**ESCOLA DE COMANDO E ESTADO-MAIOR DO EXÉRCITO**
***ESCOLA MARECHAL CASTELLO BRANCO***

Ten Cel Com JOÃO MARINONIO ENKE **CARNEIRO**

# A Guerra Cibernética: uma proposta de elementos para formulação doutrinária no Exército Brasileiro

Rio de Janeiro

2012

Ten Cel Com JOÃO MARINONIO ENKE **CARNEIRO**

# A Guerra Cibernética: uma proposta de elementos para formulação doutrinária no Exército Brasileiro

Tese apresentada à Escola de Comando e Estado-Maior do Exército, como requisito parcial para a obtenção do título de Doutor em Ciências Militares.

Orientador: Ten Cel Inf Jaime Flammarion Santos Costa
Co-orientador: Ten Cel Com Márcio Ricardo Souza Fava

Rio de Janeiro
2012

C289 Carneiro, João Marinonio Enke.
A Guerra Cibernética: uma proposta de elementos para formulação doutrinária no Exército Brasileiro / João Marinonio Enke Carneiro. 2012. 203 f. : il ; 30 cm.

Tese (Doutorado) – Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2012.
Bibliografia: f 134 - 140.

1. Guerra Cibernética. 2. Defesa Cibernética. 3. Operações de Informação. 4. Segurança Cibernética. 5. Doutrina. I. Título.

CDD 355.02

Ten Cel Com JOÃO MARINONIO ENKE **CARNEIRO**

# A Guerra Cibernética: uma proposta de elementos para formulação doutrinária no Exército Brasileiro

Tese apresentada à Escola de Comando e Estado-Maior do Exército, como requisito parcial para a obtenção do título de Doutor em Ciências Militares.

Aprovado em 08 de outubro de 2012.

BANCA EXAMINADORA

_____
Jaime Flammarion Santos Costa – Ten Cel Inf – Dr. Presidente
Escola de Comando e Estado-Maior do Exército

_____
José Carlos dos Santos – Gen Div – Dr. Membro
Centro de Defesa Cibernética

_____
Márcio Teixeira de Campos – Cel Com – Dr. Membro
Centro de Comunicações e Guerra Eletrônica

_____
Marcelo Oliveira Lopes Serrano – Cel Cav R1 – Dr. Membro
Escola de Comando e Estado-Maior do Exército

_____
Eduardo Xavier Ferreira Migon – Ten Cel Cav – Dr. Membro
Escola de Comando e Estado-Maior do Exército

À minha esposa Maristela e minhas filhas Maria Carolina e Maria Cristina, rendo a mais sincera homenagem pela paciência, apoio, carinho e compreensão, sem os quais a realização deste trabalho não teria sido possível.

## AGRADECIMENTOS

Agradeço inicialmente ao Bom Deus, o todo-poderoso, que sempre zelou pela segurança e saúde de toda a minha família e que sempre me confortou e mostrou a saída nos momentos de maior angústia e preocupação, iluminando o caminho a seguir.

Ao Tenente-Coronel Márcio Ricardo Souza Fava por ter me convencido a pesquisar esse assunto e ter me apoiado e orientado enquanto era instrutor da ECEME. Esse convencimento inicial certamente mudou o rumo da minha carreira militar.

Ao Tenente-Coronel Luiz Carlos Amaro Damasceno pela orientação segura e serena durante o meu 2º ano da ECEME.

Ao General José Carlos dos Santos, atual Chefe do Centro de Defesa Cibernética e ao Coronel Luiz Cláudio Gomes Gonçalves, Chefe do Núcleo do Centro de Defesa Cibernética por criarem a oportunidade de que eu pudesse me integrar ao CDCiber após o curso da ECEME, chefiando a Seção de Doutrina, o que, em última análise, viabilizou esse trabalho.

Ao meu atual orientador e, sobretudo, amigo Tenente-Coronel Jaime Flammarion Santos Costa, que, com muita paciência e tolerância me mostrou caminhos e alternativas, me dando confiança para "navegar em horizonte livre acreditando piamente na bússola".

Ao Chefe da Divisão de Doutrina do Centro de Defesa Cibernética, Coronel QEM José Ricardo Souza Camelo cuja grande experiência acadêmica, excepcional boa vontade e companheirismo muito me auxiliou nos momentos finais e decisivos deste trabalho. Este trabalho representa o início de uma grande jornada que ainda teremos à frente.

À minha família e aos meus companheiros na ECEME e no CDCiber, que sempre acreditaram que esse trabalho poderia ser realizado.

“O general que avançar sem ambicionar fama e retrair sem temer cair em desgraça, cujo único pensamento for proteger seu país e prestar um bom serviço ao seu Soberano, é a jóia do Estado.” (Sun Tzu)

“Nem o sábio e nem o valente descansam na trilha da história para esperar o trem do futuro passar sobre ele.” (Dwight D. Eisenhower)

"A vitória pertence àqueles que se antecipam às grandes mudanças na arte da guerra, e não aos que apenas procuram adaptar-se, depois que as mudanças ocorrem."
(Júlio Douhet)

## RESUMO

O presente trabalho tem por objetivo contribuir para o incremento do banco de dados doutrinário fornecendo subsídios, estudos e fundamentos ao Estado-Maior do Exército, a quem cabe formular, propor e manter atualizadas a doutrina vigente no Exército, apresentando elementos que possam ser utilizados para a formulação doutrinária, cujo objetivo final é o estabelecimento da Doutrina de Guerra Cibernética no âmbito do Exército Brasileiro. O estudo foi realizado entre os anos de 2010 e 2012, nas cidades do Rio de Janeiro e Brasília, na Escola de Comando e Estado-Maior do Exército e no Centro de Defesa Cibernética. Foi realizado um estudo documental, baseado no que já se tem feito em termos de Doutrina de Guerra Cibernética no Exército Brasileiro, principalmente nas 2ª e 3ª Subchefias do EME, no Departamento de Ciência e Tecnologia, no Centro de Defesa Cibernética e no Centro de Comunicações e Guerra Eletrônica do Exército. O método foi o comparativo, buscando identificar semelhanças e compreender divergências com doutrinas de Guerra Cibernética em formulação em outros países, com ênfase nos Estados Unidos da América. É feita uma análise do cenário atual, apresentando o paradigma que faz surgir o emprego das Operações de Informação, no qual está situado a Guerra Cibernética. São descritos os órgãos e atores de segurança e defesa cibernética no Brasil, mostrando as suas atribuições e o seu papel dentro do setor cibernético. Em seguida são apresentados os pontos julgados mais relevantes da doutrina de guerra cibernética dos Estados Unidos da América e de outros países, culminando com as discussões e apresentação de elementos para contribuir com formulação doutrinária pretendida. Espera-se, dessa forma, colaborar com o Exército Brasileiro na concretização de seu objetivo estratégico de transformar-se atuando sobre o vetor de transformação da doutrina.



Palavras-chave: Guerra Cibernética, Defesa Cibernética, Operações de Informação, Segurança Cibernética, Doutrina.

## ABSTRACT

This study main objective is to contribute to increase the doctrinal database providing subsidies, studies and fundamentals to the Brazilian Army General Staff, who must formulate, propose and keep the Army Doctrine updated, presenting elements that could be used in the establishment of Cyber Warfare Doctrine in the Brazilian Army. The study was conducted between 2010 and 2012, at the cities of Rio de Janeiro and Brasilia, in the Army War College (Escola de Comando de Estado-Maior do Exército) and in the Cyber Defense Center (CDCiber). A documental study was carried, based on what has already been done in terms of Cyber Warfare Doctrine in the Brazilian Army, mainly in the 2nd and 3rd Divisions of the Brazilian Army General Staff (EME), in the Science and Technology Department (DCT), in the Cyber Defense Center (CDCiber) and in the Army Signal and Electronic Warfare Center (CComGEx). The comparative method was used in order to identify similarities and understand differences in some countries that are developing their Ciber Warfare doctrine, with emphasis on the United States. We analyze the present scenario, with the paradigm that gives rise to the use of Cyber Warfare as a component of Information Operations. We describe the agencies and the stakeholders of Cyber Security and Cyber Defense in Brazil, showing their roles into the Cyber Sector. After that, the most relevant points of USA and other countries Cyber Warfare doctrine are shown, culminating in the discussions and elements presentation to contribute to the desired doctrinal formulation. It is expected, thus collaborating with the Brazilian Army in achieving its strategic objective of transforming itself acting on the doctrine transformation vector.



Keywords: Cyber Warfare, Cyber Defense, Information Operations, Doctrine.

## LISTA DE FIGURAS

## LISTA DE QUADROS

## LISTA DE ABREVIATURAS E SIGLAS

| | |
|---|---|
| ABIN | Agência Brasileira de Inteligência |
| ANATEL | Agência Nacional de Telecomunicações |
| APF | Administração Pública Federal |
| C2 | Comando e Controle |
| CASNAV | Centro de Análises de Sistemas Navais |
| CASOP | Centro de Apoio a Sistemas Operativos |
| CCA | Centro de Computação da Aeronáutica |
| CCA-BR | Centro de Computação da Aeronáutica de Brasília |
| CCA-RJ | Centro de Computação da Aeronáutica do Rio de Janeiro |
| CCA-SJ | Centro de Computação da Aeronáutica de São José dos Campos |
| CComGEx | Centro de Comunicações e Guerra Eletrônica do Exército |
| CCOp Seg | Centro de Coordenação de Operações de Segurança |
| CCOPAB | Centro Conjunto de Operações de Paz do Brasil |
| CDCiber | Centro de Defesa Cibernética |
| CDN | Conselho de Defesa Nacional |
| CDS | Centro de Desenvolvimento de Sistemas |
| CEAGAR | Centro de Estudo e Avaliação da Guerra Aérea |
| CEPESC | Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações |
| CERT.br | Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil |
| CEMIG | Centrais Elétricas de Minas Gerais |
| CGSI | Comitê Gestor da Segurança da Informação |
| CIAER | Centro de Inteligência da Aeronáutica |
| CIE | Centro de Inteligência do Exército |
| CIGE | Centro de Instrução de Guerra Eletrônica |
| CIM | Centro de Inteligência da Marinha |
| CIR / RJ | Centro de Incidentes de Rede do Rio de Janeiro |
| CITEx | Centro Integrado de Telemática do Exército |
| CLTI | Centros Locais de Tecnologia da Informação |

| | |
|---|---|
| CNA | Computer Network Attack |
| CND | Computer Network Defense |
| CNE | Computer Network Exploitation |
| COMAER | Comando da Aeronáutica |
| COR | Centro de Operações Rio |
| COTEC-TI | Comissão Técnica de Tecnologia da Informação |
| COTIM | Conselho de Tecnologia de Informação da Marinha |
| CREDEN | Câmara de Relações Exteriores e Defesa Nacional |
| CSIRT | Computer Security Incident Response Team |
| CT | Centros de Telemática |
| CTA | Centros de Telemática de Área |
| CTEx | Centro Tecnológico do Exército |
| CTIM | Centro de Tecnologia da Informação da Marinha |
| CTIR FAB | Centro de Tratamento de Incidentes de Redes da Força Aérea Brasileira |
| CTIR Gov | Centro de tratamento de incidentes de rede do governo federal |
| CTIR MB | Centro de Tratamento de Incidentes de Redes da Marinha do Brasil |
| DCT | Departamento de Ciência e Tecnologia |
| DCTIM | Diretoria de Comunicações e Tecnologia da Informação da Marinha |
| DECEA | Departamento de Controle do Espaço Aéreo |
| DFAP | Departamento das Forças Armadas do Povo |
| DGMM | Diretoria Geral da Material da Marinha |
| DIRTI | Diretoria de Tecnologia da Informação |
| DITEL | Diretoria de Telecomunicações |
| DSIC | Departamento de Segurança da Informação e Comunicações |
| DTCEATM-RJ | Destacamento de Controle do Espaço Aéreo e Telemática do Rio de Janeiro |
| DTI | Diretoria de Tecnologia da Informação da Aeronáutica |
| DTI | Divisão de Tecnologia da Informação |
| EB | Exército Brasileiro |

| | |
|---|---|
| EBNet | Rede Corporativa do Exército |
| EMAER | Estado-Maior da Aeronáutica |
| EMBRATEL | Empresa Brasileira de Telecomunicações |
| EME | Estado-Maior do Exército |
| END | Estratégia Nacional de Defesa |
| EsCom | Escola de Comunicações |
| EsIMEx | Escola de Inteligência Militar do Exército |
| EUA | Estados Unidos da América |
| FA | Forças Armadas |
| FAB | Força Aérea Brasileira |
| G Ciber | Guerra Cibernética |
| GC2 | Grupo Finalístico de Comando e Controle |
| GGE | Grupo Finalístico de Guerra Eletrônica |
| GI | Guerra da Informação |
| GRA | Grupo de Resposta a ataques do SERPRO |
| GSI | Gabinete de Segurança Institucional |
| GTSIC | Grupos Técnicos de Segurança das Infraestruturas Críticas |
| IC | Infraestruturas Críticas |
| ICI | Infraestruturas Críticas da Informação |
| IME | Instituto Militar de Engenharia |
| INEW | Integrated Network Electronic Warfare |
| INSCOM | Army Intelligence and Security Command |
| ITA | Instituto Tecnológico da Aeronáutica |
| ITI | Instituto Nacional da Tecnologia da Informação |
| MB | Marinha do Brasil |
| MD | Ministério da Defesa |
| MP | Medida Provisória |
| NuCDCiber | Núcleo do Centro de Defesa Cibernética |
| NuPDGI | Núcleo de Pesquisa e Desenvolvimento em Guerra de Informação |
| ODS | Órgão de Direção Setorial |
| OM | Organização Militar |
| OMDS | Organizações Militares Diretamente Subordinadas |

| | |
|---|---|
| Op Info | Operações de Informação |
| PBCT | Plano Básico de Ciência e Tecnologia |
| PDA | Assistentes Pessoais Digitais |
| PGED | Programa de Pós-Graduação em Engenharia de Defesa |
| PPGAO | Programa de Pós-Graduação em Análise Operacional |
| PR | Presidência da República |
| PTIM | Plano de Tecnologia da Informação da Marinha |
| PTTC | Prestador de Tarefa por Tempo Certo |
| RITEx | Rede Integrada de Telefonia do Exército |
| RRF | Redes Rádios Fixas |
| RRFP | Rede Rádio Fixa Principal |
| RRFS | Redes Rádio Fixa Secundárias |
| SC2Ex | Sistema de Comando e Controle do Exército |
| SC2FTer | Sistema de Comando e Controle da Força Terrestre |
| SCh | Subchefia |
| SCT | Secretaria de Ciência e Tecnologia |
| SCTEx | Sistema de Ciência e Tecnologia do Exército |
| SERPRO | Serviço de Processamento de Dados Federal |
| SIC | Segurança da Informação e Comunicações |
| SINFOEx | Sistema de Informação do Exército |
| SIPAM | Sistema de Proteção da Amazônia |
| SIPLEx | Sistema de Planejamento do Exército |
| SISBIN | Sistema Brasileiro de Inteligência |
| SISCOMIS | Sistema Militar de Comunicações por Satélite |
| SISMC2 | Sistema Militar de Comando e Controle |
| SisTEx | Sistema de Telemática do Exército |
| SRCC / DPF | Serviço de Repressão ao Crime Cibernético do Departamento de Polícia Federal |
| STI | Secretaria de Tecnologia da Informação |
| STIC2 | Sistema de Tecnologia de Informação e Comando e Controle |
| STIR | Seções de Tratamento de Incidentes de Rede |
| TIC | Tecnologia da Informação e das Comunicações |
| UNODC | United Nations Office on Drugs and Crime |

| | |
|---|---|
| VoIP | Voice over Internet Protocol (Protocolo de Voz sobre Internet) |
| VPN | Rede privada virtual |

## SUMÁRIO

# 1 **INTRODUÇÃO**

Desde que William Gibson[1] publicou em junho de 1984 a sua obra intitulada Neuromancer, o escritor norte-americano já antevia a criação de um novo local, um espaço virtual criado pela interação da tecnologia com o homem, onde uma nova realidade poderia surgir, trazendo modificações profundas nas relações humanas e na própria forma de conduzir suas relações, sejam elas pessoais, profissionais ou de negócios. Por extensão, as relações entre Estados e entre organizações, algumas vezes mais poderosas que muitos Estados, também sofreram grandes adaptações. Credita-se a Gibson, nessa obra, a criação do termo ciberespaço (*cyberspace*) ou espaço cibernético.

Com o passar dos anos, muitas atividades do mundo real foram paulatinamente migrando para esse espaço cibernético. Podem ser citados como exemplos a substituição das cartas enviadas pelo serviço das empresas de correios e telégrafos pelo correio eletrônico, atividades de comércio, tanto entre empresas[2] quanto destinadas ao consumidor final[3], controle de sistemas elétricos, de telecomunicações, de plantas industriais e de infraestrutura em geral, dentre muitos outros. O governo federal brasileiro também se beneficia da agilidade e da escala, utilizando o seu próprio portal para realizar as suas aquisições. O site Comprasnet[4], foi criado em 1997 e desde 2001 funciona como o portal de compras do governo.

O que aconteceria se esses serviços, que estão se tornando cada vez mais essenciais, fossem desativados ou interrompidos por longos períodos? Se infraestruturas críticas[5] como a de energia elétrica ou de fornecimento de água fossem afetadas? Qual seria o efeito dessas ações sobre a população do país? Qual seria o efeito dessas ações sobre a confiança depositada pelos cidadãos em seu governo?

A espionagem, a dissimulação, a falta de definição de fronteiras e o uso das técnicas para se obter vantagem, seja ela pessoal ou para alguma organização ou, até mesmo, um Estado visando algum objetivo não nasceram com o ciberespaço,

---

[1] GIBSON, William. **Neuromancer**. 4. ed. São Paulo: Aleph, 2008. ISBN 978-85-7657-049-3.
[2] Também chamadas de relações B2B – Business to Business
[3] Também chamadas de relações B2C – Business to Consumer
[4] Acessível em http://www.comprasnet.gov.br/
[5] O termo infraestruturas críticas tem sido substituídas pelo termo infraestruturas estratégicas pelo Estado-Maior do Exército e Ministério da Defesa, por influência dos planejamentos do projeto PROTEGER, que visa à defesa e proteção dessas infraestruturas. Como não há, até o momento, um substituto correlato para infraestruturas críticas da informação, conceito a ser abordado posteriormente, o autor optou por manter a terminologia infraestruturas críticas.

foram levadas para ele. Ele é o reflexo da própria humanidade, liberta em suas ideias e pensamentos e aprisionada em seus defeitos e imperfeições.

Existe, entretanto, uma grande diferença entre o espaço físico do mundo real e o espaço virtual do ciberespaço: as regras que se aplicam a um normalmente não se aplicam ao outro. Quem domina as técnicas e detém o conhecimento específico de cada espaço leva uma enorme vantagem.

Estamos, portanto, diante do **surgimento de um novo campo de batalha**. Antigos princípios da guerra ganham novas formas de serem executados. Por exemplo, o princípio da Massa[6], poderá ser obtido por uma rede de milhares de computadores "zumbis" (*botnet*)[7] que concentrarão seus acessos em um serviço específico durante um período de tempo determinado. Se precauções não tiverem sido tomadas e a defesa não tiver sido cuidadosamente implementada, há uma considerável chance desse tipo de ataque, que tem uma sofisticação tecnológica considerada baixa, obter sucesso.

Com isso, é natural para quem se prepara diuturnamente para proteger um Estado e combater no mundo físico, se assim for necessário, também fazer o mesmo no ciberespaço. Segundo estudos[8] da McAfee, uma respeitada empresa internacional especializada em segurança da informação, há indícios de que cerca de 120 países já estavam se preparando para responder a esse tipo de ataque, conduzindo pesquisas sobre como converter essas *botnets* em armas de ataque no ano de 2007.

Os próprios combates estão paulatinamente deixando de ser meramente convencionais, o ambiente está mudando e, normalmente, se tornando mais complexo. Dificilmente, no futuro, serão vistas as grandes massas de manobra e a mobilização de meios da forma com que foram empregados nas 1ª e 2ª Guerras Mundiais. A forma de se combater evolui constantemente. Os atores e as motivações se diversificam. Os cenários são difusos e o inimigo nem sempre é claramente definido. A tecnologia se faz cada vez mais presente e o poder de letalidade das armas cresce de maneira vertiginosa, assim como o seu custo. As

---

[6] BRASIL. Exército. Estado-Maior do Exército. C 100-5: operações. 3. Ed. Brasília, DF, 1997, p. 4-3

[7] Uma rede composta por computadores que foram infectados por programas que permitem controlar remotamente os mesmos e direciona-los para a execução de ações específicas, normalmente danosas.

[8] MCAFEE. **Virtual Criminology Report – Cybercrime: the next wave**. Santa Clara, Califórnia: p. 11-12, 2007. Disponível em <http://www.mcafee.com/us/research/criminology_report/default.html> Acesso em 17 dez. 2009.

ações necessitam ser cuidadosamente coordenadas, sincronizadas e executadas de maneira extremamente veloz. Os impactos sobre a população civil influem incisivamente nos planejamentos, decisões e no andamento dos conflitos, nem sempre com desdobramentos previsíveis. Esse é o cenário dos conflitos de 4ª geração[9], da assimetria, dos combates contra organizações e não mais contra Estados, da indefinição de fronteiras. É a introdução de um elemento de ruptura, que muda uma ideia pré-concebida. Enfim, o ciberespaço é mais um aspecto desse tipo de conflito, que já está sendo travado, mais perto do que se possa imaginar.

Os desafios são imensos, em virtude da velocidade com que avançam as tecnologias e da assimetria intrínseca ao ambiente. Um pequeno grupo de indivíduos especialmente preparados, representando uma organização ou, até mesmo um Estado, poderão causar danos ou obter informações que custariam muito caro ou não seriam exequíveis por meios convencionais. O Estado que organizar uma força que seja capaz de preparar a sua defesa e também de conduzir um ataque cibernético eficaz terá em suas mãos um poderoso elemento multiplicador do poder de combate assim como um argumento de dissuasão cada vez mais decisivo. Para isso, **é necessário o estabelecimento de uma Doutrina**. É necessário, minimamente, definir um vocabulário comum, pensar sobre a forma de se combater e na organização das forças que farão frente a essa situação.

Em matéria penal, a Lei de Segurança Nacional[10] em vigor fornece o arcabouço jurídico essencial para a tipificação de crimes contra a segurança nacional, onde podem ser enquadradas ações de Guerra Cibernética (G Ciber) contra o Estado Brasileiro. Aperfeiçoamentos na legislação brasileira estão em curso visando respaldar a atuação cibernética do Estado brasileiro.

A Política de Defesa Nacional[11] já levanta a necessidade do estabelecimento de uma Doutrina quando aborda que os avanços da tecnologia da informação e de modernos meios de comunicações criaram também vulnerabilidades que poderão ser exploradas, com o objetivo de inviabilizar o uso dos nossos sistemas ou facilitar a interferência à distância.

---

[9] SILVA, Carlos Alberto Pinto. **Guerra Assimétrica: adaptação para o êxito militar**. Padeceme nº 15. Rio de Janeiro: Escola de Comando e Estado-Maior do Exército, 2007.

[10] BRASIL. Lei nº 7.170, de 14 de dezembro de 1983. **Define os crimes contra a segurança nacional**, a ordem política e social, estabelece seu processo e julgamento e dá outras providências. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 15 de dezembro de 1983.

[11] _____. Decreto nº 5.484, de 30 de junho de 2005**.** Aprova a **Política de Defesa Nacional**, e dá outras providências. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 1º de julho de 2005.

Já a Estratégia Nacional de Defesa[12] define três setores de importância estratégica: o espacial, o cibernético e o nuclear, determinando o seu fortalecimento e o aperfeiçoamento dos dispositivos e procedimentos de segurança que reduzam a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra ataques cibernéticos e, se for o caso, que permitam seu pronto restabelecimento.

Este trabalho, portanto, tem por finalidade contribuir com elementos para a formulação de uma Doutrina de Guerra Cibernética adequada à realidade do Exército Brasileiro.

## 1.1 TEMA

O tema foi proposto inicialmente à ECEME pelo Estado-Maior do Exército no ano de 2009, em decorrência das ações requeridas pela Estratégia Nacional de Defesa e apresentado aos alunos que estavam escolhendo os temas gerais dos seus trabalhos monográficos. Esse trabalho, devidamente delimitado, objetiva apresentar uma proposta de elementos para a formulação doutrinária da Guerra Cibernética no Exército Brasileiro.

## 1.2 PROBLEMA

Os modernos centros de decisão e de Comando e Controle (C2), militares ou civis, contam presentemente com um rápido crescimento da infraestrutura de telemática, intrinsecamente heterogênea e complexa, que visa suportar as necessidades de ligações dos órgãos que apoiam.

Esta malha de redes de comunicação, seja de voz, dados ou vídeo traz consigo vulnerabilidades que podem ser exploradas por um inimigo ou oponente, não necessariamente um Estado ou organização, que pode atacar as redes de comando e controle de uma imensa variedade de serviços públicos civis e militares, buscando a desestabilização da ordem pública, a perda da confiança da população em seus governantes ou a degradação da capacidade militar de um Estado.

Este é o cenário de uma das mais recentes formas de atuação em um conflito, a Guerra Cibernética. O mesmo se apresenta intrinsecamente não convencional e assimétrico, onde recursos limitados aliados a um profundo conhecimento técnico de

[12] BRASIL. Decreto nº 6.703, de 18 de dezembro de 2008**.** Aprova a **Estratégia Nacional de Defesa**, e dá outras providências. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 19 de dezembro de 2008.

poucas pessoas podem gerar um efeito extremamente eficaz em um alvo.

A maneira como é vista a Defesa Cibernética pelo Estado Brasileiro, pelo Ministério da Defesa e pelo Exército Brasileiro ainda está em construção e apresenta, não raramente, conceitos e opiniões divergentes. Essa situação não ocorre somente no Brasil. Outros países considerados potências cibernéticas também estão construindo os seus conceitos contando com visões divergentes dentro de seus próprios órgãos.

Uma das primeiras definições encontradas na literatura traz que a Guerra Cibernética corresponde ao 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[13]. Apesar de esse assunto ter surgido na literatura a algum tempo, o incremento e a popularização da utilização dos meios computacionais e de redes de comunicação de dados elevou, nos últimos anos, esse campo a um patamar completamente novo.

O Governo Federal já definiu como estratégico o setor cibernético na recente edição da Estratégia Nacional de Defesa[14], em vigor pela força legal do Decreto nº 6703, de 18 de dezembro de 2008.

As necessidades doutrinárias, expressas em quadro de situação da doutrina, são definidas em função do Sistema de Planejamento do Exército (SIPLEx) e do banco de dados doutrinários. Este banco é construído com o tempo e engloba os manuais em vigor, cadernos de instrução, relatórios diversos, conclusões de seminários, pesquisas doutrinárias, experimentações doutrinárias, reuniões de coordenação doutrinária, informações obtidas fruto de viagens ao exterior, de cursos no exterior, contribuições pessoais, e outras contribuições.[15]

Apesar de estudos sobre Guerra Cibernética no âmbito do Exército terem sido iniciados no Departamento de Ciência e Tecnologia desde pelo menos 2004[16], ainda não ocorreu a formulação de uma Doutrina nem foi claramente definida a forma de

[13] CAMPER, A. D. ; DEARTH, D. H. ; GOODDEN, R. T. **Cyberwar: Security, Strategy, and Conflict in the Information Age**. 3. ed. Afcea Intl Pr; 1996. ISBN: 978-0916159269.
[14] BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa**. 2. ed. Brasília: 2009. Disponível em <https://www.defesa.gov.br/eventos_temporarios/2009/estrategia/arquivos/ estrategia_ defesa_ nacional_portugues.pdf> Acesso em: 16 dez. 2009.
[15] Comunicação pessoal do autor com o Coronel Luiz Carlos Almeida Santos, na 3ª SCh / EME em 12 de março de 2012.
[16] Conforme a Memória nº 010-A/4-04-SCT de 08 de abril de 2004.

implementação no âmbito do Exército Brasileiro de como essa nova maneira de atuação será tratada, embora a criação do Centro de Defesa Cibernética do Exército e a ativação do seu Núcleo[17], em 04 de agosto de 2010, aponte essa necessidade premente. Qual seria, então, a abrangência de uma Doutrina de Guerra Cibernética adequada e passível de ser implementada tendo em vista as condicionantes impostas pela realidade brasileira e do Exército?

Assim sendo, a situação-problema levantada neste trabalho é a seguinte: A Doutrina de Guerra Cibernética brasileira pode ser conformada à luz da experiência de outros países, considerando-se a sua própria realidade e o ambiente institucional do Brasil (particularmente o Ministério da Defesa e o Gabinete de Segurança Institucional da Presidência da República).

### 1.2.1 **Alcances e Limites**

O presente trabalho se propõe a levantar elementos que contribuam para a realização de uma proposta de formulação de Doutrina de Guerra Cibernética adequada à realidade brasileira, com a utilização e integração dos conceitos formulados por outros órgãos governamentais, primordialmente o Ministério da Defesa e o Gabinete de Segurança Institucional da Presidência da República.

Os pontos de partida foram os conceitos estabelecidos por outros países e a exploração das similaridades com as atividades relativas à Guerra Eletrônica e Inteligência. Foram exploradas tanto as atividades inerentes a atitudes defensivas, ligadas à proteção cibernética, quanto às atividades ligadas a atitudes como a exploração e o ataque cibernéticos.

Está fora do escopo desse estudo a utilização ou teste de softwares ou outros artefatos destinados à conduzir as ações de Guerra Cibernética, bem como a utilização de laboratórios de simulação ou redes de teste de intrusão (Honey Nets)[18] ou, ainda, a definição pormenorizada das estruturas a serem implementadas para levar a cabo os elementos levantados. Esses estudos, entretanto, são importantes e necessários, ficando como sugestão para que sejam conduzidos por outros pesquisadores.

---

[17] BRASIL. Exército. Comandante do Exército. Portarias nº 666 e 667, de 4 de agosto de 2010. **Cria o Centro de Defesa Cibernética do Exército e dá outras providências e Ativa o Núcleo de Defesa Cibernética do Exército.** Boletim do Exército nº 31. Brasília, DF, 6 de agosto de 2010.

[18] Conhecidas como "*Honey Nets*" ou Redes de Mel. São redes destinadas a capturar atividades de intrusão para realizar dissimulação e avaliação dos procedimentos e técnicas adotadas pelo invasor.

### 1.2.2 **Justificativas**

A questão da Guerra Cibernética necessita ser estudada profundamente, pois reflete uma nova área para onde os conflitos já começaram a migrar e onde os seus cenários de emprego são perigosamente mais prováveis que Hipóteses de Emprego ou Hipóteses de Conflito convencionais, com amplo emprego de um conceito que será tratado mais adiante, o de Operações de Informação. Um exemplo desse emprego ocorreu no recente conflito entre a Rússia e a Geórgia, na Ossétia do Sul, quando a invasão russa por meios convencionais foi precedida de ataques no ciberespaço, à semelhança de uma campanha aeroestratégica[19]. É, pois, uma **área importante e atual** para a condução dessa pesquisa.

Para agravar a situação, a velocidade do desenvolvimento de novas tecnologias que podem ser utilizadas para esse fim e a possibilidade de ataques serem perpetrados não somente por Estados, mas também por organizações ou, até, por pequenos grupos, com as mais diversas motivações, só tende a crescer.

Os esforços atuais têm focado somente uma face do problema: a englobada na segurança da informação, às vezes chamada de Defesa Cibernética[20], onde a finalidade principal é 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. Mas isto somente não basta. É preciso desenvolver, de forma organizada, coordenada e integrada a capacidade de dissuasão, onde identificar, repelir, rastrear e responder a ataques são capacidades fundamentais para preservar a segurança de um Estado, seus serviços e seus cidadãos. Deixar de desenvolver capacidades nessa área poderá acarretar sérios prejuízos ou danos ao Exército Brasileiro e ao Brasil no futuro.

A formulação de uma doutrina básica de Guerra Cibernética para o Exército Brasileiro **ainda não ocorreu**, o que confere **ineditismo ao trabalho proposto**. Da mesma forma, rápidas mudanças estão em curso, visando adequar a situação atual do Exército Brasileiro para atender a esse novo desafio, onde as atribuições ainda não estão completa e claramente definidas, caracterizando a proximidade da **fronteira do conhecimento** nesta área.

