileiro em um conflito causado por iniciativa de grupos de hackers nacionais. (ALLEN; DEMCHAK, 2004; BOYD, 2009).

2.5 Características da Guerra Cibernética

Ao longo da pesquisa realizada, foi possível identificar onze características que conformam a Guerra Cibernética: *necessidade de surpresa, necessidade de vulnerabilidades a explorar, dificuldade de realização do segundo ataque, efeito temporário dos ataques cibernéticos, limitação de danos físicos, uso dual das ferramentas, limitação do controle, vantagem do ataque sobre a defesa, existência de incertezas na Guerra Cibernética, presença de não combatentes no ciberespaço e o paradoxo cibernético*, as quais serão expostas a seguir.

Necessidade de surpresa – Diferentemente da guerra convencional, conforme observam Parks e Duggan (2001), a necessidade de surpresa é fundamental. Tal conceito é

corroborado por Libicki (2009a), que argumenta que o sucesso do ataque cibernético baseia-se na surpresa obtida da diferença entre aquilo que o inimigo espera e aquilo que ele realmente obtém, sendo esse o motivo pelo qual a Guerra Cibernética é perfeitamente adequada para um ataque surpresa e uma péssima escolha para ataques repetidos, pois será muito difícil surpreender um defensor mais que uma vez com o mesmo método. A partir desse conceito, tem-se que a surpresa de um ataque cibernético será obtida ao explorar uma vulnerabilidade do inimigo que ele desconheça ou, mesmo, que considere não poder ser utilizada por seus oponentes.

Dos conceitos aqui apresentados decorrem as duas próximas características.

Necessidade de vulnerabilidades a explorar – Conforme expresso por Boyd (2009), as ferramentas da Guerra Cibernética não podem ser empregadas contra um alvo desprovido de vulnerabilidades, entendidas aqui como sendo os pontos fracos dos sistemas de TI, tanto em termos de software como de hardware, que permitam a invasão e/ou o comprometimento da integridade, disponibilidade, confidencialidade ou autenticidade desses sistemas e/ou das informações nele contidas. Libicki (2009a) expressa o mesmo entendimento ao estabelecer a necessidade de que o inimigo possua sistemas de TI em rede para que a Guerra Cibernética tenha sentido, aduzindo que é isso que a difere das outras formas de combate.

Deve-se ter em mente que nem todos os sistemas possuem as mesmas vulnerabilidades e que estas são mutáveis, ou seja, ao mesmo tempo em que algumas são reparadas, outras estarão surgindo. Tem-se, consequentemente, a necessidade por um grande esforço de inteligência cibernética de modo a descobrir as vulnerabilidades existentes nos sistemas de TI inimigos.

Ocorre que para explorar as vulnerabilidades existentes, há necessidade que as mesmas estejam acessíveis por meio do ciberespaço. Logo, como argumenta Boyd (2009), a

falta de conectividade é por si só uma medida de defesa na Guerra Cibernética. Entretanto, na visão deste autor, trata-se de uma medida extrema de defesa, pois a desconexão de um sistema poderá trazer graves entraves, inclusive às próprias operações militares que porventura estejam em curso. Sua utilização dependerá de criteriosa análise e deverá constar, necessariamente, de regras de comportamento operativo para a defesa.

Dificuldade de realização do segundo ataque – Conforme os sistemas são atacados, suas vulnerabilidades são reveladas e reparadas, ou de algum modo contornadas. Isso faz com que, causando o robustecimento dos sistemas alvo, cada ataque torne o subsequente mais difícil. Libicki (2009a) argumenta que, como os ataques cibernéticos necessitam de vulnerabilidades a serem exploradas, quanto mais rápidos e pesados forem os ataques, menor será o número de vulnerabilidades remanescentes e mais rápido diminuirá o potencial para novos ataques.

Faz-se mister ressaltar que mesmo os alvos não atacados deverão estar melhor defendidos, uma vez que o inimigo já conhecerá os métodos de ataque e vulnerabilidades exploradas e espera-se que todos os seus sistemas recebam as correções necessárias e as medidas de defesa sejam incrementadas.

Assim, na opinião de Libicki (2009a), um dos grandes desafios na condução de uma campanha cibernética é assegurar que o primeiro ataque não crie condições tais que venham a enfraquecer os efeitos de um segundo ataque.

Efeito temporário dos ataques cibernéticos – Libicki argumenta que "os efeitos diretos dos ataques cibernéticos mais perversos, *se descobertos*, podem ser revertidos em questão de horas, ou, na pior das hipóteses, semanas[19]" (2009a, p. 140, tradução nossa).

Há que se observar que essa característica pressupõe uma condicionante, que é a descoberta do ataque, cuja possibilidade estará ligada diretamente ao tipo de ataque realizado

---

[19] The direct effects of the most fiendish cyberattacks, *if discovered*, can often be reversed within hours or, at most, weeks.

– uma ação ofensiva ou de exploração, sendo esta última mais difícil de ser descoberta – e, principalmente, ao nível de preparo técnico do alvo, tanto em termos de recursos humanos como em recursos materiais. Entretanto, não se deve desprezar a capacidade de qualquer inimigo possuidor de sistemas de TI, pois sua própria posse implica na existência de habilidades e capacidades cibernéticas, além do fato de que, quanto maior o valor do alvo, maiores serão as suas defesas.

Logo, essa é uma importante característica, pois representa para o atacante uma limitação temporal para os efeitos obtidos por um ataque cibernético, o que terá influência direta no planejamento das Ações Ofensivas de Guerra Cibernética, principalmente no que concerne à coordenação com as ações convencionais que, de algum modo, dependam dos efeitos produzidos pelo ataque cibernético.

Limitação de danos físicos – As armas cibernéticas não são decisivas. Um ataque cibernético não irá ganhar um conflito sozinho, particularmente contra um oponente de maior poder. Lewis (2009) explica que é por isso que, até hoje, nenhum ataque cibernético que ultrapassasse o nível da espionagem ou crime tenha sido lançado fora do escopo de um conflito armado.

Libicki (2009a) é categórico ao afirmar que um ataque cibernético não é capaz de desarmar o inimigo, muito menos causar qualquer tipo de destruição.

Atualmente, os efeitos físicos que podem ser alcançados por um ataque cibernético são incomparáveis aos obtidos por um ataque convencional. Entretanto, já se advoga a possibilidade de que ataques mais sofisticados possam afetar sistemas físicos. Há, inclusive, um experimento realizado em uma usina elétrica pelo Departamento de Energia norte-americano que comprovou tal possibilidade, conforme citado por James Lewis, diretor do *Center for Strategic and International Studies*, em entrevista à rede CBS:

> Se você se infiltrar no sistema de controle, então poderá instruir a máquina a se destruir. E isso foi realizado no teste chamado Aurora. Se você tivesse assistido ao vídeo, é algo interessante, porque a máquina começa a estremecer. Você sabe, está

> claramente vibrando. E a fumaça começa a sair. Ela se autodestrói[20] (CBS, 2009, tradução nossa).

Entretanto, tais ataques terão custos mais elevados em termos de preparação de recursos humanos, assim como para o desenvolvimento das ferramentas de ataque (DENNING, 2009). Tal assertiva é confirmada por Kenneth Geers, representante dos EUA no *Cooperative Cyber Defense Centre of Excellence*, na Estônia, que declara: "ataques cibernéticos que visam a manipular as infraestruturas críticas (de um adversário) necessitariam de maior tempo, esforço e habilidade do que o simples roubo de dados[21]" (TENNANT, 2009, tradução nossa).

Dessa forma, tem-se que, diferentemente do senso comum de que a Guerra Cibernética apresenta um baixo custo de entrada, há que se ter em conta que tal assertiva somente é válida para ataques simples e que para a elaboração de ataques mais sofisticados serão necessários investimentos que não estão disponíveis ao hacker comum e que demandarão investimento específico por parte das forças militares que almejam capacitação na Guerra Cibernética, como é o caso da Marinha do Brasil.

Uso dual das ferramentas – Na Guerra Cibernética, as mesmas ferramentas são usadas tanto por quem ataca como por quem defende. O atacante usa ferramentas de varredura de vulnerabilidades na busca por oportunidades de exploração como parte de um ataque. Por outro lado, o defensor utiliza a mesma ferramenta para localizar pontos fracos em seus sistemas. Ferramentas de captura de pacotes de dados têm origem na necessidade de diagnosticar problemas na rede por parte de seus administradores. Para o atacante são usadas para ações de exploração (PARKS; DUGGAN, 2001).

---

[20] If you can hack into that control system, you can instruct the machine to tear itself apart. And that's what the Aurora test was. And if you've seen the video, it's kind of interesting, 'cause (sic) the machine starts to shudder. You know, it's clearly shaking. And smoke starts to come out. It destroys itself.

[21] Cyberattacks which seek to manipulate [an adversary's] critical infrastructures would take more time, effort and expertise than mere data theft.

Limitação do controle – Como visto na seção sobre o ciberespaço, não há possibilidade de obtenção de supremacia em uma Guerra Cibernética. Há, porém, uma capacidade de controle limitada à parcela do ciberespaço criada por cada uma das forças oponentes, ou seja, os equipamentos e o software que cada um possui. Parks e Duggan (2001) definem que tal controle limita-se, frequentemente, ao perímetro físico das forças e que raramente se estenderá além da interface com a infraestrutura de comunicações. Ou seja, ambas as forças controlarão uma pequena parcela do ciberespaço que cada uma utiliza. Assim, surge a possibilidade para que uma das forças assuma o controle da parcela do ciberespaço utilizada por seu oponente. Tal fato traz à luz o conceito de Superioridade de Informação, apresentado no seminário realizado pela Organização do Tratado do Atlântico Norte (OTAN) sobre Guerra Cibernética e que vem a ser "a capacidade de coletar, processar e disseminar um fluxo ininterrupto de informação, enquanto explora ou nega ao inimigo a capacidade de fazer o mesmo[22]" (AZAROV; DODONOV, 2006, p.7, tradução nossa). Esse mesmo conceito é também utilizado pelas forças canadenses e norte-americanas (CANADÁ, 1998; ESTADOS UNIDOS DA AMÉRICA, 2006). Outro conceito que se adéqua, também apresentado no mesmo seminário, é o de Superioridade de Controle, definido como sendo a capacidade tecnológica potencial de interceptar os sistemas de controle de informação inimigos, ou seja, de assumir o seu controle.

Há, no entanto, outra questão que deve ser ressaltada. Em que pese o controle exercido por cada uma das partes, haverá sempre lugar no ciberespaço para ambas as forças operarem. Não há supremacia e, uma vez que a Guerra Cibernética é assimétrica por excelência, haverá a possibilidade de ambas as forças se manterem, simultânea e mutuamente, privadas do uso de suas próprias redes e sistemas.

---

[22] The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary´s ability to do the same.

Vantagem do ataque sobre a defesa – Como explica Starr (2009), na Guerra Cibernética a ofensiva possui a vantagem em relação à defesa, devido à existência de grande quantidade de alvos potenciais, o que dificulta priorizar e defender alvos específicos. Isso significa que o defensor deverá bloquear todas as vias de acesso de um ataque cibernético, enquanto ao atacante bastará explorar uma única vulnerabilidade para ter sucesso (CONTI; SURDU, 2009).

Nas palavras de John Arquilla, analista de defesa do *Naval Postgraduate School*, "há algo que influencia o equilíbrio entre a ofensiva e a defesa. Eu penso que existe vantagem para o lado atacante. Os defensores, na melhor das hipóteses, podem limitar os danos[23]" (ARQUILLA, 2003, tradução nossa).

Assim, tem-se que a Guerra Cibernética oferece substancial vantagem àquele que desfere o primeiro ataque, desde que com ele se possa degradar a capacidade de comando e controle inimiga e, por conseguinte, obter ganhos no ritmo de execução do ciclo OODA, que retroalimentará a vantagem no ambiente cibernético e proporcionará vantagem, também, à execução das ações convencionais.

Existência de incertezas na Guerra Cibernética – A "névoa da guerra" também está presente no ciberespaço. Conforme apresentado por Lewis (2009), o conflito cibernético é um problema estratégico novo e complexo e a incerteza é o seu aspecto mais proeminente – com relação à atribuição de sua autoria, ao escopo dos danos colaterais e ao efeito potencial sobre o alvo de um ataque cibernético.

O ciberespaço possibilita o anonimato. Identidades são facilmente ocultadas ou forjadas no ciberespaço e um oponente ardiloso irá, com toda certeza, fazer com que se pareça que outros foram os responsáveis por um ataque – a fonte de um ataque, em uma primeira interação, recairá sobre usuários inocentes e que desconhecem o que está se passando. O

---

[23] There is something in the balance between offense and defense. I think there is somewhat of an advantage on the offensive side. Defenses, at best, can hope to limit damage.

trabalho forense poderá, eventualmente, revelar a fonte do ataque, mas um oponente capacitado, como as forças militares, será capaz de operar clandestinamente e com um alto grau de negação de sua autoria (LEWIS, 2009).

É óbvio que no transcurso das ações de uma Guerra Cibernética propriamente dita este problema não ocorrerá, mas, ainda assim, a possibilidade de anonimato é de extrema importância às atividades de inteligência, ou seja, às ações de exploração levadas a cabo antes do início do conflito. Habiger (2010) apresenta outra implicação, que é a plausibilidade de um terceiro ator operar clandestinamente no curso de uma Guerra Cibernética em que não esteja diretamente envolvido.

A interconectividade no ciberespaço torna difícil a predição do dano colateral. Não há fronteiras limitando o tráfego de dados. Uma simples linha de código de uma ferramenta utilizada em uma ação de exploração, ofensiva ou mesmo defensiva poderá causar danos não intencionais a sistemas situados a grandes distâncias geográficas do alvo verdadeiro. Na verdade, segundo Lewis (2009), a incerteza envolve tanto os possíveis danos às redes de terceiros, conectadas ou dependentes da rede alvo, quanto os efeitos indesejados sobre o próprio alvo.

Agravando as incertezas, tem-se que a pouca experiência histórica não permite a perfeita compreensão desse fenômeno de rápida evolução que é a Guerra Cibernética (RATTRAY, 2009).

Presença de não combatentes no ciberespaço – O domínio no qual a Guerra Cibernética se desenvolve, o ciberespaço, tem uma característica peculiar em relação às operações militares convencionais: nesse domínio não estarão presentes apenas combatentes, mas, também, civis não combatentes de todas as nacionalidades – não apenas aqueles pertencentes às nações envolvidas no conflito –, envolvendo elementos das nações aliadas e

neutras. E não se deve esquecer que, a qualquer tempo, sempre haverá alguém presente no ciberespaço.

Assim, a Guerra Cibernética não será um conflito limpo, uma vez que os combatentes estarão conectados a não combatentes e um ataque a um alvo legítimo poderá, inevitavelmente, causar danos a um partido neutro. Em termos operacionais, tal fato implica que o sucesso de um ataque cibernético necessitará de um profundo conhecimento acerca das redes alvo e de suas conexões a outras redes, de modo a aumentar a probabilidade de que apenas os alvos planejados sejam afetados (LEWIS, 2009).

Paradoxo cibernético – Esta característica, a qual este autor denomina de paradoxo cibernético, reside na raiz da Guerra Cibernética, uma vez que tal paradoxo decorre dos avanços tecnológicos que, simultaneamente, conferem poder e expõem ao perigo aqueles que os utilizam.

O poder advém das capacidades conferidas pelos sistemas de TI que, em termos militares, podem ser considerados como fatores multiplicadores do poder de combate ao aumentar exponencialmente a capacidade de comando e controle.

Já o perigo é fruto das vulnerabilidades existentes em todo e qualquer sistema de TI, as quais poderão ser exploradas por potenciais inimigos. Logo, quanto maior o índice de informatização de uma sociedade, maior será sua vulnerabilidade em relação à Guerra Cibernética.

Assim, o crescimento da dependência na tecnologia fez com que a Guerra Cibernética se transformasse em uma faca de dois gumes: aqueles mais capazes de empreendê-la são, ao mesmo tempo, os mais vulneráveis a ela (WRONA, 2005).

2.6 Emprego da Guerra Cibernética

A primeira noção que se deve ter é a de que o propósito mais amplo da Guerra Cibernética é a obtenção de efeitos que ultrapassem o domínio cibernético, ou, em outras palavras, de que forma a Guerra Cibernética contribuirá para a condução das operações militares ou, mesmo, para com outras formas de expressão do poder nacional. Conforme destacado por Parks e Duggan (2001), a Guerra Cibernética não possui sentido a não ser que afete algo ou alguém no mundo não cibernético. Scott (2008), por sua vez, é mais explícito e defende que a Guerra Cibernética deve ser usada para se obter efeitos nos domínios físico e cognitivo da guerra.

O domínio físico incorpora toda a infraestrutura que suporta uma força e onde os combates convencionais são travados. Nele se encontram os sensores, o hardware dos sistemas de TI e as plataformas de armas. Já por domínio cognitivo entende-se ser aquele onde se encontram as percepções e a compreensão sobre o significado da informação, bem como os modelos mentais, preconceitos e valores que influenciam como a informação é interpretada e compreendida (ALBERTS; HAYES, 2003).

Tendo-se em mente, então, que a Guerra Cibernética não é um fim em si mesma, deve-se compreender que seu principal emprego não é a destruição da capacidade de controle inimiga, mas a obtenção da superioridade de controle. Assim, os sistemas de informação serão atacados no ciberespaço não só com o propósito de destruição da informação, mas, principalmente, para assumir o controle da infraestrutura de informação, descapacitando o inimigo e agindo diretamente em seu processo de tomada de decisão (AZAROV; DODONOV, 2006). Como observado por Libicki (2009a), é relativamente fácil constatar que um sistema não está em operação, enquanto, por outro lado, é muito difícil perceber que ele funciona, mas está gerando informação incorreta ou tomando decisões erradas. Deve-se notar

que, mesmo que o inimigo descubra que seu sistema de TI está sendo manipulado e venha a tomar as devidas contramedidas, sua confiabilidade estará irremediavelmente abalada.

Outro papel para a Guerra Cibernética é a criação de informação, de pouco significado operacional, de modo a sobrecarregar os sistemas inimigos, interferindo em seu ciclo decisório, tornando-o mais lento em função da grande quantidade de informação a processar. Deve-se enfatizar que não se trata de um ataque de negação de serviço, uma vez que o propósito aqui não é a interrupção do sistema, mas sua degradação. A informação também poderá ser manipulada de modo a gerar uma diversão tática ou operacional. Cabe, em ambos os casos, a recomendação de Libicki (2009a) de que a informação não necessita ser falsa, apenas sem valor.

A Guerra Cibernética pode, ainda, ser empregada para enfraquecer a capacidade inimiga, obtendo-se uma vantagem temporária, mas potencialmente decisiva. Isso pode ocorrer durante o conflito, de modo a facilitar uma ação militar convencional, ou mesmo antes de seu início:

> […] um ataque cibernético pode ser usado, também, para romper as defesas da nação ou distrair nossos líderes nacionais antes de um ataque convencional ou estratégico mais tradicional. Muitos líderes militares acreditam que tais ataques cibernéticos pré-ofensiva constituem o uso mais efetivo das capacidades ofensivas cibernéticas[24] (HABIGER, 2010, p. 16, tradução nossa).

Alguns analistas consideram os ataques cibernéticos sofridos pela Geórgia, em 2008, previamente à invasão russa, como um exemplo real dessa forma de emprego.

Cumpre ressaltar que esta seção não buscou esgotar o assunto, mas apresentar alguns balizamentos da Guerra Cibernética, que deverão ser considerados no seu preparo e planejamento.

---

[24] [...] a cyberattack could also be used to disrupt our nation's defenses or distract our national leaders in advance of a more traditional conventional or strategic attack. Many military leaders actually believe that such a disruptive cyber pre offensive is the most effective use of offensive cyber capabilities.

3 O NÍVEL OPERACIONAL DA GUERRA CIBERNÉTICA

Conforme já observado, a Guerra Cibernética não é um fim em si mesma, ou seja, ela por si só não pode ganhar uma guerra. Tem-se, portanto, que, como afirmado por Libicki (2009a), ela será somente uma função de apoio aos outros elementos da guerra. Tal assertiva é corroborada pelas palavras do General Keith Alexander, Comandante do *U.S. Cyber Command*: "eu acredito que a guerra cibernética não existiria por e para si mesma, mas como parte de uma campanha militar maior[25]" (NAKASHIMA, 2010, tradução nossa).

Desse modo, tem-se que a capacidade cibernética deverá ser integrada à campanha militar, como parte do plano de emprego das armas de apoio, ou seja, deverá ser considerada como um sistema de armas em apoio às operações convencionais.

3.1 Ações de Exploração de Guerra Cibernética

Consideradas como a expressão máxima da inteligência na era da informação, as ações de exploração ocorrem diariamente e envolvem a varredura de sistemas de TI em busca de vulnerabilidades de modo a permitir o aceso não autorizado a tais sistemas para a coleta de informação ou como medida de preparação para um futuro ataque.

Seu emprego como forma de inteligência é usualmente tratado como espionagem cibernética, mormente por não ser realizada apenas por Estados, mas, também, por outros atores. Especialistas consideram que tais atividades não constituem um ato de guerra, e, portanto, não justificam o emprego de força militar como resposta. Dessa forma, os Estados devem tratar a espionagem política e militar no ciberespaço da mesma maneira que a tratam no mundo físico (LEWIS, 2010).

---

[25] I believe it (cyberwar) would not exist in and of itself, but as part of a larger military campaign.

O entendimento expresso acima é corroborado pelo Senado norte-americano e constou de preâmbulo a um dos questionamentos formulados ao General Keith Alexander, por ocasião de sua indicação para o Comando do *U.S. Cyber Command* (ESTADOS UNIDOS DA AMÉRICA, 2010d).

Feitas essas considerações, convém ressaltar que a Guerra Cibernética é uma atividade com grande dependência das ações de inteligência cibernética, o que faz com que as ações de exploração tenham maior relevância em seu contexto, pois as ações ofensivas dependem diretamente dos resultados obtidos por elas, bem como as ações defensivas, que utilizarão as informações obtidas de modo a orientar a adoção de medidas adicionais de defesa cibernética.

Desse modo, tem-se que os esforços de inteligência cibernética, a serem executados por meio de ações de exploração da Guerra Cibernética, serão voltados, precipuamente, às seguintes informações (SCOTT, 2008):

a) Capacidade de ataque cibernético;
b) Iniciativas e programas de Guerra Cibernética e de desenvolvimento de armas cibernéticas;
c) Detalhes sobre programas de pesquisa e desenvolvimento de TI;
d) Projeto e implementação de códigos maliciosos – malware;
e) Esforços de inteligência sobre nossas redes.

Além desses, deve-se ter atenção aos seguintes esforços de caráter operacional:

a) Arquitetura das redes;
b) Sistemas de TI administrativos, com ênfase nos sistemas relacionados às organizações logísticas, à estrutura de comunicações administrativas e aos centros de pesquisa e desenvolvimento;
c) Sistemas de TI operativos;

d) Como os sistemas de TI interagem, ou seja, como a informação produzida por um sistema é tratada por outro e até que ponto esse último dependerá dessa informação;

e) Que sistemas de TI afetam o processo decisório;

f) Localização de vulnerabilidades existentes nos sistemas de TI.

Deve-se ter em conta que as necessidades apresentadas acima requerem a cooperação de outras agências de inteligência, uma vez que tais esforços não devem ser unicamente baseados na inteligência cibernética, em que pese ser esta a sua principal fonte.

Outro ponto a ser considerado refere-se à necessidade de que as ações de exploração com vista a atender aos esforços de inteligência elencados acima sejam desencadeadas desde os tempos de paz.

Embora os ataques cibernéticos executados no decorrer de operações militares não necessitem ser furtivos, uma vez que o próprio anonimato já não existirá, não existem dúvidas de que é mais fácil realizar toda sua preparação previamente ao desenrolar do conflito, uma vez que após sua deflagração as defesas já estarão fortalecidas. A preparação para o ataque se inicia com as ações de exploração, que poderão implantar os códigos necessários, cujos acionamentos ocorrerão oportunamente. Além disso, eventualmente as ações de exploração em andamento poderão evoluir elas próprias para uma ação ofensiva (LIBICKI, 2009a).

Como já demonstrado, a Guerra Cibernética, assim como as ações militares em geral, está impregnada de inteligência. Geralmente, a preparação do campo de batalha cibernético requer maior esforço em termos de recursos financeiros, tempo e pessoal do que a operação propriamente dita, com relações variando de 10:1 a 100:1 consideradas como muito plausíveis. A busca por vulnerabilidades é tarefa extremamente específica, em termos das vulnerabilidades em si, dos sistemas pesquisados e das ferramentas a serem desenvolvidas para o posterior ataque, e deverá ser orientada pelos esforços já descritos (LIBICKI, 2009a).

A dualidade do emprego das ações de exploração causa um problema adicional para a análise das intrusões detectadas em nossas redes. Inicialmente, deve-se ter em mente que a diferença entre uma ação de exploração e uma ação ofensiva reside apenas no "digitar de algumas teclas". A mobilização de forças no mundo físico é algo facilmente detectável, enquanto no ciberespaço tal visibilidade não é possível. Portanto, resta ao analista a dúvida se a ocorrência de intrusões em nossas redes por parte de outros Estados é somente um ato de inteligência ou se, além disso, há uma preparação para ações ofensivas em andamento, que poderá indicar a iminente deflagração de um conflito (MACAFEE, 2009).

Destarte, faz-se necessário que os resultados obtidos, ou seja, os dados e informações coletados, sejam divulgados por meio dos canais de inteligência. A difusão das informações contribuirá, assim, para melhor avaliar a situação e, por conseguinte, para a validação e o aperfeiçoamento da consciência situacional[26]. O isolamento da informação, ou seja, a compartimentação excessiva, é um grave erro operacional. A experiência vivida por forças norte-americanas aponta para a ocorrência desse tipo de erro, que deve ser evitado ao máximo (ERBACHER, 2005).

3.2 Ações Ofensivas de Guerra Cibernética

As características de efeito temporário dos ataques cibernéticos e de dificuldade de realização do segundo ataque requerem que seu uso seja realizado com parcimônia e precisão. Deve-se ter em mente que uma vez que uma arma cibernética seja utilizada, presume-se que o inimigo descobrirá a vulnerabilidade e adotará medidas para mitigá-la, tornando a arma obsoleta. Sustentando a posição apresentada por este autor, Libicki (2009a) comenta que os ataques cibernéticos são mais eficientes quando usados para ações pontuais,

---

[26] Ver glossário.

por meio de um único ataque, do que em longas campanhas.

Assim, uma vez que um ataque surpresa seja desencadeado, vale dizer o primeiro ataque, o mais provável é que a Guerra Cibernética deixe de ser tratada como uma arma de emprego geral e seja poupada para uso em ocasiões especiais e alvos de grande valor militar, os quais deverão ser cuidadosamente pesquisados em busca de vulnerabilidades incomuns ou que possam ser criadas por meio de engenharia social ou outras operações de inteligência (COLARIK; JANCZEWSKI, 2008).

A execução do ataque propriamente dito requer a observação de algumas precauções. Inicialmente deve-se evitar a criação de picos de atividade na rede a ser atacada, de modo a não alertar o inimigo quanto às ações que serão desencadeadas. Além disso, faz-se necessário coordenar as ações de exploração em curso, principalmente no caso de utilização das mesmas técnicas de infiltração nos sistemas inimigos. Por fim, deve-se evitar a utilização de muitas ferramentas com códigos semelhantes, pois a detecção de uma delas poderá levar à neutralização das demais (LIBICKI, 2009a).

Como parâmetro para o planejamento e emprego das ações ofensivas, faz-se necessário conhecer as fases que compõem um ataque cibernético. Para tanto, sugere-se a utilização do modelo proposto por Colarik e Janczewski (2008), composto de 5 fases:

a) Reconhecimento, o qual visa a identificar as vulnerabilidades existentes nos sistemas inimigos;
b) Penetração, ou seja, a invasão do sistema inimigo, sem o que há pouco a ser feito, a não ser interromper a disponibilidade ou o acesso ao sistema;
c) Identificação dos recursos internos e aumento do privilégio de acesso a áreas restritas de maior valor;
d) Execução de alterações no sistema, de acordo com o efeito desejado do ataque, ou extração de dados e/ou informação;

e) A última fase consiste na remoção de evidências da invasão e de ações posteriores executadas no sistema, que inclui, entre outras ações, a edição ou deleção de seus arquivos de *log* (registros de ocorrência).

3.3 Ações Defensivas de Guerra Cibernética

Com as operações militares cada vez mais dependentes de sistemas de TI, seja em seus sistemas de armas, seja em suas estruturas de comando e controle, as ações defensivas tornam-se de fundamental importância para a condução das operações nos modernos Teatros de Operação[27] (TO).

> Forças militares que são altamente dependentes de sistemas de informação seguros poderão ser completamente incapacitadas, da mesma forma que seriam se não possuíssem apoio de aviação no século XX. Se não possuírem um bom sistema defensivo cibernético no século XXI, estarão completamente desamparadas[28] (ARQUILLA, 2003, tradução nossa).

Na montagem da defesa cibernética, faz-se necessário conhecer como os sistemas são atacados. Desse modo, a presença de capacidade de defesa cibernética infere, ao menos, certa capacidade ofensiva. Tal dado possui relevância para a análise da capacidade inimiga que, juntamente com demais informações oriundas das ações de exploração, nortearão todo o esforço de defesa.

A presença de diversos atores no ciberespaço, operando de modo indistinguível e desenvolvendo atividades que vão do crime e espionagem a ações militares, torna o ambiente operacional da Guerra Cibernética algo complexo. Ademais, com os avanços tecnológicos e o aumento de conectividade digital, os tempos de reação às ameaças que exploram as

---

[27] Ver glossário.

[28] Militaries which are highly dependent on secure information systems will be absolutely crippled, just as if they didn't have aircraft above to protect them in the 20th century. If they don't have good cyber defenses in the 21st century, they'll be absolutely helpless.

vulnerabilidades dos sistemas de TI, ou seja, aos ataques cibernéticos, diminuíram. Consequentemente, todos estes fatores somados conferem maior dificuldade à defesa cibernética.

Outro ponto que constantemente impõe dificuldades relaciona-se ao fato de que os encarregados pela defesa cibernética são pressionados a reconhecer qualquer indício de ataque que configure o menor nível de agressão e, portanto, não são capazes de visualizar a situação como um todo. No máximo, serão relegados a reações táticas aos estímulos impostos pelo inimigo, evento a evento. Fica impossível manter-se à frente do inimigo ao se usar essa postura reativa para a defesa. Logo, sem um bom planejamento da defesa cibernética, as ações defensivas serão tão imprevisíveis quanto os ataques desencadeados pelo inimigo (GORDON, 2008; TINNEL; SAYDJARI; FARRELL, 2002).

O primeiro passo a considerar para a defesa é não relegar as normas de segurança cibernética. Parece simples e por demais notório, e o é, mas mesmo assim muitas das vulnerabilidades existentes nos sistemas são decorrentes da inobservância de normas primárias. Como observado por Boyd (2009), o desafio da defesa cibernética não é criar uma correção a uma vulnerabilidade, mas assegurar que os sistemas estejam constantemente atualizados.

Em segundo lugar, deve-se tomar medidas de modo a reduzir a vulnerabilidade das forças em operação com relação à Guerra Cibernética, que incluem, além de medidas técnicas de defesa relacionadas à segurança, mitigação dos danos e reconstrução/recuperação dos sistemas atacados, aquelas relacionadas à antecipação e avaliação corrente da situação (SHIMEALL; WILLIAMS; DUNLEVY, 2002).

A antecipação e avaliação corrente da situação são favorecidas pela consciência situacional. Deve ser observado que antes de um primeiro ataque, seja ele cibernético ou convencional, existirá, normalmente, uma prévia situação de crise, que deverá ser monitorada

de modo a possibilitar a antecipação das ações e o reforço da postura defensiva.

Além disso, as seguintes atividades cibernéticas do oponente deverão ser constantemente monitoradas (TINNEL; SAYDJARI; FARREL, 2002):

- Meios de Coleta de Informação – refere-se aos sistemas de coleta de informação inimigos. Trata-se de rastrear as atividades de programas e servidores de inteligência cibernética conhecidos, dentre os sistemas que recebem relatórios de eventos cibernéticos provenientes do TO.
- Efeitos produzidos – refere-se ao aumento de atividade, não apenas dos meios de coleta de informação do inimigo, mas dos efeitos das atividades daqueles meios em nossos próprios sistemas. Por exemplo, é previsto um aumento de atividades de sondagem e mapeamento de rede antes da execução de um ataque.
- Postura defensiva dos meios cibernéticos – refere-se a observar a postura defensiva do inimigo. Frequentemente, espera-se que o inimigo reforce suas defesas cibernéticas antes de lançar um ataque.

No advento de um ataque cibernético bem sucedido por parte do inimigo, a primeira prioridade da força atacada deverá ser avaliar se alguma ação inimiga convencional está para ser desencadeada, de modo a se aproveitar dos efeitos do ataque cibernético, uma vez que se deve levar em consideração a característica de efeito temporário dos ataques. A segunda prioridade, assumindo que o atacante está monitorando os sistemas atacados de modo a acompanhar a situação e decidir pelo ataque convencional, é fazer com que os efeitos do ataque sobre o sistema pareçam ser de pequena monta. A terceira, então, compreende o restabelecimento dos sistemas (LIBICKI, 2009a).

Há, portanto, a extrema necessidade de disseminação de que a força foi alvo de um ataque cibernético, de modo a possibilitar uma avaliação oportuna e eficaz, que, por sua vez, propiciará uma melhor consciência situacional e a manutenção do ritmo de execução do

ciclo OODA.

Os passos descritos são pontos importantes e que são frequentemente desprezados pelo elemento técnico que, por lhe faltar a mentalidade operativa, conduz suas ações pautado apenas no restabelecimento das funções do sistema atacado. Este é um dos motivos pelo qual a Guerra Cibernética deve ser tratada e conduzida como o que realmente é, ou seja, uma função de cunho operativo.