---

[19] DANCHEV, DANCHO. **Coordinated Russia vs Georgia cyber attack in progress.** ZDNet, 2008. Disponível em: <http://blogs.zdnet.com/security/?p=1670> Acesso em 31 mar. 2010.

[20] Conforme Portaria nº 45 – GSI / PR, de 8 de setembro de 2009, que institui o Grupo Técnico de Segurança Cibernética.

A relação custo / benefício desse estudo é extremamente favorável, uma vez que está centrada na formulação doutrinária que pretende contribuir para a definição de terminologia, ações e conceitos visando facilitar a implementação das atividades de Guerra Cibernética no âmbito do Exército Brasileiro, em coordenação com outros órgãos governamentais, primordialmente o Ministério da Defesa, outras Forças Armadas e o Gabinete de Segurança Institucional da Presidência da República.

### 1.2.3 **Contribuições**

A contribuição desta pesquisa está em analisar os conceitos, terminologias e propostas relativas à Guerra Cibernética em uso no país e em outras Forças Armadas, propondo elementos que contribuam para a formulação de uma Doutrina que esteja adaptada à realidade do Exército Brasileiro (EB), procurando facilitar a sua implementação e proporcionando ao Exército Brasileiro, às Forças Armadas e ao Brasil avançar no domínio desse novo campo de batalha. Este trabalho, portanto, visa contribuir para o domínio do conhecimento nesta área para o EB, facilitando os trabalhos a serem desenvolvidos ou já em desenvolvimento na área de G Ciber, conduzidos particularmente pela 2ª Subchefia (SCh) do EME, Centro de Defesa Cibernética (CDCiber), Centro Integrado de Telemática do Exército (CITEx), Centro de Desenvolvimento de Sistemas (CDS), Centro de Inteligência do Exército (CIE) e Centro de Comunicações e Guerra Eletrônica do Exército (CComGEx), buscando, em última análise, a proteção do Sistema EB. Pretende-se com isso, facilitar um salto qualitativo necessário ao EB nesta área.

A aplicabilidade desse estudo também não necessita ficar restrita ao Exército Brasileiro. Como forma de atuação conjunta e integrada, seus princípios poderão ser aproveitados pelo Ministério da Defesa, pelas demais Forças Armadas e órgãos do Governo Federal ligados à essa questão. Na realidade, isso já está ocorrendo, no âmbito de um Grupo de Trabalho Interforças, do Ministério da Defesa, para o setor cibernético, do qual o CDCiber participa desde 2010 e do qual este pesquisador fez parte dos trabalhos desde o início de 2012, chefiando a sua Seção de Doutrina.

## 1.3 REVISÃO BIBLIOGRÁFICA

A plena compreensão dos aspectos relacionados ao problema em questão somente será possível por intermédio do estudo aprofundado da literatura existente e do conhecimento de determinados conceitos que foram até aqui abordados

apenas de forma preliminar. A literatura existente vai paulatinamente proporcionando a consistência necessária à hipótese levantada neste projeto.

### 1.3.1 **Guerra Cibernética no Brasil**

Os principais antecedentes deste trabalho são caracterizados pela 4ª Reunião do Comitê Gestor da Segurança da Informação (CGSI), coordenado pelo Gabinete de Segurança Institucional (GSI) da Presidência da República, sediada pelo Ministério da Defesa em 15 de julho de 2003. Durante o evento, que contou com as presenças do Ministro-Chefe do GSI, General-de-Exército Jorge Armando Felix foi apresentada uma palestra sobre Guerra Cibernética e Segurança da Informação[21].

Após esse evento, a então Secretaria de Ciência e Tecnologia (SCT), hoje Departamento de Ciência e Tecnologia, produziu a Memória nº 010-A/4-04-SCT, de 08 de abril de 2004, que refletia as crescentes preocupações relacionadas à guerra cibernética:

> Em estudo recente conduzido por este ODS constatou-se que diversos sistemas de uso corporativo no Exército, relativos à gestão de pessoal e financeira, são vulneráveis a acessos por pessoas não autorizadas utilizando apenas técnicas e ferramentas livremente disponíveis na Internet. Alguns desses sistemas são operados pelo SERPRO e atendem a toda a administração pública federal. Nesses sistemas, verificou-se que **é possível, no mínimo, a obtenção de informações confidenciais ou sensíveis.**
>
> Devido às restrições de ordem legal, não foram realizados testes visando à verificação da possibilidade de se **alterar informações armazenadas nesses sistemas**. Entretanto, em alguns desses sistemas, já é possível especular, com razoável probabilidade de acerto, que a alteração de dados é possível.
>
> De forma análoga aos sistemas corporativos em uso no Exército, e pela experiência das vulnerabilidades encontradas em estudos semelhantes conduzidos pelo Departamento de Defesa norte-americano, acredita-se que diversos sistemas de comando e controle da infraestrutura crítica nacional sejam vulneráveis a operações de guerra cibernética. (BRASIL, 2004b)

Esta memória resultou no Ofício STI nº 091 – A4/Ch, de 22 Abr 2004, dirigido ao então Centro Integrado de Guerra Eletrônica (CIGE), que determinava que o mesmo apresentasse à Secretaria de Tecnologia da Informação (STI) e ao Alto Comando do Exército considerações sobre Guerra Cibernética e ideias para criação de um Centro de Estudos de Guerra Cibernética na Força Terrestre, com vistas a

---

[21] SILVA, M. M. ; TARANTI, C. G. R. **Ameaça Cibernética e Segurança da Informação**. São José dos Campos, 2003. Disponível em: <http:// www.defesanet.com.br/docs/cgsi.pdf>. Acesso em: 15 dez. 2009.

iniciar o estudo do assunto. Durante a apresentação do estudo em questão[22], realizada por este oficial em 21 de maio de 2004 para o Gen Div JALDEMAR RODRIGUES DE SOUZA, então Secretário de Tecnologia da Informação, foi tomada a decisão de se aguardar o embasamento legal (a ser proporcionado pelo Governo Federal) para a condução das ações propostas. Esse embasamento veio com a aprovação da Estratégia Nacional de Defesa em 2008.

As IG 20-19 (Instruções Gerais de Segurança da Informação para o Exército Brasileiro), datada de 17 Set 2001, já estabeleciam alguns parâmetros:

> Art. 10. As ameaças e vulnerabilidades, relativas ao emprego e ao acesso às informações, devem ser adequadamente consideradas no contexto de uma crescente informatização de atividades e processos.
>
> Art. 11. A eficiência no emprego dos recursos de Tecnologia da Informação constitui fator primordial para a eficácia do Exército Brasileiro.
>
> [...]
>
> Art. 29. Compete ao Estado-Maior do Exército:
>
> III - acompanhar, em âmbito nacional e internacional, a evolução doutrinária das atividades inerentes à Segurança da Informação;
>
> IV - realizar atividades de prospecção visando a melhoria da capacitação do Exército em ações inseridas no contexto de **Guerra da Informação** [grifo nosso] (BRASIL, 2001)

As IP 100-1 (Instruções Provisórias que estabelecem as "Bases para a Modernização da Doutrina de Emprego da Força Terrestre"), fazem algumas considerações sobre as características dos conflitos modernos e citam, com relação ao comando e controle:

> O Comando e Controle em combate está cada vez mais calcado em modernos e eficientes sistemas de comunicações e de inteligência, na informatização, no sensoriamento e na guerra eletrônica. (BRASIL, 1996, p. 1-3)

O Manual de Campanha, C 100-5 (Operações), de forma semelhante, descreve:

> Atualmente, o combate adquire características especiais, **influenciado pela sofisticada tecnologia** que se faz presente no campo de batalha. As exigências do combate moderno, por seu turno, **estimulam o desenvolvimento tecnológico e devem constituir-se em permanente preocupação de qualquer Força Armada**.
>
> A doutrina da Força Terrestre enfatiza, como fatores decisivos para a vitória final: o espírito ofensivo; a importância da conquista e manutenção da iniciativa; a rapidez de concepção e de execução das operações; a iniciativa dos

[22] Estudos para a criação do Centro de Estudos de Guerra Cibernética, de 30 de abril de 2004.

> subordinados; a flexibilidade para alterar atitudes, missões e constituição das forças; a **sincronização das ações no tempo e no espaço**; e a liderança e **capacidade de decisão dos comandantes em todos os escalões** [grifos nossos]. (BRASIL, 1997, p. 1-1 e 1-2)

O Manual de Comando e Controle da Força Aérea Brasileira (FAB), MCA-500-3, estabelece:

> Uma Força Armada, para ter maior probabilidade de sucesso na guerra, deve buscar sistematicamente melhorias que garantam maior eficácia e eficiência na gerência dos meios, dos homens e dos métodos a adotar no campo de batalha. Dessa forma, **cada evolução que ocorre na área da guerra é acompanhada pelas concepções e acepções de gerência desse fenômeno** [grifo nosso].
>
> O comando e controle tem sido responsável não apenas por vitórias e sucessos na guerra, mas também, por derrotas e fracassos. A tarefa de dissecá-lo reveste-se da maior importância, pois a doutrina de comando e controle de uma força é um seguro indicador de competência da gerência dos componentes do Poder Militar de uma nação.
>
> [...]
>
> Guerra na Informação
>
> Conjunto de ações efetivadas com a finalidade de se obter a superioridade das informações, afetando aquelas que servem de base aos processos do adversário, às suas redes de comunicações, ao mesmo tempo em que garante a segurança das informações das forças amigas.
>
> [...]
>
> A superioridade da informação
>
> Situação caracterizada quando há uma superação da capacidade do inimigo, no campo das informações, de tal modo que se faculte a profícua condução das operações sem possibilitar uma eficaz oposição da força inimiga.
>
> [...]
>
> A tecnologia da informação tem-se tornado parte integrante dos processos de comando e controle, pois a integração de computadores com os sistemas de comunicações é uma realidade. Esse fenômeno tem tornado as atividades de guerra cada vez mais dependentes das informações. Em consequência, têm aumentado os interesses estratégicos em focar a tecnologia da informação como alvo prioritário, com o objetivo de enfraquecer a capacidade de comando e controle do inimigo, diminuir a efetividade de suas ações e apressar o término do conflito sem muitas perdas. (BRASIL, 2000, p.7, 12, 14 e 67)

O Grupo de Trabalho de Guerra da Informação (GI), constituído pela Secretaria de Tecnologia da Informação, para realizar estudos sobre o assunto, apresentou em seu relatório:

> Compreender a dimensão humana e escrever doutrina neste século XXI será mais complexo que nunca, devido aos avanços na tecnologia. Neste ambiente contemporâneo, tecnologicamente avançado, a guerra da informação está se tornando um componente decisivo do campo de batalha moderno. Como tal, terá um papel importante em futuras operações.
>
> [...]

> Verifica-se que a GI abrange tudo o que se possa efetuar para preservar os nossos sistemas de informação, da exploração, corrupção ou destruição enquanto simultaneamente se explora, corrompe ou destrói os sistemas de informação das forças adversas, buscando assim obter a superioridade de informação.
>
> Dentre os diversos ramos de abrangência da GI, pode-se citar: Guerra de Comando e Controle (GC2), Guerra baseada em Inteligência (GIntlg), Guerra Eletrônica (GE), Guerra Psicológica (GPsico), Guerra Cibernética (GCiber) e a Guerra Econômica de Informações (GEI). (BRASIL, 2004b, p.1–2)

Na proposta do Plano Básico de Ciência e Tecnologia para o período 2004 a 2007 (PBCT 2004-2007), foi formalmente criado um Grupo de Segurança da Informação, com três objetivos, sendo o segundo deles o seguinte:

> OBJETIVO 2: Estruturar o Núcleo de Pesquisa e Desenvolvimento em Guerra de Informação (NuPDGI), constituído de recursos humanos e materiais destinados ao cumprimento das seguintes atribuições:
>
> - acompanhamento permanente da evolução das técnicas que visam ao comprometimento da segurança de redes de comunicações e sistemas computacionais;
>
> - prestar assessoramento às organizações militares, aos órgãos governamentais e às empresas que operem redes e sistemas computacionais de interesse para a defesa nacional, quanto aos procedimentos e ferramentas a serem adotados para a defesa contra ataques cibernéticos;
>
> - colaborar na formação de recursos humanos na área de guerra de informação, capazes de atuar em proveito de operações de inteligência e contra-inteligência;
>
> - desenvolver ferramentas de hardware e/ou software visando à proteção das redes e sistemas computacionais contra ações adversas de guerra de informação;
>
> - desenvolver ferramentas de hardware e/ou software visando ao **ataque cibernético** de redes e sistemas computacionais de forças adversas; e
>
> - **atuar**, quando determinado, **como força adversa simulada**, **realizando tentativas de ataques cibernéticos** contra redes e sistemas computacionais da infraestrutura de interesse da defesa nacional. [grifos nossos] (BRASIL, 2004b)

Este foi o primeiro documento a demonstrar a intenção da preparação de um ataque cibernético por parte do Exército Brasileiro. O PBCT 2004-2007 também previa a implementação, por transformação, da 1ª Companhia de Guerra de Informação, o que acabou não se concretizando.

A Doutrina Militar de Comando e Controle[23] define a Guerra Cibernética como integrante das Operações de Informações:

> A Guerra Cibernética, juntamente com a Guerra Eletrônica, as Operações Psicológicas, o Despistamento, a Segurança da Informação e a Destruição Física, com o apoio da Inteligência, integram as Operações de Informações. Estas podem ocorrer em todos os níveis de conflito, ou seja, desde o período de paz, e suas

[23] Doutrina Militar de Comando e Controle, MD31-D-03, 2006, p. 41

> ações concorrem para a consecução de objetivos políticos e militares. (BRASIL, 2006b)

Semelhante ao que existe na doutrina estadunidense[24], no âmbito do MD, a Guerra da Informação é tratada na Doutrina Militar de Comando e Controle, (manual MD31-D-03), por meio do conceito de Operações de Informação (Op Info).

A doutrina descreve que as Op Info têm por propósito influenciar um oponente real ou potencial, diminuindo sua combatividade, coesão interna e externa e, principalmente, a sua capacidade de tomada de decisão, atuando sobre os campos cognitivo (a mente dos decisores), informacional (o conteúdo da informação, os processos e seu fluxo) e físico (os Sistemas de C2 e suas infraestruturas) da informação. Ao mesmo tempo, em sua vertente defensiva, as Op Info protegem os processos e sistemas de tomada de decisão próprios.

A Doutrina Militar de C2 não estabelece um conceito formal para as Op Info, mas delimita as atividades que contribuem para a consecução dos seus objetivos e as ações que são implementadas:

> As Op Info, com o apoio da Inteligência, integram o emprego da Guerra Eletrônica, das Operações Psicológicas, do Despistamento, da Segurança da Informação, da Destruição Física e da **Guerra Cibernética**, para negar informação, influenciar, explorar, degradar ou destruir as capacidades de C2 do adversário, enquanto protegem a capacidade de C2 própria e amigas contra tais ações. (MD31-D-03, 2006b, p.41).

No Brasil, há grande carência de referências doutrinárias para a Guerra Cibernética. A Doutrina Militar de Comando e Controle, MD31-D-03, é um dos poucos textos doutrinários oficiais, que no âmbito das Forças Armadas, trata do assunto, propondo uma conceituação semelhante à estadunidense:

> A Guerra Cibernética corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper ou destruir capacidades de C2 do adversário. Compreende ações que envolvem as ferramentas de Tecnologia da Informação para desestabilizar os STIC2 do oponente e defender os próprios STIC2. Abrange, essencialmente, as Operações em Redes de Computadores. (MD31-D-03, 2006, p.44)

O Exército Brasileiro ainda não dispõe de uma Doutrina de Guerra Cibernética que possa nortear as atividades que necessitam ser desenvolvidas nessa área. Esse é o objetivo desse trabalho, que veremos a seguir.

---

[24] FM 3-13, Information Operations, 2003

### 1.3.2 **Guerra Cibernética em outros países**

Para a doutrina do exército norte-americano (FM 3-13, Information Operations, 2003), a Guerra Cibernética é tratada como Operação em Redes de Computadores e dividem-se em: Ataque a Redes de Computadores (*Computer Network Attack – CNA*), Exploração da Rede de Computadores (*Computer Network Exploitation – CNE*) e Defesa em Redes de Computadores (*Computer Network Defense – CND*).

Os escalões DE e Bda não têm responsabilidades de planejamento e execução das ações de Ataque a Redes de Computadores e de Exploração da Rede de Computadores (considerada uma função da Inteligência). Teoricamente, o planejamento dessas ações é atribuição dos escalões Corpo de Exército e superiores, ficando a execução das missões, devido à sua sensibilidade, a cargo do maior escalão do Exército presente no Teatro de Operações ou do United States Army Cyber Command / 2nd Army[25].

Em 2008, o exército americano ativou seu primeiro "*Network Warfare Battalion*"[26]. Na época, a unidade não estaria totalmente ativada, mas na maior parte operando por meio de destacamentos, apoiando forças de combate no Iraque e no Afeganistão, operações contraterror no mundo inteiro, assim como operações conjuntas e combinadas de Guerra Cibernética. O batalhão pertence à 704 th Military Intelligence Brigade[27], que é por sua vez subordinada ao *United States Army Intelligence and Security Command* (INSCOM)[28].

A China também criou um Batalhão de Guerra da Informação na cidade de Guangzhou[29]. A unidade é composta de três companhias com missões distintas, porém integradas em sua finalidade: a primeira Companhia de Comunicações, a segunda Companhia de Guerra Eletrônica e a terceira Companhia de Operações em Redes de Computadores, demonstrando, na prática, a concepção chinesa de INEW (*Integrated Network-Electronic Warfare),* que se refere ao uso integrado da Guerra Eletrônica e das Operações em Redes de Computadores, devido a grande

---

[25] http://www.arcyber.army.mil/

[26] Estados Unidos da América. Army. Departament of the Army. **Army activates network warfare unit**. Army.mil, 2008. Disponível em: <http://www.army.mil/-newsreleases/2008/07/02/10569-army-activates-network-warfare-unit/>. Acesso em: 31 mar. 2010.

[27] http://www.meade-704mi.army.mil/

[28] http://www.inscom.army.mil/

[29] NORTHROP GRUMMAN. **Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation**. McLean, Virgínia: 2009. Disponível em: <http:// www.uscc.gov/researchpapers/2009/ NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20 Report_16Oct2009.pdf> Acesso em 20 mar. 2010.

similaridade das atividades, para interromper os sistemas de informação do inimigo, buscando a Superioridade da Informação.

## 1.4 OBJETIVOS

Para melhor definição dos caminhos a serem percorridos visando a solução da questão levantada neste trabalho, foram estabelecidos o objetivo geral, com uma visão mais abrangente do tema e definidos os objetivos específicos, de caráter mais concreto, com função intermediária e instrumental.

### 1.4.1 **Objetivo Geral**

Contribuir para o incremento do banco de dados doutrinário com informações inéditas, fornecendo subsídios, estudos e fundamentos ao Estado-Maior do Exército, a quem cabe formular, propor e manter atualizada a doutrina vigente no Exército, facilitando a formulação e o estabelecimento da Doutrina de Guerra Cibernética no âmbito do Exército Brasileiro.

### 1.4.2 **Objetivos Específicos**

- Levantar as características, possibilidades e limitações da Guerra Cibernética;
- Realizar o estudo de caso da doutrina dos EUA e, no que for possível, um estudo comparativo da doutrina ou dos fundamentos doutrinários estabelecidos pela Rússia e China e a sua adequabilidade à realidade brasileira;
- Verificar a integração de procedimentos e conceitos utilizados pelo Governo Federal, notadamente o Ministério da Defesa e o Gabinete de Segurança Institucional da Presidência da República; e
- Apresentar os conhecimentos expostos no trabalho por meio de conceitos, definições, atribuição de possibilidades e limitações e ramificações relativos à Guerra Cibernética.

## 1.5 HIPÓTESE

De acordo com o problema levantado e com os objetivos apresentados, esse trabalho busca a confirmação da seguinte hipótese: A Doutrina de Guerra Cibernética brasileira pode ser conformada à luz da experiência de outros países, considerando-se a sua própria realidade e o ambiente institucional do Brasil (particularmente MD e GSI / PR).

## 1.6 VARIÁVEIS

As seguintes variáveis serão exploradas, buscando a mensuração necessária para fundamentar os estudos, possibilitando a comprovação da hipótese levantada, conforme o quadro abaixo.

| Tipo de Variável | |
|---|---|
| Dependente | - Doutrina de Guerra Cibernética do EB (fundamentos) |
| Independentes | - Doutrina de Guerra Cibernética dos EUA, China e Rússia<br>- Ambiente de risco crescente<br>- Realidade do EB / ambiente institucional |

Quadro 1 – Variáveis
Fonte: o autor

## 1.7 METODOLOGIA

O trabalho foi desenvolvido, quanto aos fundamentos técnicos, com base em pesquisa bibliográfica e documental, compreendendo as seguintes técnicas:

- um estudo documental, baseado no que já se tem feito em termos de Doutrina de Guerra Cibernética no Exército Brasileiro, principalmente na 2ª Subchefia do EME (particularmente nos arquivos da SI.2 – Tecnologia da Informação, a quem coube a missão de Guerra Cibernética no Exército e que conduz os trabalhos do GT Interforças do Setor Cibernético do MD), na 3ª Subchefia do EME, responsável pela formulação da Doutrina de emprego da Força Terrestre, no Departamento de Ciência e Tecnologia, no Centro de Defesa Cibernética (arquivos da divisão de doutrina) e no Centro de Comunicações e Guerra Eletrônica do Exército (grupo de experimentação Proteus);

- o método foi o comparativo, buscando identificar semelhanças e compreender divergências entre as doutrinas de Guerra Cibernética já formuladas ou em formulação na Rússia e China e, com ênfase, nos Estados Unidos da América;

- o tipo de pesquisa que serviu de base foi a pesquisa qualitativa.

Os passos foram:

- levantamento da bibliografia e de documentos pertinentes;

- seleção da bibliografia e documentos;

- leitura da bibliografia e dos documentos selecionados;

- levantamento de conceitos, por intermédio de entrevistas semiestruturadas, direcionadas a profissionais de notório conhecimento do assunto ou que estejam funcionalmente envolvidos com o mesmo. As entrevistas foram realizadas de forma pessoal, visando uma melhor interpretação dos dados colhidos.

- participação em cursos, reuniões e eventos de caráter oficial onde eram tratados aspectos relevantes à pesquisa;

- montagem de arquivos: ocasião em que foi elaborada a base de dados de citações, resumos e análises;

- análise crítica, tabulação das informações obtidas e consolidação das questões de estudo.

Os critérios utilizados para atribuição de relevância durante o processo de análise foram:

- Documentos oficiais, produzidos ou emitidos por Estados;

- Atas das discussões produzidas no âmbito do GT Interforças do Setor Cibernético, conduzido pelo EME e com participação do CDCiber;

- Documentos acadêmicos publicados que foram produzidos fruto de congressos, seminários, conferências e discussões;

- Análise técnicas de empresas de segurança da informação estabelecidas no mercado internacional;

- Notícias veiculadas por órgãos de imprensa, desde que confirmadas por mais de uma fonte.

A coleta de material foi realizada por meio de consultas às bibliotecas da Escola de Comando e Estado-Maior do Exército, do Instituto Militar de Engenharia, do Departamento de Ciência e Tecnologia e dos documentos e estudos produzidos pela 2ª SCh do Estado-Maior do Exército (atas do Grupo de Trabalho Interforças e relatórios de viagens realizadas) e no Centro de Defesa Cibernética (arquivos da Divisão de Doutrina e Mobilização); a legislação nacional foi obtida por intermédio de consultas ao repositório de legislação do Planalto disponível na Internet[30]; foram consultados anais de congressos, noticiários de meios de comunicação e sites especializados disponíveis na Internet; jornais e revistas militares especializadas; dados e relatórios do Ministério da Defesa; manuais do Exército Brasileiro, da Aeronáutica, da Marinha e de Forças Armadas estrangeiras; documentos emitidos

[30] http://www2.planalto.gov.br/presidencia/legislacao

pelo Gabinete de Segurança Institucional da Presidência da República; e de aquisições em livrarias virtuais na Internet, assim como por intermédio de acesso à mecanismos de busca da rede mundial de computadores.

Uma inovação na coleta de material foi a utilização da rede social de caráter profissional LinkedIn[31], que possibilitou a assinatura e acompanhamento dos seguintes fórums especializados: Associação Brasileira de Segurança da Informação e Comunicações (ABSIC), *Aurora Cyberconflict Research Group, Command and Control Centre of Excellence* (*C2CoE*), Computação Forense Brazil, CSIRT Brasil, *Cyber Conterintelligence*, *Cyber Inteligence Network*, *Cyber Security Forum Initiative* (*CSFI*), *Cyber Security Community*, Grupo de Trabalho em Segurança CGI.br (GTS) e *Information Security Network*. O acesso a esses fóruns possibilitou um acompanhamento muito ágil da situação sobre Segurança da Informação, Defesa e Guerra Cibernética, com notícias em mídia e discussões sobre documentos oficiais disponibilizados.

A catalogação das informações também foi facilitada com a utilização da ferramenta Evernote[32], que possibilita realizar a captura, indexação, pesquisa e organização de uma base de informações não estruturada.

O trabalho de campo dessa tese incluiu:

- Contatos com o Diretor do Departamento de Segurança da Informação e Comunicações (DSIC) do Gabinete de Segurança Institucional da Presidência da República;

- Contatos com integrantes do Estado-Maior do Exército, do Departamento de Ciência e Tecnologia, do Centro de Defesa Cibernética, do Centro de Comunicações e Guerra Eletrônica do Exército e do Centro de Instrução de Guerra Eletrônica;

- Realização do Curso sobre Terrorismo Cibernético no Centro de Excelência e Defesa Contra o Terrorismo (COE-DAT) da OTAN[33], na Turquia, onde se pode ainda ter contato e intercâmbio de informações com os seguintes pesquisadores:

- Alan Brill – Kroll Associates (formalmente entrevistado);

[31] http://www.linkedin.com
[32] http://www.evernote.com
[33] http://www.coedat.nato.int/

- Anna Maria Talihärm – Analista Sênior do Centro de Excelência Cooperativo de Defesa Cibernética da OTAN[34], divisão de Legislação e Políticas;

- Itamara Lockhard – Pesquisadora Sênior do International Security Studies – The Fletcher School – Tufts University – EUA;

- Dean C. Alexander – Diretor do Homeland Security Research Program – Western Illinois University – EUA.

- Participações em Reuniões Bilaterais sobre o setor cibernético

- Reunião Brasil – EUA, conduzida pelo MRE em Brasília;

- Reunião Brasil – França, conduzida pelo MD em Brasília;

- Participação em Reunião Trilateral sobre segurança regional

- Reunião Brasil – Colômbia – Peru, conduzida pelo MD em Manaus;

- Participação em reuniões para preparação de documentos oficiais ao *United Nations Office on Drugs and Crime* (UNODC), com foco em crimes cibernéticos, conduzida pelo MRE;

- Participação como conferencista convidado na Workshop de Segurança Cibernética em Infraestruturas Críticas, conduzida pela FITEC e CEMIG em Belo Horizonte,

- Participação no planejamento da atuação do Centro de Defesa Cibernética na Conferência das Nações Unidas sobre Desenvolvimento Sustentável (Rio + 20);

- Participação no estado-maior da Operação Conjunta Amazônia 2012;

- Participação no planejamento da Operação Conjunta Atlântico III;

Ao final, de acordo com a pesquisa realizada, é apresentado um capítulo e apêndices com sugestões de elementos que possam facilitar a sua inclusão no banco de dados doutrinário e permitir que sejam utilizados mais facilmente na preparação de publicações que abordem o tema apresentado, contribuindo, assim, para a formulação de uma Doutrina de Guerra Cibernética adaptada à realidade do Exército Brasileiro.

## 1.8 REFERENCIAL TEÓRICO

Theo FARRELL e Terry TERRIFF, no livro *"The sources of military changes: culture, politics, technology"* (2002, p. 3), destacam que, modernamente, são três aspectos principais que levam as estruturas militares a mudar: as mudanças no ambiente estratégico (decorrente, principalmente, do fim da Guerra Fria), as

[34] http://www.ccdcoe.org/

pressões para reduzir custos (presentes em todos os setores governamentais) e o ritmo dos avanços tecnológicos, particularmente na tecnologia da informação. Para esses autores, tais mudanças ocorreriam também por meio de três formas: adaptação (ou ajuste dos métodos existentes), inovação (ou novos meios e métodos) e emulação, pela "importação" de novas ferramentas e modos de combate por meio da imitação de outras organizações militares.

FARRELL (2002, p. 93) já dirigia sua atenção para o fato de que organizações operando em campos similares (como as organizações militares de países diferentes) frequentemente se deparam com forças que as levam a assemelharem-se umas às outras. Apesar de algumas organizações inovarem consciente e genuinamente, criando algo novo, é muito mais rápido e menos dispendioso emular uma solução de eficiência já comprovada.

RESENDE-SANTOS (2007), num trabalho muito bem documentado, também trabalhando com a emulação militar entre países, traz contribuição valiosa para o campo da teoria de relações internacionais, no contexto do neorrealismo. Nessa obra, busca explicar os esforços de modernização de Argentina, Chile e Brasil no final do século XIX e início do século XX, espelhando-se no, até então vitorioso, modelo militar alemão, ou seja, a emulação militar não é algo novo na cultura das Forças Armadas brasileiras. Esse conceito de emulação é extremamente interessante para o presente trabalho.

RESENDE-SANTOS (2007, p. 73), afirma que inovar é simultaneamente caro e arriscado, consumindo tempo e de resultado incerto. À medida que a competitividade cresce, os Estados, numa cuidadosa análise dos riscos e benefícios potenciais, tornam-se mais avessos ao risco, optando pela certeza e retorno imediato da emulação, da qual os resultados são conhecidos.[35]

RESENDE-SANTOS (2007 p. 9-10) discorre que a emulação pode ser definida como a imitação (por um Estado ou qualquer entidade) voluntária, sistemática e com um propósito (que pode ser de atualização ou modernização), numa grande variedade de áreas, técnicas e práticas de outro(a), normalmente motivada / dirigida por pressões competitivas. Isso pode ocorrer também no âmbito de práticas econômicas, administrativas, regulatórias e mesmo constitucionais.

[35] Por exemplo, no final do século XIX e início do século XX, após emular o modelo militar alemão, o Japão passou da situação de país periférico à de potência mundial. Vitorioso na Guerra Russo-Japonesa, contribuiu enormemente para a aumentar o apelo do modelo alemão, que seria emulado mundo afora.

Segundo o pesquisador, a emulação militar em larga escala implica na eliminação de procedimentos e instituições anteriores (inclusive arranjos e interesses associados), sendo, com frequência, politicamente arriscada. Ele usou a teoria da emulação para enquadrar a influência alemã (1906-1919), a francesa (1919-1940) e, depois, a norte-americana[36] no Brasil.

Num raciocínio muito próximo, DIMAGGIO (2005, p. 75-76) apresenta o conceito de isomorfismo institucional, como um processo de homogeneização por imitação (como na emulação) entre organizações, que leva uma organização a assemelhar-se a outra(s) que se depara(m) com as mesmas condições de ambiente. Nesse contexto, campos organizacionais altamente estruturados fornecem um ambiente que geralmente leva a uma homogeneidade em termos de estrutura, cultura e resultados, com o objetivo de lidar racionalmente com a incerteza e com as restrições. Moldura extremamente útil para explicar o processo pelo qual certas inovações difundem-se entre organizações, enquanto outras não, o isomorfismo institucional, com a emulação sempre implícita, apresenta-se em três modelos, que serão detalhados a seguir: o mimético, o coercitivo e o normativo.

O Isomorfismo Mimético é mais frequente nas situações onde os objetivos da organização são ambíguos (não claramente definidos) e/ou o ambiente externo é de grande instabilidade. A experiência comprova que a incerteza constitui uma força poderosa a encorajar a imitação: nessa situação, as organizações tendem a copiar práticas de outra(s) percebida(s) como bem sucedida(s), tendo como atrativo adicional o menor custo de implantação, por demandar menor investimento com pesquisa e desenvolvimento de projetos. O isomorfismo mimético (como as demais modalidades) apenas se diferencia da emulação por acrescentar uma condicionante ou requisito, nesse primeiro caso, o de uma situação de indefinição ou ambiguidade para o emulador, aspecto considerado pertinente.