3.4 Níveis de Condução e o Comando e Controle na Guerra Cibernética

É necessário salientar que, no ciberespaço, em função de suas características e de seu ambiente operacional, não há como distinguir os níveis tático e operacional para as ações ofensivas e de exploração da Guerra Cibernética. Portanto, a estrutura de comando e controle da Guerra Cibernética no TO deve ser única, em que pese a existência de estruturas distintas para os níveis tático e operacional para os componentes convencionais de uma força. Tal arranjo se faz necessário, pois este autor entende existir a necessidade de centralização das ações da Guerra Cibernética (com exceção para as ações defensivas), imposta pela necessidade de observar, principalmente, as características de necessidade de surpresa, dificuldade de realização do segundo ataque, limitação dos efeitos no tempo, limitação de controle e as incertezas, em especial quanto ao dano colateral e aos efeitos no alvo.

Assim, sugere-se a seguinte estrutura de comando e controle:

a) Comando Cibernético Estratégico – constituído pela estrutura de Guerra Cibernética do Ministério da Defesa, é responsável pela execução de ações contra as infraestruturas críticas situadas no território do país inimigo. Devido às altas implicações decorrentes desse tipo de ação, sugere-se que esta somente ocorra mediante autorização do Presidente da República.

b) Comando Cibernético Operacional da Força – constituído pela estrutura de Guerra Cibernética da Marinha do Brasil não alocada ao TO[29], é responsável pela execução de ações em alvos militares situados fisicamente fora do TO, em apoio às operações nele conduzidas. Devido à possibilidade de dano colateral, bem como implicações políticas decorrentes da atuação fora dos limites do TO, sugere-se que sua atuação ocorra mediante autorização do Ministério da Defesa.

c) Componente Cibernético Operacional do TO – é o comando responsável pela condução operacional e tática da Guerra Cibernética, estando sua área de atuação limitada aos alvos militares localizados no interior do TO.

Impende considerar que a atuação dos Comandos Cibernéticos da Força e Estratégico demandará estreita coordenação com o Comandante do TO, sendo que, normalmente, esses Comandos atuarão em atendimento às solicitações provenientes do próprio Comandante do TO.

Observa-se que no modelo apresentado acima, as ações de exploração e ofensivas no TO serão executadas exclusivamente pelo Componente Cibernético Operacional, que será, também, o responsável pela coordenação de toda a defesa cibernética, sendo as ações defensivas executadas de forma descentralizada. Vale dizer que cada Comando será responsável por prover sua defesa e deverá dispor de pessoal devidamente qualificado e adestrado nas ações de Guerra Cibernética. Nesse caso, as equipes de defesa cibernética das unidades deverão ser chefiadas por um Oficial de Guerra Cibernética, que responderá pelas ações defensivas de seu navio ou unidade – a Guerra Cibernética no nível tático, representada pelas ações de defesa.

Convém ressaltar que o Componente Cibernético Operacional deverá estar

---

[29] Cabe salientar que nem sempre será estabelecido um TO. Nessas ocasiões, portanto, deverá ser considerada a "área de operações".

desdobrado no TO, ou área de operações caso não se estabeleça um TO, fazendo parte das forças em operação, e sua composição será definida durante a fase de planejamento, com base nos condicionantes do processo de planejamento militar.

Em termos de comparação, cita-se que, atualmente, a Força Aérea norte-americana estuda a adoção, em função de sua experiência em diversos exercícios e em emprego real, do desdobramento expedicionário de seu Comando Cibernético na área de operações, que atuará de forma centralizada, para melhor apoiar as forças em operação (JABBOUR, 2010).

3.5 Planejamento da Guerra Cibernética

Na fase de planejamento, quando o Componente Cibernético Operacional do TO ainda não foi ativado, o elemento organizacional da Marinha do Brasil responsável pela Guerra Cibernética, doravante denominado de Comando Cibernético, deverá designar Oficiais de Ligação a serem destacados junto ao Comandante do Teatro de Operações, caso seja constituído um TO, e ao(s) Comandante(s) da(s) Força(s)-Tarefa responsável(is) pela execução das operações. A tarefa dos Oficiais de Ligação de Guerra Cibernética será facilitar a coordenação e assessorar os Comandos apoiados quanto ao planejamento e ao emprego das ações de Guerra Cibernética. Estes elementos deverão trabalhar como assessores diretos dos Oficiais de Operações e serão os responsáveis pela elaboração da Estimativa e do Plano de Guerra Cibernética.

Durante o planejamento deverão ser levantadas as necessidades de inteligência cibernética, de modo a orientar o esforço de coleta e de busca, que será realizado pelo Comando Cibernético por meio de ações de exploração de Guerra Cibernética. Tais conhecimentos serão fundamentais para, inicialmente, fundamentar a Estimativa de Guerra

Cibernética, que deverá abordar, além de aspectos relativos às estruturas das forças amigas, a estrutura de TI das forças inimigas, incluindo informações sobre suas tecnologias de defesa e ataque cibernéticos, bem como o levantamento inicial de vulnerabilidades de seus sistemas. Posteriormente, tais informações servirão para retroalimentar e focalizar as ações de exploração em curso.

Com o advento de novas capacidades do inimigo que podem influenciar o cumprimento da missão de forças amigas, torna-se necessário conferir especial atenção à formulação de novas Possibilidades do Inimigo[30] (PI) referentes à Guerra Cibernética. Para tanto, é fundamental a participação do Oficial de Ligação de Guerra Cibernética, junto ao Oficial de Inteligência, para auxiliar na correta formulação e análise dessas PI. Ocorre que para a Guerra Cibernética, especificamente, há uma particularidade que faz com que tal PI seja sempre contemplada, pois, mesmo que o inimigo não possua capacidade própria nesse campo, há uma miríade de recursos de rápida aquisição, desde ferramentas de ataque a mercenários cibernéticos, com os quais poderá contar.

O Plano de Guerra Cibernética deverá definir a composição do Componente Cibernético Operacional, bem como a distribuição de recursos e as tarefas afetas aos elementos responsáveis pela execução das ações de Guerra Cibernética, devendo, também, identificar as relações de comando existentes. Tal plano deverá definir, ainda, as Regras de Comportamento Operativo, com enfoque principal às ações defensivas, uma vez que serão as únicas ações descentralizadas. Além dos itens já elencados, o plano deverá abordar os riscos a que estão expostos os sistemas das forças amigas, as ameaças apresentadas pelos recursos cibernéticos inimigos e, principalmente, os critérios e prioridades de aplicação dos recursos cibernéticos.

---

[30] Ver glossário.

4 OUTRAS CONSIDERAÇÕES SOBRE GUERRA CIBERNÉTICA

Consequência de suas vulnerabilidades, exemplo mor do paradoxo cibernético, os Estados Unidos da América (EUA) são o país onde mais se estuda a Guerra Cibernética fora dos setores militares. Por essa razão, é também a origem da maior parte das referências sobre o tema, motivo pelo qual há maior quantidade de informação disponível sobre a visão norte-americana. As informações sobre outros países são bastante limitadas, não só pela exiguidade de fontes, mas, também, pela barreira da língua, uma vez que, das fontes disponíveis, um número ainda menor é encontrado em versões traduzidas para o inglês.

4.1 A visão norte-americana

Os EUA começaram a se preocupar com a defesa do ciberespaço a partir do governo do Presidente Clinton, o qual emitiu a Diretiva Presidencial número 68, intitulada "Proteção das Infraestruturas Críticas". Em 2002, já no governo de George Bush, foi lançada a "Estratégia Nacional para a Segurança do Ciberespaço". Ambos os documentos delineavam as preocupações daquele país com as ameaças provenientes do ciberespaço, entretanto não eram precisos em suas ações. Em dezembro de 2006, foi publicada a "Estratégia Militar Nacional para as Operações no Ciberespaço", a qual estabelece que os EUA devem possuir superioridade no ciberespaço para garantir sua liberdade de ação e negar o mesmo aos seus oponentes, por meio da integração da defesa, exploração e ataque cibernéticos (ESTADOS UNIDOS DA AMÉRICA, 2010d; RATTRAY, 2009).

Recentemente, em maio de 2010, foi lançada a Estratégia de Segurança Nacional, a qual tece considerações diretas sobre o tema e atesta existir vulnerabilidades que colocam em risco tanto a vida em sociedade como as operações militares dos EUA. A esse respeito,

declara que aquele país deve estar preparado às ameaças assimétricas que têm como alvo sua dependência no espaço e no ciberespaço, classificando a ameaça cibernética como o maior desafio nas áreas econômica e de segurança. No campo militar, estabelece que devem ser garantidas às forças armadas norte-americanas as capacidades necessárias à operação em terra, ar, mar, espaço e ciberespaço, o que remete à ideia de que os EUA consideram o ciberespaço como um ambiente operacional tal qual os demais (ESTADOS UNIDOS DA AMÉRICA, 2010e).

Em termos da estrutura, há uma divisão de funções entre o Departamento de Segurança Interna (DHS), responsável pela segurança cibernética no território dos EUA, e o Departamento de Defesa (DoD), responsável pela Guerra Cibernética e a realização de ações cibernéticas em apoio ao DHS. Entretanto, não há uma clara definição quanto à coordenação entre esses dois departamentos, mormente como ocorrerá a atuação de ambos por ocasião de uma crise (KRAMER; STARR; WENTZ, 2009; NAKASHIMA, 2010).

Em 2002, a responsabilidade pela condução da Guerra Cibernética no âmbito do DoD foi atribuída ao "Comando Estratégico dos EUA" (USSTRATCOM), cujas tarefas incluem a operação das redes de informação do DoD, realizada por meio da "Agência de Sistemas de Informação de Defesa" (DISA), o planejamento contra ameaças cibernéticas, a promoção de novas capacidades e a coordenação com outros comandos e agências. Àquela ocasião, as tarefas encontravam-se divididas entre dois componentes, o *Joint Functional Component Command for Network Warfare* (JFCC NW), de caráter ofensivo, e o *Joint Task Force for Global Network Operations* (JTF GNO), voltado à defesa (LIBICKI, 2009a).

Em 2008, ao observar que a segregação das operações defensivas e ofensivas no ciberespaço diminuía a sinergia natural e ignorava a experiência em se organizar para operações nos ambientes aéreo, terrestre, marítimo e espacial, o DoD reorganizou os elementos e o componente defensivo (JTF GNO) foi posto sob controle operacional do

ofensivo (JFCC NW). Em continuação ao esforço de reorganização, em 2009, foi ativado o "Comando Cibernético dos EUA" (USCYBERCOM), em substituição aos componentes existentes, os quais serão desativados quando o novo comando atingir sua capacidade operacional total. Cabe frisar que o USCYBERCOM tornou-se operacional, com capacidade limitada, em 21 de maio de 2010. O apoio à operação e à segurança das redes do DoD permaneceu como responsabilidade da DISA, que também é responsável por projetar e prover a infraestrutura de comando e controle em operações, além de prestar assessoria técnica ao USCYBERCOM (CHILTON, 2010; ESTADOS UNIDOS DA AMÉRICA, 2010a, 2010f; GATES, 2009).

A missão do USCYBERCOM compreende: integrar as operações no ciberespaço e sincronizar os efeitos do combate; prestar apoio às autoridades civis e aos aliados internacionais; operar a Rede de Informação Global[31] e executar sua defesa; executar operações militares no ciberespaço; coordenar, no âmbito do DoD, as operações ofensivas no ciberespaço de modo a evitar interferência entre as ações; aprimorar a consciência situacional das operações no ciberespaço, incluindo alertas, e compartilhá-la; e representar o setor militar junto às agências nacionais e comerciais do governo e agencias internacionais, nos assuntos relacionados ao ciberespaço; a fim de possibilitar ações em todos os domínios, assegurar a liberdade de ação no ciberespaço aos EUA e seus aliados e negá-la aos seus oponentes (ESTADOS UNIDOS DA AMÉRICA, 2010d, 2010f).

Seguindo a reorganização realizada pelo DoD, cada uma das forças armadas norte-americanas realinhou seus comandos cibernéticos em uma organização unificada. Os novos comandos, que estão sob controle operacional do USCYBERCOM, são o *Army Forces Cyber Command* – do Exército, *Marine Corps Forces Cyberspace Command* – do Corpo de Fuzileiros Navais, *Fleet Cyber Command* – da Marinha, e a *24th Air Force* – da Força Aérea

---

[31] Ver glossário.

(CHILTON, 2010).

Com relação à Marinha norte-americana, após o lançamento da "Estratégia Militar Nacional para as Operações no Ciberespaço", em 2006, o Almirante Mike Mullen, então Comandante de Operações Navais, determinou ao "Grupo de Estudos Estratégicos" do *Naval War College*[32] desenvolver um conceito para "o combate no ciberespaço em 2030", visando a determinar as relações entre o ciberespaço e os demais ambientes operacionais, e pesquisar os aperfeiçoamentos, na área operacional, tecnológica e de procedimentos, necessários para a Marinha norte-americana dominar o ambiente operacional do ciberespaço (KUEHL, 2009).

Com a reorganização dos elementos responsáveis pelas operações cibernéticas, a Marinha norte-americana comissionou dois novos comandos em janeiro de 2010. O *Fleet Cyber Command* (FLTCYBERCOM), já citado, que funcionará como o elemento operacional da Marinha para o USCYBERCOM, também operará como a *Tenth Fleet* e, nesse caso, estará sob controle administrativo do Comando de Operações Navais (CNO) norte-americano e proverá apoio na área de operações cibernéticas aos comandos daquela força. Outra função desse comando é servir como o elemento naval de criptologia a serviço da Agência de Segurança Nacional (NSA). As organizações pré-existentes serão subordinadas ao FLTCYBERCOM, conforme apresentado na FIG. 2 (APÊNDICE B). O outro comando é o *Navy Cyber Forces* (CYBERFOR), que é o "Comando Tipo" (TYCON) da Marinha norte-americana para as forças cibernéticas, sendo responsável por prover pessoal e material nas áreas de criptologia, inteligência de sinais, cibernética, guerra eletrônica, operações de informação, redes e espaço. O CYBERFOR é subordinado ao *U. S. Fleet Forces Command* e tem como missão organizar e priorizar os requisitos de treinamento, modernização e manutenção de recursos humanos; arquitetura e redes de comando e controle; sistemas

---

[32] Equivalente norte-americana à Escola de Guerra Naval do Brasil.

criptológicos e relativos ao espaço; atividades de operações de informação e inteligência; e coordenar com outros TYCON para proporcionar forças prontas, apropriadas e interoperáveis no tempo certo e ao melhor custo, hoje e no futuro (COLARIK; JANCZEWSKI, 2008; ESTADOS UNIDOS DA AMÉRICA, 2010B, 2010C; ROUGHEAD, 2009).

Como aspecto final da visão norte-americana, deve ser ressaltado que, em termos doutrinários, as forças armadas dos EUA não utilizam o termo Guerra Cibernética, que é tratada como Operações de Redes de Computadores e faz parte, juntamente com a guerra eletrônica, as operações psicológicas, as operações de diversão e a segurança das operações, das funções essenciais das Operações de Informação[33] (ESTADOS UNIDOS DA AMÉRICA, 2006).

Com relação à preparação de recursos humanos, as escolas de formação dos oficiais do Exército e da Força Aérea norte-americanos já incluíram a Guerra Cibernética em seus currículos. Com relação à Marinha, sua Escola Naval criou, ao final de 2009, um Centro de Estudos de Segurança Cibernética, para o qual construirão instalações dedicadas à instrução e prática das ações no ciberespaço, e encontra-se em estudos a inclusão curricular da Guerra Cibernética nos cursos daquela academia (WITTE, 2010).

4.2 Dificuldades enfrentadas

A adoção de medidas acerca da Guerra Cibernética, mesmo em se tratando apenas de medidas defensivas, tem enfrentado uma série de dificuldades. Tomando como referência as considerações apresentadas pelo General Keith Alexander, Comandante do USCYBERCOM, por ocasião da sabatina a que foi submetido no Senado norte-americano, pode-se verificar os desafios e problemas de seu comando:

---

[33] O propósito das Operações de Informação é a obtenção da superioridade de informação e sua manutenção.

> Eu acredito que o maior desafio a ser enfrentado pelo Comandante do USCYBERCOM será o aperfeiçoamento das defesas das redes militares existentes. Adicionalmente, a fim de defender e tomar boas decisões no exercício do controle operacional dessas redes, o USCYBERCOM necessitará de uma maior consciência situacional e capacidade de visualizar, em tempo real, as intrusões a nossas redes. Por último, acredito que, na medida em que as tecnologias da computação e comunicações evoluam, o Comandante do USCYBERCOM deverá identificar, continuamente, os hiatos de autoridade e de políticas existentes entre o USSTRATCOM e nossas lideranças civis[34] (ESTADOS UNIDOS DA AMÉRICA, 2010d, p. 8, tradução nossa).

Tem-se, pois, que um dos dados mais relevantes reside na dificuldade de relacionamento do setor militar com os demais setores, dentre os quais não pode ser esquecido o setor privado, que está intimamente ligado à segurança cibernética dos EUA por ser o detentor de diversas infraestruturas críticas que poderão ser alvo de um ataque cibernético. Para agravar esse problema, não existe definição com relação à coordenação de trabalho entre o USCYBERCOM e o Departamento de Segurança Interna (DHS) e há falta de normas e políticas específicas (BALDOR, 2010; ESTADOS UNIDOS DA AMÉRICA, 2010d).

A raiz das dificuldades, entretanto, reside na falta de uniformização sobre o entendimento do que vem a ser a Guerra Cibernética. Como já abordado anteriormente, não há consenso sobre vários pontos, o que dificulta a harmonização de políticas e de doutrina sobre o tema. Tal fato já foi reconhecido pelo atual governo norte-americano, que iniciou um esforço de revisão em sua política para o ciberespaço, mas ainda restam várias lacunas em termos de normas e políticas a preencher (BOYD, 2009; LEWIS, 2010).

O problema de unidade doutrinária também atinge as forças armadas norte-americanas, que carecem de uma doutrina comum e atualizada sobre as operações no ciberespaço. Recentemente, o Vice-Chefe do Estado-Maior Conjunto norte-americano argumentou sobre a necessidade de definições legais e doutrinárias de modo a permitir que as

---

[34] I believe the major challenge that will confront the Commander, U.S. Cyber Command will be improving the defense of our military networks as they exist today. Additionally, in order to defend those networks and make good decisions in exercising operational control over them, U.S. Cyber Command will require much greater situational awareness and real time visibility of intrusions into our networks. Finally, I believe the Commander, U.S. Cyber Command will have to identify continuously policy and authority gaps to U.S. Strategic Command and our civilian leadership as computer and communication technologies evolve.

forças cibernéticas possam ir além de apenas defender suas redes. A doutrina militar atual não é clara com relação aos limites que configuram um ato de agressão no ciberespaço e que ações poderão ser tomadas em resposta ao ataque. Nesse sentido, James N. Miller, subsecretário de defesa para políticas, declarou que está em elaboração uma nova doutrina para Guerra Cibernética, que considera a possibilidade de resposta a um ataque cibernético por meio do emprego de forças militares convencionais (ESTADOS UNIDOS DA AMÉRICA, 2010d; LAKE, 2010).

4.3 Aspectos jurídicos

Como visto na seção anterior, um dos problemas que afligem os responsáveis não só por defender os sistemas das ameaças do ciberespaço, mas, também, por realizar ações de exploração e ofensivas, é a falta de um marco regulatório legal que oriente e ampare a aplicação militar da capacidade cibernética.

Na área da segurança e da defesa cibernéticas o principal problema recai na necessidade de cooperação de legisladores, agentes da lei e provedores de serviços da Internet além da fronteira dos países. Logo, a criação de um ciberespaço mais seguro exige que iniciativas na área legal sejam tomadas não só no âmbito nacional, como internacional, conforme abordado por John Arquilla:

> Eu penso que nossos esforços atuais (para a identificação do atacante) são limitados em parte por nossas próprias leis. O limite até onde podemos rastrear a rede para localizar um usuário é imposto por nossas leis e a noção de uma perseguição internacional através do ciberespaço é algo que, também, ultrapassa as leis internacionais. Portanto, precisamos começar a pensar sobre a harmonização das leis de segurança da informação em todo o mundo[35] (ARQUILLA, 2003, tradução nossa).

[35] I think that our current approaches are limited in part by our own laws. How far back we can hack to trace a user is limited under our existing laws, and the notion of international hot pursuit through cyberspace is also something that has run far ahead of existing international law. So we need to start thinking about a harmonization of information security law around the world.

Com relação às ações de exploração e ofensivas, tem-se que, baseado nas intenções com as quais tais ações são realizadas, a maioria pode ser interpretada como ato antiético e ilegal. Entretanto, o fator de maior relevância recai sobre a definição do limite a partir do qual uma ação no ciberespaço passa a ser considerada como um ato de agressão, sendo, portanto, passível de retaliação.

Como ponto de partida, deve-se identificar um limiar a partir do qual as ações no ciberespaço poderiam ser consideradas como um ato de guerra, ou seja, uma agressão similar a um ataque por forças convencionais. Assim, tanto o uso de tropas para causar danos na infraestrutura crítica de um Estado – sabotar ou explodir um gasoduto, um oleoduto ou uma usina de geração elétrica – e uma ação similar no ciberespaço configurariam um ato de agressão e poderiam justificar uma resposta por força militar. Deve-se observar, ainda, que as ações de exploração não são consideradas como um ato de agressão, sendo tratadas como espionagem. Portanto, o limiar estará localizado entre o reconhecimento e a interrupção ou dano (FIG. 3, APÊNDICE B). A transposição desse limite poderia escalar qualquer conflito cibernético. Pode-se, ainda, considerar um segundo limiar, caracterizado pela mudança de ataque a alvos militares para as infraestruturas críticas e outros alvos civis (LEWIS, 2009).

No entanto, não há acordo ou entendimento explícito sobre o que é um alvo legítimo no ciberespaço. Pode-se, por aproximação, declarar que se é legítimo atacar um alvo fisicamente, também o seria atacá-lo com o uso de armas cibernéticas. Discussões sobre transformar algumas redes em santuários, como hospitais, por exemplo, em que os beligerantes concordariam não atacar, ignoram o nível de interconexão do ciberespaço e a possibilidade de efeitos colaterais que obscurece a perfeita distinção entre alvos legítimos e não legítimos, contrariando, portanto, o princípio da distinção insculpido no Protocolo Adicional I da Convenção de Genebra (BRITTIN, 1991; LEWIS, 2009).

Os argumentos usados acima remetem ao exame da Guerra Cibernética sob a ótica

do Direito Internacional dos Conflitos Armados. Com relação ao *jus ad bellum*[36], sua aplicabilidade dependerá da exata noção do que venha a ser um ato de agressão no ciberespaço, o que já foi analisado. No que concerne ao *jus in bello*[37], alguns especialistas advogam que a legislação atual pode ser integralmente aplicada à Guerra Cibernética. Neste ponto, em particular, este autor se reserva o direito de não corroborar integralmente tal posicionamento. Como já argumentado acima, o princípio da distinção, que visa a preservar a integridade de não combatentes, é de difícil implementação. Igualmente, as características da Guerra Cibernética, abordadas no início deste estudo, impõem limitações à aplicabilidade do princípio de limitação dos danos e ao respeito à neutralidade. Portanto, a Guerra Cibernética, uma forma relativamente nova de conflito, cuja experiência em sua aplicação é praticamente irrisória no que concerne ao aspecto legal, enseja a necessidade de atualização do corpo legal que governa os conflitos armados. Nesse mister, cabe reproduzir a opinião de Eneken Tikk, assessora jurídica do *Cooperative Cyber Defence Centre of Excellence*[38], de que "as leis internacionais atuais não são adequadas à Guerra Cibernética[39]" (MCAFEE, 2009, p. 29).

4.4 A Guerra Cibernética e as Relações Internacionais

À luz do que já foi apresentado, pode-se dizer que as discussões acerca da Guerra Cibernética não devem ficar restritas somente ao âmbito nacional. Conforme ilustrado por Kramer (2009), o ciberespaço é produto da globalização e, portanto, necessita ser analisado e revisado sob a ótica internacional.

Como demonstrado na seção pertinente aos aspectos jurídicos, a normatização

---

[36] Ver glossário.
[37] Ver glossário.
[38] Centro pertencente à OTAN, que foi estabelecido em Talin, capital da Estônia, após os ataques cibernéticos sofridos por aquele país em 2007.
[39] Current international law is not adequate for addressing cyber war.

internacional acerca do conflito cibernético é inexistente e o corpo jurídico relativo ao conflito armado não se aplica inteiramente à Guerra Cibernética. Há necessidade de se prover uma normatização para esse tema, envolvendo não só a questão de uso militar do ciberespaço, mas, também, a participação de grupos de civis que poderão se envolver em um conflito, seja patrocinado por um Estado, ou atuando de forma autônoma. Dificulta, ainda, a falta de uniformização de entendimento sobre o significado de vários termos relacionados à Guerra Cibernética. Para tanto, são necessários a cooperação e a colaboração internacionais, que podem ter como foro as Nações Unidas, para a formulação da terminologia comum e de uma doutrina legal.

Atualmente, a Convenção sobre Crime Cibernético do Conselho da Europa[40], embora não relacionada à Guerra Cibernética, é o único tratado internacional que aborda assuntos relacionados às práticas ilegais no ciberespaço. Seu propósito é o aprimoramento da capacidade dos governos em lidar com o crime cibernético por meio da harmonização das legislações internas e da cooperação contra os crimes transnacionais. O Brasil, em que pese não ser signatário, usa as diretrizes constantes nessa convenção como base para a elaboração de sua legislação interna (COUNCIL OF EUROPE, 2010; KWALWASSER, 2009; WILSON, 2006).

Os EUA, país singularmente vulnerável no que tange à ameaça cibernética, têm grande interesse na criação de normas internacionais relativas ao assunto. Há três pontos que são usualmente mencionados por autoridades do governo e especialistas norte-americanos como de particular interesse à pauta de acordos internacionais daquele país. O primeiro diz respeito a que penalidades poderão ser aplicadas quando um Estado falha no uso do exercício de sua soberania para impor responsabilidades aos atos realizados no ciberespaço sob sua jurisdição. Outra ideia defendida pelos EUA é tornar os Estados responsáveis pelas ações no

---

[40] Council of Europe Convention on Cybercrime.

ciberespaço efetuadas por indivíduos residentes em seu território, de modo a invalidar a desculpa recorrente de que foram hackers patrióticos e não o governo os responsáveis por ataques no ciberespaço. O terceiro ponto refere-se a um acordo de controle de armas cibernéticas, cuja necessidade já foi apresentada pelo Congresso norte-americano, pelo atual Comandante do USCYBERCOM e por Richard Clarke, encarregado das ações de contraterrorismo nos governos Clinton e Bush (KAKUTANI, 2010; LEWIS, 2009, 2010; WILSON, 2006).

As propostas acima merecem especial atenção por parte da comunidade internacional, não por serem de interesse maior aos EUA do que a qualquer outro Estado, mas por representarem riscos potenciais, particularmente àqueles Estados que buscam capacidade ofensiva cibernética e, também, àqueles que de algum modo não consigam o efetivo controle do que ocorre no ciberespaço sob sua jurisdição. Esta última pode ensejar uma "intervenção cibernética", que pode se dar exclusivamente no ciberespaço, por meio da assunção de sua governança, em afronta à soberania do Estado, ou por outras ações fora do ciberespaço, como retaliações diplomáticas e chegando, até mesmo, ao uso de força militar.

O Brasil deve estar atento, particularmente, às propostas de limitação ou banimento de uso de armas cibernéticas, de modo a não perder a oportunidade de possuir plena capacidade de empreender a Guerra Cibernética antes da assinatura de qualquer acordo internacional relacionado à não proliferação de armas cibernéticas. Entretanto, as demais medidas relacionadas à normatização internacional, mormente as relativas à Guerra Cibernética, são necessárias e devem ser encorajadas, lembrando-se de que, segundo Lewis (2010), o ciberespaço continuará a ser um ambiente hobbesiano até que exista o engajamento e o trabalho cooperativo internacional no sentido de definir o que se entende por comportamento responsável no ciberespaço.

5 A GUERRA CIBERNÉTICA NA MARINHA DO BRASIL

5.1 Estrutura Nacional

Antes de abordar o tema sob a ótica da Marinha do Brasil, faz-se mister verificar como a Guerra Cibernética é tratada pelo Estado brasileiro. A nível nacional, o tema é dividido em duas esferas: a Segurança Cibernética[41] e a Defesa Cibernética. Tal entendimento foi consolidado pela Câmara de Relações Exteriores e Defesa Nacional (CREDEN), em reunião realizada em nove de outubro de 2008, a qual definiu que as ações cibernéticas caracterizadas como crime, bem como as ações de terrorismo cibernético e a sabotagem, seriam tratadas na esfera da Segurança Cibernética, por meio de ações preventivas e repressivas. A Defesa Cibernética trataria da Guerra Cibernética, que, por estar na esfera de um estado de beligerância entre o Brasil e uma força hostil, não foi objeto de deliberação da citada reunião, que ponderou ser uma incumbência do Conselho de Defesa Nacional (CDN) (MANDARINO JUNIOR, 2009; ZUCCARO, 2010).

Dentro da estrutura hierárquica da Administração Pública Federal (APF) brasileira, o Gabinete de Segurança Institucional da Presidência da República (GSI-PR) é o órgão responsável pela segurança cibernética, onde é tratada como segurança da informação, a qual é operacionalizada por meio de seu Departamento de Segurança da Informação e Comunicações (DSIC). O DSIC, por sua vez, é responsável, entre outras atribuições, pelo planejamento e coordenação das atividades de segurança da informação e comunicações na APF; pela definição dos requisitos metodológicos para implementação da segurança da informação e comunicações na APF; e pela operacionalização de um centro de tratamento e resposta a incidentes ocorridos nas redes de computadores da APF (BRASIL, 2003, 2006b,

---

[41] Ver glossário.

2009e).

No que concerne à defesa cibernética, sua importância foi ressaltada e priorizada pela Estratégia Nacional de Defesa, que estabeleceu o fortalecimento de “três setores de importância estratégica: o espacial, o cibernético e o nuclear” (BRASIL, 2008, p. 11). Entretanto, há que se salientar a falta das Estratégias de Defesa e de Segurança Cibernéticas, cujas iniciativas de formulação deverão pertencer, respectivamente, ao Ministério da Defesa e ao GSI-PR.

5.2 Retrospecto da Guerra Cibernética na Marinha do Brasil

Assunto recente à Marinha do Brasil, a Guerra Cibernética começou a ser tratada com maior profundidade no ano de 2006. A par das ameaças existentes, visualizou-se a necessidade de se preparar a Força para enfrentar os novos desafios impostos pelo constante avanço das Tecnologias da Informação (TI). Assim, a primeira iniciativa do gênero foi a criação da Seção de Guerra Cibernética no Comando de Operações Navais, que se encontrava subordinada à Subchefia de Inteligência (CON-20). O conhecimento que se detinha sobre o assunto era muito limitado, tanto em termos técnicos, como doutrinários, e restringia-se ao esforço de alguns poucos elementos que, por iniciativa própria, buscavam se atualizar. A cada movimentação de um desses militares, se perdia um pouco da incipiente capacidade existente.

A partir de 2008, a Marinha do Brasil realiza uma forte guinada na maneira de tratar a Guerra Cibernética, ao transferi-la do Setor Operativo ao Setor de Apoio, mais precisamente sob a estrutura da Diretoria-Geral de Material da Marinha. Compreende-se que a adoção de tal postura foi motivada, entre outros fatores, pela forte e natural relação que as TI mantêm com a Guerra Cibernética, fazendo com que a competência fosse atribuída à recém-criada Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM),

responsável por elaborar normas, instruções técnicas e procedimentos padronizados para áreas de conhecimento concernentes ao emprego da Tecnologia da Informação na MB, incluindo a Guerra Cibernética. Nesse diapasão, o Centro de Tecnologia da Informação da Marinha (CTIM) foi designado como Órgão de Execução Operacional para a Guerra Cibernética (GC), sendo responsável por: operar os recursos tecnológicos para a GC; planejar os exercícios gerais de GC; subsidiar a DCTIM nos aspectos de capacitação técnica do pessoal envolvido com as atividades específicas de GC; e mobilizar o pessoal qualificado, para o emprego em situações de conflito, de acordo com a doutrina estabelecida.

Com referência à alusão feita à doutrina, cumpre salientar que, desde a época em que o tema esteve afeto ao Setor Operativo até os dias atuais, a Marinha do Brasil carece de uma doutrina relativa ao emprego da Guerra Cibernética. A Doutrina Básica da Marinha, em sua versão atual, não faz referência ao tema e tampouco há manual pertinente ao seu emprego operativo. Apenas na Doutrina de Tecnologia da Informação da Marinha, publicação de viés mais técnico, é que se encontram as questões relativas ao tema e que se define o termo Guerra Cibernética, com as deficiências já abordadas neste trabalho. Todavia, não se pode esquecer que a Guerra Cibernética se constitui em um diferencial fundamental às operações de qualquer força militar que se disponha a operar eficaz e eficientemente em qualquer conflito, sendo, portanto, uma capacidade operativa por excelência, podendo até ser vista como um novo sistema de armas. Destarte, a Marinha do Brasil necessita sanar essa carência por meio da atualização de sua Doutrina Básica, bem como a elaboração de uma doutrina específica para o emprego operativo da Guerra Cibernética.

5.3 Estudos em andamento

Recentemente, fruto das diretrizes da Estratégia Nacional de Defesa, o Ministro da Defesa definiu as responsabilidades de cada Força com relação aos setores de importância estratégica, cabendo ao Exército Brasileiro o setor cibernético. Determinou, também, a realização de estudos no sentido de, em uma primeira fase, analisar e definir a abrangência do tema e propor objetivos setoriais. Essa fase inicial, conduzida pelo Exército com a participação das demais Forças e do Ministério da Defesa, definiu os seguintes objetivos setoriais (BRASIL, 2009b, 2009d):

> a. Assegurar, de forma conjunta, o uso efetivo do espaço cibernético pelas Forças Armadas, e impedir ou dificultar a sua utilização contra interesses da Defesa Nacional;
> b. Promover a gestão dos recursos humanos necessários à condução das atividades do setor cibernético no âmbito das Forças Armadas;
> c. Colaborar com a produção do conhecimento de inteligência oriundo da fonte cibernética de interesse para o Sistema de Inteligência de Defesa (SINDE);
> d. Desenvolver e manter atualizada a doutrina de emprego das atividades do setor cibernético;
> e. Implementar medidas que contribuam para a gestão da Segurança da Informação e Comunicações no âmbito das Forças Armadas;
> f. Adequar as estruturas de C&T das três Forças para atender às necessidades do setor cibernético;
> g. Propor a criação de legislação e normas específicas para o emprego do setor cibernético; e (sic)
> h. Desenvolver o potencial de mobilização militar e nacional para assegurar a capacidade dissuasória e operacional do setor cibernético (BRASIL, 2009b).