Tal conceito (mimetismo) aplica-se bem às transformações sofridas pelo Exército Brasileiro no início do século XX, quando, com uma missão pouco clara e em busca de modernização, adota uma série de mudanças estruturais e doutrinárias seguindo inicialmente o modelo alemão (1906-1919).

O Isomorfismo Coercitivo enquadra as situações onde surge uma relação de dependência entre as organizações envolvidas (no caso militar, necessidades em

[36] O autor não entra em detalhes, mas sinaliza nesse mesmo sentido em relação ao período de influência norte-americana pós-II GM sobre as Forças Armadas brasileiras como um todo.

termos de equipamentos, suprimentos, apoio para treinamento e, eventualmente, para o combate), associada a uma pressão, formal ou informal, para a adoção das mudanças implementadas pela organização / instituição que lidera a relação. Verificar-se-á mais adiante, também, que tal modelo é adequado para explicar tanto o período de atuação da Missão Militar Francesa no Brasil, de 1919 a 1940, como o período inicial da influência norte-americana, da II Guerra Mundial até o início da década de 60.

Finalmente, há o Isomorfismo Normativo, cuja maior diferença para o mimético é a influência bastante menor do fator incerteza e/ou de clareza de objetivos que marca este último. DIMAGGIO (2005, p. 80) aborda que o modelo normativo se originaria de uma maior profissionalização das organizações e em decorrência da similaridade da educação formal e da presença de uma base cognitiva comum. Outro aspecto importante que perpassa esse modelo é a constituição de redes profissionais, por meio das quais novos modelos são mais rapidamente difundidos. Isso explica satisfatoriamente a facilidade com que conceitos / modelos militares são transferidos rapidamente de um exército / país para outro.

No ambiente militar moderno, essas redes podem ser representadas pelas organizações internacionais multilaterais em que os países (e eventualmente suas Forças Armadas) fazem-se presentes e/ou atuam em conjunto. Podemos citar como exemplos a ONU, a OEA, a OTAN e, também, a participação em missões conjuntas de paz ou coalizões em situações de conflito. O intercâmbio de militares entre os países, para realização de cursos, treinamentos ou missões diplomáticas, constitui-se também num poderoso meio de difusão (exportação e importação) de ideias e modelos.

Segundo TERRIFF (2002, p. 107-108), o Isomorfismo Normativo sugere que uma organização central e com elevado status no seu ambiente (como o as Forças Armadas dos EUA para as dos demais países, ao menos os ocidentais) pode ser copiada inclusive pela percepção do ganho ou influência que essa emulação pode trazer aos olhos de seus competidores.

Esse é o melhor modelo para enquadrar, também, a fase final do período de influência estadunidense no Exército Brasileiro (do afastamento progressivo a partir da década de 1960, até o rompimento do Acordo Militar de Cooperação Brasil-EUA, em 1977) e o período subsequente, de maior autonomia, até a atualidade. Nessa fase é verificado um esforço maior da instituição para o desenvolvimento de uma

doutrina e estrutura organizacional próprias, mais adequadas à sua realidade e ao ambiente operacional brasileiro.

O Exército Brasileiro é uma instituição que entrou no século XX em estado de crise. A Guerra de Canudos, em particular, ajudou a desnudar suas principais mazelas: treinamento deficiente; promoções fortemente influenciadas por fatores políticos; ausência de um serviço militar organizado; sistema disciplinar cruel e mal regulamentado; remuneração baixa; sistema logístico precário e deficiente; inexistência de regulamentos para operações em campanha; e falta generalizada de recursos financeiros.

O caminho escolhido para a profissionalização foi através da emulação de modelos bem sucedidos de potências militares estrangeiras. Em função da precariedade da situação então existente, inicialmente havia que se aceitar praticamente tudo o que (e da maneira como) era apresentado – ou mesmo imposto – pela potência espelhada.

Com o passar do tempo, num processo de crescente maturidade institucional, o Exército Brasileiro chegou a um estágio de profissionalização que, por sua vez, lhe permitiu abandonar o isomorfismo mimético (assim como o coercitivo) e praticar o isomorfismo normativo, forma mais desejável. Nesse ponto, em meados da década de 1970[37], já podia escolher exatamente o que, de quem, quando e em que proporção emular, adaptando o modelo escolhido às suas peculiaridades ou, na inviabilidade disso, desenvolvendo sua própria doutrina e, eventualmente, seus equipamentos.

No caso da Guerra Eletrônica, particularmente nas décadas de 1980 e 1990, o envio de pessoal para o exterior pode ser assinalado como mais um bom exemplo de emulação militar, num contexto de isomorfismo normativo: o Exército Brasileiro, com plena noção do que lhe faltava, das especificidades do território nacional e das restrições aos conhecimentos nessa área, determinou a realização de pesquisas em diversos países, a fim de estabelecer sua própria doutrina.

Isso agora está ocorrendo com a Guerra Cibernética. Os projetos estruturantes coordenados pelo Centro de Defesa Cibernética, detalhados mais à frente, estão se valendo das teorias da Emulação Militar no contexto de Isomorfismo Normativo para reduzir riscos, ganhar agilidade e construir uma base cognitiva comum (que inclui a

[37] O marco histórico disso foi a denúncia, em 11 de março de 1977, no governo Geisel, do Acordo de Cooperação Militar Brasil-EUA, que vigorava desde 1952.

formulação de uma doutrina), buscando a cooperação e o intercâmbio de informações. Desta forma, essas teorias constituem a base do referencial teórico deste trabalho.

# 2 **ENTENDIMENTO DO CENÁRIO ATUAL**

Antes de estudarmos mais profundamente a Guerra Cibernética, é fundamental o entendimento do cenário atual, onde está se descortinando uma mudança na forma de como se comporta o combate moderno. Essa mudança está ocorrendo às vistas de todos os chefes militares, todos os dias se mostra nos noticiários mas nem todos estão se dando conta disso. Esse entendimento é necessário para que se possa situar o conceito de Operações de Informação e, posteriormente, entender como a Guerra Cibernética interage com os outros componentes dessas operações, fornecendo a base sólida onde os conceitos inerentes à Guerra e Defesa Cibernética se assentam.

## 2.1 O PARADIGMA DA ERA INDUSTRIAL

As guerras típicas da era industrial, travadas durante a 2ª onda, segundo TOFLER (2001)[38], eram lutadas em forma de batalhas, inicialmente em campo aberto. Esse conceito foi evoluindo, com o emprego de combinação de atitudes ofensivas e defensivas, onde os oponentes eram dois Estados ou, eventualmente, coligações. Dois exércitos normalmente lutavam buscando uma batalha decisiva, onde o objetivo estratégico seria conquistado. Este objetivo estratégico poderia ser a destruição das forças armadas, a conquista de um acidente capital ou outro de igual importância.

Essa oposição de forças normalmente utilizava os meios típicos da era industrial: predominantemente forças blindadas, apoiadas massivamente por fogos (terrestres, aéreos ou navais), manobrando rapidamente, buscando concentrar meios em um ponto fraco do inimigo, realizar uma ruptura ou manobra desbordante, cercar e, finalmente, destruir o inimigo.

Segundo SMITH (2007)[39], o auge dessa concepção de guerra foi atingido durante a 2ª Guerra Mundial, e seguiu modernizando-se até 1973, com o conflito árabe-israelense, com carros de combate manobrando no deserto do Sinai e nas Colinas de Golan, apoiados por fogos de artilharia e aviação. Ainda na 1ª Guerra do Golfo, em 1991, esse paradigma foi aplicado, em uma versão modernizada, com a aplicação intensa de tecnologia, operações conjuntas, mas ainda com uso massivo de blindados combatendo no deserto, onde Saddam Hussein aprendeu, da pior

[38] TOFLER, Alvin. **A Terceira Onda**. 25. ed., São Paulo: Record; 2001, 491p. ISBN: 8501017973.
[39] SMITH, Rupert. **The Utility of Force: the Art of War in the Modern World**. New York: Alfred A. Knopf, 2007. eISBN: 978-0-307-26741-2

maneira, que no conflito utilizando meios e concepção da era industrial, leva grande vantagem quem possui mais meios militares de combate e logísticos para impor a sua força.

Segundo MIRANDA (2012)[40], apesar desse paradigma estar sendo paulatinamente superado, muitas Forças Armadas não abrem mão de dispor de meios de combate suficientes e de manter e ensinar uma base doutrinária compatível com o emprego desses meios. Isso se deve à falta de uma melhor compreensão do paradigma da era da informação, que será explicado a seguir, ou se deve à necessidade de dissuadir uma ameaça e manter um delicado equilíbrio de forças, particularmente quando se trata de problemas não resolvidos em suas fronteiras, ou ainda, porque a ganância, poder e influência da indústria de materiais de defesa também contribuem para a manutenção do mesmo. Cabe aqui se fazer a ressalva de que, no caso de se ter problemas históricos em uma fronteira instável, seria por demais leviano abrir mão de manter esses meios de força. Uma grande quantidade de países enfrentam essa realidade.

Desta forma, manter uma parcela das Forças Armadas nesse modelo, pode ser uma necessidade, mas empregá-la somente seguindo essa lógica, na Era do Conhecimento, vem se mostrando um erro muito grave.

## 2.2 O PARADIGMA DA ERA DO CONHECIMENTO

Ainda segundo MIRANDA (2012), no novo paradigma, as grandes batalhas ainda podem ocorrer, porém tendem a representar uma exceção. A busca pela "batalha decisiva" tende a ser paulatinamente substituída por operações que se desenrolam nas cidades e no meio da população (que também não deixa de ser uma batalha, mas de caráter menos intenso e normalmente mais continuado). O mais fraco tende a trazer o seu exército para combater na cidade, evitando a contraposição de forças em campo aberto, diminuindo os efeitos das armas da era industrial, visando proteger as suas forças.

Esse combate travado nas cidades, ao qual nos referimos, não é o combate em localidade, tradicionalmente estudado nas escolas militares, no qual o inimigo se entrincheirava na orla da localidade, que estava evacuada ou semi-evacuada,

[40] MIRANDA, André L. Novaes. Entrevista concedida ao autor em 06 de junho de 2012, constante do Apêndice "E" a este trabalho. A leitura da transcrição dessa entrevista é altamente recomendável para o entendimento correto das nuances que envolvem a evolução dessa forma de combater em particular.

normalmente em escombros após intenso fogo de artilharia e/ou de aviação, onde o combate tinha grande intensidade, abordagem sistemática, casa a casa, quarteirão a quarteirão, como ocorreu em Leningrado na 2ª Guerra Mundial ou, ainda, em Grozni no ano de 2000.

Na guerra da Era do Conhecimento, o oponente provavelmente se mistura à população e, quando é percebido, pode estar dentro de escolas, hospitais, igrejas, mesquitas ou outras instalações públicas com grande volume de população civil. Esse oponente, que anteriormente era um Estado, pode ser uma organização terrorista ou criminosa, um grupo ativista, um grupo guerrilheiro ou uma facção desertora de uma força armada, com ou sem apoio de outros Estados. Em contrapartida, as forças amigas atualmente podem ser multinacionais, conjuntas e podem necessitar operar em coordenação com outras agências, sejam elas nacionais ou, até mesmo, agências internacionais, como a ONU, por exemplo. Ou seja, poderão operar em um ambiente interagências, com a participação cooperativa entre as Forças Armadas, Polícia e outras agências governamentais de nível federal, estadual e municipal. Poderão interagir dentro de organismos internacionais e organizações não governamentais, nacionais e internacionais.

A conquista do objetivo estratégico poderá caber a uma ou mais agências civis e poderá estar relacionado com o retorno ou com o nascimento do Estado de Direito, ou de uma democracia ou, ainda, apoiar ações de reconstrução e/ou estabilização. Em suma, esse objetivo estratégico provavelmente incluirá a conquista do apoio da população da área, nacional e internacional, para a causa pela qual se está lutando, intervindo ou pacificando. O foco poderá mudar da busca da “batalha decisiva” para se tornar um objetivo mais amplo, como a conquista dos corações e mentes.

Segundo SMITH (2007), esse novo paradigma começou a se configurar com o surgimento da bomba atômica, que impediu a utilização plena dos meios de destruição em massa da guerra industrial e tornou-se claro com a queda do muro de Berlim. Enquanto esse novo paradigma não for plenamente entendido e adotado, ou ocorrerá a derrota, ou será necessária a adequação dos meios existentes e, principalmente, dos métodos do seu emprego.

A guerra de hoje tende a ser travada entre a população, e o seu alcance naturalmente é ampliado pela mídia, em todas as suas formas. Operações são conduzidas nas ruas e bairros e as suas imagens e relatos rapidamente chegam a todas as partes, seja pela mídia convencional, seja pela utilização da mídia social

pelas pessoas, que filmam, fotografam, compartilham na Internet, comentam e divulgam de forma viral[41] o que está se passando. Nessa luta, é perseguido o apoio político nacional e internacional enquanto busca-se reduzir a legitimidade da luta conduzida pelo oponente. O uso da força provavelmente produzirá o efeito desejado somente se for bem dirigido contra os alvos e, principalmente, se for bem comunicado, se a comunidade nacional e internacional puder compreender o porquê da utilização da força naquela situação e aceitar que foi uma ação justificada.

Na Era do Conhecimento, as baixas entre nossas forças também são provavelmente potencializadas. A liberdade para empregar armas de destruição em massa é cada vez mais reduzida. Mesmo as missões com justificativas mais plausíveis, de caráter humanitário ou de estabilização de um país são acompanhadas de perto pela população e pela imprensa. A população de um país normalmente não admite sem protestos perder soldados em um contexto de Operações de Paz, por exemplo.

A guerra moderna tende a ser feita no meio da população, com fuzileiros bem protegidos e com armas de letalidade inteligente. O emprego de ferramentas que proporcionem uma ampla consciência situacional visam fornecer a superioridade informacional ao combatente. Nesse contexto, uma das formas de se obter a multiplicação do poder de combate se dá pelo uso intensivo das Operações de Informação.

Nas Operações de Informação, a Guerra Cibernética, Guerra Eletrônica, Comunicação Social, Operações Psicológicas e Inteligência[42] são agrupadas sob uma mesma estrutura para ganhar sinergia, gerando a necessidade de uma integração, coordenação e sincronização cada vez mais efetiva e eficaz. Essa sinergia deve ser entendida como a troca rápida de informações, o apoio mútuo e a sincronização das ações entre esses sistemas, potencializando as ações e resultando em operações de grande eficácia e com baixos danos colaterais.

---

[41] Técnicas de divulgação que tentam explorar redes sociais pré-existentes, blogs, correio eletrônico ou outros serviços para produzir aumentos exponenciais na divulgação de eventos e fatos, com processos similares à extensão de uma epidemia que se dissemina rapidamente sem controle. O que se assume é que a divulgação de tal evento ou fato ao alcançar um usuário "susceptível", esse usuário será também "infectado" e reenviará o mesmo a outras pessoas susceptíveis, "infectando-as" também, desencadeando assim uma reação em cadeia.

[42] Alguns autores também colocam nessa estrutura os Assuntos Civis. Outros, pela grande complexidade inerente a essa atividade, preferem manter os Assuntos Civis fora desse agrupamento. O manual de Operações Conjuntas do Ministério da Defesa (MD31-M-01) adota essa última abordagem.


Figura 1 – Sinergia das Operações de Informação
Fonte: o autor

Segundo MIRANDA (2012), neste paradigma, mais importante que o emprego da força bruta e massiva, típicas da 2ª onda, é a capacidade de comunicar para as próprias forças, para a população da área de operações e para a opinião pública nacional e internacional, que o seu objetivo estratégico é mais relevante e mais legítimo que o do oponente e que a utilização daqueles meios foi necessária, adequada e proporcional. E isso se faz pela interação sinérgica e eficiente da Inteligência, Comunicação Social, Operações Psicológicas, Guerra Eletrônica e pela Guerra Cibernética, utilizando-se de todos os meios disponíveis.

Esse novo paradigma é a síntese da guerra por corações e mentes. No modelo das guerras da 2ª onda, normalmente perdia quem fosse derrotado na “batalha decisiva”. No modelo atual, onde provavelmente as ações terão caráter mais duradouro e continuado, os sinais de derrota tendem a ser a condenação pela opinião pública (interna ou externa), que podem evoluir para recomendações de organismos internacionais e, finalmente, para resoluções desses mesmos organismos (por exemplo, resoluções do Conselho de Segurança da ONU) que pressionam o governo a interromper as operações e retirar as tropas antes da conquista do objetivo estratégico.

Dessa forma, é essencial o entendimento do paradigma da Era do Conhecimento, uma vez que o emprego da Guerra Cibernética está diretamente

relacionado a essa nova realidade, ou seja, provavelmente estará inserida dentro do contexto das Operações de Informação.

## 2.3 O CONTEXTO NACIONAL

No contexto nacional, particularmente na área governamental, o tema foi tratado, inicialmente, com a roupagem da Segurança da Informação, o que se caracterizou com a criação do Gabinete de Segurança Institucional da Presidência da República (GSI/PR) por meio da Medida Provisória (MP) nº 2.216-37, de 31 de agosto de 2001[43], que alterou dispositivos da Lei nº 9.649, de 27 de maio de 1998[44]. Ao novo órgão, entre outras competências, coube a coordenação das atividades de segurança da informação.

Pelo decreto nº 5772, de 8 de maio de 2006[45], foi criado o Departamento de Segurança da Informação e Comunicações (DSIC), no GSI/PR, com a missão de planejar e coordenar a execução das atividades de Segurança da Informação e Comunicações (SIC) na Administração Pública Federal (APF). Posteriormente, em 2009, o conceito de Segurança Cibernética passou a ser adotado, materializando a aplicação da SIC no contexto das informações de interesse do estado brasileiro.

Com a adoção do conceito de Segurança Cibernética, o GSI/PR foi gradativamente definindo o seu escopo de atuação e caracterizando a diferença entre Segurança Cibernética, de sua competência, e Defesa Cibernética, da competência do Ministério da Defesa, por intermédio das Forças Armadas. Embora tal distinção ainda não esteja oficializada, é a ideia vigente naquele órgão.

Em dezembro de 2008, a Estratégia Nacional de Defesa (END) constituiu três setores estratégicos da defesa, atribuindo a cada uma das Forças Armadas (FA) a responsabilidade de coordenação e integração de cada um deles, conforme abaixo:

a) Setor Nuclear: Marinha do Brasil (MB);

b) Setor Cibernético: Exército Brasileiro (EB); e

---

[43] BRASIL. Medida Provisória nº 2.216-37, de 31 de agosto 2001. **Altera dispositivos da Lei nº 9.649, de 27 de maio de 1998, que dispõe sobre a organização da Presidência da República e dos Ministérios**, e dá outras providências. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 1 de setembro de 2001.

[44] BRASIL. Lei nº 9.649, de 27 de maio de 1998. Dispõe sobre a **organização da Presidência da República e dos Ministérios**, e dá outras providências. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 5 de junho de 1998.

[45] BRASIL. Decreto nº 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] República Federativa do Brasil. Brasília, DF, 9 de maio de 2006.

c) Setor Espacial: Força Aérea Brasileira (FAB).

Finalmente, a Diretriz Ministerial nº 14/2009, de 9 de novembro de 2009[46], definiu providências para o cumprimento da END nos setores estratégicos da defesa, estabelecendo que, numa primeira fase, deveriam ser definidos, em cada setor, a abrangência do tema e os objetivos setoriais, e, numa segunda fase, os objetivos setoriais seriam detalhados em ações estratégicas e a adequabilidade das estruturas existentes seria estudada, propondo-se alternativas e soluções.

Dentro do Exército Brasileiro, a coordenação desse trabalho coube ao Estado-Maior do Exército, particularmente a sua 2ª Subchefia, que decidiu pela criação e ativação do Núcleo do Centro de Defesa Cibernética, o que veremos mais detalhadamente no próximo capítulo.

A seguir analisaremos mais detalhadamente os órgãos e atores envolvidos com a segurança e defesa cibernética no Brasil.

[46] BRASIL. Ministério da Defesa. **Diretriz Ministerial nº 14. Integração e Coordenação dos Setores Estratégicos da Defesa**. Brasília, DF, 9 de novembro de 2009.

# 3 **ÓRGÃOS E ATORES DE SEGURANÇA E DEFESA CIBERNÉTICA NO BRASIL**

Segundo MANDARINO (2010, p.107), as atuações dos principais atores e órgãos do governo, no setor cibernético, dividem-se em duas vertentes:

a. Segurança Cibernética, contemplando ações que podem ser preventivas ou repressivas; e

b. Defesa Cibernética, mediante ações operacionais, caracterizadas por ações operacionais, de caráter defensivo e ofensivo.

Podemos resumir, mas não esgotar, a atuação desses atores segundo o quadro abaixo:

| **Vertente** | **Ações / Atitudes** | **Medidas** |
|---|---|---|
| Segurança Cibernética | Preventivas | - Criação e aplicação de metodologias de gestão de risco<br>- Desenvolvimento de planos de contingência e continuidade de infraestruturas críticas<br>- Resposta à incidentes de rede<br>- Correções contra artefatos maliciosos<br>- Disseminação de melhores práticas para proteção de redes e segurança das informações<br>- Especificação e desenvolvimento de algoritmos criptográficos e equipamentos de segurança cibernética |
| | Repressivas | - Identificação e combate à conduta criminosa caracterizada como crime cibernético<br>- Medidas contra terrorismo cibernético e sabotagem |
| Defesa Cibernética | Ações operacionais ofensivas e defensivas | - Medidas contra terrorismo cibernético e sabotagem<br>- Medidas de apoio à operações militares conduzidas em situação de emprego militar |

Quadro 2 – Formas de atuação de atores e órgãos do governo no setor cibernético
Fonte: o autor

Passaremos, então, a apresentar uma lista dos órgãos e atores que de alguma forma se relacionam com as vertentes de segurança e defesa cibernética no Brasil.

## 3.1 CONSELHO DE DEFESA NACIONAL (CDN)

O CDN é um órgão de consulta do Presidente da República nos assuntos relacionados à soberania nacional e à defesa do Estado democrático[47]. Sua composição abrange o Vice-Presidente da República, o Presidente da Câmara dos Deputados, o Presidente do Senado Federal, o Ministro da Justiça, o Ministro de Estado da Defesa, o Ministro das Relações Exteriores, o Ministro do Planejamento e os Comandantes da Marinha, do Exército e da Aeronáutica. Cabe ao Gabinete de Segurança Institucional da Presidência da República executar as atividades permanentes necessárias ao exercício da competência do Conselho de Defesa Nacional.

Suas competências constitucionais são:

I - opinar nas hipóteses de declaração de guerra e de celebração da paz, nos termos da Constituição;

II - opinar sobre a decretação do estado de defesa, do estado de sítio e da intervenção federal;

III - propor os critérios e condições de utilização de áreas indispensáveis à segurança do território nacional e opinar sobre seu efetivo uso, especialmente na faixa de fronteira e nas relacionadas com a preservação e a exploração dos recursos naturais de qualquer tipo;

IV - estudar, propor e acompanhar o desenvolvimento de iniciativas necessárias a garantir a independência nacional e a defesa do Estado democrático.

MANDARINO (2010, p.110) afirma que, dada a sua importância estratégica, o CDN deve manter-se como palco para as decisões estratégicas relativas às ações de segurança e de defesa cibernética. Entretanto, vislumbram-se grandes desafios na adaptação das competências constitucionais descritas acima. Por exemplo, o próprio conceito de soberania no ciberespaço não foi ainda estabelecido.

---

[47] BRASIL. Lei nº 8.183, de 11 de abril de 1991. **Dispõe sobre a organização e o funcionamento do Conselho de Defesa Nacional** e dá outras providências. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 12 de abril de 1991.

## 3.2 CÂMARA DE RELAÇÕES EXTERIORES E DEFESA NACIONAL (CREDEN)

A Câmara de Relações Exteriores e Defesa Nacional (CREDEN) do Conselho de Governo foi criada pelo decreto nº 4.801, de 6 de agosto de 2003[48]. É presidida pelo Ministro-Chefe do GSI/PR e tem por finalidade formular políticas, estabelecer diretrizes, bem como aprovar e acompanhar programas e ações a serem implantados em matérias relacionadas à: cooperação internacional em assuntos de segurança e defesa; integração fronteiriça; populações indígenas; direitos humanos; operações de paz; narcotráfico e outros delitos de configuração internacional; imigração; atividade de inteligência; segurança para as infraestruturas críticas; segurança da informação; e segurança cibernética. Cabe, ainda, à CREDEN o permanente acompanhamento e estudo de questões e fatos relevantes, com potencial de risco à estabilidade institucional, para prover informações ao Presidente da República. Como se trata de um órgão de governo, suas atribuições podem ser alteradas e até mesmo a sua existência não está assegurada no próximo governo.

A CREDEN é integrada pelos seguintes Ministros de Estado: Chefe do Gabinete de Segurança Institucional da Presidência da República, que a preside; Chefe da Casa Civil da Presidência da República; Justiça; Defesa; Relações Exteriores; Planejamento, Orçamento e Gestão; Meio Ambiente; e da Ciência e Tecnologia. Os comandantes das Forças Armadas são convidados para participar das reuniões em caráter permanente.

No âmbito do CREDEN, sob a coordenação do GSI/PR, foi criado também o Grupo Técnico de Segurança Cibernética, através da Portaria GSI/PR n° 45, de 8 de setembro de 2009[49].

O Grupo Técnico é integrado por dois representantes, titular e suplente, de cada um dos seguintes órgãos: Gabinete de Segurança Institucional da Presidência da República, a quem cabe a coordenação dos trabalhos por intermédio do Departamento de Segurança da Informação e das Comunicações; Ministério da Justiça; Ministério da Defesa; Ministério das Relações Exteriores; Comando da Marinha; Comando do Exército; Comando da Aeronáutica.

---

[48] BRASIL. Decreto nº 4.801, de 6 de agosto de 2003**. Cria a Câmara de Relações Exteriores e Defesa Nacional**, do Conselho de Governo. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 7 de agosto de 2003.

[49] BRASIL. Gabinete de Segurança Institucional da Presidência da República. Portaria nº 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] República Federativa do Brasil. Brasília, DF, 9 de setembro de 2009.

Este grupo poderá, quando necessário, convidar e interagir com órgãos e especialistas para o fornecimento de informações e adoção das providências necessárias à complementação das atividades a ele atribuídas.

## 3.3 CASA CIVIL

A Lei nº 10.683, de 28 de maio de 2003[50], alterada pela Lei nº 10.869, de 13 de maio de 2004, juntamente com o Decreto nº 5.135, de 7 de julho de 2004 e novamente alterada pela Lei nº 12.462, de 4 de agosto de 2011 definem as competências, a organização e a estrutura regimental da Casa Civil da Presidência da República.

Dentre as suas competências que estão diretamente relacionadas com o assunto da segurança cibernética e segurança da informação estão:

I - assistir direta e imediatamente ao Presidente da República no desempenho de suas atribuições, especialmente:

a) na coordenação e na integração das ações do Governo;

A estrutura da Casa Civil conta com três órgãos importantes na elaboração das normas e regulamentos da segurança da informação e comunicações e segurança cibernética: o Instituto Nacional da Tecnologia da Informação (ITI), a Diretoria de Tecnologia da Informação (DIRTI) e a Diretoria de Telecomunicações (DITEL).

O ITI tem a sua Estrutura Regimental definida pelo decreto nº 4.689, de 7 de maio de 2003[51], sendo uma autarquia federal vinculada à Casa Civil da Presidência da República, com a finalidade de ser a Autoridade Certificadora Raiz - AC Raiz, da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil. A ele compete estimular e articular projetos de pesquisa científica e de desenvolvimento tecnológico voltados à ampliação da cidadania digital, por meio da utilização de certificação e assinatura digitais ou de outras tecnologias que garantam a privacidade, autenticidade e integridade de informações eletrônicas. Nesse sentido, o ITI visa à popularização da certificação e a inclusão digitais, atuando sobre temas como sistemas criptográficos,

---

[50] BRASIL. Lei nº 10.683, de 28 de maio de 2003. Dispõe sobre a **organização da Presidência da República e dos Ministérios**, e dá outras providências. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 29 de maio de 2003.

[51] BRASIL. Decreto nº 4.689, de 6 de maio de 2003**. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão do Instituto Nacional de Tecnologia da Informação - ITI**, e dá outras providências. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 8 de maio de 2003.

software e hardware compatíveis com padrões abertos e universais, convergência digital de mídias, entre outras.

A DIRTI é responsável pelo desenvolvimento, manutenção e acompanhamento de todos os sistemas informatizados utilizados na Presidência da República.

A DITEL é responsável pela instalação, manutenção e acompanhamento de todos os sistemas de comunicações empregados na Presidência da República.

## 3.4 GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA (GSI/PR)

A Lei nº 10.683, de 28 de maio de 2003, estabelece no seu artigo 6º as competências do GSI/PR, dentre as quais podemos destacar:

[...]

II - prevenir a ocorrência e articular o gerenciamento de crises, em caso de grave e iminente ameaça à estabilidade institucional;

III - realizar o assessoramento pessoal em assuntos militares e de segurança;

IV - coordenar as atividades de inteligência federal e de segurança da informação;

O Decreto n° 4801, de 6 de agosto de 2003, criou a Câmara de Relações Exteriores e Defesa Nacional e atribuiu a sua presidência ao GSI/PR, tornando o mesmo responsável pela coordenação das medidas de Segurança da Informação e das Comunicações, Segurança Cibernética e Segurança das Infraestruturas Críticas, a serem tomadas pelos diversos órgãos da Administração Pública Federal. O GSI/PR tem, conforme citado acima, a responsabilidade pelo gerenciamento de crises graves envolvendo a Administração Pública Federal (APF) ou o Estado brasileiro, que tenham potencial de afetar a segurança nacional, coordenando a inteligência e a segurança da informação, compondo o Conselho de Defesa Nacional (CDN) e a CREDEN do Conselho de Governo. O Ministro Chefe do GSI é o Secretário-Executivo do CDN e Presidente da CREDEN.

O GSI/PR coordena com os órgãos da Administração Pública Federal: atividades relativas à Segurança das Infraestruturas Críticas[52] nacionais; Segurança da Informação e das Comunicações, visando, principalmente, à proteção das informações estratégicas nacionais, que transitam por documentos, redes de

[52] A utilização do termo “Infraestruturas Críticas” vem recentemente sendo substituída pelo termo “Estruturas Estratégicas”, com significado similar.

comunicações e redes computacionais; e Segurança Cibernética, visando à proteção e à própria garantia de utilização das redes e dos sistemas informatizados estratégicos do País. **Essas atribuições fazem do GSI/PR a engrenagem central da coordenação da estratégia de segurança cibernética do Brasil.**

Deve ser ressaltado que as atividades de Segurança da Informação e das Comunicações e de Segurança Cibernética permeiam todas as infraestruturas críticas nacionais, razão pela qual, em 2008, foram criados, os Grupos Técnicos de Segurança das Infraestruturas Críticas (GTSIC). Estes encontram-se sob coordenação do GSI/PR, no âmbito do Comitê Gestor de Segurança da Informação. Da estrutura do GSI/PR destacam-se os órgãos a seguir descritos.

### 3.4.1 **Departamento de Segurança da Informação e Comunicações (DSIC)**

Segundo MANDARINO (2010, p. 113 e 114), o DSIC tem como atribuição operacionalizar as atividades de segurança da informação e comunicações (SIC) na APF nos seguintes aspectos: regulamentar a SIC para a APF; capacitar todos os servidores públicos federais, bem como os terceirizados a respeito de SIC; realizar acordos internacionais de troca de informações sigilosas; operar o sistema de credenciamento de pessoas e entidades no trato de informações sigilosas; ser o ponto de contato junto à OEA para assuntos de terrorismo cibernético; e manter o centro de tratamento e resposta de incidentes nas redes de computadores da APF – CTIR Gov. O Decreto nº 7.411, de 29 de dezembro de 2010[53], traz no seu anexo I art 6º as atribuições do DSIC:

I - adotar as medidas necessárias e coordenar a implantação e o funcionamento do Sistema de Segurança e Credenciamento - SISEC, de pessoas e empresas, no trato de assuntos, documentos e tecnologia sigilosos;

II - planejar e coordenar a execução das atividades de segurança cibernética e de segurança da informação e comunicações na administração pública federal;

III - definir requisitos metodológicos para implementação da segurança cibernética e da segurança da informação e comunicações pelos órgãos e entidades da administração pública federal;

---

[53] BRASIL. Decreto Nº 7.411, de 29 de dezembro de 2010**.** Dispõe sobre remanejamento de cargos em comissão do Grupo-Direção e Assessoramento Superiores - DAS, **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] República Federativa do Brasil. Brasília, DF, 30 de dezembro de 2010.

IV - operacionalizar e manter centro de tratamento e resposta a incidentes ocorridos nas redes de computadores da administração pública federal;

V - estudar legislações correlatas e implementar as propostas sobre matérias relacionadas à segurança cibernética e à segurança da informação e comunicações;

VI - avaliar tratados, acordos ou atos internacionais relacionados à segurança cibernética e à segurança da informação e comunicações, referentes ao inciso I;

VII - coordenar a implementação de laboratório de pesquisa aplicada de desenvolvimento e de inovação metodológica e tecnológica, bem como de produtos, serviços e processos, no âmbito da segurança cibernética e da segurança da informação e comunicações; e

VIII - realizar outras atividades determinadas pelo Ministro de Estado ou pelo Secretário-Executivo.

Da estrutura do DSIC, merece destaque o Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, o CTIR Gov.

### 3.4.1.1 CTIR Gov

A portaria nº 12 - CH/GSI, de 27 de junho de 2003[54], instituiu, no âmbito do Comitê Gestor de Segurança da Informação, um grupo de trabalho para estudar e propor as medidas necessárias para a criação e implantação de um centro de emergência de computação do Governo Federal.

O relatório final deste grupo de trabalho destacou a relevância estratégica de um centro de tratamento de incidentes em redes da Administração Pública Federal. Enfatizou ainda, a importância da articulação entre administrações de redes por intermédio de um permanente serviço à disposição de todo o Governo Federal.

O modelo de referência que pauta o trabalho do CTIR Gov é o de articulação, coordenando os esforços dos órgãos da administração pública federal.

Dentre as missões do CTIR Gov[55] estão o auxílio ao desenvolvimento da cooperação entre os grupos de respostas de incidentes existentes no Brasil e no exterior; o fomento das iniciativas de gerenciamento de incidentes; e a distribuição

---

[54] BRASIL. Gabinete de Segurança Institucional da Presidência da República. Portaria nº 12 – CH/GSI, de 27 de junho de 2003. Instituiu o **Grupo de Trabalho do Centro de Emergência de Computação para estudar e propor as medidas necessárias para a criação e implantação de um centro de emergência de computação do Governo Federal**. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 30 de junho de 2003.

[55] http://www.ctir.gov.br/missao.html

de informações, alertas e recomendações para os administradores de segurança em redes de computadores da APF.

Os serviços prestados pelo CTIR Gov podem ter caráter reativo ou proativo. Em ambos os casos, o Centro tem condições de determinar tendências e padrões das ameaças no ciberespaço que afetam não só a APF, mas, trabalhando em conjunto com os demais Centros, também as instituições que compõem as infraestruturas críticas de Estado.

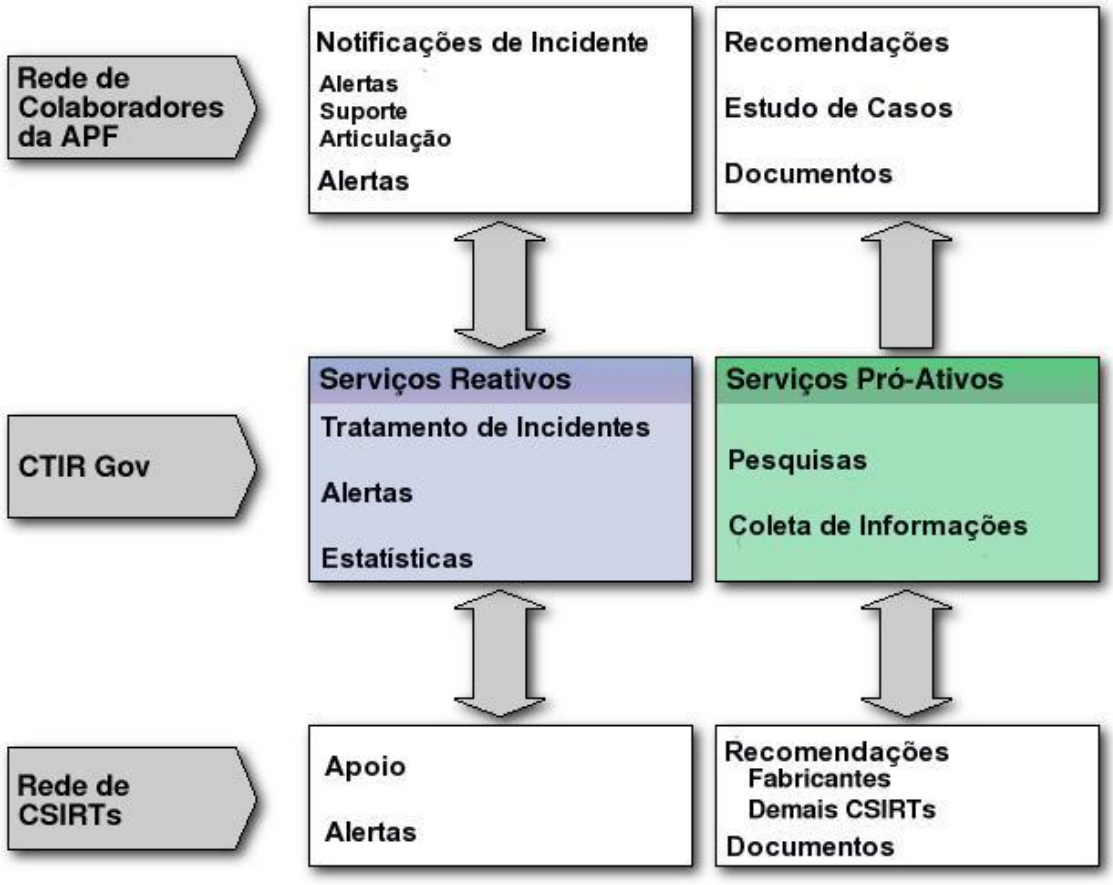



Figura 2 – Interações do CTIR Gov
Fonte: CTIR Gov[56]

O CTIR Gov funciona, portanto, como o ponto central da rede colaborativa de grupos de tratamentos de incidentes de segurança computacionais por todo o país, com destaque para o CERT.br. [57]

[56] Disponível em < http://www.ctir.gov.br/interacoes.html>. Acesso em 28 de maio de 2011.
[57] O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) é mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil, e atende a qualquer rede brasileira conectada à Internet, sendo responsável por receber, analisar e responder a incidentes de segurança envolvendo redes conectadas à Internet no Brasil.

### 3.4.2 **Agência Brasileira de Inteligência (ABIN)**

A lei nº 9.883, de 7 de dezembro de 1999[58] instituiu o Sistema Brasileiro de Inteligência (SISBIN) e criou a Agência Brasileira de Inteligência (ABIN) como o seu órgão central. É atualmente subordinada ao GSI/PR e tem como missões planejar, executar, coordenar, supervisionar e controlar as atividades de inteligência do País; planejar e executar ações, inclusive sigilosas, relativas à obtenção e análise de dados para a produção de conhecimentos destinados a assessorar o Presidente da República; planejar e executar a proteção de conhecimentos sensíveis, relativos aos interesses e à segurança do Estado e da sociedade; avaliar as ameaças, internas e externas, à ordem constitucional; e promover o desenvolvimento de recursos humanos e da doutrina de inteligência, e realizar estudos e pesquisas para o exercício e aprimoramento da atividade de inteligência.

Seu objetivo estratégico[59] é desenvolver atividades de inteligência voltadas para a defesa do Estado Democrático de Direito, da sociedade, da eficácia do poder público e da soberania nacional.

A atribuição de avaliação das ameaças, citada anteriormente, propicia melhores condições para que se construam mecanismos de segurança cibernética de forma mais eficiente, uma vez que se disponha da percepção das ameaças em tempo útil. Na estrutura da ABIN, merece destaque o Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações (CEPESC).

#### 3.4.2.1 Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações (CEPESC)

De acordo com a ABIN[60], o CEPESC foi criado em 19 de maio de 1982 para sanar a deficiência em salvaguardar o sigilo das transmissões oficiais, uma vez que havia, naquela época, falta de meios criptográficos próprios e de capacitação nesta área no Brasil. Dentre outras atribuições, destaca-se a promoção da pesquisa científica e tecnológica aplicada a projetos de segurança das comunicações, tais

---

[58] BRASIL. Lei nº 9.883, de 7 de dezembro de 1999. **Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN**, e dá outras providências. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 8 de dezembro de 1999.

[59] Segundo site da ABIN. Disponível em <http://www.abin.gov.br/modules/mastop_publish/?tac=Institucional#objestrat> Acesso em 28 Mai 2011.

[60] Disponível em <http://www.abin.gov.br/modules/mastop_publish/?tac=CEPESC> Acesso em 28 Mai 2011.

como o projeto e fabricação de soluções de criptografia utilizadas pelas Forças Armadas e Ministério das Relações Exteriores. Sua importância está na capacidade de desenvolver soluções criptológicas próprias, construindo algoritmos cujo nível de segurança seria adequado a proteger informações de Estado e equipamentos de proteção e de transmissão de informações. Além de fornecer equipamentos e sistemas de segurança, criptográfica a diversos órgãos governamentais, o CEPESC tem participação técnica no Comitê Gestor de Segurança da Informação (CGSI) e na elaboração das especificações do sistema de infraestrutura de chave pública para o País.

## 3.5 MINISTÉRIO DA DEFESA

As Forças Armadas atualmente exercem a proteção de suas estruturas instaladas no território nacional de forma independente, sem a coordenação do Ministério da Defesa (MD). O MD somente passou a dar relevância ao setor cibernético com a aprovação da Estratégia Nacional de Defesa, em 18 de dezembro de 2008. No presente momento estão em curso trabalhos para a definição, por parte do MD, com a colaboração das Forças Armadas, da Política de Defesa Cibernética, da Doutrina Militar de Defesa Cibernética e de um documento conceitual do Sistema Militar de Defesa Cibernética.

O Ministério da Defesa não conta, em sua estrutura organizacional com nenhum órgão exclusivamente voltado para o setor cibernético. Uma solução de curto prazo seria esta atribuição ser acumulada pela SC1 – Secretaria de Comando e Controle do Estado-Maior Conjunto das Forças Armadas. Durante visita do Ministro da Defesa, junto com o Comandante do Exército, ao Núcleo de Defesa Cibernética, realizada em 14 de junho de 2012, o Ministro da Defesa decidiu designar o NuCDCiber como a OM responsável pelo setor cibernético do MD. O CDCiber iniciou a sua atuação em operações com a Conferência das Nações Unidas sobre Desenvolvimento Sustentável (Rio +20) e nas Operações Conjuntas a cargo do MD, embora ainda não estivesse completamente ativado. O decreto nº 7.809, de 20 de setembro de 2012, que aprovou modificações nas estruturas regimentais dos Comandos da Marinha, do Exército e da Aeronáutica criou o Centro de Defesa Cibernética. Posteriormente, a portaria nº 3028 / Ministério da Defesa, de 14 de novembro de 2012, atribuiu ao CDCiber a responsabilidade pela coordenação e integração das atividades de defesa cibernética, no âmbito do Ministério da Defesa.

### 3.5.1 **Marinha do Brasil**

Ao contrário do MD, a Marinha do Brasil (MB) possui órgãos vocacionados para tratar do assunto em pauta. Além do Estado-Maior da Armada e do Centro de Inteligência da Marinha (CIM), pode-se mencionar, por exemplo, o Centro de Tecnologia da Informação da Marinha (CTIM), subordinado à Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM) e à Diretoria Geral da Material da Marinha (DGMM). A MB conta ainda com o Centro de Apoio a Sistemas Operativos (CASOP), que realiza inclusive atividades de guerra eletrônica, além do Centro de Análises de Sistemas Navais (CASNAV), vocacionado ao desenvolvimento de uma doutrina de defesa cibernética. Está ainda prevista a implantação dos Centros Locais de Tecnologia da Informação (CLTI) nos Distritos Navais, no Comando da Esquadra e no Comando da Força de Fuzileiros da Esquadra, os quais deverão conferir maior capilaridade à estrutura de governança de TI dessa Força.

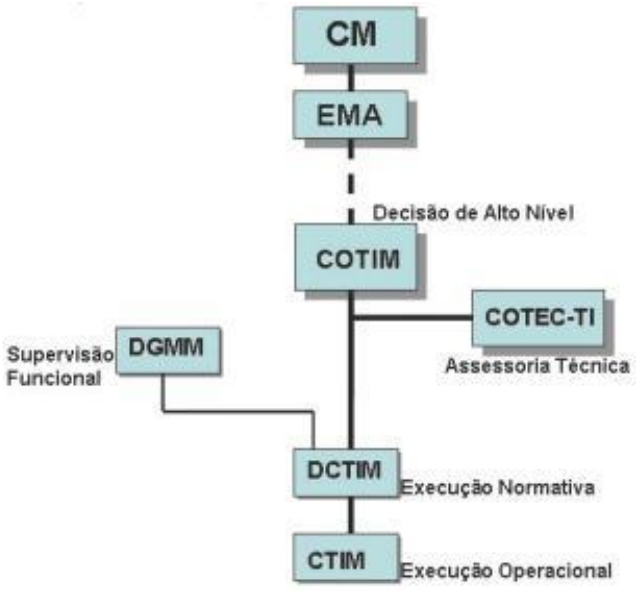



Figura 3 – Estrutura de Governança de TI em vigor na Marinha do Brasil
Fonte: AMARO, 2011

Segundo AMARO (2010, p. 12) a implantação da governança de TI na MB concentrou a tomada de decisão no Conselho de Tecnologia de Informação da Marinha (COTIM) a quem cabe tomar as decisões de alto nível. O Chefe do Estado-Maior da Armada, presidente do COTIM, é a autoridade de TI da MB e responde

pela formulação e disseminação corporativa dos princípios que orientam o emprego da TI. Para isso, é assessorado pela Comissão Técnica de Tecnologia da Informação (COTEC-TI).

Enquanto no nível decisório o COTIM desempenha seu papel de Governança assessorado pela COTEC-TI, no nível de coordenação gerencial cabe à DCTIM tornar efetivas as deliberações emanadas daquele Conselho e ratificadas pelo Comandante da Marinha. Sob a supervisão funcional do órgão de direção setorial DGMM, essa diretoria especializada tem uma extensa relação de atribuições em razão da centralização, em uma única OM, das principais responsabilidades pela consecução dos objetivos definidos para a Governança de TI na MB. Dentre estas atribuições destaca-se a de coordenar, executar e analisar todos os projetos que impliquem atividades de segurança da informação digital e de guerra cibernética.

Os principais órgãos de desenvolvimento de sistemas da Marinha estão em São Paulo e no Rio de Janeiro, sendo que o desenvolvimento de alguns sistemas é terceirizado em universidades e empresas.

### 3.5.2 **Força Aérea Brasileira**

Além do Estado-Maior da Aeronáutica (EMAER) e do Centro de Inteligência da Aeronáutica (CIAER), a FAB conta com o Centro de Estudo e Avaliação da Guerra Aérea (CEAGAR) e o Centro de Computação da Aeronáutica (CCA). Ademais, possui a Diretoria de Tecnologia da Informação da Aeronáutica (DTI), a qual tem como objetivos normatizar as atividades de segurança cibernética, promover a integração dos diversos Sistemas de Informação, no âmbito do Comando da Aeronáutica (COMAER), devendo organizar, normatizar, planejar, adquirir, implantar, integrar, coordenar, controlar e fiscalizar as atividades relativas à Tecnologia da Informação do COMAER. Adicionalmente, visa a garantir a interoperabilidade com os demais sistemas da APF, mantendo o alinhamento permanente à missão da Aeronáutica.

Como OM subordinadas à DTI, estão os Centros de Computação da Aeronáutica do Rio de Janeiro (CCA-RJ), de Brasília (CCA-BR) e de São José dos Campos (CCA-SJ), os quais dão capilaridade à estrutura de governança de TI da Força Aérea, sendo responsáveis pela execução do que é normatizado por aquela diretoria, dando suporte aos elos de Serviço de TI, que são as redes de computadores de cada Base Aérea e OM do Brasil.

A gerência centralizada de todos os equipamentos de infraestrutura de rede do Brasil responsáveis pelas telecomunicações digitais e de voz é encargo do Destacamento de Controle do Espaço Aéreo e Telemática do Rio de Janeiro (DTCEATM-RJ), subordinado ao Departamento de Controle do Espaço Aéreo (DECEA).

No que concerne à capacitação de RH, merece ser feita referência ao Curso de Segurança da Informação que foi realizado no CCA-RJ em 2010, e ao Programa de Pós-Graduação em Análise Operacional (PPGAO) do Instituto Tecnológico da Aeronáutica (ITA) em São José dos Campos – SP, que oferecem regularmente vagas ao Exército Brasileiro. Além disso, ressalta-se a participação de militares da FAB em seminários, reuniões técnicas, entre outros eventos promovidos pelo GSI/PR.

### 3.5.3 **Exército Brasileiro**

No mais alto nível, o Escritório de Projetos do Exército exerce a gerência executiva dos projetos do setor cibernético no âmbito da Força. O EB conta também com o Estado-Maior do Exército (EME) que é o Órgão de Direção Geral responsável pela elaboração da Política Militar Terrestre, pelo Planejamento Estratégico e pela orientação do preparo e do emprego da Força Terrestre[61]. A 2ª Subchefia do EME[62], dentre outras atribuições, é a responsável por planejar, orientar, coordenar e avaliar, no nível de direção geral, as atividades referentes aos Sistemas de Inteligência, Informações Organizacionais, Comunicação Social, Comunicações, Informática, Guerra Eletrônica, Imagens e Informações Geográficas, Informações Operacionais e Operações Psicológicas, integrantes do SINFOEx, objetivando a modernização do Sistema de Comando e Controle do Exército (SC2Ex) e a otimização do processo decisório no âmbito da Força. Desta forma, a 2ª SCh do EME assumiu também as atribuições correlatas da implantação do Setor Cibernético.

Todavia, as organizações militares do EB diretamente relacionadas ao Setor Cibernético estão, em sua maioria, subordinadas ao Departamento de Ciência e Tecnologia (DCT), cujo organograma será visto mais adiante.

No DCT, merece destaque o Grupo Finalístico de Segurança da Informação, responsável por realizar a pesquisa científica, o desenvolvimento experimental, o

[61] http://www.eme.eb.mil.br/
[62] http://www.eme.eb.mil.br/2sch.html

assessoramento científico tecnológico e a aplicação do conhecimento e das tecnologias dominadas de Segurança das Informações. Sua estrutura matricial permeia o DCT e todas as suas organizações militares diretamente subordinadas.

Outra OM que também possui relação com o setor cibernético é o Centro de Inteligência do Exército (CIE), órgão de assessoramento diretamente subordinado ao Comandante do Exército, que tem como missão assessorar o processo decisório, produzindo o conhecimento de Inteligência para o cumprimento da missão constitucional do Exército. Com base na integração e análise dos dados proporcionados pelas fontes humanas, de sinais, de imagens e outras[63], propicia ao EB o estabelecimento de sua política e estratégia, para o preparo e emprego da Força. O CIE possui, ainda, em sua estrutura organizacional, a Escola de Inteligência Militar do Exército (EsIMEx), que apoia os cursos de inteligência do sinal e de Guerra Cibernética, além de realizar os cursos de informações geográficas do Exército, de inteligência e de imagens.

3.5.3.1 Departamento de Ciência e Tecnologia (DCT)

O DCT é o Órgão de Direção Setorial do EB que tem como missão gerenciar o Sistema de Ciência e Tecnologia do Exército (SCTEx) para produzir os resultados científico-tecnológicos para a Força Terrestre[64]. Dentro do DCT, as OMDS ligadas ao Setor Cibernético são: Instituto Militar de Engenharia (IME), Centro Tecnológico do Exército (CTEx), Centro Integrado de Telemática do Exército (CITEx), Centro de Comunicações e Guerra Eletrônica do Exército (CComGEx) e Centro de Desenvolvimento de Sistemas (CDS). O Centro de Defesa Cibernética, quando ativado, irá constar também do quadro a seguir, no mesmo nível de todas as outras OM.

[63] Está em estudo a Fonte Cibernética ser considerada formalmente a 4ª fonte de dados do sistema operacional Inteligência.
[64] http://www.dct.eb.mil.br/index.php?option=com_content&view=article&id=56&Itemid=73

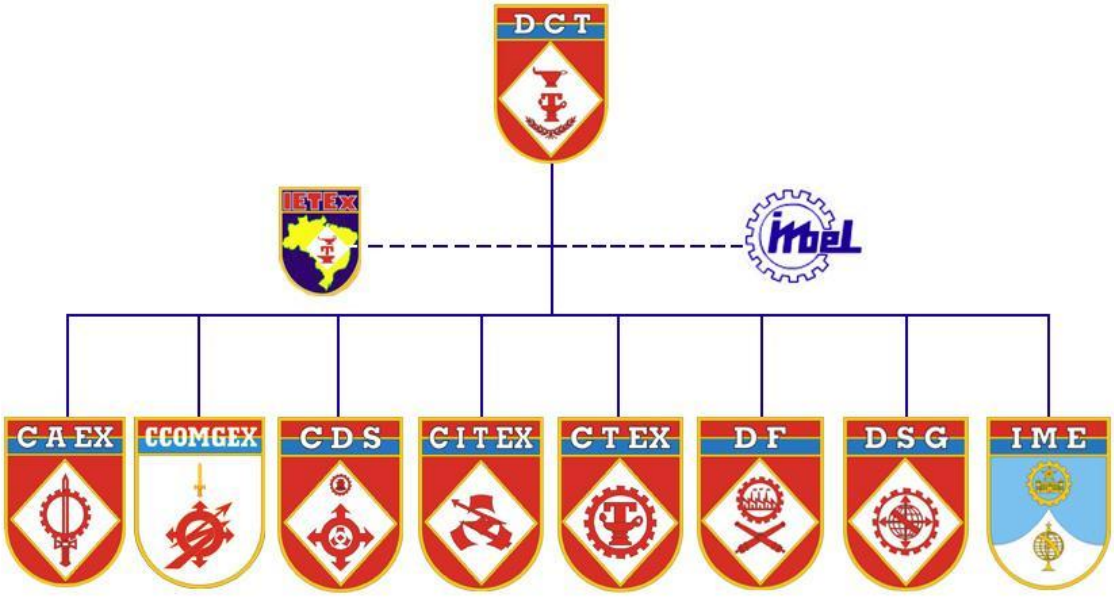



Figura 4 – Organizações Militares diretamente subordinadas ao DCT

Fonte: http://www.dct.eb.mil.br/index.php?option=com_content&view=article&id=58&Itemid=74

3.5.3.1.1 Centro de Comunicações e Guerra Eletrônica do Exército (CComGEx)

O CComGEx tem a missão de atuar em proveito da Força Terrestre, por intermédio dos vetores Comunicações e Guerra Eletrônica, desempenhando atividades nas vertentes operacional, de ensino e de logística, bem como gerenciando a inteligência do sinal e cooperando na área de ciência e tecnologia [65].

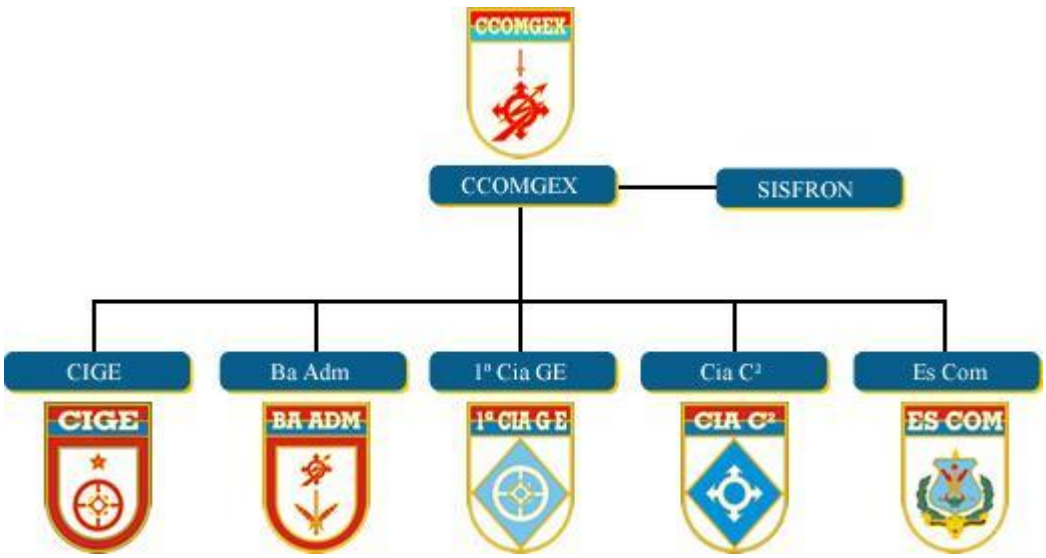



Figura 5 – Organograma do CComGEx

Fonte: http://www.ccomgex.eb.mil.br/ccomgex_organograma.php

[65] <http://www.ccomgex.eb.br/ccomgex_missao.php>

O CComGEx é integrado pelo Centro de Instrução de Guerra Eletrônica (CIGE), pela Escola de Comunicações (EsCom), pela 1ª Companhia de Guerra Eletrônica (1ª Cia GE) e pela Companhia de Comando e Controle (Cia C2), constituindo-se na OM do DCT com a vertente operacional de comando e controle.

Dentro do CComGEx, destaca-se o Centro de Instrução de Guerra Eletrônica (CIGE), o qual possui especialistas em segurança da informação e inteligência de sinais que têm ministrado os estágios de Defesa Cibernética do Exército. Em 2012, para cooperar com a capacitação do setor cibernético, passaram a funcionar no CIGE o Curso de Guerra Cibernética e na EsCom o curso de Gestão de Sistemas Táticos de Comando e Controle. Dentro do CComGEx opera ainda o Centro de Inteligência do sinal (CIS) que é o provedor da inteligência do sinal do sistema de inteligência do EB, operando em ligação com o CIE.

3.5.3.1.2 Sistema de Telemática do Exército (SisTEx)

Fazem parte da estrutura do SisTEx o Centro Integrado de Telemática do Exército (CITEx), sete Centros de Telemática de Área (CTA) e cinco Centros de Telemática (CT). Os CTAs e CTs devem cumprir a missão do CITEx na área da sua Região Militar e/ou Divisão de Exército, conforme o organograma a seguir. Essa estrutura de Telecomunicações e Informática cobre todo o território nacional, apoiando com seus serviços o Comando do Exército, o EME, os ODS, os Comandos Militares de Área e as Regiões Militares.

O CITEx tem, portanto, a missão de proporcionar a base física e lógica para a operação dos sistemas de Informática e Comunicações de interesse do Sistema de Comando e Controle do Exército. Desta forma, o CITEx é encarregado de estabelecer, manter e operar a estrutura de Telemática de interesse do Exército, no seu mais alto nível, integrando-o ao Sistema de Comando e Controle da Força Terrestre (SC2FTer) e ao Sistema Militar de Comando e Controle (SISMC2), mantendo constante ligação com o CTIR Gov. O CITEx também é responsável pela infraestrutura de TI para hospedagem de diversos servidores de rede e banco de dados corporativos do EB.

Destacam-se entre os serviços prestados: as Redes Rádio Fixas (RRF), a Rede Corporativa do Exército (EBNet) e a Rede Integrada de Telefonia do Exército (RITEx).


Figura 6 – Estrutura do CITEx
Fonte: http://www.citex.eb.mil.br/paginas/estrutura.php

A Rede Rádio Fixa Principal (RRFP) e Redes Rádio Fixas Secundárias (RRFS) são redes de segurança, capazes de serem utilizadas em caso de colapso das demais redes, possuindo capilaridade e autonomia próprias. A EBNet é a intranet do Exército, com acesso por rede privada virtual (VPN) ou por rede metropolitana própria, e atende mais de 500 organizações militares. A RITEx é uma rede fechada, própria do Exército, que, trafegando sobre a EBNet, permite a transmissão de voz em tecnologia Voz sobre IP (VoIP), a qual disponibiliza um conjunto de serviços amplamente utilizados de que se valem mais de 20 diferentes sistemas corporativos, videoconferências e a própria RITEx. Para aumentar a interoperabilidade da RITEx, esta conta com interfaces com o Sistema de Proteção da Amazônia (SIPAM) em Manaus e com o Sistema Militar de Comunicações por Satélite (SISCOMIS) em Brasília e no Rio de Janeiro. Para viabilizar esta comunicação por todo território nacional, a Empresa Brasileira de Telecomunicações (EMBRATEL) disponibiliza pontos de conexão com seu *backbone*[66], os quais geram enlaces que viabilizam a comunicação por todo o País.

[66] No contexto de redes de computadores, o backbone (backbone traduzindo para o português, espinha dorsal, embora no contexto de redes, backbone signifique rede de transporte) designa o esquema de ligações centrais de um sistema mais amplo, tipicamente de elevado desempenho.

3.5.3.1.3 Centro de desenvolvimento de Sistemas (CDS)

O CDS tem a missão de conceber, desenvolver, integrar e aperfeiçoar sistemas, programas, aplicativos e estruturas lógicas dos diversos sistemas corporativos e sistemas de informações operacionais do Exército, atribuídos ao DCT[67].

Além disso, o CDS busca garantir a segurança de suas instalações e da documentação técnica, bem como a integridade, privacidade e segurança das informações processadas no âmbito daquele centro. Em relação ao tratamento de incidentes, está sendo desenvolvido um projeto corporativo em conjunto com o CITEx, para a criação de um CSIRT – Time de Resposta a Incidentes de Segurança Computacionais (*Computer Security Incident Response Team)* - no âmbito da EBNet. A estrutura central situa-se no CITEx, enquanto Seções de Tratamento de Incidentes de Rede (STIR) estão instaladas nos CT/CTA, atuando conjuntamente sob a coordenação do CITEx.

3.5.3.1.4 Instituto Militar de Engenharia (IME)

No IME, há o Programa de Pós-Graduação em Sistemas e Computação da Seção de Engenharia de Computação, incluindo o mestrado em Sistemas e Computação, com as seguintes linhas de pesquisa[68]: Algoritmos e Linguagens de Programação; Tecnologias para Tratamento e Transmissão da Informação; e Sistemas de Informação.

A partir de fevereiro de 2007, foram iniciadas as atividades docentes do Programa de Pós-Graduação em Engenharia de Defesa (PGED), com o qual o Instituto busca orientar efetivamente seus cursos e pesquisas para a área de Defesa e para as necessidades do Exército Brasileiro. Este objetivo encontra-se em consonância com as diretrizes do Departamento de Ciência e Tecnologia do EB e com a Política de Defesa Nacional, lançada em junho de 2005 pelo Ministério da Defesa, no que se refere à capacitação científica e tecnológica das Forças Armadas e da Sociedade Civil.

[67] http://www.cds.eb.br/index.php/missao
[68] http://www.ime.eb.br/index.php?option=com_content&view=article&id=207&Itemid=317

3.5.3.1.5 Centro Tecnológico do Exército (CTEx)

O CTEx tem por missão realizar a pesquisa científica, o desenvolvimento experimental, o assessoramento científico-tecnológico e a aplicação do conhecimento visando à obtenção de produtos de defesa de interesse do Exército [69]. O CTEx possui, em sua Divisão de Tecnologia da Informação (DTI), laboratórios destinados à pesquisa e ao desenvolvimento dos projetos dos Grupos Finalísticos de Guerra Eletrônica (GGE) e de Comando e Controle (GC2), entre outros projetos. Ademais, foi o responsável pelo desenvolvimento do Módulo de Telemática, o qual constitui a base física do Sistema C2 em Combate.