Após aprovação[42] pelo Ministério da Defesa dos objetivos setoriais propostos, os estudos passarão para uma segunda fase, que tratará de estratégias setoriais e da adequabilidade das estruturas existentes.

---

[42] Até a conclusão do presente trabalho os objetivos setoriais propostos não haviam sido aprovados pelo Ministro da Defesa.

5.4 Vulnerabilidades

As vulnerabilidades dos sistemas de informação não são fatores imutáveis e, geralmente, sua presença está associada às diferenças existentes entre a teoria e a prática. Teoricamente, um sistema deveria fazer apenas aquilo que seu desenvolvedor e usuário demandem que ele faça. Na prática, isso não ocorre. Destarte, tem-se que não há sistema totalmente seguro (ALFORD, 2000; LIBICKI, 2009a).

Devido às pressões mercadológicas para a redução do ciclo de desenvolvimento de produtos de TI, em virtude da grande velocidade de evolução tecnológica, a indústria de software, em geral, tem relegado a segurança ao segundo plano. Atualmente, os desenvolvedores de software preferem lançar produtos o mais rápido possível, mesmo que estes ainda incorporem imperfeições, e disponibilizar as correções à medida que os erros são detectados. Hoje em dia, é notória entre os profissionais de segurança da informação a existência de vulnerabilidades conhecidas exclusivamente por determinados grupos, normalmente pertencentes ao submundo cibernético, uma vez que precedem qualquer notificação sobre sua existência (COLARIK, JANCZEWSKI, 2008; CSIS, 2008; SHIMEALL, WILLIAMS, DUNLEVY, 2002).

Os problemas descritos acima são de particular interesse, uma vez que vários dos sistemas de informação utilizados por forças militares são baseados em soluções comerciais, como é o caso da Marinha do Brasil, incluindo o uso da Internet como parte de sua infraestrutura de comando e controle. Contribui para o agravamento desse problema a existência de vícios de procedimento com relação às correções que são disponibilizadas aos softwares comerciais, que nem sempre são aplicadas oportunamente. Um fator que agrava esse problema é o uso de programas sem licença, condição impeditiva para que o produto seja atualizado. Faz-se necessário, pois, a constante supervisão das redes de modo a banir a

utilização de qualquer software que não esteja devidamente licenciado para uso. Vale lembrar que, ao oponente, basta a existência de uma única estação de trabalho vulnerável e conectada à rede para possibilitar um ataque de exploração ou ofensivo.

As medidas de segurança cibernética podem ser divididas em três tipos, de acordo com sua orientação. Assim, têm-se as medidas técnicas, orientadas ao uso de recursos de TI voltados precipuamente à segurança, como sistemas de detecção de intrusão, firewalls, recursos criptográficos, ferramentas de análise de rede etc. A segunda refere-se às políticas e doutrinas de segurança, ou seja, são medidas orientadas ao processo. Por fim, o terceiro tipo está relacionado às medidas orientadas aos usuários, que se referem à conscientização de segurança voltada às boas práticas no uso de sistemas de informação.

Com relação à implementação das medidas de segurança na Marinha do Brasil, observa-se um profícuo papel no desempenho das medidas técnicas e as orientadas ao processo. Com relação à primeira, o Centro de Tecnologia da Informação da Marinha (CTIM) exerce papel fundamental, por meio do emprego eficaz e eficiente de recursos técnicos e o correto uso de procedimentos de segurança. Outro ponto a destacar refere-se às medidas orientadas ao processo, baseadas em normatização atualizada, que compreende a Doutrina de Tecnologia da Informação da Marinha – EMA-416, as Normas de Tecnologia da Informação da Marinha – DGMM-540 e as Normas para a Gestão de Segurança das Informações Digitais em Redes Locais – DGMM-520 (QUEIROZ, 2010).

Entretanto, quando se trata das medidas orientadas ao usuário, verifica-se a existência de falhas relacionadas à adoção de práticas básicas de segurança, elencadas na normatização supracitada. Nesse contexto, tem-se que o maior risco é o proveniente das vulnerabilidades associadas ao comportamento humano, ou seja, aquelas diretamente associadas à falta de conscientização de segurança por parte do usuário. Tais vulnerabilidades são as mais fáceis de explorar e as mais difíceis de prevenir e detectar. Conforme declarado

por Kevin Mitnick[43], “o fator humano é o principal culpado pela maioria das falhas de segurança que levam a invasões de sistemas, roubos de dados e golpes cibernéticos em geral” (ALMEIDA, 2010).

Para se ter uma ideia da dimensão do problema relacionado à conscientização do usuário, vale recorrer a um exemplo real de vulnerabilidade explorada em um dos principais comandos dos EUA, o *U.S. Central Command* (CENTCOM), responsável pela condução das operações no Iraque e Afeganistão, entre outros países. Em novembro de 2008, oponentes não identificados conseguiram invadir as redes mais seguras do CENTCOM, burlando restrições físicas de acesso, firewalls e recursos criptográficos, por meio de *pen-drives* infectados, que foram deixados em locais próximos ao CENTCOM e de fácil acesso, frequentados por militares lotados naquele comando. A total falta de conscientização de segurança cibernética, aliada ao impulso da curiosidade, fez com que componentes do CENTCOM utilizassem os dispositivos infectados nos computadores daquele comando, comprometendo os sistemas mais sigilosos e expondo todo o tráfego de dados, comunicações e operações durante várias semanas. Cabe ressaltar que, durante o período em que permaneceu conectado, o invasor poderia ter realizado ações ofensivas contra aqueles sistemas (CBS, 2009; HABIGER, 2010).

Como consequência da falha de segurança relatada acima, foi proibido o uso de *pen-drives* e outras mídias removíveis, conforme pode ser observado na mensagem transmitida pelo USSTRATCOM, comando enquadrante do CENTCOM:

> Fica aparente que, ao longo do tempo, nossa postura de proteção às redes e às infraestruturas de informação associadas não acompanharam os esforços adversários para penetrar, interromper, explorar ou destruir elementos críticos da Rede Global de Informação (GIG) [...] A decisão de proibir o uso de mídias de armazenamento removíveis é um componente chave para a estratégia de defesa contra ataques cibernéticos e o estabelecimento de um patamar para a proteção de sistemas de informação. Cartões de memória, pen-drives e memórias flash removíveis conferiram ao adversário a capacidade de explorar a deficiência de boas-práticas de nosso pessoal e forneceram uma via de ataque [...] Nossos sistemas foram infectados por código malicioso (malware) embutido em dispositivos de memória. Somente por

[43] Ex-hacker, hoje consultor de segurança, foi o hacker mais procurado nos EUA na década de 90 (ALMEIDA, 2010).

> meio de uma defesa baseada na instrução, na tecnologia, nos procedimentos e no comprometimento pessoal é que poderemos recuperar a vantagem[44] (SHACHTMAN, 2008, tradução nossa).

Observa-se que a falta de conscientização de segurança levou ao uso de medidas extremas, que podem até configurar desvantagens operativas, uma vez que a proibição do uso de dispositivos de armazenagem removíveis priva os militares de um recurso simples, barato e de grande utilidade para a transferência de informações e dados entre computadores, desde que bem utilizados. A respeito dessa proibição, Habiger teceu o seguinte comentário: "ao reduzir nossas capacidades, nosso adversário, seja ele quem for, obteve uma pequena vitória[45]" (HABIGER, 2010, p. 41).

Portanto, a solução não está simplesmente na proibição, mas em um controle eficaz de uso e uma rotina automática de varredura em todos os dispositivos portáteis usados via USB, assim como outras mídias de armazenamento, tais como o CD e o DVD, além de, é claro, uma forte política de conscientização de segurança cibernética.

Deve-se ter a consciência de que as ações de exploração cibernética necessárias para a realização de uma ação ofensiva serão desenvolvidas desde os tempos de paz. Os integrantes da Marinha do Brasil devem entender que cada computador ligado à RECIM[46] está, constantemente, na linha de contato[47] da Guerra Cibernética, pois no ciberespaço não há área de retaguarda e suas características não admitem a existência de uma zona protegida. Logo, cada militar que estiver "logado" na rede deve ser considerado como um defensor cibernético. Assim, é fundamental que cada um compreenda que a defesa cibernética da

---

[44] It is apparent that over time, our posture to protect networks and associated information infrastructure has not kept pace with adversary efforts to penetrate, disrupt, interrupt, exploit or destroy critical elements of the GIG [Global Information Grid] … The decision to terminate use of removable rewritable media is a key component in the strategy to defend against attacks and establish a baseline for information system protection. Memory sticks, thumb drives and camera flash memory cards have given the adversary the capability to exploit our poor personal practices and have provided an avenue of attack … Malicious software (malware) programmed to embed itself in memory devices has entered our systems. Only through a layered defense of training, technology, procedures and personal recognizance, can we regain the high ground.

[45] By reducing our mission critical capabilities, our adversary, whoever it was, scored a small victory.

[46] Ver glossário.

[47] Ver glossário.

Marinha do Brasil começa em sua estação de trabalho, sendo este pensamento o principal motivador para a criação de uma conscientização de segurança em todos os usuários.

5.5 Recursos Humanos

Conforme já abordado, o ciberespaço é uma construção do homem que depende, particularmente, de sua engenhosidade e capacidade tecnológica. A Guerra Cibernética não é diferente e, portanto, depende de pessoal com alto nível de qualificação. Ocorre que esse tipo de capital humano, especializado no ciberespaço, é um recurso cada vez mais disputado pelo setor privado, o que faz com que as crescentes demandas dos setores militar e governamental enfrentem um grande desafio para atrair e manter esses recursos (KRAMER, 2009; RATTRAY, 2009).

Portanto, uma solução que pode ser adotada é o investimento na formação de pessoal próprio. Atualmente, não há a menor menção ao tema Guerra Cibernética nos currículos dos cursos de formação de oficiais e praças na Marinha do Brasil. Uma das necessidades prementes diz respeito à introdução de matérias relacionadas aos fundamentos de segurança cibernética em todos os cursos de formação, bem como os de especialização e de aperfeiçoamento. Tal medida visa a criar uma base de conhecimento comum mínima, de modo a fundamentar uma cultura cibernética. Esse é o primeiro passo para a montagem de nossa defesa cibernética.

Contudo, a preparação de recursos humanos para a Guerra Cibernética exige que se diferencie instrução e formação. A instrução permite fazer com que se opere com proficiência as ferramentas disponíveis, enquanto a formação constrói uma base de conhecimentos que possibilita lidar com toda a gama de desafios futuros. Por esse motivo é que se faz necessária uma formação dedicada aos nossos combatentes cibernéticos, que deve

incluir tanto a ciência da computação como a arte das operações cibernéticas (JABBOUR, 2010).

Não se pode, portanto, dissociar os fundamentos técnicos dos operativos, uma vez que não se trata apenas de segurança cibernética, mas, sim, de ações desenvolvidas no ciberespaço em prol de uma operação militar. Surgem, então, dois modelos para a formação de oficiais para a Guerra Cibernética: prover uma formação técnica aos oficiais combatentes, oriundos da Escola Naval, ou prover uma formação operativa aos oficiais técnicos.

Qual a melhor? No caso, propõe-se a adoção de ambas as soluções, de modo balanceado. Dessa forma, espera-se que o convívio entre esses guerreiros cibernéticos proporcione as condições para consolidar e harmonizar conhecimento e capacidades em ambos os campos, técnico e operativo.

A complexidade dos sistemas eletrônicos e de informação, que atualmente permeiam todas as funções militares, estando incorporados às ações da guerra convencional, já impõem um forte traço tecnológico à formação de pessoal. Isso pode ser observado na formação diversificada da Escola Naval, que prevê a formação técnica dos futuros oficiais combatentes, nas áreas de eletrônica, mecânica e sistemas de armas.

Os desafios impostos pela Guerra Cibernética impõem, de igual modo, que novas formações sejam previstas, voltadas às ciências exatas, com grande ênfase em ciências da computação. Assim, propõe-se que, à base multidisciplinar comum a todos os cursos da Escola Naval, seja acrescido conteúdo cibernético, provendo uma noção sobre Guerra Cibernética a todos os oficiais, que vai além da mera, porém fundamental, conscientização de segurança cibernética já proposta. Para a formação específica do combatente cibernético, faz-se necessário introduzir módulos pertinentes no contexto da formação diversificada, no curso de sistemas de armas, de modo a habilitar técnica e operacionalmente um seleto grupo de oficiais para a condução das ações defensivas da Guerra Cibernética. Essa formação seria

aprimorada com o curso de aperfeiçoamento, que complementaria os conhecimentos necessários, habilitando-os tecnicamente às ações ofensivas e de exploração.

Haveria, ainda, a necessidade de criação de um curso ou estágio, de modo a habilitar os guerreiros cibernéticos operacionalmente. Sugere-se que tanto os oficiais técnicos, como os oriundos da Escola Naval, após a realização do curso de aperfeiçoamento, realizem esta etapa.

5.6 Pesquisa e Desenvolvimento

Os programas e ferramentas utilizados na Guerra Cibernética são produtos customizados, uma vez que devem ser adaptados ao ambiente do sistema alvo e à finalidade específica a que se destinam. Os códigos maliciosos – malware – devem receber instruções explícitas e específicas sobre as ações que deverão desenvolver. As verdadeiras armas da Guerra Cibernética são muito mais complexas do que os simples códigos utilizados pelos hackers e, até mesmo, pelo crime cibernético, ainda que nada impeça que estes códigos mais simples possam ser utilizados, desde que existam vulnerabilidades que possam ser exploradas por essas ferramentas e que produzam os efeitos desejados para determinada ação. Entretanto, o uso operacional das ações de exploração e ofensivas requer um grande esforço de desenvolvimento de software dedicado para tais finalidades.

Esse fato gera a necessidade por uma capacidade de programação específica, ou seja, a existência de centros de desenvolvimento de ferramentas para a Guerra Cibernética, que trabalharão desde os tempos de paz e continuarão produzindo códigos específicos durante o conflito. Aqueles que possuem essa competência, considerada estratégica, a preservam, assim como os produtos desenvolvidos que, muitas das vezes, são mantidos em sigilo, de modo a não desvendar suas reais capacidades. Fica patente, pois, que nenhum governo

permitirá a transferência de ferramentas no estado da arte. O que se percebe é que, nos cursos desenvolvidos para elementos de outros países, como é o caso dos cursos realizados por militares brasileiros, as ferramentas utilizadas não passam de programas para exploração de vulnerabilidades conhecidas, muito similares em termos de complexidade ao que existe no mercado negro cibernético e utilizado por hackers em todo o mundo. Falta, portanto, acesso às reais armas da Guerra Cibernética.

O uso de armas cibernéticas adquiridas ou fornecidas por governos ou empresas estrangeiras, por aquisição ou por meio de cursos, apresenta um grave risco intrínseco. Certamente, essas soluções importadas poderão ser, na melhor das hipóteses, “desligadas”, ou seja, ter suas funções neutralizadas, tornadas sem uso, seja por sua inutilização por meio de desligamento digital, ou por meio da venda de contramedidas a nossos possíveis adversários, além de constituírem grave ameaça à segurança de nossos próprios sistemas, que poderão estar sendo vítimas de ações de exploração. Na pior das hipóteses, esses programas poderão conter códigos que as façam se voltar contra nossas próprias forças.

Decorre, então, a necessidade de uma solução autóctone. Confiar somente na solução adquirida pode significar não só a destruição de toda a capacidade, como também por em risco as operações militares. Portanto, a Marinha do Brasil deve buscar a capacidade de desenvolvimento de suas ferramentas para a Guerra Cibernética, o que gera a demanda por pessoal qualificado e por centros de desenvolvimento.

Ademais, o modelo de segurança e defesa do espaço cibernético brasileiro, idealizado pelo diretor do DSIC, prevê interações entre aquele departamento e as Forças Armadas, no que tange à análise de códigos maliciosos, com o intuito de propor soluções para neutralização das ameaças, bem como, a partir do conhecimento adquirido, a criação de produtos (armas cibernéticas) que podem ser usados em caso de guerra cibernética. Nesse caso, as interações seriam realizadas com os centros de desenvolvimento das Forças, que no

caso da Marinha do Brasil, estaria representado pelo CASNAV – Centro de Análise de Sistemas Navais (MANDARINO JUNIOR, 2009).

5.7 Segurança Cibernética x Guerra Cibernética

Dutra (2007, p. 3) afirma que “grande parte das pesquisas desenvolvidas voltadas para Segurança da Informação possuem (sic) aplicações em Guerra Cibernética”, uma vez que a principal diferença entre esses dois campos reside na origem e intenção do autor da ação, e não nas técnicas, ferramentas e conhecimentos empregados.

A assertiva acima reflete bem a relação existente entre Segurança e Guerra Cibernética, não havendo dúvidas de que a Segurança faz parte das ações de defesa da Guerra Cibernética. Ou seja, a segurança concorre para a defesa. Entretanto, não raro este relacionamento é confundido e toma-se o todo pela sua parte. Há que se ter em mente que a principal diferença entre essas duas funções reside na mentalidade de quem as executa: uma mentalidade técnico-administrativa versus uma mentalidade operativa.

Deve-se ter a perfeita compreensão de que a segurança representa apenas uma das ações da Guerra Cibernética. Há ainda as ações de exploração, que conforme abordado na seção pertinente, demandam um grande esforço de recursos humanos, e as ações ofensivas, cuja aplicação requer uma série de cuidados em função das características da Guerra Cibernética e suas implicações operacionais. Ao se buscar otimizar a aplicação de recursos financeiros e humanos por meio da centralização de atividades que são comuns apenas em parte, tem-se como resultado a diminuição da capacidade total de uma dessas atividades, normalmente aquela exógena à organização centralizadora, ou, até mesmo, de ambas.

Não é o fato de a Guerra Cibernética ser impregnada de tecnologia e dela depender integralmente que a fará deixar de ser um elemento operativo para ser tratada

essencialmente por técnicos. Assim fosse verdade, bastariam às marinhas modernas apenas engenheiros navais para operarem seus sistemas de mísseis a bordo dos modernos Centros de Operações de Combate[48] (COC). Não há dúvida quanto à competência técnica de analistas e engenheiros de sistemas, mas, em termos práticos, para a Guerra Cibernética eles fazem parte, juntamente com o software e o hardware, de um sistema de armas. Contudo, diferentemente dos sistemas de informação, os elementos técnicos não podem ser programados. Como usar, então, um sistema de armas em que o homem é parte integrante desse sistema? Este autor crê que a resposta é simples e, de certo modo, foi tratada na seção pertinente aos recursos humanos: deve-se proporcionar ao elemento técnico uma apropriada formação operacional e vice-versa.

As técnicas e táticas do combate cibernético, além de demandarem uma mentalidade operativa, vão muito além das normas de segurança cibernética. Infelizmente, essa é uma postura que não se observa frequentemente.

Vê-se, portanto, que o principal problema reside na mentalidade essencialmente técnica daqueles responsáveis pela condução da Guerra Cibernética. Ou seja, confunde-se o todo pela parte. A expressão Guerra Cibernética é utilizada, equivocadamente, para tratar de todo e qualquer incidente de segurança nas redes, conforme abordado na seção referente aos elementos conceituais.

Ao centralizarem-se as ações da Guerra Cibernética na organização responsável, entre outras tarefas de cunho técnico-administrativo, pela segurança cibernética, a primeira teve sua eficiência comprometida. É natural a preocupação com a segurança cibernética, em função do elevado número de incidentes acometidos às redes da Marinha do Brasil, que em três meses ultrapassa o número de quatro milhões (QUEIROZ, 2010). Entretanto, não se pode tratar a Guerra Cibernética apenas como segurança, pois significa denegrir as ações de defesa

---

[48] Ver glossário.

e abdicar da capacidade de executar ações de exploração e ofensivas. Ademais, a Guerra Cibernética deve ser tratada como uma função essencial às operações navais, não podendo ser delegada, exclusivamente, a uma organização de cunho técnico-administrativo, também responsável por outras tarefas diversas.

Recentemente a Marinha do Brasil criou uma Organização Militar (OM) dedicada à guerra eletrônica. Ocorre que a Guerra Cibernética é tão importante quanto aquela, mas, atualmente, é exercida como uma função secundária do CTIM. A Guerra Cibernética não pode ser relegada a uma função de segunda categoria, sob pena de privar a Marinha do Brasil de possuir capacitação nessa área. Impende, pois, que a Guerra Cibernética seja alçada a um patamar compatível com sua relevância às atuais operações militares, pois só assim poder-se-á assegurar as capacidades necessárias para enfrentar eficazmente as ameaças tecnológicas dos conflitos da atualidade.

Dos fatos expostos depreende-se, pois, haver necessidade de reestruturar a Guerra Cibernética na Marinha do Brasil. Não se deve, entretanto, olvidar que, em face de sua dimensão e constante restrição de recursos, se faz necessária alguma forma de racionalização de pessoal, o que se torna factível ao se tratar das ações de defesa da Guerra Cibernética. E é com base nessas premissas que se sugere uma nova estrutura.

Propõe-se, então, a criação do Comando Cibernético da Marinha do Brasil (CCMB). Organizacionalmente situado no Setor Operativo, sua estrutura operativa compreenderia três departamentos, correspondentes a cada uma das ações: de exploração, ofensivas e defensivas. Em função da grande dependência que a Guerra Cibernética possui dos esforços de inteligência, o CCMB deverá receber o status de órgão de inteligência, sendo o responsável pela execução da inteligência cibernética, por meio das ações de exploração.

O CCMB seria, portanto, o responsável pelo preparo e emprego da Guerra Cibernética na Marinha do Brasil, cabendo a ele planejar e executar os exercícios pertinentes,

que deverão ser do tipo “dupla ação”. Esse tipo de exercício é fundamental para o adestramento de todo o escopo das ações de Guerra Cibernética, por meio da formação de equipes que atuarão em ambos os partidos do exercício, proporcionando a cada uma dessas equipes um oponente capaz de oferecer níveis de ameaça adequados. Além de exercícios integrados aos da Esquadra, recomenda-se a execução de exercícios interdepartamentais, de modo a aprimorar as habilidades específicas de cada departamento.

Devido às restrições de pessoal e de modo a possibilitar a racionalização de recursos, há necessidade de quebra de paradigmas com relação aos conceitos de subordinação. Assim, sugere-se que o Departamento de Ações Defensivas de Guerra Cibernética seja subordinado administrativa e tecnicamente ao CTIM, enquanto seu emprego operacional estaria a cargo do CCMB. Entretanto, faz-se necessário um contínuo acompanhamento do modelo de subordinação proposto, de modo a realizar os ajustes necessários e, se for o caso, tão logo cessem tais restrições, subordinar aquele departamento unicamente ao CCMB. Em todos os casos, a orientação técnica permanecerá afeta à DCTIM.

Cumpre, porém, considerar que qualquer solução que seja adotada ensejará a quebra de paradigmas, uma vez que a Guerra Cibernética possui ambas as características técnica e operativa. Ou seja, subordiná-la a um ou outro setor demandará adaptações de antigos conceitos e a aceitação de que funções técnicas serão exercidas em unidades do Setor Operativo ou vice-versa. Contudo, deve-se observar que todos os modernos sistemas de armas possuem características técnicas, fruto de toda a tecnologia incorporada, e nem por isso deixam de estar sob a égide operacional, uma vez que sua destinação final é o emprego em operações militares. Com a Guerra Cibernética não é diferente, deve-se reconhecer que suas características operativas sobrepõem-se às técnicas, justificando, assim, seu posicionamento junto ao Setor Operativo.

6 CONCLUSÃO

Sem ter a veleidade em ser uma obra definitiva e respeitando os esforços pretéritos, o presente trabalho buscou o amparo da metodologia científica para analisar diversos aspectos da Guerra Cibernética. Deve ser ressaltado que não há fonte disponível que apresente o assunto na forma utilizada neste texto. Os conceitos apresentados foram montados a partir da pesquisa realizada e da experiência do autor. Portanto, faz-se mister que os preceitos operativos sejam submetidos a avaliação operacional, de modo a conferir validade à base doutrinária neles contida.

Uma das maiores carências atuais diz respeito à falta de uma doutrina de Guerra Cibernética. Há, portanto, necessidade de formulação de uma doutrina conjunta pertinente pelo Ministério da Defesa, de modo que as Forças possam adaptar suas próprias doutrinas, em função de suas particularidades, pautadas em uma base doutrinária comum. Em que pese o setor cibernético estar sob a responsabilidade do Exército Brasileiro, a Marinha do Brasil deve buscar manter-se na vanguarda do conhecimento, fruto de sua experiência na Governança de TI, de modo a poder ser ouvida no trato do tema, influenciando de forma positiva as decisões a serem tomadas no Ministério da Defesa.

A esse respeito, o presente trabalho apresentou em seus capítulos iniciais os fundamentos doutrinários que poderão contribuir à normatização da Guerra Cibernética. Cabe destacar o conceito de que a Guerra Cibernética é a guerra travada entre dois ou mais Estados no ciberespaço, seu ambiente operacional. Trata-se, portanto, de atividade realizada em apoio às operações militares que deve ser entendida como uma função eminentemente operativa.

Em seu emprego operacional, deve-se ter em mente que a Guerra Cibernética não é um fim em si mesma, pois não possui sentido a não ser que afete algo ou alguém no mundo

não cibernético. Portanto, seu principal emprego não é a destruição da capacidade de controle inimiga, mas a obtenção da superioridade de controle.

Diferentemente do senso comum de que a Guerra Cibernética apresenta um baixo custo de entrada, há que se ter em conta que tal assertiva somente é válida para ataques simples e que para a elaboração de ataques mais sofisticados serão necessários investimentos específicos por parte das forças militares que almejam capacitação na Guerra Cibernética, como se acredita ser o caso da Marinha do Brasil.

Reforça-se, pois, a ideia sobre a necessidade de investimento na preparação de recursos humanos para a condução das ações da Guerra Cibernética, cuja formação deve envolver, necessariamente, as vertentes técnica e operativa. Nesse sentido, sugere-se a modificação do currículo da Escola Naval, de modo iniciar a preparação de nossos oficiais, que seria complementada por um curso de aperfeiçoamento específico. O preparo se completaria com um curso de cunho operativo, criado especificamente para capacitar tanto os oficiais oriundos da Escola Naval como os oficiais de formação técnica.

O nível de interconectividade a que se chegou na Marinha do Brasil e a dependência cada vez maior nos sistemas de informação expõem a Força às vulnerabilidades inerentes e demandam que esteja preparada para a defesa cibernética de seus sistemas de informação. O primeiro passo para a montagem dessa defesa reside na formação de uma cultura de segurança cibernética em toda a Força, que deve estar focada na conscientização de todos os seus militares. Os riscos envolvidos exigem uma postura pró-ativa e, portanto, sugere-se incluir o tema nos currículos dos diversos cursos de carreira existentes.

A Guerra Cibernética já é uma realidade e o sucesso das operações militares depende diretamente da capacidade da Força com relação às ações operativas no ciberespaço. Não basta pensar apenas em defender nossos sistemas. Há necessidade de desenvolver capacidade ofensiva e de exploração.

Com base nos fundamentos apresentados ao longo do trabalho, acredita-se na necessidade de se reformular a estrutura organizacional da Guerra Cibernética na Marinha do Brasil. Portanto, a sugestão de criação de um comando operativo voltado especificamente às suas ações, o Comando Cibernético da Marinha do Brasil, busca prover a Força com um elemento adequado à condução eficaz e eficiente das ações da Guerra Cibernética, alçando-a a um patamar compatível com sua relevância às atuais operações militares.

O comprometimento com o efeito desejado é imanente a todos aqueles responsáveis pelo cumprimento de uma determinada missão. No caso da Guerra Cibernética como elemento operacional, o efeito desejado não diz respeito apenas à integridade dos sistemas de TI, mas guarda relação à preservação de vidas humanas, da condução de campanhas militares e, primordialmente, da própria missão. É com essa visão mais ampla que se deve enxergar a contribuição da Guerra Cibernética às operações militares, uma capacidade cada vez mais necessária às Forças Armadas que desejam cumprir seu papel em face dos desafios impostos pelos modernos campos de batalha de hoje e do futuro.

Atualmente, seria arriscado considerar que a Marinha do Brasil esteja plenamente preparada para enfrentar a Guerra Cibernética, entretanto a Força reconhece sua importância e envida esforços no sentido de sanar as atuais deficiências. Os novos conceitos oriundos dos avanços tecnológicos, o advento de um novo ambiente operacional caracterizado pelo ciberespaço, o qual não pode ser desprezado pelas modernas forças militares, e as características e preceitos operacionais da Guerra Cibernética impõem a ruptura de paradigmas e a adoção de soluções autóctones, de modo que a Marinha do Brasil possa alcançar a desejada capacidade operacional da Guerra Cibernética.

REFERÊNCIAS

ALBERTS, David S; HAYES, Richard E. **Power to the Edge**: Command and Control in the Information Age. EUA: DoD Command and Control Research Program, 2003. Disponível em: <http://www.dodccrp.org/files/Alberts_Power.pdf>. Acesso em : 20 jun. 2010.

ALLEN, Patrick D.; DEMCHAK, Chris. A Guerra Cibernética entre a Palestina e Israel. **Military Review**: Edição Brasileira, Kansas, EUA, v. 84, n. 1, p. 51-58, 1. trim. 2004.

ALMEIDA, Eduardo. Ex-hacker mais procurado dos EUA ensina na Campus Party como evitar ser vítima de golpes cibernéticos. **O Globo**, Rio de Janeiro, 26 jan. 2010. Disponível em: <http://oglobo.globo.com/tecnologia/mat/2010/01/26/ex-hacker-mais-procurado-dos-eua-ensina-na-campus-party-como-evitar-ser-vitima-de-golpes-ciberneticos-915714071.asp>. Acesso em: 27 jan. 2010.

ARQUILLA, John. **Frontline interview John Arquilla**. EUA, 4 mar. 2003. Entrevista concedida ao programa Frontline. Disponível em: <http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/arquilla.html>. Acesso em: 2 abr. 2010.

AZAROV, Serge S.; DODONOV, Alexander G. Instrumental Corrections for a Definition of Cyberwar. In: CARVALHO, F. D.; SILVA, E. M. da (Ed.). **Cyberwar – Netwar:** Security in the Information Age. Amsterdan, Holanda: IOS Press, 2006, cap. 1, p. 3-32.

BOLENG, Jeff; SCHWEITZER, Dennis; GIBSON, David S. **Developing Cyber Warriors**. EUA: U.S. Air Force Academy, 2008. Disponível em: <http://www.edocfind.com/download/pdf/Developing%20Cyber%20Warriors%20LtCol%20Jeff%20Boleng,%20Dr%20Dennis%20Schweitzer/aHR0cDovL3d3dy51c2FmYS5lZHUvZGYvZGZjcy9hY2NyL2RvY3MvRGV2ZWxvcGluZ19jeWJlcndhcnJpb3JzLnBkZg>. Acesso em: 15 mar. 2010.

BOYD, Bradley L. **Cyber Warfare: Armageddon in a Teacup?** 2009. 96 f. Dissertação (Master of Military Art and Science) – U.S. Army Command and General Staff College, Fort Leavenworth, EUA, 2009. Disponível em: <http://cgsc.contentdm.oclc.org/cgi-bin/showfile.exe?CISOROOT=/p4013coll2&CISOPTR=2601&filename=2652.pdf>. Acesso em: 24 de fev. 2010.

BRASIL. Congresso Nacional. Lei n. 10.683 de 29 de maio de 2003. Dispõe sobre a organização da Presidência da República e dos Ministérios e dá outras providências. **Diário Oficial da União**, Brasília, DF, 29 maio 2003, p. 2. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/2003/l10.683.htm>. Acesso em: 15 mar. 2010.

BRASIL. Diretoria-Geral do Material da Marinha. **DGMM-540**: Normas de Tecnologia da Informação da Marinha. 1 rev. Rio de Janeiro, 2009a.

BRASIL. Estado-Maior da Armada. **EMA-305**: Doutrina Básica da Marinha. 2 rev. Brasília, 2002.

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

BRASIL. Gabinete do Comandante do Exército. Ofício n. 1046, de 22 de dezembro de 2009, ao Chefe de Gabinete do Ministro de Estado da Defesa. **Integração e Coordenação dos Setores Estratégicos da Defesa**. Brasília, 22 dez. 2009b.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. Portaria n. 45 de 8 de setembro de 2009. Institui, no âmbito da Câmara de Relações Exteriores e Defesa Nacional (CREDEN), o Grupo Técnico de Segurança Cibernética e dá outras providências. **Diário Oficial da União**, Brasília, DF, 9 set. 2009c, p. 2. Disponível em: <http://www.in.gov.br/imprensa/visualiza/index.jsp?jornal=1&pagina=2&data=09/09/2009>. Acesso em: 05 abr. 2010.

BRASIL. Ministério da Defesa. **Diretriz Ministerial n. 14**. Integração e Coordenação dos Setores Estratégicos da Defesa. Brasília, 9 nov. 2009d.

BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa**: paz e segurança para o Brasil. Brasília, 2008.

BRASIL. Ministério da Defesa. **MD35-G-01**: Glossário das Forças Armadas. 4. ed. Brasília, 2007b.

BRASIL. Ministério da Defesa. **Política de Defesa Nacional**. Brasília. 2005.

BRASIL. Presidência da República. Decreto n. 5.772 de 8 de maio de 2006. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Gratificações de Exercício em Cargo de Confiança do Gabinete de Segurança Institucional da Presidência da República e dá outras providências. **Diário Oficial da União**, Brasília, DF, 9 maio 2006, p. 3. Disponível em: <https://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2006/Decreto/D5772.htm>. Acesso em: 15 mar. 2010.

BRASIL. Presidência da República. Decreto n. 6.931 de 11 de agosto de 2009. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Gratificações de Exercício em Cargo de Confiança do Gabinete de Segurança Institucional da Presidência da República e dá outras providências. **Diário Oficial da União**, Brasília, DF, 12 ago. 2009e, p. 1. Disponível em: <https://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2009/Decreto/D6931.htm>. Acesso em: 15 mar. 2010.