3.5.3.1.6 Centro de Defesa Cibernética (CDCiber)

O Núcleo do Centro de Defesa Cibernética (NuCDCiber) foi ativado em 02 de agosto de 2010 pela Portaria nº 667 - Comandante do Exército, de 04 de agosto de 2010[70] e passou a coordenar a execução dos seguintes projetos:

- Projeto de gestão de pessoal, com apoio do DCT e suas OMDS, na fase inicial, incluindo temas como a definição dos perfis do pessoal envolvido, identificação de talentos, seleção, capacitação e a permanência na atividade. O projeto envolve, ainda, a elaboração do fluxo de carreira e a proposta para a movimentação do pessoal, além da mobilização e a desmobilização, contando com a participação do DGP;

- Projeto da estrutura de capacitação e de preparo e emprego operacional;

- Projeto da estrutura para produção do conhecimento oriundo de fonte cibernética;

- Projeto do arcabouço documental, com apoio do DCT e suas OMDS, devendo abranger a adequação das normas existentes e a criação de novas normas em face das necessidades do Setor Cibernético, com apoio do Sistema de Ensino do Exército, de especialistas "*Ad Hoc"* e definições doutrinárias;

- Projeto de estrutura de pesquisa científica na área cibernética;

- Projeto de estrutura de apoio tecnológico e desenvolvimento de sistemas;

---

[69] http://www.ctex.eb.br/missao.htm

[70] BRASIL. Exército. Comandante do Exército. Portaria nº 667, de 4 de agosto de 2010. **Ativa do Núcleo do Centro de Defesa Cibernética do Exército e dá outras providências.** Boletim do Exército nº 31. Brasília, DF, 6 de agosto de 2010.

- Projeto de implantação do Centro de Defesa Cibernética, correspondente à evolução do atual Núcleo;

- Planejamento e execução da Segurança Cibernética;

Os seguintes projetos foram incluídos posteriormente, em 2012, por determinação do Estado-Maior do Exército:

- Rede Nacional de Segurança da Informação e Criptografia (RENASIC); e

- Rádio Definido por Software (RDS).

De forma sintética, no quadro a seguir, têm-se uma visão dos principais projetos do setor cibernético e os respectivos órgãos responsáveis:

| **Projeto** | **Responsabilidade** |
|---|---|
| Estrutura de capacitação e de preparo e emprego operacional | CCOMGEx |
| Estrutura de Apoio Tecnológico e desenvolvimento de sistemas | CDS |
| Planejamento e execução da Segurança Cibernética | CITEx |
| Rádio Definido por Software | CTEx |
| Estrutura de pesquisa científica na área cibernética | DCT, por intermédio de seu Grupo Finalístico da Segurança da Informação, com apoio do IME |
| Gestão de Pessoal | Centro de Defesa Cibernética |
| Arcabouço Documental | |
| Estrutura para produção do conhecimento oriundo da fonte cibernética | |
| Implantação do Centro de Defesa Cibernética | |
| Rede Nacional de Segurança da Informação e Criptografia | |

Quadro 3 - principais projetos do setor cibernético

Fonte: o autor

Em julho de 2012, o Ministro da Defesa, após a já mencionada visita ao NuCDCiber, acompanhado pelo Alto Comando do Exército, decidiu tornar o mesmo uma estrutura conjunta. Em 20 de setembro de 2012, o Decreto nº 7.809 alterou a estrutura regimental da Marinha, do Exército e da Aeronáutica, criando o Centro de

Defesa Cibernética. Posteriormente, o Ministério da Defesa, por intermédio da Portaria nº 3.028, de 14 de novembro de 2012, atribuiu ao CDCiber a responsabilidade pela coordenação e integração das atividades de defesa cibernética no âmbito do Ministério da Defesa.

## 3.6 MINISTÉRIO DA JUSTIÇA

Segundo MANDARINO (2010 p. 117), o Ministério da Justiça tem por missão garantir e promover a cidadania, a justiça e a segurança pública, através de ação conjunta entre Estado e sociedade. Na sua área de competência, destacam-se as ações de Polícia Judiciária, prevenção e repressão à lavagem de dinheiro e cooperação jurídica internacional.

A atuação do Ministério da Justiça cresce de importância na medida em que a motivação dos crimes cibernéticos envolve frequentemente obtenção de recursos financeiros de forma ilegal, além de ameaçar o sistema financeiro, considerado infraestrutura crítica. Da estrutura do Ministério da Justiça, exerce papel relevante a Polícia Federal.

### 3.6.1 **Polícia Federal**

A Polícia Federal é um órgão de caráter permanente, organizado e mantido pela União[71]. Dentre as suas atribuições, merecem destaque por se relacionarem com o campo cibernético as seguintes:

- apurar infrações penais contra a ordem política e social ou em detrimento de bens, serviços e interesses da União ou de suas entidades autárquicas e empresas públicas, assim como outras infrações cuja prática tenha repercussão interestadual ou internacional e exija repressão uniforme, segundo se dispuser em lei; e

- exercer, com exclusividade, as funções de Polícia Judiciária da União.

Em 4 de junho de 2012, a Polícia Federal inaugurou o Centro de Monitoramento do Serviço de Repressão a Crimes Cibernéticos no Distrito Federal, em Brasília. Este centro destina-se a ser um instrumento de prevenção e investigação a ataques cibernéticos contra sistemas de informação e infraestruturas críticas do Governo Federal.

---

[71] Constituição da República Federativa do Brasil de 1988, Art 144, §1º.

Após conhecer os principais órgãos e atores que atuam na Segurança e na Defesa Cibernética no Brasil, suas atribuições e particularidades, será abordado o estudo da Doutrina de Guerra Cibernética na Rússia e China e, com mais ênfase, nos Estados Unidos da América (EUA), que é atualmente o país que mais publica e difunde os seus esforços nessa área.

# 4 DOUTRINA DE GUERRA CIBERNÉTICA DOS ESTADOS UNIDOS DA AMÉRICA

Neste capítulo será abordada a doutrina de Guerra Cibernética em construção pelos Estados Unidos da América. Desta forma, serão apresentados os conceitos doutrinários julgados relevantes e aplicáveis à realidade brasileira, sem que os mesmos sigam necessariamente a ordem ou encadeamento originalmente utilizados. Os documentos que trazem os conceitos originais podem ser consultados na íntegra através das referências.

## 4.1 NOVOS CONCEITOS – O MODELO CONCEITUAL DAS OPERAÇÕES NO CIBERESPAÇO

De todos os documentos buscados para a pesquisa sobre doutrina de operações no ciberespaço, nenhum apresentou uma abordagem tão interessante e inovadora quanto as publicações do *US Army War College - Information Operation Primer AY12 Edition*[72], do Comando de Treinamento e Doutrina do Exército Americano - TRADOC Pam 525-7-8[73] e o documento doutrinário da Força Aérea Americana *3-12 Cyberspace Operations*[74]. Estas publicações representam a última atualização da doutrina militar americana para as Operações de Informação e o domínio do ciberespaço, mostrando claramente que fazem parte de um trabalho em andamento, buscando influenciar o desenvolvimento doutrinário nesta área, inclusive a doutrina conjunta americana:

> Both Army and Joint doctrine for Information Operations are being revised and will also be affected by the recent activation of U.S. Cyber Command. As of this writing, **Joint IO and Cyberspace Operations doctrine are being developed in parallel with expected publication in summer 2012.** (Information Operations Primer, 2011, p.3)[75]

---

[72] ESTADOS UNIDOS DA AMÉRICA. Army. Department of the Army. **Information Operations Primer**. Army.mil, 19 out. 2011. Disponível em: <http://www.carlisle.army.mil/usawc/dmspo/Publications/Publications.htm>. Acesso em: 15 dez. 2011.

[73] ESTADOS UNIDOS DA AMÉRICA. Army. Department of the Army. **Cyberspace Operations Concept Capability Plan 2016-2028**. Army.mil, 22 fev. 2010. Disponível em: <http://www.tradoc.army.mil/tpubs/pamndx.htm>. Acesso em: 25 nov. 2010.

[74] ESTADOS UNIDOS DA AMÉRICA. Air Force. Department of the Air Force. **Air Force Doctrine Document 3-12 Cyberspace Operations**. AF.mil, 15 jul. 2010. Disponível em: <http://www.e-publishing.af.mil/shared/media/epubs/AFDD3-12.pdf>. Acesso em: 25 nov. 2010.

[75] Tanto a doutrina do Exército quanto a doutrina conjunta para Operações de Informação estão sendo revisadas e serão também afetadas pela recente ativação do Comando Cibernético dos Estados Unidos. **Quando desta publicação, a doutrina conjunta de Operações de Informação e Operações no Ciberespaço estão sendo desenvolvidas em paralelo, com a publicação prevista para o verão de 2012.**

TRADOC Pam 525-7-8 **is the foundation for future force development and the base for subsequent developments of supporting concepts, concept capability plans, and the Joint Capabilities Integration and Development System (JCIDS) process**. It supports experimentation described in the Army Capabilities Integration Center (ARCIC) Campaign Plan and functions as the basis for developing solutions related to the future force within the doctrine, organizations, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) domains. This pamphlet applies to all TRADOC, Department of Army (DA) and Army Reserve component activities that develop DOTMLPF requirements. (Pam 525-7-8, 2010, p.1)[76]

[…]

TRADOC Pam 525-7-8 provides an initial examination of how CyberOps are integrated with the commander's other capabilities to gain advantage, to protect that advantage, and to place adversaries at a disadvantage in Full Spectrum Operations. **The examination will be refined through the Capabilities Based Assesment and doctrine development process**. (Pam 525-7-8, 2010, p.5) [77]

Air Force Doctrine Document (AFDD) 3-12, Cyberspace Operations, **is the Air Force's foundational doctrine publication for Air Force operations in, through, and from the cyberspace domain.** (AFDD 3-12, 2010, p. v)[78]

[…]

Although cyberspace operations are integral to all combatant commands, Services, and agency boundaries, as of the date of publication of this AFDD, there is no overarching joint doctrine for planning or operations in cyberspace. **The development of this Service doctrine document is intended to influence the eventual creation of corresponding joint and allied doctrine. Joint cyberspace operations doctrine is under development. Air Force doctrine seeks compatibility and to influence joint doctrine.** [destaques nossos] (AFDD 3-12, 2010, p. 14)[79]

---

[76] A publicação do TRADOC Pam 525-7-8 **é o fundamento para o desenvolvimento futuro da força e a base para o desenvolvimento subsequente de conceitos de suporte, planos conceituais de capacidade e o sistema de desenvolvimento e integração de capacidades conjuntas (JCIDS)**. Ela baseia a experimentação descrita no Plano de Campanha do Centro de Integração de Capacidades do Exército (ARCIC) e serve como base para o desenvolvimento de soluções relacionadas à força do futuro dentro dos domínios da doutrina, organizações, treinamento, material, liderança e educação, pessoal e instalações (DOTMLPF). Este panfleto se aplica a todas as atividades do TRADOC, Departamento do Exército e componentes da Reserva do Exército que desenvolvem requisitos do DOTMLPF.

[77] A publicação do TRADOC Pam 525-7-8 fornece um exame inicial de como as Operações Cibernéticas são integradas com as outras capacidades do comandante para obter vantagem, para proteger essa vantagem e para colocar os adversários em desvantagem em Operações de Amplo Espectro**. Esse exame será refinado por meio de avaliação baseada em capacidades e no processo de desenvolvimento da doutrina.**

[78] O Documento de Doutrina da Força Aérea (AFDD) 3-12, Operações no Ciberespaço, **é a publicação doutrinária fundamental da Força Aérea para operações da Força Aérea dentro, através e oriundas do domínio do espaço cibernético**.

[79] Embora as operações no espaço cibernético sejam parte integrante de todos os comandos combatentes, serviços e agências, na data de publicação deste AFDD, ainda não há uma doutrina conjunta abrangente para planejamento ou operações no espaço cibernético. **O desenvolvimento deste documento de doutrina da Força Aérea tem a intenção de influenciar a criação eventual de uma correspondente doutrina conjunta e aliada. A doutrina conjunta de operações no espaço cibernético está em desenvolvimento. A doutrina da Força Aérea busca influenciar a doutrina conjunta e ficar compatível com a mesma.**

Com exceção do *Information Operations Primer*, estes documentos eram inicialmente classificados. Como esse fato poderia atrasar o desenvolvimento doutrinário, suas partes sensíveis foram transformadas em anexos (que foram publicados separadamente) e as publicações ostensivas resultantes vieram a público na segunda quinzena de novembro de 2010.

Desta forma, é extremamente interessante aproveitar os conceitos apresentados por esses documentos, que se aplicam quase que integralmente à situação brasileira.

## 4.2 A RELEVÂNCIA

É natural que os EUA sejam um dos países mais preocupados com o risco de atividade adversa trazida pelo ciberespaço. Os alvos mais visados são as infraestruturas críticas (instalações, serviços e bens que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico e/ou político[80]) incluído nestas os serviços financeiros e também outros elementos do poder nacional. O seu alto grau tecnológico e a sua crescente dependência da interconexão por redes de comunicação de dados, aumentam a sua vulnerabilidade a esse risco, que incluem hackers, organizados ou não e nem sempre mal intencionados, nações e Estados tradicionais, corporações transnacionais não combatentes, organizações criminosas, terroristas, ativistas e indivíduos, cada qual com diversos níveis de competência. Isto cria uma condição de turbulência permanente que não leva às condições de resolução de conflitos tradicionais que sempre foram buscadas. Estes conceitos são plenamente aplicáveis à realidade brasileira, inserida no contexto das potências emergentes e com uma das maiores infraestruturas de telecomunicações e de serviços bancários do mundo.

A convergência de redes cabeadas, redes sem fio e tecnologias ópticas está levando à integração de redes de computadores e de telecomunicações. Sistemas de nova geração estão sendo criados, formando uma rede global, híbrida e adaptativa que combinará tecnologias cabeadas, sem fio, ópticas, comunicações por satélite, redes celulares e outros sistemas. Em breve essas redes irão prover acesso

---

[80] BRASIL. Portaria nº 2, de 8 de fevereiro de 2008**. Institui Grupos Técnicos de Segurança de Infraestruturas Críticas** (GTSIC) e dá outras providências. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 11 de fevereiro de 2008. Art 1º § único.

universal aos usuários e permitirá que os mesmos colaborem quando necessário em tempo quase real.

Assim, a habilidade dos adversários em se atualizar dentro do ritmo acelerado de mudanças tecnológicas traz uma série de complicações ao ambiente operacional. Normalmente o adversário irá utilizar o próprio mercado comercial como o seu desenvolvedor de equipamentos e técnicas, o que lhe proporcionará uma agilidade e adaptabilidade maior que o longo ciclo de pesquisa, desenvolvimento, testes e aquisição, normalmente utilizado nos meios governamentais, acadêmicos e militares. Uma vantagem significativa irá para o lado que for capaz de obter, proteger e explorar vantagens no contestado e congestionado ciberespaço e no espectro eletromagnético. Da mesma forma, o lado que falhar nessa disputa ou que não for capaz de operar efetivamente quando os seus sistemas estiverem degradados ou interrompidos, cederá uma significante vantagem ao adversário.

Esse é o imenso desafio que se apresenta. As forças do Exército necessitam fazer do ciberespaço e do espectro eletromagnético um fator central e um componente rotineiro das suas operações assim como os Comandantes irão necessitar, dentre outras coisas, das capacidades associadas e do conhecimento necessário para aplicar essas capacidades.

## 4.3 DEFINIÇÃO DO AMBIENTE

### 4.3.1 **O Ciberespaço**

O ciberespaço pode ser definido como um domínio global dentro de um ambiente de informações, consistindo de redes interdependentes de infraestruturas de tecnologias de informação, incluindo a Internet, redes de telecomunicações, sistemas computacionais, processadores embutidos e controladores.[81]

### 4.3.2 **Os Domínios Operacionais**

O ciberespaço é um dos cinco domínios operacionais e permeia todos os outros domínios. Os outros domínios são: o terrestre, o marítimo, o aéreo e o espacial. Estes cinco domínios são interdependentes. Atividades no ciberespaço podem criar liberdade de ação para atividades em outros domínios assim como atividades em outros domínios também criam efeitos dentro e através do

[81] ESTADOS UNIDOS DA AMÉRICA, 2010a, p. 6

ciberespaço. O objetivo central da integração entre os domínios é a habilidade de se alavancar capacidades de vários domínios para sejam criados efeitos únicos e, frequentemente, decisivos. No combate moderno, todos os domínios são interconectados pelas operações no ciberespaço. A representação deste conceito pode ser vista na figura a seguir:

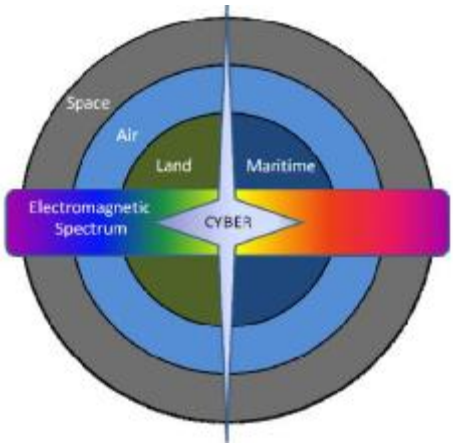



Figura 7 – Relacionamento dos domínios operacionais
Fonte: ESTADOS UNIDOS DA AMÉRICA, 2010b

### 4.3.3 **As Camadas do Ciberespaço**

O ciberespaço pode ser visualizado como três camadas (física, lógica e social) compostas por cinco componentes (geográfico, físicos de rede, lógicos de rede, da persona e da persona cibernética [82]), conforme a figura a seguir:

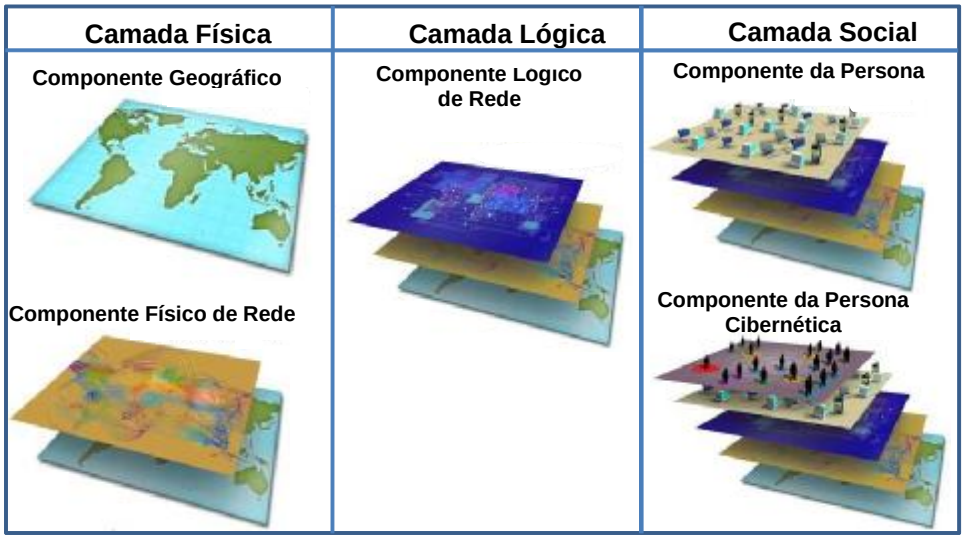



Figura 8 – As camadas do Ciberespaço
Fonte: ESTADOS UNIDOS DA AMÉRICA, 2010a

[82] Personalidade que o indivíduo apresenta em público como real, mas que, na verdade, pode ser uma variante às vezes muito diferente da verdadeira.

#### 4.3.3.1 A Camada Física

A camada física inclui o componente geográfico e o componente físico de rede. O componente geográfico é a localização física dos elementos da rede. Enquanto fronteiras geopolíticas podem facilmente ser cruzadas no ciberespaço em uma velocidade próxima à da luz, ainda existe um aspecto físico ligado aos outros domínios. O componente físico de rede inclui todo o hardware[83] e a infraestrutura (cabeada, sem fio e óptica) que suporta a rede e os conectores físicos (fios, cabos, rádio frequência, roteadores, servidores e computadores).

#### 4.3.3.2 A Camada Lógica

A camada lógica inclui o componente lógico de rede, que é técnico por natureza e consiste das conexões lógicas que existem entre os nós da rede. Esses nós são quaisquer dispositivos conectados a uma rede de computadores. Podem ser computadores, assistentes pessoais digitais (PDA)[84], telefones celulares ou quaisquer outras ferramentas de rede. Em uma rede baseada no protocolo de Internet (rede IP), um nó é qualquer dispositivo que receba um endereço IP.

#### 4.3.3.3 A Camada Social

A camada social representa os aspectos humanos e cognitivos e inclui o componente da persona e o componente da persona cibernética. O componente da persona cibernética inclui a identificação de uma pessoa ou persona na rede (endereço de correio eletrônico, endereço IP de um computador, número de telefone celular, etc). O componente da persona consiste de pessoas de fato na rede. Um indivíduo pode ter múltiplas personas cibernéticas (por exemplo, diferentes contas de endereço eletrônico em computadores diferentes) e uma única persona cibernética pode ter usuários múltiplos (por exemplo, vários usuários acessando uma única conta de correio eletrônico corporativo). Isto traz implicações importantes para as Forças Armadas em termos de atribuição de responsabilidades e localização de alvos que são fontes de ações cibernéticas. Isto também significa que será necessário desenvolver significativas capacidades de se obter consciência

---

[83] Conjunto dos componentes físicos (material eletrônico, placas, monitor, equipamentos periféricos etc.) de um equipamento eletrônico ou sistema computacional.
[84] Personal Digital Assistants.

situacional, realizar perícias forenses e trabalhos de inteligência para conter a complexa ameaça cibernética.

Há indícios de que os EUA estejam desenvolvendo atividades, dentro do contexto das Operações de Informação, utilizando redes sociais para influenciar o comportamento de público alvo selecionado, buscando alterar o seu processo decisório e conduzir atividades provavelmente relacionadas à Operações Psicológicas e Comunicação Social, de maneira velada, dentro dessas redes[85]. Esses indícios são corroborados pelo edital de licitação lançado em 22 de junho de 2010 no site www.FedBizOpps.gov, que é um site de pregões online do governo estadunidense similar ao ComprasNet do governo brasileiro. Uma reprodução do edital pode ser vista no Anexo C.

No edital é licitada a prestação de um serviço de gerenciamento de personas cibernéticas online, cujo software permitiria que cada operador gerenciasse dez personas, completas, com contexto, histórico, detalhes de suporte e presenças cibernéticas que sejam técnica, cultural e geograficamente consistentes. As aplicações individuais deveriam permitir ao operador exercitar um número de diferentes pessoas online da mesma estação de trabalho, sem preocupação de ser descoberto por adversários sofisticados. As personas deveriam ser capazes de parecer originarem-se em qualquer parte do mundo e poder interagir através dos serviços online convencionais e nas plataformas de mídias sociais. O serviço incluiria também um ambiente amigável ao usuário para maximizar a consciência situacional, mostrando informações locais em tempo real.

### 4.3.4 **Redes no Ciberespaço**

O ciberespaço consiste de muitos nós e redes diferentes. Apesar de nem todos os nós e redes estarem globalmente conectados e acessíveis, o ciberespaço está cada vez mais interconectado. É fácil transpor fronteiras geográficas utilizando a Internet, quando se compara a outras formas de transmissão ou de viagem. Redes, entretanto, podem ser isoladas utilizando-se protocolos, firewalls, criptografia e separação física de outras redes. São agrupadas tipicamente em domínios, que podem especificar países, como o .br, ou atividades, como .mil, .gov, .com e .org.

---

[85] WEBSTER, Stephen C. **Military's 'persona' software cost millions, used for 'classified social media activities'**. The Raw History. Disponível em: < http://www.rawstory.com/rs/2011/02/22/exclusive-militarys-persona-software-cost-millions-used-for-classified-social-media-activities/>. Acesso em: 07 jul. 2011.

Estes domínios são específicos para uma organização ou missão e são organizados de acordo com a proximidade física ou função.

Enquanto alguma forma de acesso possa ser obtida global ou remotamente, o acesso a redes fechadas e especializadas normalmente requer proximidade física.

## 4.4 OS TIPOS DE OPERAÇÕES CIBERNÉTICAS

Durante o seminário *Cyber Warfare 2011*, realizado nos dias 27 e 28 de janeiro de 2011, em Londres, no Reino Unido[86], o Comandante do 2º Batalhão de Operações de Informação do Exército dos EUA apresentou os conceitos abaixo, que diferem dos conceitos apresentados no TRADOC Pamphlet 525-7-8. Como essa última publicação é um Plano Conceitual de Capacidades, com data anterior à apresentação do Comandante do Batalhão, assumiu-se que os conceitos mostrados na apresentação representam a última aproximação da doutrina estadunidense de Guerra Cibernética.

Este batalhão tem por missão conduzir operações contra ameaças cibernéticas (counter-cyber operations) na dimensão cibernética do espaço de batalha, em apoio ao Comando Cibernético do Exército, a fim de afetar, neutralizar, negar ou mitigar tentativas de penetração ou ataques aos sistemas de informação que dão suporte às atividades operacionais do Exército.

Essa missão apresenta uma inovação doutrinária, abandonando o conceito de Operações em Redes de Computadores (Computer Network Operations), com suas três vertentes clássicas: Defesa de Redes de Computadores (Computer Network Defense), Exploração de Redes de Computadores (Computer Network Exploitation) e Ataque à Redes de Computadores (Computer Network Attack).

### 4.4.1 **Operações Contra-Ameaças Cibernéticas (counter-cyber operations)**

As operações contra-ameaças cibernéticas contemplam as ações defensivas e ofensivas necessárias para obter e manter o desejado grau de superioridade no ciberespaço. Se subdividem em Operações Cibernéticas Defensivas (*Defensive Cyber Operations*) e Operações Contra-Ameaças Cibernéticas Defensivas (*Defensive Counter-Cyber Operations*).

---

[86] Descrito no relatório de viagem da atividade, retirado dos arquivos da Divisão de Doutrina do CDCiber

4.4.1.1 Operações Cibernéticas Defensivas (*Defensive Cyber Operations*)

São um conjunto de ações realizadas para **detectar, analisar, conter e mitigar** ameaças e vulnerabilidades cibernéticas, a fim de conquistar e manter a liberdade de ação no ciberespaço.

4.4.1.2 Operações Contra-Ameaças Cibernéticas Defensivas (*Defensive Counter-Cyber Operations*)

São as contramedidas defensivas realizadas para **detectar, identificar, interceptar, destruir ou negar** atividades maliciosas de penetração ou ataque através do ciberespaço.

Essa nova abordagem insere, definitivamente, a necessidade de se adotar ações ofensivas no nível estratégico e operacional, mesmo que o conceito exposto atenue essa ideia e se prenda apenas às medidas a serem desencadeadas contra um oponente que esteja tentando invadir os sistemas de informação que dão suporte ao comando e controle das operações militares do exército dos EUA.

Talvez essa mudança seja decorrente do novo paradigma descrito por BRILL[87] onde o foco anterior era de, principalmente, proteger o perímetro das redes e sistemas (“mantenham os atacantes fora”) que mudou para melhorar a detecção de intrusão e a recuperação das redes e sistemas (“tentem manter os atacantes fora, mas gastem os recursos necessários para reconhecer quando um oponente penetrou a sua segurança da informação e está agora operando de dentro da sua rede”).

Essa indefinição na terminologia básica a ser utilizada reflete a incipiência na formulação doutrinária estadunidense, visto que, como será mostrado mais adiante, na bilateral Rússia – EUA sobre segurança cibernética outras terminologias também surgirão.

## 4.5 PRINCÍPIOS DAS OPERAÇÕES CONJUNTAS E O CIBERESPAÇO

A doutrina estadunidense aponta que princípios de guerra utilizados nas operações conjuntas podem ser aplicados e demonstrados através das operações cibernéticas, conforme o quadro a seguir:

[87] Entrevista concedida ao autor em 10 de maio de 2012, constante do Apêndice E.

| PRINCÍPIO | PROPÓSITO | OBSERVAÇÕES | EXEMPLO DE OPERAÇÃO CIBERNÉTICA |
|---|---|---|---|
| **Objetivo** | Dirigir cada operação militar visando um objetivo claramente definido, decisivo e atingível | Objetivos militares devem dar suporte a metas políticas mais abrangentes | Ataques cibernéticos dirigidos pelo C T Op para desligar a energia em redes elétricas-chave para a liderança inimiga |
| **Ofensiva** | Conquistar, manter e explorar a iniciativa | Maneira mais efetiva e decisiva de se atingir os objetivos | Ataque distribuído de negação de serviço na Estônia em 2007, sobrecarregando as redes do país |
| **Massa** | Concentrar os efeitos nos lugares e momentos mais vantajosos | Necessita haver integração e sincronização com outras forças | Suspeita de ataques preemptivos por atores Russos em redes da Geórgia para interromper a coordenação de forças da Geórgia durante a invasão de 2008 |
| **Economia de Forças** | Alocar a força mínima necessária em esforços secundários | Menor efetivo necessário para criar efeitos massivos através do domínio do ciberespaço | Utilização de ataques cibernéticos em nós-chave do inimigo para liberar meios “cinéticos” para outras operações |
| **Manobra** | Colocar o inimigo em uma posição de desvantagem | Manter o inimigo em uma situação instável | Utilização de numerosos endereços IP para evitar a atribuição de responsabilidade durante um ataque cibernético |
| **Unidade de Comando** | Assegurar a unidade de esforços sob a responsabilidade de um comandante | Tenta garantir a unidade de esforços | Controle do Grid de Informação Global por meio de uma Força Tarefa designada |

| PRINCÍPIO | PROPÓSITO | OBSERVAÇÕES | EXEMPLO DE OPERAÇÃO CIBERNÉTICA |
|---|---|---|---|
| **Segurança** | Manter o acesso sem interrupções | Reduzir a vulnerabilidade amiga a atos hostis, influência e surpresa | Proteger e permitir a operacionalidade de redes de C2 por meio de defesas em camadas e reconfigurações robustas e auto ajustáveis |
| **Surpresa** | Ataque no momento, lugar ou forma para a qual o inimigo não esteja preparado | Pode alterar a vantagem desproporcionalmente ao esforço dispendido | Ataques cibernéticos não anunciados em sistemas vulneráveis ou comprometidos |
| **Simplicidade** | Ordens claras e concisas para assegurar o entendimento | Minimiza a “fricção” da guerra ao máximo possível | Equipar a força em todos os níveis com acesso amigável a dados e estruturas de rede |
| **Restrição** | Limitar dano colateral, prevenir o uso desnecessário da força | Prevenir consequências políticas e sociais danosas | Prover opções independentes e não cinéticas aos comandantes; criar efeitos sem destruir os alvos |
| **Perseverança** | Assegurar o comprometimento necessário para atingir o estado final estratégico desejado | A guerra é raramente concluída por um “único e decisivo golpe” | Provê a endurance necessária para a operação dos sistemas; cria uma capacidade cibernética robusta em nações parceiras |
| **Legitimidade** | Assegurar que as ações são legais, morais e legítimas aos olhos da população alvo e parceiros de coalisão | Construir a confiança e a cooperação necessária para atingir o estado final desejado | Uso de meios cibernéticos não cinéticos para criar os efeitos desejados contra o inimigo sob circunstâncias que são vantajosas sobre ataques cinéticos |

Quadro 4 – Princípios das Operações Conjuntas aplicados às Operações Cibernéticas

Fonte: ESTADOS UNIDOS DA AMÉRICA, 2010b

## 4.6 FUNDAMENTOS DAS OPERAÇÕES CIBERNÉTICAS

Ainda segundo a doutrina da Força Aérea estadunidense as operações cibernéticas possuem fundamentos baseados nas experiências colhidas ao longo da história e podem ser resumidos conforme o quadro a seguir:

| FUNDAMENTO | PROPÓSITO | OBSERVAÇÕES | EXEMPLO DE OPERAÇÃO CIBERNÉTICA |
|---|---|---|---|
| **Controle Centralizado, Execução Descentralizada** | Controle exercido pelo comandante com perspectiva ampla; execução realizada por aqueles que melhor compreendem as complicações de uma operação dinâmica | Permite o Comando e Controle mais efetivo das capacidades e forças | Ações conjuntas entre centros de operações regionais e centros de operações de redes locais |
| **Flexibilidade e Versatilidade** | Explorar simultaneamente massa e manobra; empregar em todos os níveis da guerra | Operações cibernéticas flexíveis e versáteis agem como um multiplicador do poder de combate das forças | A flexibilidade (emprego simultâneo da massa e manobra) é inerente a natureza do ciberespaço. A versatilidade permite que um pequeno fragmento de código possa criar efeitos táticos, operacionais ou estratégicos, dependendo do alvo |
| **Efeitos Sinérgicos** | Integrar o uso de forças para criar efeitos maiores do que as contribuições de elementos individuais | Habilidade de observar livremente o ambiente operacional permitindo velocidade e agilidade sem precedentes | Suportar a integração de conectividade de C2, Inteligência, Reconhecimento e Vigilância robustas, persistentes e tolerantes a falhas |

| FUNDAMENTO | PROPÓSITO | OBSERVAÇÕES | EXEMPLO DE OPERAÇÃO CIBERNÉTICA |
|---|---|---|---|
| **Persistência** | Habilidade de conduzir operações continuadas; visitar e revisitar alvos quando necessário | Semelhante à velocidade e alcance | Ataques distribuídos de negação de serviço (persistir até que sejam deliberada e especificamente contidos) |
| **Concentração** | Concentrar forças com superioridade no momento e local correto | Evitar a diluição de forças | Ataques cibernéticos simultâneos ou defesa de múltiplas redes |
| **Prioridade** | O Comandante deve estabelecer prioridades claras para emprego da força | Necessidades podem exceder às disponibilidade de forças | Priorizar as fontes de Inteligência, Reconhecimento e Vigilância |
| **Balanço** | Necessita balancear oportunidade, necessidade, efetividade e eficiência contra o risco para forças amigas | Operações cibernéticas dão suporte a outras missões dentro das operações militares, fornecendo aos comandantes maior capacidade e opções para balancear os recursos | Redes da força podem ser utilizadas por membros de outras forças singulares, agências governamentais ou não governamentais e membros de coalisões militares (caso necessário) para atingir as necessidades de segurança nacional |

Quadro 5 – Fundamentos das Operações Cibernéticas

Fonte: ESTADOS UNIDOS DA AMÉRICA, 2010b

## 4.7 A TRÍADE DEFENSIVA

CLARKE[88] (2010, cap. 5) propõe que uma estratégia defensiva para conter ou mitigar os riscos trazidos pela cibernética seria baseada em três medidas: defender o *backbone*[89], defender o sistema elétrico de geração e distribuição de energia e proteger as redes do Departamento de Defesa estadunidense.

[88] CLARKE, R. A.; KNAKE R. K.. **Cyber War: The Next Threat to National Security and What to Do About It**. HarperCollins e-books, 2010. ISBN: 978-0061962240.

[89] No contexto de redes, backbone significa a rede de transporte, de elevado desempenho, onde as redes de menor capacidade se conectam.

A defesa do backbone baseia-se no fato de que 90% do tráfego da internet passa pelos links "*Tier 1*"[90]. A forma de realizar isso seria monitorar as entradas e saídas desses backbones, realizando uma inspeção do tráfego pela análise mais aprofundada dos pacotes que compõem o mesmo ("*deep packet inspection*"). Apesar disso ser tecnicamente possível hoje, muitos provedores de serviços internet e companhias de telecomunicações não o fazem pela ausência de garantias legais estabelecidas por regulamentação específica de que, ao realizar essa "inspeção" e bloquear tráfego julgado perigoso, não seriam processadas pelos usuários. Caso essa análise fosse realizada, um ataque de negação de serviço ou a disseminação de um malware poderiam ser contidos muito mais facilmente. Chegará o dia em que esse tipo de atuação poderá se tornar mandatória, regulada por normas aceitas pela comunidade da internet ou, pelo menos, pelo país onde está a infraestrutura que suporta o link de comunicação de dados.

A segunda medida de proteção é defender o sistema elétrico de geração e distribuição de energia. Essa medida é autoexplicativa e, apesar de ser possível utilizar geradores locais para manter funcionando a infraestrutura julgada mais crítica, dificilmente isso poderá ser mantido por longos períodos. Com a interconexão dos sistemas de geração local em um sistema nacional ou, até mesmo a interconexão de sistemas de vários países (como na Europa, por exemplo) sendo controlados por novas tecnologias de monitoração e controle (os chamados "*smart grids*"), que se interconectam por redes de computadores, fechadas ou não, essa vulnerabilidade se torna cada vez mais crítica.

A terceira medida de proteção é a proteção das redes do Departamento de Defesa. CLARKE (2010, cap. 5) sugere que um atacante provavelmente irá tentar reduzir a capacidade militar estadunidense de responder por meios convencionais (ou cineticamente), para evitar retaliações. Para isso, um dos alvos prioritários seriam as redes do Departamento de Defesa estadunidense.

Embora esses últimos pontos citados não sejam constantes de uma doutrina militar citada em um dos manuais das forças armadas, essa tríade defensiva sugere um bom caminho para a montagem de uma estratégia defensiva que proteja as infraestruturas críticas de um país.

---

[90] No sentido abordado, uma rede "Tier 1" é uma rede de transporte de grande capacidade e disponibilidade, que se conecta a outras redes "Tier 1" ou a redes "Tier 2" de grande tamanho. Resumindo, seria parte de uma rede que interconecta redes de grande capacidade.

Após a realização de uma análise dos principais pontos da doutrina cibernética dos EUA, que servem de embasamento para fornecer elementos úteis para a construção de uma doutrina básica de guerra cibernética aplicável à realidade brasileira, veremos elementos presentes em outros países.

# 5 **DOUTRINA DE GUERRA CIBERNÉTICA DE OUTROS PAÍSES**

Passaremos neste capítulo a analisar os esforços de outros países, como a Rússia e a China, na busca de uma regulamentação ou uma doutrina que atenda aos interesses destes, bem como ao desenvolvimento de linguagem comum que facilite a cooperação e o desenvolvimento de táticas, técnicas e procedimentos que se apliquem as atividades situadas no ciberespaço.

Estes países foram selecionados por serem conhecidos pela execução de operações cibernéticas e representarem uma linha de pensamento diversa do pensamento ocidental, presente nos EUA e nos países da Europa signatários da OTAN.

Nos últimos anos, os EUA, Rússia e China desenvolveram os seus próprios conceitos de Guerra da Informação, Operações de Informação e Superioridade da Informação. A visão dos EUA sobre esses conceitos é mais acessível, uma vez que esse país publica a maioria da sua doutrina ostensivamente como publicações conjuntas (JP – *Joint Publications*) ou manuais de campanha (FM – *Field Manuals*).

Nem Rússia, nem China publicam esse tipo de documentos e, em consequência, a análise necessita ser realizada em descrições plausíveis desses conceitos encontradas em trabalhos acadêmicos e militares (visões não oficiais).

Os nomes de alguns termos e instituições foram preservados, tanto quanto possível, no seu idioma original, visando facilitar buscas futuras e preservar o sentido original dos mesmos.

## 5.1 BILATERAL RUSSIA – EUA SOBRE SEGURANÇA CIBERNÉTICA

Durante o ano de 2010, o *EastWest Institute's Worldwide Cybersecurity Initiative* (EUA) e a *Moscow State University's Information Security Initiative* (Rússia), concordaram em desenvolver um esforço conjunto entre especialistas dos Estados Unidos da América e da Rússia, buscando definições de consenso na terminologia de segurança cibernética, esperando que isso seja um primeiro passo para o desenvolvimento de um vocabulário internacional comum. Este trabalho resultou, em abril de 2011, na publicação de um documento denominado "Critical Terminology Foundations"[91] que foi apresentado a quarenta países, dentre eles o Brasil, na

[91] EASTWEST INSTITUTE'S WORLDWIDE CYBERSECURITY INITIATIVE. MOSCOW STATE UNIVERSITY'S INFORMATION SECURITY INITIATIVE. **Russia – U.S. Bilateral on Cybersecurity : Critical Terminology Foundations**. Issue 1. New York, 2011. Disponível em <http://www.ewi.info/russia-us-bilateral-cybersecurity-critical-terminology-foundations>. Acesso em: 30 abr. 2011

Segunda Cúpula Mundial de Segurança Cibernética[92], que ocorreu nos dias 1 e 2 de Junho de 2011 em Londres. Este documento traz vinte definições de termos chave, divididos em três partes: O Teatro (The Theatre), Os Modos de Agravamento (The Modes of Aggravation) e A Arte (The Art), conforme o quadro a seguir:

| **Áreas** | **Termos** |
|---|---|
| O Teatro | • Ciberespaço<br>• Infraestrutura Cibernética<br>• Serviços Cibernéticos<br>• Ciberespaço Crítico<br>• Infraestrutura Crítica Cibernética<br>• Serviços Críticos Cibernéticos |
| Os Modos de Agravamento | • Crime Cibernético<br>• Terrorismo Cibernético<br>• Conflito Cibernético<br>• Guerra Cibernética<br>• Segurança Cibernética |
| A Arte | • Guerra Cibernética<br>• Ataque Cibernético<br>• Contra-ataque Cibernético<br>• Contramedida Defensiva Cibernética<br>• Defesa Cibernética<br>• Capacidade Cibernética Defensiva<br>• Capacidade Cibernética Ofensiva<br>• Exploração Cibernética<br>• Dissuasão Cibernética |

Quadro 6 – Termos de definições consensuais
Fonte: EASTWEST (2011, p. 18)

A seguir, apresentaremos cada termo adotado.

[92] *Second Worldwide Cybersecurity Summit* - http://www.cybersummit2011.com/

### 5.1.1 **O Teatro**

#### 5.1.1.1 Ciberespaço

É um meio eletrônico através do qual informação é criada, transmitida, recebida, armazenada, processada e apagada.[93]

#### 5.1.1.2 Infraestrutura Cibernética

É o conjunto de pessoas, processos e sistemas que constituem o espaço cibernético.[94]

#### 5.1.1.3 Serviços Cibernéticos

São uma gama de troca de dados no espaço cibernético para o benefício direto ou indireto de humanos. [95]

#### 5.1.1.4 Ciberespaço Crítico

É a infraestrutura cibernética e os serviços cibernéticos que são vitais para a preservação da segurança pública, estabilidade econômica e segurança nacional e estabilidade internacional.[96]

#### 5.1.1.5 Infraestrutura Crítica Cibernética

É a infraestrutura cibernética que é essencial aos serviços vitais para a segurança pública, estabilidade econômica, estabilidade internacional e para a sustentabilidade e restauração do ciberespaço crítico.[97]

#### 5.1.1.6 Serviços Críticos Cibernéticos

São os serviços cibernéticos que são vitais para a preservação da segurança pública, estabilidade econômica, segurança nacional e estabilidade internacional. [98]

---

[93] "Cyberspace is an electronic medium through which information is created, transmitted, received, stored, processed and deleted."

[94] "Cyber Infrastructure is the aggregation of people, processes and systems that constitute cyberspace."

[95] "Cyber Services are a range of data exchanges in cyberspace for the direct or indirect benefit of humans."

[96] "Critical Cyberspace is cyber intrastructure and cyber services that are vital to preservation of public safety, economic stability, national security and international stability."

[97] "Critical Cyber Infrastructure is the cyber infrastructure that is essential to vital services for public safety, economic stability, national security, international, stability and to the sustainability and restoration of critical cyberspace."

### 5.1.2 **Os Modos de Agravamento**

#### 5.1.2.1 Crime Cibernético

É o uso do espaço cibernético para propósitos criminais definidos por leis nacionais ou internacionais.[99]

#### 5.1.2.2 Terrorismo Cibernético

É o uso do espaço cibernético para propósitos terroristas definidos por leis nacionais ou internationais.[100]

#### 5.1.2.3 Conflito Cibernético

É a situação tensa entre Estados-Nações ou grupos organizados onde ataques cibernéticos indesejáveis resultam em retaliação.[101]

#### 5.1.2.4 Guerra Cibernética

É um estado de conflito cibernético escalado entre Estados no qual ataques cibernéticos são conduzidos por atores estatais contra a infraestrutura cibernética como parte de uma campanha militar que pode ser:

a) Declarada: quando é formalmente declarada por uma autoridade de uma das partes;
b) De Fato: com a ausência de uma declaração.[102]

#### 5.1.2.5 Segurança Cibernética

É a propriedade do espaço cibernético que denota a habilidade de resistir a ameaças intencionais e não intencionais, responder e se recuperar.[103]

---

[98] "Critical Cyber Services are cyber services that are vital to preservation of public safety, economic stability, national security and international stability."
[99] "Cyber Crime is the use of cyberspace for criminal purposes as defined by national or international law".
[100] "Cyber Terrorism is the use of cyberspace for terrorista purposes as defined by national or international law"
[101] "Cyber Conflict is tense situation between or among nation-states or organized groups where unwelcome cyber attacks result in retaliation."
[102] "Cyber War is an escalated state of cyber conflict between or among states in which cyber attacks are carried out by state actors against cyber infrastructure as parto f military campaign (i) Declared: that is formally declared by na authority o fone of the parties; (ii) De Facto: with the absence of a declaration."

### 5.1.3 **A Arte**

#### 5.1.3.1 Combate Cibernético

São os ataques cibernéticos que são autorizados por atores estatais contra infraestrutura cibernética em conjunto com uma campanha governamental.[104]

#### 5.1.3.2 Ataque Cibernético

É o uso ofensivo de uma arma cibernética com a intenção de causar danos a um alvo designado.[105]

#### 5.1.3.3 Contra Ataque Cibernético

É o uso de uma arma cibernética com a intenção de causar danos a um alvo designado em resposta a um ataque.[106]

#### 5.1.3.4 Contramedida Cibernética Defensiva

É o desdobramento de uma capacidade defensiva cibernética específica para desviar ou redirecionar um ataque cibernético.[107]

#### 5.1.3.5 Defesa Cibernética

São capacidades organizadas para se proteger, mitigar e rapidamente se recuperar dos efeitos de um ataque cibernético.[108]

#### 5.1.3.6 Capacidade Cibernética Defensiva

É a capacidade de efetivamente proteger e repelir uma exploração cibernética ou ataque cibernético que pode ser utilizada como um dissuasor cibernético.[109]

---

[103] "Cybersecurity is a property of cyber space that is an ability to resist intentional and unintentional threats and respond and recover".
[104] "Cyber Warfare is cyber attacks that are authorized by state actors against cyber infrastructure in conjunction with a government campaign."
[105] "Cyber Attack is an offensive use of a cyber weapon intended to harm a designated target."
[106] "Cyber Counter-Attack is the use of a cyber weapon intended to harm a designated target in response to an attack."
[107] "Cyber Defensive Countermeasure is the deployment of a specific cyber defensive capability to deflect or to redirect a cyber attack."
[108] "Cyber Defense is organized capabilities to protect against, mitigate from, and rapidly recover from the effects of cyber attack".

5.1.3.7 Capacidade Cibernética Ofensiva

É a capacidade de iniciar um ataque cibernético que possa ser utilizada como um dissuasor cibernético.[110]

5.1.3.8 Exploração Cibernética

É aproveitar a vantagem de uma oportunidade no espaço cibernético para atingir um objetivo.[111]

5.1.3.9 Dissuasão Cibernética

É um mecanismo declarado que se presume eficaz em desencorajar um conflito cibernético ou uma atividade ameaçadora no espaço cibernético. [112]

## 5.2 GUERRA DA INFORMAÇÃO RUSSA

Apesar de a Rússia estar se ocidentalizando nos últimos anos, diferenças culturais acentuadas e uma forma de governar diferente da ocidental influenciam decisivamente na forma de como o Estado visualiza a Guerra da Informação, dentro da qual a Segurança da Informação está inserida.

Como outros países, a Rússia está desenvolvendo capacidades em Guerra da Informação e Operações de Informação. Dentro da administração russa, diversas organizações são responsáveis por lidar com operações de redes de computadores, guerra eletrônica, operações psicológicas, campanhas de dissimulação e impacto de programação matemática. Este último pode ser interpretado como a atividade que inclui a introdução de *malware* e funcionalidades como "*backdoors*"[113] e "bombas lógicas".

---

[109] "Cyber Defensive Capability is a capability to effectively protect and repel against a cyber exploitation or cyber attack, that may be used as a cyber deterrent".
[110] "Cyber Offensive Capability is a capability to initiate a cyber attack that may be used as a cyber deterrent."
[111] "Cyber Exploitation is taking advantage of na opportunity in cyber space to achieve an objective".
[112] "Cyber Deterrent is a declared mechanism that is presumed effective in discouraging cyber conflict or a threatening activity in cyberspace".
[113] Literalmente "porta dos fundos". Uma backdoor permite acesso não autorizado a um sistema, utilizando uma maneira de entrar não disponível ou não prevista para o usuário legítimo.

Segundo HEICKERÖ[114] (2010, p. 4), do ponto de vista russo, a informação em si já é um ativo valioso, que deve ser protegido em tempo de paz e guerra. Na doutrina de segurança da informação de 2000, a proteção da informação tem valor estratégico, sendo vista como um fator chave não somente para a estabilidade do Estado como também para o regime e para atores que exercem liderança e influência. Na doutrina militar publicada na primavera de 2010, a Rússia destaca a importância da Guerra da Informação nas fases iniciais de um conflito, para enfraquecer a capacidade de comando e controle do oponente na forma de uma campanha de informação durante a batalha, visando criar uma visão favorável na comunidade internacional para a Rússia.

Segundo THOMAS[115] (2004, p. 2), a Rússia, na sua doutrina, divide Operações de Informação em dois aspectos: técnico-informacional e psicológico-informacional. Esses aspectos não têm correlação direta com as capacidades de atuação e atividades de suporte descritas na doutrina dos EUA. Os teóricos russos colocam muito mais ênfase em "desorganizar" o inimigo do que na obtenção da superioridade da informação. Na realidade, eles acreditam que o primeiro aspecto acaba por levar ao segundo, o que de certo modo faz sentido.

Segundo CARR (2011, p.161), a Rússia tem sido um dos países mais ativos na implementação de ataques cibernéticos contra os seus adversários, que incluem, dentre outros, a Chechênia, Estônia, Lituânia e Geórgia. Apesar de não ser possível provar que algum desses ataques ocorreu com a ordem ou anuência do Kremlin, cada um deles proporcionou o avanço de políticas russas e o Kremlin nada fez para deter esses ataques, se beneficiando da situação.

A Rússia também foi publicamente acusada ao longo dos anos de não agir com a força necessária contra atividades maliciosas originadas no espaço cibernético do país. As acusações envolvem uma grande quantidade de comportamentos, tais como a criminalidade na Internet, espionagem cibernética e o "hacktivismo"[116] politicamente orientado. Os mais críticos apontam que as autoridades legais russas têm sido relutantes em lidar com esses criminosos. Dois casos em particular

[114] HEICKERÖ, Roland. **Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations**. FOI Swedish Defence Research Agency, Stockholm, mar. 2010. Disponível em: <http://www2.foi.se/rapp/foir2970.pdf> Acesso em 15 jun 2012.
[115] THOMAS, Timothy L. **Comparing Us, Russian, and Chinese Information Operations Concepts**. Disponível em: <http://www.dodccrp.org/events/2004_CCRTS/CD/papers/064.pdf> Acesso em 20 abr. 2012.
[116] Hacktivismo (uma junção dos termos hacker e ativismo) é a utilização de computadores e redes de computadores como meio de protesto normalmente utilizado para promover fins políticos**.**

suscitaram discussões nos últimos anos a respeito de operações cibernéticas que provavelmente foram executadas da Rússia: os ataques cibernéticos contra a Estônia (2007) e contra a Geórgia (2008). A operação direcionada contra a Estônia foi um dos primeiros ataques cibernéticos publicamente conhecidos contra um país, utilizando *botnets* e ataques distribuídos de negação de serviço em larga escala por "civis nacionalistas". Na invasão da Geórgia houve, inclusive, um refinamento nas técnicas utilizadas, que apoiaram, sincronizadas com a manobra, a utilização de meios militares para a realização de uma operação militar convencional[117]. Inclusive, nos ataques distribuídos de negação de serviço, foram utilizadas *botnets* pertencentes a um conhecido grupo de criminosos e fraudadores cibernéticos russos conhecidos como *Russian Business Network*[118]. Este grupo atuava como um provedor de serviços internet entre 2006 e 2007, mas alugava servidores que podiam ser utilizados em crimes cibernéticos desde 2002.

Em ambos os casos não há evidências conclusivas do envolvimento do governo russo. Se isso ocorreu, como parece provável, uma vez que o mesmo foi o principal beneficiado das ações, os rastros foram astuta e minunciosamente cobertos. Os dois incidentes mostram que um grupo relativamente pequeno, qualificado e dedicado de pessoas, fazendo uso de redes sociais como ferramentas para recrutar e prover *malware* para ser utilizado por hackers, podem alcançar um impacto significativo. Esses casos estabeleceram um novo padrão, onde futuros conflitos cibernéticos poderão ser conduzidos à distância, permitindo aos atores negar a participação nos mesmos ao mesmo tempo em que obtêm benefícios estratégicos ao atingir objetivos políticos.

Só recentemente a Rússia divulgou a sua estratégia de Guerra da Informação. O documento intitulado "Visões conceituais sobre as ações das Forças Armadas da Federação da Rússia no espaço de informação"[119] foi elaborado em 2011 e

---

[117] SHAKARIAN, Paulo. **Análise da Campanha Cibernética da Rússia Contra a Geórgia, em 2008**. MILITARY REVIEW Edição Brasileira Novembro-Dezembro 2011. Disponível em: <http://usacac.army.mil/CAC2/MilitaryReview/Archives/Portuguese/MilitaryReview_20111231_art011POR.pdf>. Acesso em: 27 mai. 2012.

[118] McQUAID, James. **The RBN Operatives Who Attacked Georgia.** 18 ago. 2008. Disponível em: <http://securehomenetwork.blogspot.com.br/2008/08/rbn-operatives-who-attacked-georgia.html> Acesso em 4 jun. 2012.

[119] RUSSIA. Ministério da Defesa. Moscow, 2011. **Visões conceituais sobre as ações das Forças Armadas da Federação da Rússia no espaço de informação**. Disponível em: < http://www.ens.mil.ru/science/publications/more.htm?id=10845074 @cmsArticle>. Acesso em 15 abr. 2012.

divulgado no site do Ministério da Defesa no início de 2012, não tendo ocorrido, até agora, discussões públicas.

O conceito em si ocupa a menor parte do documento e não menciona se a Rússia realizará ações ofensivas no ciberespaço, resumindo-se a três principais aspectos: dissuadir, prevenir e resolver conflitos de guerra no espaço virtual.

Ao mesmo tempo, entretanto, os ideólogos russos da guerra cibernética não excluem a possibilidade de reagir a uma ameaça no espaço virtual com métodos adotados em guerras reais.

Essa tese transparece no item 3.2.3 do documento, segundo o qual “face à escalada de um conflito no espaço de informação e sua passagem para a fase de crise, é preciso defender-se individual ou coletivamente, mediante o emprego de todos os meios e métodos escolhidos, desde que estes não sejam contrários aos princípios do direito internacional universalmente aceitos”.

Outro conceito, que pode ser visto como favorável às ações ofensivas, refere-se ao estacionamento das forças de segurança de informação no território de outros países, com o consentimento voluntário da parte anfitriã ou “em conformidade com o direito internacional”.

De acordo com Aleklsêi Lukátski, especialista russo em Guerra Cibernética que aceitou comentar o documento para o site *CNews.ru*, o conceito postado no site do Ministério da Defesa é o primeiro documento nacional dedicado às atividades de guerra da Rússia no espaço virtual.

Lukátski declarou-se surpreso ao saber que um conceito de guerra cibernética foi elaborado pelo Ministério da Defesa, que, até recentemente, dificilmente podia ser relacionado ao interesse por uma guerra cibernética. Para Lukátski, seria mais lógico esperar um documento como este do Serviço Federal de Segurança (FSB, na sigla em russo) ou do Conselho de Segurança, junto à Presidência do país.

Este documento é, no entender do perito, bastante vago. Este julga que deve haver outros documentos que contenham um conjunto de medidas práticas para a implementação do conceito, além de seus princípios gerais.

### 5.2.1 **Termos básicos e definições utilizados pela Rússia**

As definições e termos mais atualizados da doutrina russa são trazidos pelo documento “Visões conceituais sobre as ações das Forças Armadas da Federação

da Rússia no espaço de informação", já citado anteriormente, que passaremos a abordar em seguida.

5.2.1.1 Atividades das Forças Armadas no espaço da informação

É a utilização de recursos militares de informação para fazer face aos desafios de defesa e segurança.

5.2.1.2 Conflito militar no espaço da informação

É a forma de resolução de conflitos entre Estados ou dentro do próprio Estado, com a utilização de armas da informação.

5.2.1.3 Forças de Segurança da Informação

São as forças de segurança dos recursos de informação de um Estado que asseguram o mesmo dos efeitos da guerra da informação.

5.2.1.4 Guerra da Informação

É o confronto entre dois ou mais Estados no espaço da informação, com o objetivo de danificar sistemas de informação, processos, recursos e outras estruturas críticas que minem os sistemas políticos, econômicos e sociais, um tratamento psicológico massivo da população para desestabilizar o Estado e a sociedade, assim como coagir o Estado a tomar decisões do interesse do lado opositor.

5.2.1.5 Infraestrutura da Informação

É o conjunto de ferramentas técnicas e sistemas para a formação, criação, transformação, transmissão, uso e armazenamento da informação.

5.2.1.6 Armas da Informação

Tecnologia da informação, ferramentas e métodos utilizados para conduzir guerra da informação.

5.2.1.7 Espaço da Informação

Esfera de atividade associada com a formação, criação, transformação, transmissão, utilização e armazenamento em mídia que exerça impacto, inclusive

nos indivíduos e na consciência social, na infraestrutura da informação e na informação em si.

5.2.1.8 Recursos de Informação

Corresponde à infraestrutura da informação, assim como a própria informação e o seu fluxo.

5.2.1.9 Crise

É o estágio de escalação do conflito, caracterizado pelo emprego da força militar para resolvê-lo.

5.2.1.10 Segurança da Informação Internacional

É o estado das relações internacionais, excluindo a violação da estabilidade global e o risco à segurança dos Estados e comunidade mundial no espaço da informação.

5.2.1.11 Sistema de Segurança da Informação da Federação Russa

Parte do sistema nacional de segurança do país, destinado à implementação da política do Estado na esfera da segurança da informação.

## 5.3 A GUERRA DA INFORMAÇÃO CHINESA

Da mesma forma que a Rússia, a China mantém como classificada a sua doutrina de Operações de Informação e de Guerra Cibernética. Além disso, as grandes diferenças culturais, a influência do Partido Comunista nas Forças Armadas[120] e a barreira imposta pelo idioma fazem com que a análise doutrinária necessite ser realizada com base em descrições plausíveis desses conceitos baseadas na leitura de trabalhos acadêmicos e militares (visões não oficiais), além de inferências das notícias de fonte aberta, que também podem ser parte de uma campanha de contrapropaganda.

A China procura tirar proveito do fato de que, na área de Tecnologia da Informação, nenhuma nação pode se declarar dominante, o que não ocorre quando

[120] Na realidade, as Forças Armadas Chinesas são do partido único e não do Estado Chinês. O regime de governo adotado (ou imposto) mistura propositalmente as funções de manutenção do Partido com a sobrevivência do Estado.

se trata de capacidade industrial ou equipamentos bélicos. Como resultado, a tecnologia da informação e a sua contraparte militar, a guerra da informação, são consideradas muito importantes para a China, que tem enormes recursos em sua numerosa quantidade de graduados de alta qualidade em matemática, engenharia e ciências (CARR, 2001, p. 171).

A China visualiza os conflitos do futuro da mesma forma que os EUA, ou seja, conflitos limitados ao invés de uma guerra total. Para isto, o que mais deve ser enfatizado é o emprego combinado de medidas nos campos militar, político, econômico e diplomático. O objetivo não é esmagar o oponente, mas tornar o custo da guerra inaceitável.

Segundo THOMAS[121] (2004, p. 6), a China desenvolveu seis “formas” para a sua doutrina de Operações de Informação: segurança operacional, dissimulação militar, guerra psicológica, guerra eletrônica, guerra de redes de computadores e destruição física.

A doutrina chinesa considera que o “controle” (da atividade de comando e controle) é tão importante quanto a superioridade de informação. Da mesma forma que os russos, os chineses consideram que o primeiro leva ao segundo. O foco chinês para a obtenção da superioridade / controle é construído por meio de estratagemas, enquanto que os EUA focam em velocidade e eficiência. Para o nosso estudo, é interessante observar esse contraponto.

A visão chinesa sobre operações centradas em redes é ligeiramente diferente da visão dos EUA, compondo unidades “mistas” de Guerra Eletrônica e Guerra Cibernética e chamando a sua teoria de Guerra Eletrônica e de Redes Integrada (INEW – integrated network-electronic warfare).

Tal como acontece com todas as suas teorias militares e perspectivas estratégicas, a sabedoria tradicional chinesa e o pensamento estratégico é aplicado a todos os novos conceitos e preceitos emanados dos EUA, Rússia ou de outro país. A primeira onda de escritos chineses sobre Guerra da Informação apareceu em meados dos anos 1990, após o sucesso de tecnologias de informação dos EUA na primeira Guerra do Golfo de 1991. O general *Wang Pufeng*, do Exército de Libertação do Povo, escrevendo sobre os desafios e importância da Guerra da

[121] THOMAS, Timothy L. **Comparing US, Russian, and Chinese Information Operations Concepts**. Disponível em: <http://www.dodccrp.org/events/2004_CCRTS/CD/papers/064.pdf> Acesso em 20 abr. 2012.

Informação[122], observou que, no futuro próximo, a guerra de informação iria controlar a forma e o futuro da guerra. Reconheceu essa tendência de desenvolvimento da Guerra da Informação e viu-a como uma força motriz para os militares chineses e a sua prontidão para o combate. Esta tendência foi assumida como altamente crítica para se conseguir a vitória nas guerras futuras.

Segundo ANAND (2006), analistas militares chineses[123], por causa da crescente importância da tecnologia da informação na vida das pessoas, os indivíduos que participam da Guerra da Informação não são necessariamente soldados e qualquer pessoa que entenda de computadores pode tornar-se um guerreiro. A Guerra da Informação é barata, uma vez que o alvo pode receber um golpe paralisante através da rede. ficando difícil para o mesmo discernir de onde o ataque se originou. Grande quantidade de informações inúteis pode ser plantada para bloquear ou impedir o funcionamento do sistema de informação do adversário. Assim, uma “Guerra do Povo” no contexto da Guerra de Informação pode ser realizada por centenas de milhões de pessoas, usando modernos sistemas abertos de informação. Mesmo a mobilização política para a guerra pode ser alcançada através da internet, enviando-se mensagens de correio eletrônico de caráter patriótico e através da criação de bases de dados para influenciar a educação.

Esta concepção encontra apoio adicional de outro autor chinês, *Wang Xiaodong*[124], que observa que "mesmo com as tropas do governo mobilizadas, o número de guerreiros tradicionais será drasticamente inferior aos de técnicos ... uma vez que milhares de computadores pessoais podem ser conectados para executar uma operação comum, ou ainda, conectados para executar muitas tarefas no lugar de um computador militar de grande porte. Uma vitória na Guerra da Informação muito provavelmente será determinada por qual país poderá mobilizar mais peritos de computador e mais simpatizantes de tempo parcial... Isso seria realmente uma Guerra do Povo."

---

[122] PUFENG, Wang. **Challenge of Information Warfare. Chinese Views of Future Warfare**. Institute for National Strategic Studies, National Defense University. Washington D.C., 1997. National Defense University Press. Disponível em <http://www.au.af.mil/au/awc/awcgate/ndu/chinview/chinacont.html> Acesso em 5 jun. 2012.

[123] ANAND, Vinod. **Chinese Concepts and Capabilities of Information Warfare**. Institute for Defence Studies and Analyses, Strategic Analysis. Nova Delhi, India. Vol. 30, No. 4, Oct-Dec 2006. Disponível em: < http://www.idsa.in/strategicanalysis/ChineseConceptsandCapabilitiesofInformationWarfare_vanand_1006>. Acesso em: 4 jul. 2012.

[124] THOMAS, Timothy L. **Like Adding Wings to the Tiger: Chinese Information War Theory and Practice**. Foreign Military Studies Office Fort Leavenworth, KS. Disponível em: < http://fmso.leavenworth.army.mil/documents/chinaiw.htm> Acesso em 20 abr. 2012.