BRITTIN, Burdick H. **Derecho Internacional para oficiales en el mar**. 2 ed. Buenos Aires, Argentina: Instituto de Publicaciones Navales Del Centro Naval, 1991. 624 p.

CANADÁ. Department of National Defense. **B-GG-005-004/AF-010**: Information Operations. 1998.

CBS. Cyber War: Sabotaging the System. **CBS News: 60 minutes**. EUA, 8 nov. 2009. Disponível em: <http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml>. Acesso em: 22 mar. 2010.

CLARK, Richard A.; KNAKE, Robert. **Cyber War**: The Next Threat to National Security and What to Do About It. EUA: Ecco, 2010. 304 p.

COLARIK, Andrew M.; JANCZEWSKI, Lech J. **Cyber Warfare and Cyber Terrorism**. Hershey, EUA: Information Science Reference, 2008. 532 p.

CONTI, Gregory; SURDU, John. Army, Navy, Air Force, and Cyber - Is it Time for a Cyberwarfare Branch of Military? **IAnewsletter**, EUA, v. 12, n. 1, p. 14-18, 2009. Disponível em: <http://iac.dtic.mil/iatac/download/Vol12_No1.pdf>. Acesso em: 24 fev. 2010.

COUNCIL OF EUROPE. **Global reach of the Council of Europe Convention on Cybercrime**. UE, 9 mar. 2010. Disponível em: <http://www.coe.int/t/dc/files/themes/cybercrime/WorldMapCybercrime_E.pdf>. Acesso em: 26 maio 2010.

CHILTON, Kevin P. **Statement of General Kevin P. Chilton, Commander, United States Strategic Command, Before the Strategic Forces Subcommittee**, 16 mar. 2010. Disponível em: <http://www.stratcom.mil/posture/>. Acesso em: 26 abr. 2010.

CSIS, Threat Working Group of the CSIS Commission on Cybersecurity for the 44th Presidency. **Threats Posed by Internet**. CSIS: EUA, 28 out. 2008. Disponível em: <http://csis.org/files/media/csis/pubs/081028_threats_working_group.pdf>. Acesso em: 19 fev. 2010.

DENNING, Dorothy E. **A View of Cyberterrorism Five Years Later**. Naval Postgraduate School: EUA, 2006. Disponível em: <http://faculty.nps.edu/dedennin/publications/Cyberterror%202006.pdf>. Acesso em: 17 maio 2010.

DENNING, Dorothy E. Barriers to Entry: Are they lower for Cyber Warfare?. **IO Journal**, EUA, p. 6-10, abr. 2009. Disponível em: <http://faculty.nps.edu/dedennin/publications/Denning-BarriersToEntry.pdf>. Acesso em: 17 maio 2010.

DUTRA, André Melo Carvalhais. Introdução à Guerra Cibernética: a necessidade de um despertar brasileiro para o assunto. In: SIMPÓSIO DE GUERRA ELETRÔNICA: PESQUISA APLICADA À DEFESA NACIONAL, 9., 2007, São José dos Campos. **Artigos**... Disponível em: <http://www.sige.ita.br/IX_SIGE/Artigos/GE_39.pdf>. Acesso em: 15 mar. 2010.

ERBACHER, Robert F. Extending Command and Control Infrastructures to Cyber Warfare Assets. In: IEEE WORKSHOP ON INFORMATION ASSURANCE, 2005, West Point, NY-EUA. **Proceedings**... p. 446 – 447. Disponível em: <http://digital.cs.usu.edu/~erbacher/publications/CommandControl2.pdf>. Acesso em: 23 abr. 2010.

ESTADOS UNIDOS DA AMÉRICA. Defense Information Systems Agency Website. Sítio institucional da Agência de Sistemas de Informação do Departamento de Defesa norte-americano, 2010a. Disponível em: < http://www.disa.mil>. Acesso em: 1 jul. 2010.

ESTADOS UNIDOS DA AMÉRICA. Joint Chiefs of Staff. **JP 3-13**: Information Operations. 2006.

ESTADOS UNIDOS DA AMÉRICA. National Security Agency. **Global Information Grid**. EUA, 18 jun. 2009. Disponível em: <http://www.nsa.gov/ia/programs/global_industry_grid/index.shtml>. Acesso em: 1 jul. 2010.

ESTADOS UNIDOS DA AMÉRICA. Official Website of the United States Navy. **Navy Cyber Forces Established**. Norfolk, 26 jan. 2010b. Disponível em: <http://www.navy.mil/search/display.asp?story_id=50853>. Acesso em: 24 fev. 2010.

ESTADOS UNIDOS DA AMÉRICA. Official Website of the United States Navy. **Navy Stands Up Fleet Cyber Command, Reestablishes U.S. 10th Fleet**. Meade: Fleet Cyber Command Public Affairs, 29 jan. 2010c. Disponível em: <http://www.navy.mil/search/display.asp?story_id=50954>. Acesso em: 24 fev. 2010.

ESTADOS UNIDOS DA AMÉRICA. Senado Federal. **Advanced Questions for Lieutenant General Keith Alexander, USA Nominee for Commander, United States Cyber Command**. EUA, 2010d. 32 p.

ESTADOS UNIDOS DA AMÉRICA. The White House. **United States National Security Strategy**. EUA, maio 2010e. Disponível em: <http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf>. Acesso em: 28 maio 2010.

ESTADOS UNIDOS DA AMÉRICA. US Department of Defense. **U.S. Cyber Command Fact Sheet**. EUA, 25 maio 2010f. Disponível em: <http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf>. Acesso em: 1 jul. 2010.

FRANÇA, Junia Lessa; VASCONCELOS, Ana Cristina de. **Manual para normalização de publicações técnico-científicas.** 8. ed. Belo Horizonte: UFMG, 2007.

GATES, Robert. **Memorandum for Secretaries of the Military Departments**, Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations, Washington – EUA, 23 jun. 2009. Disponível em: <http://www.govexec.com/nextgov/0609/gates_cybercommand_memo.pdf>. Acesso em: 8 abr. 2010.

GORDON, Jason. Cyber Weaponization: Analysis of Internet Arms Development. In: COMPUTER SECURITY CONFERENCE, 2008, EUA. **Proceedings**… Disponível em: <http://www.computersecurityconference.com/2008/CSC2008-Gordon.pdf>. Acesso em: 23 abr. 2010.

GORMAN, Siobhan; DREAZEN, Yochi J.; COLE, August. Insurgents Hack U.S. Drones. **The Wall Street Journal**, Washington – EUA, 17 dez. 2009. Disponível em: <http://online.wsj.com/article/SB126102247889095011.html>. Acesso em: 28 maio 2010.

HABIGER, Eugene E. **Cyberwarfare and Cyberterrorism**: the need for a new U.S. Strategic Approach. EUA: The Cyber Secure Institute, 54 p., 1 fev. 2010. Disponível em: <http://cybersecureinstitute.org/docs/whitepapers/Habiger_2_1_10.pdf>. Acesso em: 24 fev. 2010.

INFORMATION WARFARE MONITOR. **Tracking GhostNet: Investigating a Cyber Espionage Network**. Information Warfare Monitor: Canadá, 29 mar. 2009. Disponível em: <http://www.nartv.org/mirror/ghostnet.pdf>. Acesso em: 19 fev. 2010.

JABBOUR, Kamal. CyberVision and Cyber Force Development. **Strategic Studies Quarterly**, EUA, v. 4, n. 1, p. 63-73, 2010. Disponível em: <http://www.au.af.mil/au/ssq/2010/spring/jabbour.pdf>. Acesso em: 21 abr. 2010.

KAKUTANI, Michiko. The Attack Coming from Bytes, not Bombs. **The Washington Times**, Washington, EUA, 26 abr. 2010. Disponível em: <http://www.nytimes.com/2010/04/27/books/27book.html>. Acesso em: 28 abr. 2010.

KRAMER, Franklin D. Cyberpower and National Security: Policy Recommendations for a Strategic Framework. 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. 1, p. 3-23.

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.

KUEHL, Daniel T. From Cyberspace to Cyber power: Defining the Problem. 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. 2, p. 24-42.

KWALWASSER, Harold. Internet Governance. 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. 21, p. 491-524.

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.

LAKE, Eli. Military needs cyberwar doctrine. **The Washington Times**, Washington, EUA, 14 maio 2010. Disponível em: <http://www.washingtontimes.com/news/2010/may/14/general-says-military-needs-cy/>. Acesso em: 31 maio 2010.

LEWIS, A. James. **The Cyber War Has Not Begun**. Washington, EUA: Center for Strategic and International Studies, 2010. Disponível em: <http://csis.org/files/publication/100311_TheCyberWarHasNotBegun.pdf>. Acesso em: 11 mar. 2010.

LEWIS, A. James. **The Korean Cyber Attacks and Their Implications for Cyber Conflict**. Washington, EUA: Center for Strategic and International Studies, 2009. Disponível em: <http://csis.org/publication/korean-cyber-attacks-and-their-implications-cyber-conflict>. Acesso em: 19 fev. 2010.

LIBICKI, Martin C. **Cyberdeterrence and Cyberwar**. Santa Mônica – Califórnia – EUA: Rand Corporation, 2009a. Disponível em: < http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf>. Acesso em: 27 maio 2010.

LIBICKI, Martin C. Military Cyberpower. 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, 2009b. cap. 11, p. 275-284.

MANDARINO JUNIOR, Raphael. **Um Estudo sobre a Segurança e a Defesa do Espaço Cibernético Brasileiro**. 2009b. 156 f. (Especialização em Ciência da Computação: Gestão da Segurança da Informação e Comunicações) – Departamento de Ciência da Computação, Universidade de Brasília, Brasília, 2009.

MANDEL, Arnaldo; SIMON, Imre; LYRA, Jorge L. de. A ARPANET. In: ____. **Informação: Computação e Comunicação**. São Paulo: USP, 1997. Disponível em: <http://www.ime.usp.br/~is/abc/abc/node20.html>. Acesso em: 13 mar. 2010.

MCAFEE. **Virtual Criminology Report 2009** - Virtually Here: The Age of Cyber Warfare. McAfee Inc: Santa Clara, EUA, 2009. Disponível em: <http://www.mcafee.com/us/local_content/reports/virtual_criminology_2009.pdf>. Acesso em: 23 abr. 2010.

MUTTIK, Igor. RÚSSIA: a economia, e não a máfia, alimenta o malware. **Sage**, Santa Clara, EUA, v. 2, n. 1, p. 16-21, fev. 2008. Disponível em: <www.mcafee.com/br/local_content/reports/sage_2008.pdf>. Acesso em: 11 mar. 2010.

NAKASHIMA, Ellen. Senators on key panel express confidence in cybersecurity nominee. **The Washington Post**, Washington, EUA, 16 abr. 2010. Disponível em: <http://www.washingtonpost.com/wp-dyn/content/article/2010/04/15/AR2010041505799.html>. Acesso em: 14 maio 2010.

PARKS, Raymon C.; DUGGAN, David P. Principles of Cyber-warfare. in: **Proceedings of the IEEE Workshop on Information Assurance**, West Point, NY-EUA, p 122 – 125, 2001. Disponível em: <http://www.periwork.com/peri_db/wr_db/2004_May_11_11_30_41/DOCS%20WEBREVIEW/PrinciplesCYBER%20WARFARE.pdf>. Acesso em: 15 mar. 2010.

QUEIROZ, João Augusto Gomes. Rio de Janeiro, 2010. Entrevista concedida a Luiz Artur Rodrigues Nunes.

RATTRAY, Gregory J. An Environmental Approach to Understanding Cyberpower. 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. 10, p. 253-274.

REUTERS. Estrago de botnet "Mariposa" poderia ter sido maior, diz polícia. **UOL Tecnologia**: Últimas Notícias. Madri, Espanha, 3 mar. 2010. Disponível em: <http://tecnologia.uol.com.br/ultimas-noticias/reuters/2010/03/03/estrago-de-botnet-mariposa-poderia-ter-sido-maior-diz-policia.jhtm>. Acesso em: 20 mar. 2010.

ROUGHEAD, Adm. Gary. **Memorandun 5440, CNO, for Commander of U.S. Fleet Forces and Director of Naval Intelligence**, Fleet Cyber Command/Tenth Fleet Implementation Plan, Washington – EUA, 23 jul. 2009.

SCOTT, Chris. **Cyber Warfare**: A Perspective on Cyber Threats and Technology in the Network-Centric Warfare Battlespace. Set. 2008. Apresentação realizada no US Army Cyber Symposium. Disponível em: <http://usacac.army.mil/cac2/CEW/repository/presentations/12_Dr%20Scott_MIT_%20Army_Cyber_Symposium_(Publicly_Releasable).pdf>. Acesso em: 24 fev. 2010.

SHACHTMAN, Noah. Military USB Ban Meant to Stop ‘Adversary Attacks’. **WIRED** – Danger Room. EUA, 20 nov. 2008. Disponível em: <http://www.wired.com/dangerroom/2008/11/military-usb-ba>. Acesso em: 28 maio 2010.

SHIMEALL, Timothy; WILLIAMS, Phil; DUNLEVY, Casey. Countering cyber war. **Nato Review**, Bruxelas, Bélgica, v. 49, p. 16-18, 2002. Disponível em: <http://www.nato.int/docu/rev-pdf/eng/0104-en.pdf>. Acesso em: 24 abr. 2010.

STARR. Stuart H. Toward a Preliminary Theory of Cyberpower. 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. 3, p. 43-88.

TENNANT, Don. The fog of (cyber) war. **Computerworld**, EUA, 27 abr. 2009. Disponível em: <http://www.computerworld.com/s/article/9130830/The_fog_of_cyber_war>. Acesso em: 24 fev. 2010.

TERRA, Redação. Primeiro Computador do Mundo Completa 60 anos. **Terra Notícias – Tecnologia**, São Paulo, 23 fev. 2006. Disponível em: <http://tecnologia.terra.com.br/interna/0,,OI892512-EI4799,00.html>. Acesso em: 13 mar. 2010.

TINNEL, Laura S.; SAYDJARI, O. Sami; FARRELL, Dave. Cyberwar Strategy and Tactics: An Analysis of Cyber Goals, Strategies, Tactics, and Techniques. In: IEEE WORKSHOP ON INFORMATION ASSURANCE, 2002, West Point, NY, EUA. **Proceedings**… p. 228-234. Disponível em: <http://www.cyberdefenseagency.com/publications/Cyberwar_Strategy_and_Tactics.pdf>. Acesso em: 15 mar. 2010.

VALLE, James Della. Brasil é campeão em conteúdo malicioso na AL. **INFO Online**. São Paulo, 10 fev. 2010. Disponível em: <http://info.abril.com.br/noticias/seguranca/brasil-e-campeao-em-conteudo-malicioso-10022010-10.shl>. Acesso em: 15 mar. 2010.

WILSON, Clay. Information Operations and Cyberwar: Capabilities and Related Policy Issues. In: **CRS Report for Congress**, EUA, 14 set. 2006. Disponível em: <http://www.fas.org/irp/crs/RL31787.pdf>. Acesso em: 11 mar. 2010.

WITTE, Brian. Naval Academy developing plan for cyber building. **The Baltimore Sun**, Baltimore-EUA, 26 jun. 2010. Disponível em: <http://www.baltimoresun.com/news/maryland/bs-md-naval-academy-cybersecurity-20100628,0,4653137.story>. Acesso em: 7 jul. 2010.

WRONA, Jacqueline-Marie Wilson. **From Sticks and Stones to Zeros and Ones**: the development of computer network operations as an element of warfare. 2005. 151 f. Dissertação (Mestrado em Tecnologia de Sistemas – Comando, Controle e Comunicações – C3) – Naval Postgraduate School, Monterey, Califórnia: EUA, 2005. Disponível em <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA439507&Location=U2&doc=GetTRDoc.pdf>. Acesso em: 24 fev. 2010.

ZENTGRAF, Maria Christina. **Introdução ao estudo da metodologia científica.** Rio de Janeiro: COPPEAD/UFRJ, 2009. Apostila.

ZUCCARO, Paulo Martino. Brasília, 2010. Entrevista concedida a Luiz Artur Rodrigues Nunes.

GLOSSÁRIO

Ativos de Informação: Os Ativos de Informação são os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso (BRASIL, 2009c).

Botnet: Rede formada por computadores infectados por malware, conhecidos por *bots* (forma reduzida da palavra inglesa *robot*) e controlados remotamente, de forma coordenada, por meio da Internet. O número de *bots* que a compõem pode variar, podendo chegar a números superiores a 13 milhões – rede Mariposa, descoberta em uma investigação em conjunto do FBI e da empresa Canadense Defence Intelligence. Por esse motivo, John Arquilla considerou que o computador mais poderoso do mundo não é um mainframe sendo construído nos EUA, mas um "computador paralelo" sendo criado por um hacker a partir de sua *botnet* (ARQUILLA, 2003; REUTERS, 2010; WILSON, 2009).

Centro de Operações de Combate: Estação do sistema de combate de uma força ou navio, capaz de coletar, filtrar, apresentar, avaliar e disseminar informações, além de controlar e coordenar as ações de combate (BRASIL, 2007b).