Preparar-se para a Guerra do Povo é um tema recorrente na escrita chinesa, tal como a Guerra da Informação será realizada pelo Exército e pela sociedade como um todo. Este conceito tem encontrado expressão prática na transformação de parte das forças reservistas, de 1,5 milhão de soldados, em pequenos Regimentos de Guerra da Informação. O Departamento das Forças Armadas do Povo – DFAP - (análogo a um Ministério da Defesa) tem organizado uma milícia e regimentos de reserva de Guerra da Informação em níveis distritais em muitas províncias. Por exemplo, em *Echeng*, distrito da província de *Hubei*, há um batalhão de Guerra de Redes, bem como batalhões de Guerra Eletrônica, Inteligência e de Guerra Psicológica, assim como uma base de treinamento para atividades de Guerra da Informação. O DFAP também realiza exercícios de simulação de Guerra de Redes. Uma versão deste conceito foi posta em prática na sequência do bombardeamento da embaixada chinesa em Belgrado, em 08 de maio de 1999, durante a “Operação *Allied Force*”. Os chineses invadiram uma série de sites políticos, militares e diplomáticos dos EUA e também realizaram uma batalha de rede através da mobilização de milhares de usuários da rede para enviar e-mails e vírus. Isso fez com que os servidores ficassem sobrecarregados, paralisando um grande número de sites dos EUA.

Desta forma, o governo Chinês visualiza a guerra da informação como uma verdadeira “Guerra do Povo”, significando que provavelmente irá estimular e recorrer a um recrutamento massivo de expertise técnica a partir da população civil.

### 5.3.1 **Definição e Objetivos da Guerra da Informação**

O entendimento chinês de Guerra da Informação, que inicialmente foi baseado em conceitos ocidentais, tem cada vez mais evoluído para adequar-se à sua própria orientação. Especialistas chineses acreditam que a essência da Guerra da Informação é a soma das capacidades de informação capazes de quebrar a vontade de resistir, atacando a compreensão cognitiva de um inimigo e suas convicções, forçando-o a desistir de toda a resistência e terminar a guerra. O objetivo é "forçar o inimigo a considerar seu objetivo como o nosso objetivo, para forçar o oponente a desistir da vontade de resistir, acabar com o confronto e parar de lutar, atacando as percepções e crenças do inimigo através da energia da informação".

As ferramentas específicas da Guerra da Informação, tanto ofensiva quanto defensiva incluem: a destruição física, a dominância do espectro eletromagnético, a guerra de redes de computadores e a manipulação psicológica.

### 5.3.2 **Ideias Força**

A China adota as seguintes regras gerais, que descreve como sendo “ideias força:

- Nada é exatamente como parece;
- O ideograma representativo da China literalmente significa o “Reino do Meio” ou o “Império do Centro”;
- O Exército Popular de Libertação controla tudo;
- Funcionamento com base no regime econômico capitalista, mas mantendo o comunismo como cerne do regime político;
- Observação do princípio de Sun Tzu: “mantenha os seus amigos próximos de ti, mas os inimigos mais próximos ainda”;
- O mandarim é uma língua fácil e deve ser empregada;
- A capacidade cinética da China ainda não está plenamente desenvolvida.

Algumas dessas “ideias força” guardam acentuada semelhança com os “36 Estratagemas”[125], uma coletânea de provérbios marciais chineses que provavelmente foram escritos na dinastia *Qi* (479-502 d.C.). Estes estratagemas, diferentemente da obra Arte da Guerra, de *Sun Tzu*, têm o seu foco mais voltado para a trapaça e dissimulação, um domínio mais adequado a espiões.

Diferentemente da Rússia, a China, até o presente momento, não se engajou em ações militares onde o componente cibernético fosse perceptível. A sua opção tem sido pela prática de atividades de espionagem cibernética.

### 5.3.3 **Guerra Cibernética na China**

As preocupações com as forças de redes da China cresceram após ataques sobre os sistemas de computador dos EUA e depois que a milícia chinesa realizou exercícios de Guerra da Informação que incluíram a Índia, EUA, Taiwan e Japão como países alvos. O objetivo desse treinamento foi degradar (e provavelmente explorar) a infraestrutura crítica desses países, tais como o sistema bancário, o

[125] http://wengu.tartarie.com/wg/wengu.php?l=36ji

fornecimento de energia e redes de telecomunicações, como parte da estratégia da China de abordagem assimétrica para a guerra. No domínio cibernético, os chineses adotaram três métodos para atacar tais redes: o primeiro foi o uso de correio eletrônico para a infiltração de vírus; em seguida, *phishing*[126] e, finalmente, a introdução de "*trojans* inteligentes" e "*trojans* capturadores de dados". Diversas maneiras para plantar *trojans* e vírus foram usadas para atacar computadores pessoais considerados críticos, que, por sua vez, enviaram arquivos ou causaram danos. As ferramentas dos *hackers* estão se tornando cada vez mais automatizadas e simples: por exemplo, um *trojan* capturador de dados irá extrair informações a partir de um *pen drive* automaticamente quando este for conectado a uma porta USB.

Em *Nanjing*, o Exército de Libertação do Povo já desenvolveu centenas de *trojans* e ferramentas similares. Além disso, a Academia Chinesa de Ciências, que fornece sugestões sobre a Política Nacional de Segurança da Informação e do Direito, criou o Laboratório de Estado da Segurança da Informação. O laboratório conduz o "Projeto Nacional de Ataque" como um dos seus programas de pesquisa. Além disso, profissionais selecionados foram infiltrados nas organizações milicianas para aumentar a capacidade de combate em guerras futuras. Desta forma, a China tem prestado muita atenção às estratégias ofensivas no ciberespaço ao mesmo tempo em que se concentra em Guerra da Informação defensiva.

### 5.3.4 **Princípios da Guerra Cibernética do Exército da China**

Os seguintes princípios foram citados na Guerra Cibernética do Exército da China:

- Atuação em todas as direções;
- Sincronismo;
- Objetivos limitados;
- Medidas ilimitadas;
- Assimetria;
- Utilização mínima de meios;
- Coordenação multidimensional; e
- Ajuste e controle de todo o processo.

[126] Palavra derivada de "password fishing" ou, literalmente, "pesca de senhas".

No capítulo a seguir, serão abordados as discussões e os elementos para formulação doutrinária que correspondem à contribuição do autor para o levantamento de elementos que possam contribuir para a composição do banco de informações doutrinárias necessário à formulação de uma Doutrina Básica de Guerra Cibernética para o Exército Brasileiro.

# 6 **RESULTADOS DA APLICAÇÃO DO MÉTODO**

Passaremos nesse capítulo a apresentar os resultados da aplicação do método e discorrer sobre as observações que foram realizadas fruto do estudo realizado.

Este capítulo representa o fio que une os diversos capítulos deste trabalho, resumindo as observações que foram sendo paulatinamente abordadas nos capítulos anteriores e que influenciaram a produção do capítulo 7, que traz elementos para formulação doutrinária de Guerra Cibernética para o EB.

## 6.1 CONSTRUÇÃO DOUTRINÁRIA

A primeira pergunta que necessitou ser respondida para que essa pesquisa pudesse prosseguir é: como é realizada a construção da doutrina dentro do Exército Brasileiro?

A melhor resposta que esse pesquisador obteve não foi propriamente algo que estava somente escrito em manuais, mas advinda da experiência do mais antigo formulador doutrinário da 3ª SCh do Estado-Maior do Exército, a quem cabe formular, gerenciar e manter a doutrina no Exército Brasileiro.

As necessidades doutrinárias, expressas em quadro de situação da doutrina, são definidas em função do Sistema de Planejamento do Exército (SIPLEx) e do banco de dados doutrinários. Este banco é **construído com o tempo** e engloba os manuais em vigor, cadernos de instrução, relatórios diversos, conclusões de seminários, pesquisas doutrinárias, experimentações doutrinárias, reuniões de coordenação doutrinária, informações obtidas fruto de viagens ao exterior, de cursos no exterior, contribuições pessoais, e outras contribuições[127]. Essa resposta orientou grande parte do esforço de busca e organização da pesquisa.

As Instruções Gerais para Organização e Funcionamento do Sistema de Doutrina Militar Terrestre (SIDOMT), IG 20-13, fixam as normas gerais orientadoras e descrevem as principais atividades e eventos relativos ao SIDOMT.

As contribuições desse trabalho se encaixam na 3ª fase do sistema, na subfase “a. Formulação Propriamente Dita” (BRASIL, 1999. p. 5). Segundo esta mesma IG, a atividade desenvolvida, de pesquisa doutrinária, para este trabalho, tem como produto final um manual de campanha (BRASIL, 1999, p. 3). Mesmo que não seja objetivo desta pesquisa produzir um manual de campanha, algo que não é

[127] Comunicação pessoal do autor com o Coronel Luiz Carlos Almeida Santos, na 3ª SCh / EME em 12 de março de 2012.

costumeiramente realizado por uma só pessoa no EB, o capítulo 7 Discussões e Elementos para Formulação Doutrinária, já foi intencionalmente escrito com um formato próximo a um manual de campanha para facilitar trabalhos futuros.

A proposta apresentada é de elementos doutrinários básicos, genéricos e de alto nível, baseados em princípios, possibilidades e limitações. Também foram apresentadas sugestões de organização e modelos de documentos de planejamento (Apêndices “A” a “D”). Esta proposta está coerente com os princípios ressaltados por BRILL, durante a entrevista realizada.

## 6.2 CENÁRIO ATUAL

A utilização do conceito de Operações de Informação está alterando os paradigmas e a concepção de emprego nos conflitos mais recentes. O emprego da Guerra Cibernética está diretamente relacionado a essa nova realidade, ou seja, está inserido dentro do contexto das Operações de Informação.

Os paradigmas apresentados, da “Era Industrial” e da “Era do Conhecimento”, não são mutuamente excludentes. A grande maioria dos países têm problemas sérios de fronteira ou de instabilidade regional que requerem meios de força, da “Era Industrial”, em quantidade, qualidade e nível de aprestamento adequado para representarem, no mínimo, um poder dissuasório julgado adequado para aquele quadro geopolítico, que é mutável e instável. As diferenças foram ressaltadas para que fossem levadas em consideração as peculiaridades do paradigma mais recente.

Do estudo realizado, pode-se perceber que nessa área há uma sutil diferença do emprego entre a Guerra Cibernética e a Guerra Eletrônica. O emprego da G Ciber dentro do contexto das Operações de Informação, com a interação sinérgica entre inteligência, operações psicológicas, comunicação social e a própria guerra eletrônica enseja um emprego geral mais amplo. Tanto a coleta realizada em fontes abertas quanto a busca por dados negados é realizada sem as restrições de terreno impostas à guerra eletrônica pela propagação eletromagnética. Da mesma forma, um ataque eletrônico e um ataque cibernético diferem na amplitude que possam tomar. Tecnicamente falando, nada impede que artefatos maliciosos genéricos, escritos para degradar ou interferir em sistemas digitais de segurança de instalações industriais venham a se tornar verdadeiras “armas de destruição em massa” da era

digital[128]. A popularização das redes sociais na internet e a sua influência nos meios de comunicação de massa também representa uma nova faceta de atuação das Operações de Informação, onde a Guerra Cibernética desenvolve um papel relevante.

## 6.3 ÓRGÃOS E ATORES DE SEGURANÇA E DEFESA CIBERNÉTICA NO BRASIL

O setor cibernético nacional envolve a atuação integrada de muitos órgãos, cada um com atribuições específicas, normalmente definidas por legislação (leis, decretos e portarias ministeriais).

É necessário o conhecimento dessas atribuições, uma vez que o modelo de atuação cibernética mais provável para os próximos anos, onde a segurança aos grandes eventos no Brasil terá o componente cibernético, é o de operações interagências.

A primeira operação desse tipo em que houve a participação de um componente de defesa cibernética foi a Conferência das Nações Unidas sobre Desenvolvimento Sustentável (Rio + 20). Nesse grande evento, o destacamento de defesa cibernética, chefiado pelo CDCiber, integrava elementos não só das três Forças Armadas mas também da Polícia Federal, além de coordenar e integrar os esforços de uma plêiade de elementos civis, como o CERT.br, CTIR Gov, Agência Nacional de Telecomunicações, Serviço de Processamento de Dados Federal além de operadoras de telecomunicações e diversas empresas civis nacionais que prestavam serviços de assessoria técnica e operação assistida[129].

Outra situação onde provavelmente haverá o emprego do componente cibernético será em operações interagências de repressão a ilícitos transfronteiriços, representados, em 2011 e 2012, pelas operações Ágata.

A participação do CDCiber em Operações Conjuntas do Ministério da Defesa, tais como Amazônia 2012 e Atlântico III, apesar de terem foco no adestramento dos estados-maiores, representaram um grande avanço em termos de lições aprendidas e testes de procedimentos para a modelagem conceitual das operações que apoiarão os grandes eventos vindouros.

---

[128] Esse conceito pode ser entendido com mais profundidade em http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html.

[129] A composição do Destacamento de Defesa Cibernética e o fluxo de informações da Central de Monitoração Cibernética da Rio+20 estão nos Anexos A e B.

No âmbito do Exército Brasileiro, os dez projetos estruturantes do setor cibernético, já citados anteriormente, promovem uma oportunidade de se trabalhar matricialmente, com o CDCiber no papel de responsável pela coordenação e integração dos projetos e com diversas OM executando os mesmos. Essa experiência gerencial é de suma importância, uma vez que o conhecimento a respeito da gestão desses processos influencia o desenvolvimento das atividades que serão executadas fruto da doutrina a ser formulada.

## 6.4 COMPARAÇÃO DOS ASPECTOS DA DOUTRINA DE GUERRA CIBERNÉTICA DE OUTROS PAÍSES

Do estudo realizado, foi constatado que nenhum dos países estudados já possui uma doutrina de guerra cibernética formulada. De forma geral, a doutrina nessa área do conhecimento está em processo de formulação e grandes mudanças podem ocorrer rapidamente.

Desta forma, há necessidade de se manter um acompanhamento permanente da situação, verificando o que está sendo publicado oficialmente sobre o assunto e, com senso crítico bastante apurado, as notícias que são veiculadas na mídia e os pronunciamentos oficiais de autoridades ligadas ao setor.

Há indícios que os países estudados estejam agindo dessa maneira, também buscando as lições aprendidas e realizando análises tipo “engenharia reversa”, em concordância com a Teoria da Emulação Militar, dentro de um contexto de Isomorfismo Normativo.

Também pode ser observado que a dualidade sem precedentes da utilização de tecnologias de “*hacking*” acelerou o ciclo de desenvolvimento de técnicas e ferramentas, que facilitam o emprego por elementos de nível técnico intermediário. Chegará o momento em que, por exemplo, tropas de infantaria serão capazes de fazer uma “análise forense preliminar” para obtenção rápida e oportuna de inteligência de combate em material apreendido durante operações militares, antes de enviar esse material para uma análise mais aprofundada por elementos técnicos especializados.

As ações perpetradas por Estados ainda detêm maior grau de complexidade e sofisticação, mas esse cenário poderá se inverter. Grupos terroristas e criminosos, por exemplo, vem aumentando paulatinamente a sua qualificação técnica. Para

proteger o Estado, então, há necessidade de se manter uma contínua progressividade nos trabalhos do setor cibernético.

De forma geral, das pesquisas realizadas, foi percebido que as abordagens ocidentais para lidar com o setor cibernético são semelhantes. Em contatos com oficiais integrantes do CDCiber, foi constatado à época que os planos e abordagens dos EUA foram muito semelhantes às soluções desenhadas naquele centro, mesmo sem o conhecimento mais aprofundado dos projetos estadunidenses. A diferença, óbvia até, foi principalmente na ordem de grandeza dos recursos materiais e humanos a serem empregados para lidar com o cenário visualizado.

Também foi constatado que os EUA exercem forte influência nas concepções da OTAN, cujo *Cooperative Cyber Defence Centre of Excellence*[130] fica em Tallinn, na Estônia. Um ponto basilar na estratégia dos EUA é o fortalecimento de parcerias estratégicas para cooperação com outros países. Internamente a cooperação também é valorizada, com ênfase nas operações interagências.

A Rússia foi provavelmente o primeiro país a realizar atuação cibernética tática, sendo a precursora em utilizar uma “preparação cibernética do campo de batalha”. Apesar de não haver um reconhecimento oficial, há fortes indícios desse tipo de atuação contra a Estônia (2007) e Geórgia (2008), nessa última em apoio a uma operação militar convencional. Isso corrobora com o seu conceito abrangente de Operações de Informação, onde o objetivo a ser alcançado é a desorganização do inimigo.

Em contrapartida, a China provavelmente realiza uma ação sistemática voltada para obtenção de segredos militares, industriais e comerciais, caracterizando uma atuação cibernética estratégica, com maior ênfase na área de inteligência. Adota um conceito diferente, integrando a Guerra Eletrônica e a Guerra Cibernética no que foi chamado de INEW – integrated network-electronic warfare. Seu conceito de operações de informação são aderentes ao conceito de “Guerra do Povo” e há, no meio acadêmico e militar, uma forte cultura de “engenharia reversa”.

Resumidamente, podemos comparar as doutrinas desses três países no quadro a seguir:

[130] https://www.ccdcoe.org/

| | EUA | RÚSSIA | CHINA |
|---|---|---|---|
| Classificação | Predominantemente ostensiva | Classificada | Classificada |
| Acesso | Publicações conjuntas<br>Manuais de campanha | Trabalhos acadêmicos<br>mídia | Trabalhos acadêmicos<br>Análise governamental |
| Contexto | Operações de Informação | Guerra da Informação<br>Desorganização do Inimigo | “INEW” – Com, GE e G Ciber na mesma OM<br>“Guerra do Povo” |
| Similaridade cultural | Ocidental com forte influência na OTAN | Própria | Própria, derivada de conceitos ocidentais |
| Conceitos | Tentativa de alinhamento | Tentativa de alinhamento | Próprios |
| Parcerias | Parcerias estratégicas<br>Indústria de Software<br>Meio acadêmico | Serviços de segurança<br>Crime organizado? | Dissimulação no meio acadêmico<br>Milícias cibernéticas |
| Tipo de atuação | Predominantemente estratégica | Tática, sincronizada com a manobra | Estratégica |
| Admitem resposta cinética ? | Sim, expressamente | Sim, expressamente | Não declarada |

Quadro 7 – Comparação entre aspectos doutrinários dos EUA, Rússia e China

Fonte: o autor

# 7 **DISCUSSÕES E ELEMENTOS PARA FORMULAÇÃO DOUTRINÁRIA**

Como na maioria dos países que foram estudados durante a pesquisa, ainda não há consenso na formulação doutrinária da Defesa Cibernética brasileira no âmbito das três Forças Armadas nem no Ministério da Defesa. Esse consenso vem sendo buscado nas reuniões mensais do Grupo de Trabalho Interforças do Ministério da Defesa, cujo coordenador é o Estado-Maior do Exército, por intermédio da 2ª Subchefia, onde, desde 2010, as questões acerca da Defesa Cibernética vêm sendo apresentadas, discutidas e, normalmente, pacificadas. O avanço desse trabalho por vezes é lento, uma vez que nem todas as questões são resolvidas por consenso e existem assuntos onde há posições diametralmente opostas. Evita-se o confronto, investe-se em negociação e assuntos são colocados para análise posterior. É melhor gastar um pouco mais de tempo do que deixar que ânimos mais exacerbados conduzam a decisões equivocadas que podem levar anos para serem revertidas. Entretanto, pode-se afirmar que, de forma geral, a soma vetorial dos esforços vem progredindo.

Em ata de reunião do Grupo de Trabalho Interforças sobre a consolidação do setor cibernético na Defesa, realizada em 10 e 11 de março de 2011, foi observada a necessidade de se refrear o que ocorreu com a Guerra Eletrônica, ou seja, é importante evitar que cada Força Armada comece a desenvolver a sua doutrina de Guerra Cibernética de forma descentralizada e tenha dificuldades para uniformizar conceitos e terminologias posteriormente. Também foi ressaltado que o documento base para a discussão doutrinária é a Diretriz Ministerial nº 14/2009, de 09 de novembro de 2009, que designa o Exército Brasileiro como coordenador dos trabalhos, ou seja, **a Doutrina Básica de Guerra Cibernética para o Exército deve começar com o desenvolvimento de uma doutrina conjunta, geral, formulada por conceitos aceitos pelas três Forças Armadas**.

Desta forma, a presente proposta de elementos para formulação doutrinária também pretende contribuir tanto para as reuniões do Grupo de Trabalho Interforças, que está voltando os seus esforços para a confecção de um Manual do Ministério da Defesa, intitulado Doutrina Militar de Defesa Cibernética, quanto leva em conta os documentos publicados pelo DSIC do GSI/PR, alinhando-se às propostas apresentadas, porém não se limitando às mesmas. Os apêndices de “A” a “D” também são propostas desse trabalho para a inclusão da Guerra Cibernética no

Planejamento das Operações Conjuntas, por meio da atualização do manual MD-30-M-01 – Doutrina de Operações Conjuntas[131], prevista para ocorrer em 2013.

O formato utilizado para apresentar os elementos para formulação doutrinária que se seguem foi propositalmente simplificado para assemelhar-se ao modelo empregado na redação dos manuais militares. Busca-se, com isso, facilitar a sua inclusão no banco de dados doutrinário e permitir que sejam utilizados mais facilmente na preparação de publicações que abordem o tema apresentado.

Outra mudança interessante de postura é o novo paradigma descrito por BRILL[132] onde o foco anterior era de, principalmente, proteger o perímetro das redes e sistemas que mudou para melhorar a detecção de intrusão e a recuperação das redes e sistemas.

Do estudo comparativo realizado no capítulo anterior, a proposta apresentada nesse trabalho para a formulação doutrinária da Guerra Cibernética no Brasil pode ser resumida no quadro a seguir:

| | **EUA** | **BRASIL** |
|---|---|---|
| Classificação | Predominantemente ostensiva | Predominantemente ostensiva |
| Acesso | Publicações conjuntas<br>Manuais de campanha | Publicações do Ministério da Defesa<br>Manuais de campanha |
| Contexto | Operações de Informação | Operações de Informação<br>Simplificado – Com Soc, Op Psc, GE e G Ciber |
| Similaridade cultural | Ocidental com forte influência na OTAN | Ocidental, observando aspectos colaborativos da OTAN |
| Conceitos | Tentativa de alinhamento | Tentativa de alinhamento |
| Parcerias | Parcerias estratégicas<br>Indústria de Software<br>Meio acadêmico | Parcerias estratégicas<br>Indústria de Software<br>Meio acadêmico |
| Tipo de atuação | Predominantemente estratégica | Inicialmente tática defensiva<br>Buscar capacidade estratégica |
| Admitem resposta cinética ? | Sim, expressamente | Não declarar (dissuasão não ofensiva) |

Quadro 8 – Comparação entre os aspectos doutrinários dos EUA e a proposta brasileira

Fonte: o autor

[131] BRASIL. Ministério da Defesa. **MD31-M-01: doutrina de operações conjuntas**. 1. Ed. Brasília, DF, 2011.

[132] Entrevista concedida ao autor em 10 de maio de 2012, constante do Apêndice E.

## 7.1 GENERALIDADES

Com a instituição, em 2009, do conceito de Segurança Cibernética, que será apresentado adiante, o Gabinete de Segurança Institucional da Presidência da República (GSI/PR) definiu o seu escopo de atuação e caracterizou a diferença entre Segurança Cibernética, de sua competência, e Defesa Cibernética, da competência do Ministério da Defesa, por intermédio das Forças Armadas.

### 7.1.1 **Níveis de tratamento**

No contexto do Ministério da Defesa, as ações no espaço cibernético, de acordo com o nível de tratamento, seguirão as seguintes denominações:

- Nível político - Segurança da Informação e Comunicações (SIC) e Segurança Cibernética, coordenadas pelo GSI/PR e abrangendo a Administração Pública Federal direta e indireta, bem como as infraestruturas críticas da informação nacionais dos setores público e privado;

- Nível estratégico: Defesa Cibernética, a cargo do Ministério da Defesa, interagindo com o GSI/PR e Administração Pública Federal;

- Níveis operacional e tático: Guerra Cibernética, denominação restrita ao âmbito interno das Forças Armadas.

Em conformidade com o parágrafo anterior, será utilizada a denominação Defesa Cibernética quando estivermos planejando e executando ações cibernéticas afetas ao nível estratégico de decisão. Da mesma forma, será utilizada a denominação Guerra Cibernética quando o nível de decisão considerado for o operacional ou tático.

De forma análoga, os conceitos formulados para Defesa Cibernética são aplicados no contexto da Guerra Cibernética, uma vez que esta última está contida na primeira.

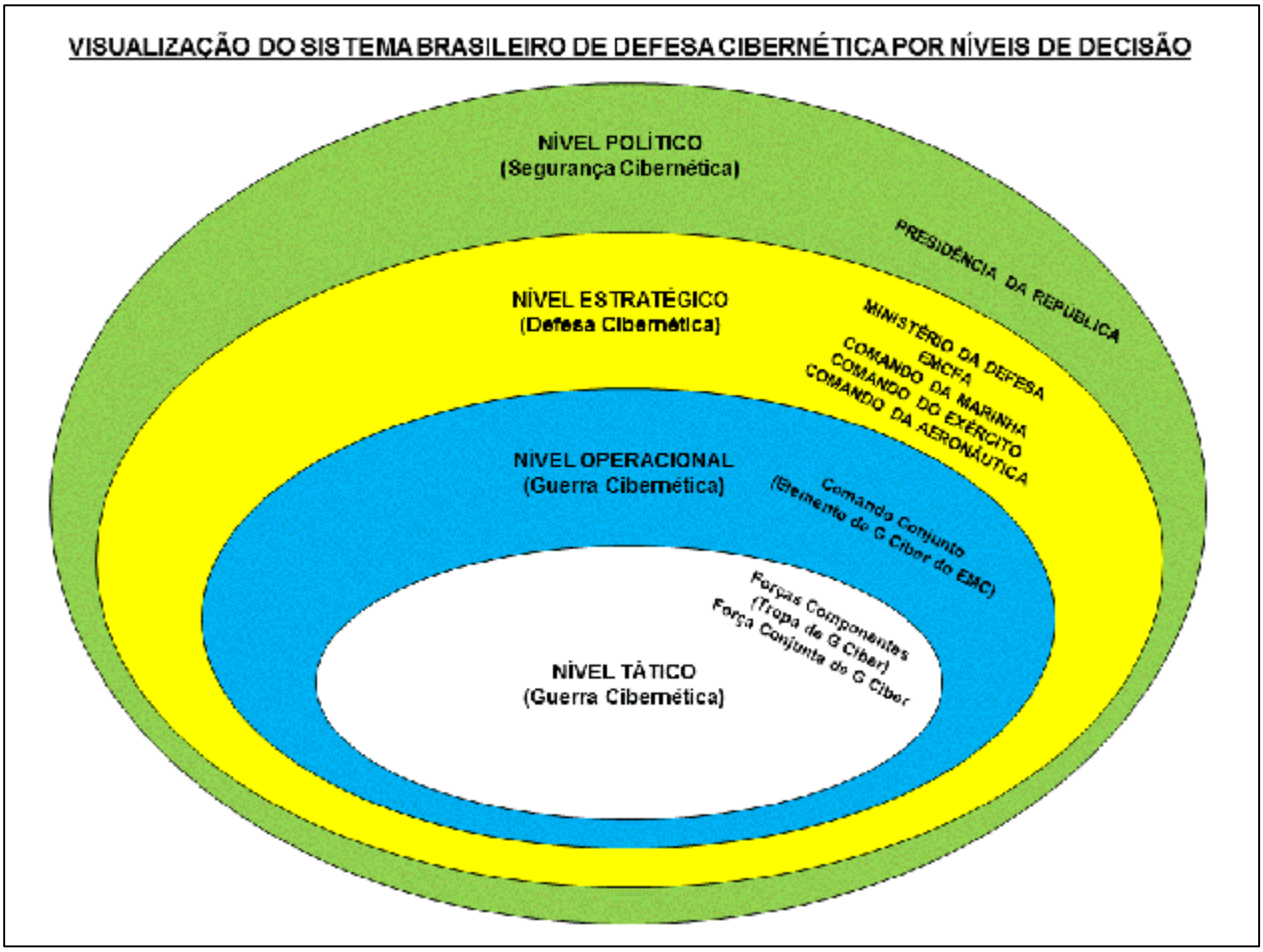



Figura 9 – Visualização do Sistema Brasileiro de Defesa Cibernética por Níveis de Decisão
Fonte: Centro de Defesa Cibernética

## 7.2 CONCEITOS

### 7.2.1 **Cibernética**

Termo que se refere ao uso de redes de computadores e de comunicações e sua interação dentro de sistemas utilizados por instituições públicas e privadas, de cunho estratégico, a exemplo do MD/FA. No campo da Defesa Nacional, inclui os recursos informatizados que compõem o Sistema Militar de Comando e Controle (SISMC2), bem como os sistemas de armas e vigilância.

### 7.2.2 **Espaço Cibernético**

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

Ações ofensivas no espaço cibernético podem impactar, inclusive, a segurança nacional.

### 7.2.3 **Os Domínios Operacionais**

O espaço cibernético é um dos cinco domínios operacionais e permeia todos os outros domínios. Os outros domínios são: o terrestre, o marítimo, o aéreo e o espacial. Estes cinco domínios são interdependentes. Atividades no espaço cibernético podem criar liberdade de ação para atividades em outros domínios assim como atividades em outros domínios também criam efeitos dentro e através do ciberespaço. O objetivo central da integração entre os domínios é a habilidade de se alavancar capacidades de vários domínios para sejam criados efeitos únicos e, frequentemente, decisivos.

### 7.2.4 **Poder Cibernético**

Capacidade de utilizar o domínio cibernético para criar vantagens e eventos de influência em todos os outros ambientes operacionais e em instrumentos de poder.

### 7.2.5 **Segurança Cibernética**

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.

### 7.2.6 **Defesa Cibernética**

Conjunto de ações defensivas, exploratórias e ofensivas, no contexto de um planejamento nacional de nível estratégico, realizadas no espaço cibernético, com as finalidades de proteger os nossos sistemas de informação, obter dados para a produção de conhecimento de inteligência e de causar prejuízos aos sistemas de informação do oponente.

### 7.2.7 **Guerra Cibernética**

Corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C2 do adversário, no contexto de um planejamento militar de nível operacional ou tático. Compreende ações que envolvem as ferramentas de Tecnologia da Informação e

Comunicações (TIC) para desestabilizar os Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC2) do oponente e defender os próprios STIC2. Abrange, essencialmente, as Ações Cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação à TIC.

7.2.8 **Inteligência Cibernética**

Processo de obtenção e aplicação de conhecimentos, no espaço cibernético, necessários à tomada de decisão.

7.2.9 **Segurança da Informação e Comunicações (SIC)**

Ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

7.2.10 **Infraestruturas Críticas (IC)**

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.

7.2.11 **Infraestrutura Crítica da Informação (ICI)**

Subconjunto dos ativos de informação que afeta diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade.

7.2.12 **Ativos de informação**

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

7.3 PRINCÍPIOS DE EMPREGO DA DEFESA CIBERNÉTICA

Como já mostrado no item 4.5, os tradicionais Princípios de Guerra são, de certo modo, genéricos e podem ser aplicados a todos os tipos de operações militares, incluindo as realizadas no espaço cibernético. As peculiaridades da

Defesa, no entanto, impõem que alguns outros princípios específicos sejam considerados, a saber:

### 7.3.1 **Princípio do Efeito**

As ações no espaço cibernético devem produzir efeitos que afetem o mundo real, mesmo que esses efeitos não sejam cinéticos. Não há sentido em desencadear quaisquer ações contra entidades cibernéticas, a menos que estas ações produzam algum efeito no mundo real, e que este efeito se traduza em vantagem.

### 7.3.2 **Princípio da Dissimulação**

Medidas ativas devem ser adotadas para se dissimular no espaço cibernético, dificultando a rastreabilidade das ações cibernéticas ofensivas e exploratórias levadas a efeito contra os sistemas de tecnologia da informação e de comunicações do oponente. Objetiva-se, assim, mascarar a autoria e o ponto de origem dessas ações.

### 7.3.3 **Princípio da Rastreabilidade**

Medidas efetivas devem ser adotadas para se detectar ações cibernéticas ofensivas e exploratórias contra os sistemas de tecnologia da informação e de comunicações amigos. Quase sempre, as ações adotadas no espaço cibernético envolvem a movimentação ou manipulação de dados, e estes permanecem registrados nos sistemas de Tecnologia da Informação e das Comunicações (TIC).

### 7.3.4 **Princípio da Adaptabilidade**

Consiste na capacidade da Defesa Cibernética de adaptar-se à característica de mutabilidade do espaço cibernético, mantendo a proatividade mesmo diante de mudanças súbitas e imprevisíveis.