Ciclo OODA: Sequência na qual as ações em combate são desenvolvidas, de forma cíclica: observação – orientação – decisão – ação (OODA). Na primeira etapa, é percebida uma mudança no curso dos acontecimentos; na segunda, é produzida uma imagem mental da nova situação; na terceira etapa, chega-se à decisão da conduta a ser desenvolvida; e, na última, são implementadas as ações decorrentes da decisão tomada, voltando-se à da observação para um novo ciclo. Deve-se buscar realizar o ciclo completo mais rapidamente que o oponente (BRASIL, 2007b).

Consciência Situacional: Percepção precisa dos fatores e condições que afetam a execução da tarefa durante um período determinado de tempo, permitindo ou proporcionando ao seu decisor, estar ciente do que se passa ao seu redor e assim ter condições de focar o pensamento à frente do objetivo. É a perfeita sintonia entre a situação percebida e a situação real (BRASIL, 2007b).

Forense Computacional: É o emprego de técnicas e de procedimentos para aquisição, preservação, identificação, extração, restauração, análise e documentação de provas computacionais armazenadas em mídias eletrônicas, a fim de atender demandas administrativas, jurídicas ou judiciais (BRASIL, 2007a).

Infraestrutura Crítica: As Infraestruturas Críticas são as instalações, serviços, bens e sistemas que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade (BRASIL, 2009c).

IP – Internet Protocol: Conjunto de padrões e especificações que descrevem a forma pela qual os dados são divididos em pacotes – pequenos grupos de dados aos quais são adicionadas instruções de distribuição. O endereço IP é um número único que identifica um computador ou dispositivo ligado a uma rede (KRAMER; STARR; WENTZ, 2009).

Jus ad Bellum: Diz respeito à legalidade do emprego da força por um Estado contra outro, também conhecido como direito à guerra. Encontra-se regulado na Carta das Nações Unidas.

Jus in Bello: Corpo legal que regula a condução das ações em um conflito armado, constitui o direito da guerra. Sua principal fonte jurídica encontra-se nas Convenções de Genebra e seus protocolos Adicionais.

Linha de Contato: Limite avançado das posições amigas em um conflito convencional, quando há possibilidade de observação e fogos diretos entre as forças oponentes (BRASIL, 2007b).

Malware: Termo proveniente da fusão das palavras "*malicious software*", é também conhecido por código malicioso e consiste de um software – programa de computador – destinado a se infiltrar em um sistema de TI alheio, de forma não consentida, com o intuito de assumir seu controle, causar algum dano ou subtrair informações. Os vírus de computador, *worms*, cavalos de Tróia – *trojan horses* – e spywares são exemplos de malware.

Negação de Serviço (Denial of Service – DoS): Um ataque de negação de serviço busca paralisar o acesso aos serviços de TI saturando-os com um alto volume de requisições. O sucesso dessa prática está no volume de requisições, e não na sua natureza, de forma que é muito difícil preveni-lo.

Possibilidade do Inimigo – PI: Ação que o inimigo tem capacidade de adotar e que deve preencher dois requisitos: ser compatível com os meios de que ele dispõe e ser capaz de interferir ou afetar o cumprimento da missão do comandante (BRASIL, 2007b).

RECIM – Rede de Comunicações Integradas da Marinha: Conjunto de elementos computacionais, organizados em rede, que compõem a infraestrutura responsável pelo trafego de informações (digitais e analógicas) no âmbito da Marinha do Brasil (BRASIL, 2009a).

Rede de Informação Global – GIG (Global Information Grid): Sistema centrado em rede que opera em contexto global, para a coleta, processamento, armazenamento, disseminação e gerenciamento da informação, em apoio a todo o Departamento de Defesa norte-americano, à segurança nacional e à comunidade de inteligência, em tempos de guerra, crise e paz. Seu foco é a consciência situacional (ESTADOS UNIDOS DA AMÉRICA, 2009).

Segurança Cibernética: O GSI-PR define Segurança Cibernética 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.

Teatro de Operações: Parte do teatro de guerra - todo o espaço geográfico (terrestre, marítimo e aéreo) que seja ou possa ser diretamente envolvido nas operações militares de uma guerra – necessária à condução de operações militares de grande vulto, para o cumprimento de determinada missão e para o consequente apoio

logístico. Na Estrutura Militar de Guerra e na de Defesa, estão previstos o Teatro de Operações Terrestres e o Teatro de Operações Marítimo (BRASIL, 2007b).

APÊNDICE A – Exemplos de emprego real da Guerra Cibernética

O uso da capacidade de empreender ações de Guerra Cibernética em um conflito é um tema tratado com extrema cautela e poucas são as informações obtidas. As fontes da informação normalmente solicitam que não sejam identificadas, ou então prestam informações vagas. Há um exemplo claro, quando em uma matéria sobre as contratações realizadas pelas forças armadas norte-americanas o exército daquele país apenas reconheceu já ter feito uso de ataques cibernéticos, não informando nada mais.

Assim, considerando o entendimento de Guerra Cibernética constante do capítulo dois do presente trabalho, somente foram encontrados três exemplos de emprego real em operações militares: em Kosovo, no Iraque e no ataque Israelense à Síria.

Segundo John Arquilla, professor e analista de defesa da *Naval Postgraduate School*, da Marinha norte-americana, as ações ofensivas de Guerra Cibernética foram utilizadas de modo a incapacitar o sistema de defesa antiaérea da Sérvia:

> Kosovo foi, de certo modo, um campo de provas para certas capacidades cibernéticas. Estamos entrando em um tema muito sensível. Mas o que pode ser revelado é que alguns meios foram usados para distorcer as imagens geradas pelo sistema de defesa aérea integrada sérvio. Isso, com certeza, foi de importância crucial ao sucesso da campanha aérea[49] (ARQUILLA, 2003, tradução nossa).

Durante a guerra do Kosovo, algumas ações no campo cibernético não foram realizadas deliberadamente, porque os EUA queriam limitar seu emprego e, desse modo, enviar uma clara mensagem de que levavam a sério a Guerra Cibernética e de que um limite estaria sendo estabelecido, tornando-a uma forma aceitável de guerra (ARQUILLA, 2003).

Do lado sérvio ocorreram alguns ataques que foram facilmente debelados pelas defesas cibernéticas da OTAN. Porém, mesmo após o armistício e a retirada de tropas sérvias

---

[49] Kosovo was, in some ways, a proving ground of certain cyber capabilities. We get into a very sensitive area here. But what can be said is that some means may have been used to distort the images that the Serbian integrated air defense systems were generating. This, of course, was crucially important to waging a successful air campaign..

do Kosovo, um grupo de hackers, intitulado *Black Hand* – que não teve que se retirar, pois não estavam fisicamente lá –, começou uma campanha cibernética com o propósito de impedir a reconstrução do país. Naquele tempo, o Kosovo estava com sua infraestrutura de telecomunicações seriamente deficiente – as chances de se completar uma chamada telefônica eram inferiores a 25%. Desse modo, a Internet era crucial para o esforço de reconstrução, como elemento complementar de comunicações, e foi alvo de contínuos ataques cibernéticos por aquele e outros grupos de hackers. Tal fato traz à luz um aspecto interessante nesse tipo de conflito, que nem sempre poderá ser enquadrado como Guerra Cibernética de acordo com a definição apresentada, que é o envolvimento de civis, já explorado em outro tópico deste trabalho (ARQUILLA, 2003).

Com relação ao Iraque, em maio de 2007, os EUA realizaram ataques cibernéticos, por meio da *National Security Agency*, tendo como alvos os computadores utilizados pelos insurgentes no Iraque e a rede de telefonia celular daquele país. O propósito desses ataques foi o de negar aos insurgentes sua capacidade de comando e controle, uma vez que tais meios eram utilizados na coordenação e execução de atentados à bomba nas estradas iraquianas, contra as forças norte-americanas, cujas filmagens eram veiculadas por meio da Internet. Tais meios passaram a ser controlados por aquela agência, que, em uma combinação de ações ofensivas e exploratórias, os utilizou para conduzir os insurgentes iraquianos a locais de emboscada preparados por forças norte-americanas (HABIGER, 2010).

Outra ação, que consistia em um ataque cibernético a computadores do sistema financeiro iraquiano, chegou a ser planejada. Entretanto, tal ação não foi autorizada, uma vez que a rede bancária iraquiana é ligada à rede europeia e temia-se que a realização do ataque pudesse causar efeitos colaterais em bancos e caixas eletrônicos localizados na Europa. A interconectividade global das redes e a existência de ligações das redes militares iraquianas à infraestrutura civil foram causas que notadamente frustraram as tentativas das forças norte-

americanas de montar um ataque cibernético limitado aos alvos militares localizados no Iraque (WILSON, 2006).

Com relação às forças iraquianas, o único uso comprovado consistiu de ações de exploração realizadas por um grupo de insurgentes que, munidos de um laptop e software de compartilhamento de arquivos, de custo irrisório, em torno de US$ 30, conseguiu acesso às informações em vídeo transmitidas pelos veículos aéreos não tripulados (VANT) norte-americanos Predator. Dessa forma, os insurgentes podiam facilmente monitorar as operações militares norte-americanas, privando-as muitas vezes do elemento surpresa e permitindo aos insurgentes evitar as áreas sob vigilância (GORMAN; DREAZEN; COLE, 2009; HABIGER, 2010).

Em 6 de setembro de 2007, Israel lançou um ataque aéreo a instalações nucleares sírias, que estavam sendo construídas com o apoio da Coréia do Norte. Ocorre que, na véspera do ataque aéreo, foi realizado um ataque cibernético que paralisou o sofisticado sistema de defesa aérea sírio, recém-adquirido da Rússia. Na verdade o sistema parecia estar funcionando normalmente, entretanto, os radares estavam sob controle israelense. Esses são os fatos, ou seja, Israel planejou e executou com perfeição uma ação ofensiva de Guerra Cibernética, de modo a permitir a entrada de seus caças no espaço aéreo sírio sem serem detectados (CLARK; KNAKE, 2010).

Existem três opções de como o ataque foi realizado. Inicialmente, há a possibilidade de utilização de um VANT com características *stealth* que introduziu um código malicioso por meio da frequência radar. Nesse caso, deve-se ter em mente que o radar é, por seu princípio de funcionamento, uma porta de entrada de sinais que serão processados de modo a calcular dados sobre o alvo detectado, ou seja, o radar permite naturalmente a entrada de um sinal eletrônico que alimentará seus sistemas computadorizados. Desse modo, o VANT pode ter captado e utilizado a frequência do radar para enviar pacotes de dados contendo o

código malicioso para os computadores do sistema de defesa aérea sírio. Há indícios de que os EUA possuem um sistema de ataque cibernético semelhante, chamado *Senior Sutter*. A segunda possibilidade diz respeito ao uso de um elemento infiltrado, ou seja, o elemento interno. Por fim, o acesso aos sistemas sírios pode ter sido realizado por meio de agentes israelenses que interceptaram a infraestrutura física do sistema, como, por exemplo, os cabos de fibra ótica do sistema de defesa aérea. De qualquer modo, a ação israelense configura um exemplo clássico de emprego da Guerra Cibernética, por meio da qual se obteve o controle de sistemas do oponente de modo a possibilitar a realização de ações no mundo real (CLARK; KNAKE, 2010).

APÊNDICE B – Figuras

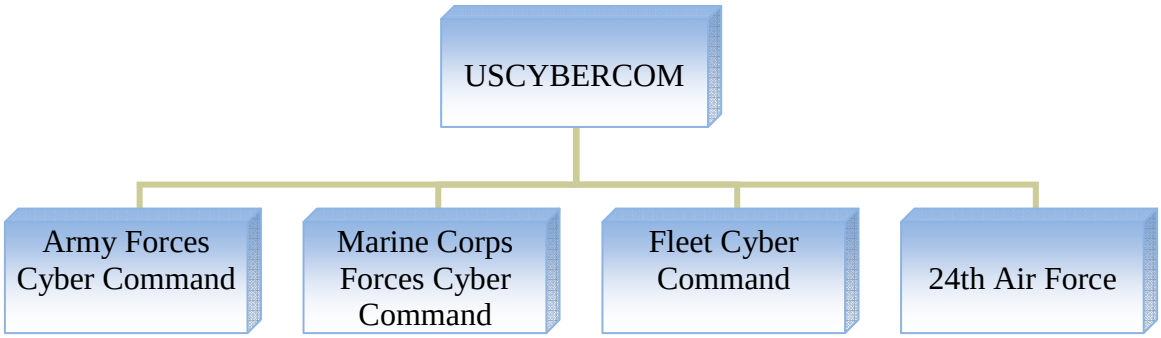

FIGURA 1 – Organização do USCYBERCOM

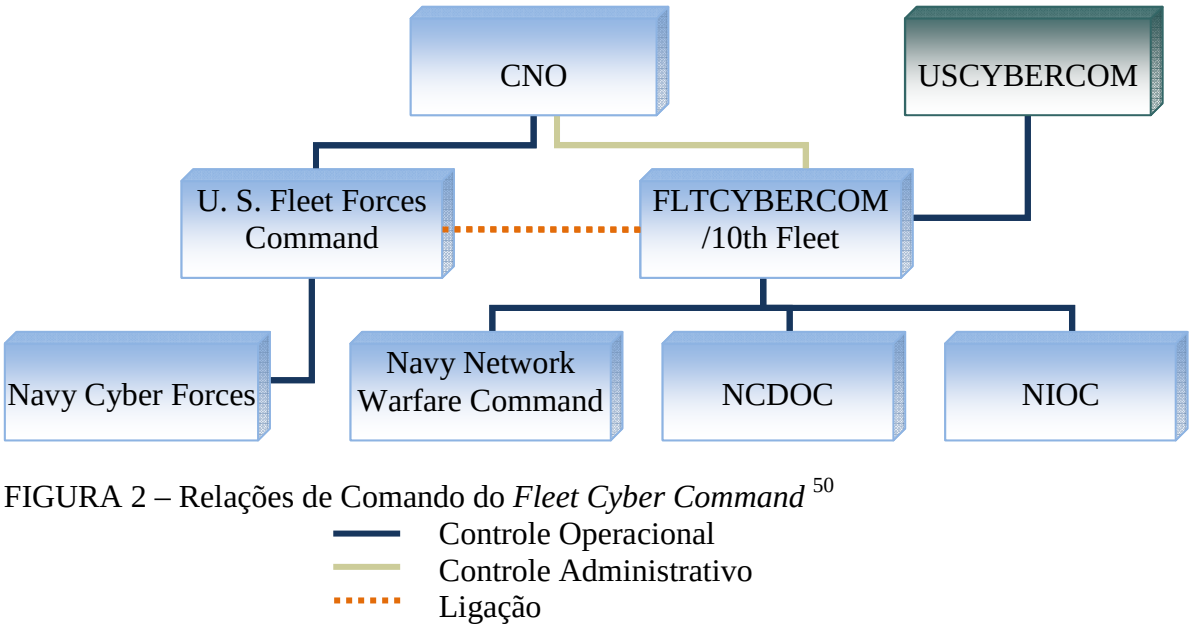

FIGURA 2 – Relações de Comando do *Fleet Cyber Command* [50]

---

[50] Navy Network Warfare Command: unidade de operações de informação, inteligência, redes e espaço, é responsável pelo estabelecimento de redes seguras para a condução de operações de informação e cibernéticas.

NCDOC – Navy Cyber Defense Operations Command: responsável pela condução da segurança cibernética, consiste, basicamente, de equipes de tratamento e resposta a incidentes de rede.

NIOC – Navy Information Operations Command: responsável pela condução de operações de informação e criptologia.

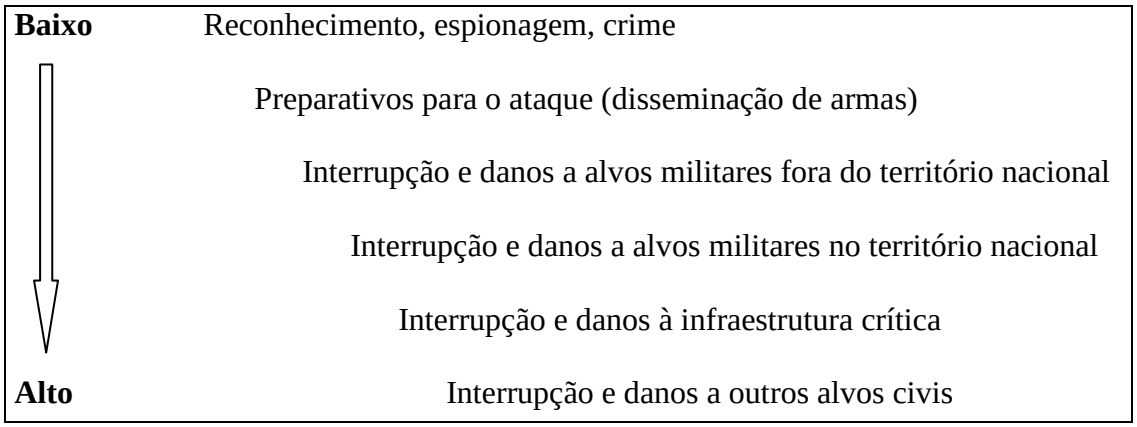

FIGURA 3 – Limiares do conflito cibernético (LEWIS, 2009)