## 7.4 CARACTERÍSTICAS DA DEFESA CIBERNÉTICA

Além de atender aos seus princípios específicos e de guerra, a Defesa Cibernética dispõe de algumas características, as quais serão, a seguir, apresentadas:

### 7.4.1 **Insegurança Latente**

Nenhum sistema computacional é totalmente seguro, tendo em vista que as vulnerabilidades nos ativos de informação serão sempre objeto de exploração por ameaças cibernéticas.

### 7.4.2 **Alcance Global**

A Defesa Cibernética possibilita a condução de ações em escala mundial, simultaneamente, em diferentes frentes de combate. Limitações físicas de distância e espaço não se aplicam ao espaço cibernético.

### 7.4.3 **Ausência de Fronteiras Geográficas**

As ações de defesa cibernética não se limitam a fronteiras definidas, pois os agentes podem atuar a partir de qualquer local.

### 7.4.4 **Mutabilidade**

Não existem leis de comportamento imutáveis no espaço cibernético porque as suas regras são arbitradas pelo homem e não pela natureza.

### 7.4.5 **Incerteza**

As ações no espaço cibernético podem não gerar os efeitos desejados em decorrência das diversas variáveis que afetam o comportamento dos sistemas informatizados.

### 7.4.6 **Dualidade**

Na Defesa Cibernética, as mesmas ferramentas podem ser usadas por atacantes e administradores de sistemas com finalidades distintas: uma ferramenta que busque as vulnerabilidades do sistema, por exemplo, pode ser usada por atacantes para encontrar pontos que representem oportunidades de ataque em seus sistemas alvos e por administradores para descobrir as fraquezas de equipamentos e redes.

### 7.4.7 **Paradoxo Tecnológico**

Quanto maior é o estágio de desenvolvimento do oponente, maior é sua dependência da Tecnologia da Informação (TI) e, por conseguinte, mais propenso às

ameaças cibernéticas ele estará. Contudo, paradoxalmente, este mesmo oponente possuirá maior possibilidade de se defender dos ataques cibernéticos em virtude de seu alto grau de desenvolvimento tecnológico.

### 7.4.8 **Dilema do Atacante**

Há uma constante tensão no relacionamento entre as ações de Defesa Cibernética: pode-se propor medidas de segurança alertando o fabricante para corrigir o sistema, ou manter o segredo para uso oportuno. Quando uma vulnerabilidade de um determinado sistema é descoberta, o profissional de Segurança / Defesa Cibernética se depara com o dilema entre alertar o fabricante para que ela seja corrigida ou mantê-la em segredo para uso oportuno, explorando-a em um eventual ataque cibernético.

### 7.4.9 **Função Acessória**

As ações de Defesa Cibernética não são um fim em si mesmas, sendo, geralmente, empregadas para apoiar a condução de outros tipos de operação.

### 7.4.10 **Assimetria**

Baseada no desbalanceamento de forças causado pela introdução de um ou mais elementos de ruptura tecnológicos, metodológicos ou procedimentais.

## 7.5 POSSIBILIDADES DA DEFESA CIBERNÉTICA

São possibilidades da Defesa Cibernética:

a) atuar no espaço cibernético por meio de ações ofensivas, defensivas e exploratórias;

b) cooperar na produção do conhecimento por meio da Inteligência Cibernética;

c) atingir infraestruturas críticas de um oponente sem limitação de alcance;

d) cooperar com a Segurança Cibernética, inclusive, de órgãos externos ao MD;

e) cooperar com o esforço de mobilização para assegurar a capacidade dissuasória da Defesa Cibernética;

f) obter a surpresa com mais facilidade, baseado na capacidade de inovação tecnológica;

g) realizar ações contra oponentes mais fortes, dentro do conceito de guerra assimétrica.

## 7.6 LIMITAÇÕES DA DEFESA CIBERNÉTICA

São limitações da Defesa Cibernética:

a) limitada capacidade de identificação da origem de ataques cibernéticos.

b) existência de vulnerabilidades nos sistemas computacionais.

c) dificuldade de identificação de talentos humanos.

d) grande vulnerabilidade a ações de oponentes com poder assimétrico.

e) dificuldade de acompanhamento da evolução tecnológica na área cibernética.

f) facilidade de ser surpreendido com base na inovação tecnológica.

## 7.7 FORMAS DE ATUAÇÃO CIBERNÉTICA

As formas de atuação cibernética podem variar de acordo com o nível dos objetivos (político, estratégico ou tático), nível de envolvimento nacional, contexto de emprego, nível tecnológico empregado, sincronização e tempo de preparação, como veremos a segur.

### 7.7.1 **Atuação Cibernética Estratégica**

A atuação cibernética estratégica ocorre desde o tempo de paz, para atingir um objetivo político ou estratégico definido no mais alto nível, normalmente dentro do contexto de uma Operação de Informação ou de Inteligência.

Um exemplo de objetivo político que resulte em atuação cibernética estratégica seria “Dificultar a obtenção de capacidade nuclear por parte do País Alfa”. Nesse contexto, vários órgãos e agências de um governo iriam empreender ações para a conquista desse objetivo. Provavelmente o Ministério das Relações Exteriores desse país iria empreender ações diplomáticas com o objetivo de influenciar o Conselho de Segurança da ONU a impor sanções econômicas e restrições à importação de tecnologia para negar o acesso a tecnologias e equipamentos considerados essenciais para obter a capacidade nuclear. No contexto da Cibernética, provavelmente seriam empreendidas inicialmente ações de exploração cibernética visando conhecer os sistemas computacionais de Alfa e levantar vulnerabilidades que seriam posteriormente exploradas em um ataque cibernético, utilizando um ou

mais artefatos especialmente produzidos para explorar essas vulnerabilidades. Normalmente há emprego de elevado nível tecnológico e ações meticulosamente preparadas e desencadeadas provavelmente como uma operação clandestina. Como essa ação está inserida no contexto das Operações de Informação, também poderiam ser empreendidas, nesse contexto, campanhas de Operações Psicológicas com propaganda de todos os tipos, além de um suporte massivo de Operações de Inteligência para obtenção de conhecimento e desinformação.

### 7.7.2 **Atuação Cibernética Tática**

A atuação cibernética tática é tipicamente empregada no contexto de uma operação militar, contribuindo para a obtenção de um objetivo tático.

Embora, por simplificação, não seja citado diretamente, as ações desse tipo de atuação podem ocorrer tanto no nível operacional e quanto no nível tático.

Um exemplo de objetivo que resulte em atuação cibernética tática seria “Isolar, conquistar e manter a Região de ‘Esqueleto’, estabelecendo uma faixa de segurança, dentro da região em litígio”. A inteligência de combate, ao levantar que as forças na região em litígio utilizam determinadas rede computacionais e redes rádio para realizar o seu Comando e Controle, alimentou a célula de Operações de Informação que, por sua vez, planejou um ataque cibernético de negação de serviço[133] a essa rede, sincronizado com Medidas de Ataque Eletrônico às redes rádio levantadas, precedendo em poucos minutos à manobra de desbordamento e cerco que seriam levadas a cabo por uma operação militar convencional. A degradação dos sistemas de Comando e Controle do inimigo contribuiria para a obtenção do sucesso da operação.

Podemos, então, sintetizar as formas de atuação cibernética com o seguinte quadro:

[133] Um ataque de negação de serviço (também conhecido como DoS Attack, um acrônimo em inglês para Denial of Service), é uma tentativa em tornar os recursos de um sistema indisponíveis para seus usuários. Não se trata de uma invasão do sistema, mas sim de tornar o serviço indisponível por sobrecarga. Esse tipo de ataque normalmente não necessita de ferramentas e conhecimento tecnológico avançados para ser executado.

| FORMA DE ATUAÇÃO CIBERNÉTICA | ESTRATÉGICA | TÁTICA |
|---|---|---|
| Nível dos Objetivos | Políticos e Estratégicos | Operacionais e Táticos |
| Foco principal | Obtenção de inteligência | Preparação do campo de batalha |
| Nível de envolvimento nacional | Interministerial, podendo requerer ações diplomáticas e de vários ministérios e agências (Defesa, Relações Exteriores, Ciência, Tecnologia e Inovação, GSI/PR, ABIN, etc.) | Normalmente dentro do Ministério da Defesa, podendo contar com apoio do Ministério das Relações Exteriores |
| Contexto | Desde o tempo de paz, podendo fazer parte de uma operação clandestina ou de inteligência | Em um ambiente de crise ou conflito, apoiando uma ação militar |
| Nível tecnológico empregado | Normalmente alto ou muito alto | Normalmente médio ou baixo |
| Sincronização | Dentro do contexto de uma sofisticada operação de inteligência, podendo requerer ações diplomáticas anteriores ou posteriores | Dentro do contexto dos sistemas operacionais de uma operação militar, sincronizado com a manobra |
| Tempo de Preparação e Duração | Duração prolongada, com tempo de preparação normalmente mais longo, com desenvolvimento de técnicas inovadoras | Duração limitada, com moderado ou curto tempo de preparação, utilizando conhecimentos já levantados e técnicas previamente preparadas |

Quadro 9 – Características das formas de atuação cibernética

Fonte: o autor

## 7.8 TIPOS DE AÇÕES CIBERNÉTICAS

As ações cibernéticas guardam similaridades com as ações de Guerra Eletrônica, o que simplifica o entendimento e permite a correlação das ações, ao se considerar o emprego utilizando a filosofia das Operações de Informação.

### 7.8.1 **Exploração Cibernética**

Consiste em ações de busca, nos Sistemas Tecnologia da Informação de interesse, a fim de obter dados negados, de preferência evitando o rastreamento,

para a produção de conhecimento e/ou identificar as vulnerabilidades desses sistemas.

### 7.8.2 **Ataque Cibernético**

Compreende ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes computacionais e de comunicações do oponente.

### 7.8.3 **Proteção Cibernética**

Abrange as ações para neutralizar ataques e exploração cibernética contra os nossos dispositivos computacionais e redes de computadores e de comunicações, incrementando as ações de Segurança Cibernética em face de uma situação de paz, crise ou conflito. É uma atividade de caráter permanente.

O quadro a seguir demonstra a correlação entre as ações de Guerra Cibernética e Guerra Eletrônica.

| Ação | Guerra Eletrônica | Ação | Guerra Cibernética |
|---|---|---|---|
| Medidas de Apoio à Guerra Eletrônica (MAGE) | - Interceptar e identificar passivamente sinais eletromagnéticos e localizar as fontes emissoras.<br>- Prover o reconhecimento imediato da ameaça.<br>- Obter a “Assinatura Eletrônica” do emissor alvo. | Exploração Cibernética | - Obtenção de dados negados, de preferência evitando o rastreamento.<br>- Levantar características e vulnerabilidades dos sistemas do alvo.<br>- Obter as características (“Assinatura Digital”) do sistema alvo. |
| Medidas de Ataque Eletrônico (MAE) | - Utilizar energia eletromagnética para:<br>- Impedir ou reduzir o emprego eficiente do espectro eletromagnético pelo oponente.<br>- Destruir, neutralizar ou degradar sua capacidade de combate. | Ataque Cibernético | - Empregar ferramentas computacionais para:<br>- Alterar ou destruir dados;<br>- Reduzir a eficiência dos sistemas computacionais;<br>- causar danos a sistemas computacionais ou unidades físicas. |
| Medidas de Proteção Eletrônica (MPE) | - Assegurar a utilização eficiente do espectro eletromagnético, a despeito do emprego das MAGE e MAE do oponente | Proteção Cibernética | - Ações ou esforços para proteger nossas redes contra os ataques cibernéticos realizados pelo oponente. |

Quadro 10 – Similaridade entre ações de Guerra Eletrônica e Guerra Cibernética

Fonte: o autor

## 7.9 ESTRUTURA DE GUERRA CIBERNÉTICA NAS OPERAÇÕES

A Guerra Cibernética em Operações deverá ser conduzida, sempre que possível, no nível do Comando Conjunto, integrando a célula de Operações de Informação (Op Info) e no Comando do Teatro de Operações, conforme se segue:

### 7.9.1 **Célula de Operações de Informação no Estado-Maior Conjunto**

A célula de Operações de Informação deve ser mobiliada com, pelo menos, 1 (um) Oficial de Ligação (especialista em G Ciber) de cada Força. Preferencialmente nos postos de Major ou Tenente-Coronel e com Curso de Comando e Estado-Maior.

Os três militares designados deverão participar da fase de planejamento operacional, elaborando o Apêndice de Guerra Cibernética ao Anexo de Operações de Informação ao Plano Operacional e cooperando com os assuntos de G Ciber que deverão constar do Anexo de Operações de Informação e de outros documentos integrantes do planejamento conjunto.

#### 7.9.1.1 Principais Atribuições dos O Lig G Ciber Durante as Operações

a) Assessorar o Chefe da célula de Op Info do EM Cj no que se refere às possíveis ações cibernéticas e efeitos que poderiam ser obtidos em proveito das operações em curso, juntamente com as demais células do EM Cj;

b) Sincronizar os efeitos desejados com a manobra concebida, de forma a maximizar o impacto das ações de Op Info, negando, dificultando ou influenciando o processo decisório do oponente, ou mesmo protegendo o nosso próprio processo decisório. O ponto focal sempre será a obtenção da superioridade da informação. [134]

### 7.9.2 **Destacamento Conjunto de Guerra Cibernética**

Deverá ser adjudicado ao Comando do Teatro de Operações 01 (um) Destacamento Conjunto de Guerra Cibernética (Dst Cj G Ciber), diretamente subordinado ao Comando do TO (integrando a tropa do TO) e vinculado à Célula de Op Info do Estado-Maior Conjunto.

O Dst Cj G Ciber poderá ser constituído da seguinte maneira:

---

[134] Vantagem operacional resultante da habilidade de coletar, processar e disseminar um fluxo ininterrupto de informação, enquanto explora ou nega ao oponente a capacidade de fazer o mesmo.

a) Exército Brasileiro: 01 (um) Cel / Tenente-Coronel (Comandante do Dst Cj G Ciber) e 02 (dois) Maj/Cap/Ten/ST/Sgt;

b) Marinha do Brasil: 03 (três) CC/CT/Ten/SO/Sgt;

c) Força Aérea: 03 (três) Maj/Cap/Ten/SO/Sgt;

d) Elementos de ligação interagências;

e) Elementos civis especialistas, para operação assistida e assessoria.

f) O detalhamento da estrutura e o efetivo do Dst Cj G Ciber deverá ser definido e proposto após estudo específico elaborado por seu comandante, levando em conta as necessidades específicas de cada operação, segundo os fatores da decisão. [135]

7.9.2.1 Possibilidades do Destacamento Conjunto de Guerra Cibernética:

a) Identificar e analisar vulnerabilidades (conhecidas) nas redes de computadores e aplicações empregadas no Sistema de C2 desdobrado para a operação;

b) Recomendar ações para corrigir as vulnerabilidades identificadas;

c) Verificar a conformidade de Segurança da Informação e Comunicações (SIC) no Sistema de C2 desdobrado para a operação;

d) Planejar ações cibernéticas (proteção, exploração e ataque cibernéticos), no contexto da operação conjunta, em cumprimento às orientações e diretrizes emanadas pela célula de Op Info do EM Cj;

e) Realizar ações de inteligência cibernética, no contexto da operação conjunta, em cumprimento às orientações e diretrizes emanadas pela célula de Op Info do EM Cj.

7.9.3 **Destacamento de Guerra Cibernética**

Quando a operação a apoiar não for de caráter conjunto, os mesmos princípios gerais se aplicam. Nesse caso, o O Lig G Ciber integra a célula de Operações de Informação (Op Info) ou estrutura similar do Estado-Maior do mais alto escalão em presença e o Destacamento de Guerra Cibernética será diretamente subordinado à esse escalão, ficando vinculado à Célula de Op Info do Estado-Maior.

---

[135] Os Anexos “A” e “B” trazem, como forma de ilustração e exemplo, a composição da central de monitoramento cibernético e o fluxo de informações adotados pelo Destacamento de Defesa Cibernética empregado pelo Centro de Defesa Cibernética durante a Operação Rio + 20, primeira operação real onde houve o emprego militar das ações de Proteção Cibernética a um grande evento.

O detalhamento da estrutura e o efetivo do Dst G Ciber deverá ser definido e proposto após estudo específico elaborado por seu comandante, levando em conta as necessidades específicas de cada operação, segundo os fatores da decisão. A composição sugerida acima pode servir de base para o planejamento.

## 7.10 DOCUMENTOS DE PLANEJAMENTO DE GUERRA CIBERNÉTICA

O manual MD31-M-01 – doutrina de operações conjuntas, aprovado em 8 de dezembro de 2011, apesar de já contar com inclusões propostas pelo NuCDCiber, ainda não traz modelos de Análise de Guerra Cibernética e nem do Apêndice de Guerra Cibernética ao Anexo de Operações de Informação. Esse manual tem a revisão prevista para o ano de 2013.

Os apêndices A e B trazem uma proposta de memento comentado de Análise de Guerra Cibernética e os apêndices C e D trazem uma proposta de Apêndice de Guerra Cibernética ao Anexo de Operações de Informação de um Plano Operacional. Por serem extensos, estes documentos foram incorporados ao presente trabalho como apêndices, para facilitar a consulta e o manuseio.

Estas propostas refletem a discussão entre elementos da Divisão de Doutrina e Mobilização, Divisão de Operações e Divisão de Inteligência do CDCiber e a participação do autor nos planejamentos da Operação Conjunta Amazônia 2012 e incorpora lições aprendidas durante a operação do NuCDCiber na Conferência das Nações Unidas sobre Desenvolvimento Sustentável (também chamada de Rio+20) que foram consideradas aplicáveis a esse tipo de planejamento.

# 8 **CONCLUSÃO**

O ponto inicial do presente trabalho é o entendimento da utilização da Teoria da Emulação Militar num contexto de Isomorfismo Normativo para sua construção. Todo o esforço de pesquisa teve por base essa teoria, cujo emprego não é novo no Exército Brasileiro, mas que permitiu que as propostas apresentadas tivessem um grau de risco menor, fossem construídas de forma ágil e se apoiassem em uma base cognitiva comum com outros países.

Foi analisado o entendimento do cenário atual, que faz a sua transição do paradigma de emprego de meios militares típicos da Era Industrial, para o emprego em uma nova concepção de atuação, utilizando as tecnologias, os meios e a agilidade da Era do Conhecimento. Essa mudança ou, por vezes, mesclagem de paradigmas levou à necessidade de se combinar, coordenar e sincronizar ações de Inteligência, Comunicação Social, Operações Psicológicas, Guerra Eletrônica e, finalmente, Guerra Cibernética, o que vem sendo chamado de Operações de Informação.

Posteriormente, visando proporcionar um melhor entendimento da realidade brasileira, foram descritos os principais órgãos e atores relacionados à Segurança e Defesa Cibernética no Brasil, seu embasamento legal, suas dependências e relações. A compreensão de como os atores atuam no setor cibernético nacional é fundamental para o planejamento das operações interagências, cenário mais provável de emprego das Forças Armadas no setor cibernético atualmente.

Em seguida, foi realizado um estudo de caso da Doutrina de Defesa Cibernética dos Estados Unidos da América, da Rússia e da China, destacando os pontos julgados essenciais para o levantamento inicial de elementos que poderiam contribuir para o que seria uma Doutrina Básica de Guerra Cibernética que fosse aplicável à realidade brasileira. Pela análise da documentação selecionada e pelas entrevistas realizadas, constatou-se que a doutrina nessa área do conhecimento está em processo de formulação e grandes mudanças ainda podem ser esperadas nos próximos anos, com a necessidade de evolução de estruturas e adoção de novos conceitos e princípios para tentar mitigar os riscos e tratar as situações que estão sendo descobertas.

A dualidade sem precedentes entre a utilização de tecnologias de "*hacking*", tanto para fins militares, quanto para fins criminosos, acelerou ainda mais o ciclo entre o desenvolvimento das ações de ataque e exploração cibernéticas e o

desenvolvimento das técnicas de proteção cibernética para fazer face aos primeiros. As ações de exploração e ataque cibernéticos, perpetradas por Estados, ainda possuem um nível de sofisticação maior, devido aos recursos humanos e financeiros disponíveis. Poderá haver um momento onde ações criminosas ganhem um nível de sofisticação maior e essa equação se inverta ou, ainda, existe a possibilidade de se descortinar um cenário onde Estados utilizem serviços de redes criminosas ou mesmo organizem redes criminosas para desenvolver operações cobertas de atuação cibernética estratégica visando não serem detectados. Esses cenários impõem uma contínua progressividade dos trabalhos no setor cibernético, com a finalidade de proteger o Estado, uma vez que grupos terroristas, criminosos ou outro tipo de organização com objetivos similares fora das Forças Armadas normalmente não possuem códigos de conduta, não obedecem a tratados e regulamentações internacionais ou seguem procedimentos diplomáticos como os que regem as relações entre Estados. No curso realizado pelo autor sobre terrorismo cibernético no Centro de Excelência - Defesa contra o Terrorismo da OTAN, na Turquia, ficou claro que o nível de conhecimento técnico dos principais grupos terroristas ativos no mundo atualmente já é bastante alto e tende a subir cada vez mais, apesar de todos os esforços feitos no combate a essas atividades.

As necessidades doutrinárias, expressas em quadro de situação da doutrina, são definidas em função do Sistema de Planejamento do Exército (SIPLEx) e do banco de dados doutrinários, que é construído pelos manuais em vigor, cadernos de instrução, relatórios diversos, conclusões de seminários, pesquisas doutrinárias, experimentações doutrinárias, reuniões de coordenação doutrinária, informações obtidas fruto de viagens ao exterior, de cursos no exterior, contribuições pessoais, e outras contribuições. Dessa forma, este trabalho seria mais um dos vários componentes necessários à formulação de uma doutrina de Guerra Cibernética.

O início da formulação de uma doutrina básica nessa área deveria ser de alto nível, enfatizando princípios e aspectos de longo prazo, para que não seja necessária uma revisão constante. Sua implementação poderia ser realizada, então, por intermédio de políticas e procedimentos que seriam muito mais específicos. Dessa forma, este trabalho teve o seu foco principal em tentar contribuir na busca desses princípios, visando facilitar a formulação doutrinária pelo EME.

A atuação do Grupo de Trabalho Interforças do Ministério da Defesa sobre a consolidação do setor cibernético é de fundamental importância. Ao concluir que

seria importante evitar que cada Força Armada desenvolvesse a sua doutrina descentralizadamente e encontrasse dificuldades para uniformizar conceitos e terminologias posteriormente, o que ocorreu, por exemplo, com a Guerra Eletrônica, definiu que a Doutrina Básica de Guerra Cibernética para o Exército deveria começar com o desenvolvimento de uma doutrina conjunta, geral, formulada por conceitos aceitos pelas três Forças Armadas, daí o foco desse trabalho nas operações e doutrina conjuntas, apesar de ter no seu título “Guerra Cibernética: uma proposta de elementos de formulação doutrinária para o Exército Brasileiro”.

As discussões nesse grupo até o momento levaram, no campo doutrinário, à inserção da Guerra Cibernética no manual de Doutrina de Operações Conjuntas (MD31-M-01), ainda de forma sucinta e preliminar e na formulação da Política Cibernética de Defesa. Outras sugestões continuam sendo apresentadas, como a formatação dos documentos de planejamento e os procedimentos para integração dos Centros de Tratamento de Incidentes de Rede das três Forças Armadas, por exemplo. O autor também participa das discussões desse grupo como chefe da Seção de Doutrina do Centro de Defesa Cibernética.

A participação efetiva do CDCiber no adestramento de operações conjuntas, tais como as operações Amazônia 2011, Anhanduí 2011, Amazônia 2012 e Atlântico III estão permitindo o avanço nas ações de planejamento. A atuação em grandes eventos, tal como ocorreu na Rio+20, trouxe uma nova dimensão à necessidade de planejamento detalhado e, principalmente, operação interagências integrada e sincronizada, para fazer frente à ameaças reais que poderiam ganhar visibilidade internacional, diretamente relacionadas ao novo paradigma das Operações de Informação. Outro cenário foi a participação do CDCiber na operação real de combate a ilícitos transfronteiriços Ágata 6. As lições aprendidas permitirão a paulatina experimentação dos conceitos levantados, que levarão, com a coordenação do GT Interforças, à proposta de um Manual de Defesa Cibernética Conjunta no MD.

Desta forma, a proposta deste trabalho é que a formulação inicial da Doutrina Básica de Guerra Cibernética deverá ser ampla e ainda genérica, baseada em princípios, capacidades, possibilidades e limitações, definição de terminologia comum e propostas de formatação de documentos de planejamento, tal como foi proposto.

Sugere-se que detalhes de operação, técnicas, táticas e procedimentos poderão ser regulados em Procedimentos Operacionais Padrão (POP), que serão bem mais específicos e terão caráter particular a cada tipo de operação apoiada.

A sugestão desse pesquisador é que os principais documentos doutrinários, de maneira análoga ao manual MD31-M-01 – Doutrina de Operações Conjuntas, devem ter o seu prazo de revisão inicial relativamente curto, permitindo o ajuste mais significativo da documentação nos primeiros anos. Depois, essa documentação poderá ser tratada de forma mais duradoura, quando os esforços mais intensos deverão se concentrar nos POP.

Como a principal fonte de doutrina é a experiência, e esta vai sendo adquirida aos poucos e ao longo do tempo, cabe ao EME e ao CDCiber planejar a gestão do conhecimento necessário para que seja possível converter essa experiência em documentação que possa ser aplicada em Operações. Esta é a função principal da Divisão de Doutrina do Centro de Defesa Cibernética.

O presente estudo procurou trazer novos elementos para a composição do banco de dados doutrinário, esperando, dessa forma, colaborar com o Exército Brasileiro na concretização de seu objetivo estratégico de desenvolver uma doutrina moderna, ágil e plenamente adaptada ao cenário brasileiro.

_____

JOÃO MARINONIO ENKE CARNEIRO – Ten Cel Com

# REFERÊNCIAS

AMARO, Marisa de Oliveira Santos. **Evolução da Governança de Tecnologia da Informação na Marinha do Brasil**. XXXIV Encontro da ANPAD, Rio de Janeiro, RJ, 2010. Disponível em: <http://tupi.fisica.ufmg.br/~michel/docs/Artigos_e_textos/Gestao/GC%20evolucao%20TI.pdf>. Acesso em: 28 mai. 2011

ANAND, Vinod. **Chinese Concepts and Capabilities of Information Warfare**. Institute for Defence Studies and Analyses, Strategic Analysis. Nova Delhi, India. Vol. 30, No. 4, Oct-Dec 2006. Disponível em: < http://www.idsa.in/strategicanalysis/ChineseConceptsandCapabilitiesofInformationWarfare_vanand_1006>. Acesso em: 4 jul. 2012.

BRASIL. Aeronáutica. Comando Geral do Ar. **MCA 500-3: comando e controle na guerra**. Brasília, DF, 2000.

_____. Constituição (1988). **Constituição da República Federativa do Brasil**; Promulgada em 5 de outubro de 1988: atualizada até a Emenda Constitucional nº 67, de 22 de dezembro de 2010. Disponível em: < http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Acesso em: 28 mai. 2011.

_____. Decreto nº 4.689, de 6 de maio de 2003**. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão do Instituto Nacional de Tecnologia da Informação - ITI**, e dá outras providências. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 8 de maio de 2003.

_____. Decreto nº 4.801, de 6 de agosto de 2003**. Cria a Câmara de Relações Exteriores e Defesa Nacional**, do Conselho de Governo. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 7 de agosto de 2003.

_____. Decreto nº 5.135, de 7 de julho de 2004**. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções Gratificadas da Casa Civil da Presidência da República**, e dá outras providências. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 8 de julho de 2004.

_____. Decreto nº 5.484, de 30 de junho de 2005**.** Aprova a **Política de Defesa Nacional**, e dá outras providências. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 1º de julho de 2005.

_____. Decreto nº 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] República Federativa do Brasil. Brasília, DF, 9 de maio de 2006.

_____. Decreto nº 6.703, de 18 de dezembro de 2008**.** Aprova a **Estratégia Nacional de Defesa**, e dá outras providências. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 19 de dezembro de 2008.

BRASIL. Decreto nº 7.411, de 29 de dezembro de 2010**.** Dispõe sobre remanejamento de cargos em comissão do Grupo-Direção e Assessoramento Superiores - DAS, **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] República Federativa do Brasil. Brasília, DF, 30 de dezembro de 2010.

_____. Decreto nº 7.809, de 20 de setembro de 2012. Altera os Decretos nº 5.417, de 13 de abril de 2005, nº 5.751, de 12 de abril de 2006, e nº 6.834, de 30 de abril de 2009, que **aprovam as estruturas regimentais e os quadros demonstrativos dos cargos em comissão e das funções gratificadas dos Comandos da Marinha, do Exército e da Aeronáutica, do Ministério da Defesa**. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 21 de setembro de 2012.

_____. Exército. Comandante do Exército. Portaria nº 666, de 4 de agosto de 2010. **Cria o Centro de Defesa Cibernética do Exército e dá outras providências.** Boletim do Exército nº 31. Brasília, DF, 6 de agosto de 2010.

_____. Exército. Comandante do Exército. Portaria nº 667, de 4 de agosto de 2010. **Ativa do Núcleo do Centro de Defesa Cibernética do Exército e dá outras providências.** Boletim do Exército nº 31. Brasília, DF, 6 de agosto de 2010.

_____. Exército. Estado-Maior do Exército. **IP 100-1: bases para a modernização da doutrina de emprego da Força Terrestre (doutrina delta)**. 1. Ed. Brasília, DF, 1996.

_____. Exército. Estado-Maior do Exército. **C 100-5: operações**. 3. Ed. Brasília, DF, 1997.

_____. Exército. **IG 20-13: instruções gerais para a organização e funcionamento do sistema de doutrina militar (SIDOMT).** Brasília, DF, 1999.

_____. Exército. **IG 20-19: instruções gerais de segurança da informação para o Exército Brasileiro.** Brasília, DF, 2001.

_____. Exército. Centro Integrado de Guerra Eletrônica. **Estudos para a criação do Centro de Estudos de Guerra Cibernética, de 30 de abril de 2004**. Brasília, DF, 2004a.

_____. Exército. Secretaria de Ciência e Tecnologia. **Memória nº 010-A/4-04-SCT de 08 de abril de 2004**. Guerra Cibernética e Segurança da Informação. Brasília, DF, 2004b.

_____. Gabinete de Segurança Institucional da Presidência da República. Portaria nº 12 – CH/GSI, de 27 de junho de 2003. Instituiu o **Grupo de Trabalho do Centro de Emergência de Computação para estudar e propor as medidas necessárias para a criação e implantação de um centro de emergência de computação do Governo Federal**. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 30 de junho de 2003.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. Portaria nº 2, de 8 de fevereiro de 2008**. Institui Grupos Técnicos de Segurança de Infraestruturas Críticas** (GTSIC) e dá outras providências. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 11 de fevereiro de 2008.

_____. Gabinete de Segurança Institucional da Presidência da República. Portaria nº 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] República Federativa do Brasil. Brasília, DF, 9 de setembro de 2009.

_____. Lei nº 7.170, de 14 de dezembro de 1983. Define os **crimes contra a segurança nacional**, a ordem política e social, estabelece seu processo e julgamento e dá outras providências. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 15 de dezembro de 1983.

_____. Lei nº 8.183, de 11 de abril de 1991. **Dispõe sobre a organização e o funcionamento do Conselho de Defesa Nacional** e dá outras providências. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 12 de abril de 1991.

_____. Lei nº 9.883, de 7 de dezembro de 1999. **Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN**, e dá outras providências. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 8 de dezembro de 1999.

_____. Lei nº 9.649, de 27 de maio de 1998. Dispõe sobre a **organização da Presidência da República e dos Ministérios**, e dá outras providências. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 5 de junho de 1998.

_____. Lei nº 10.683, de 28 de maio de 2003. Dispõe sobre a **organização da Presidência da República e dos Ministérios**, e dá outras providências. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 29 de maio de 2003.

_____. Medida Provisória nº 2.216-37, de 31 de agosto 2001. **Altera dispositivos da Lei nº 9.649, de 27 de maio de 1998, que dispõe sobre a organização da Presidência da República e dos Ministérios**, e dá outras providências. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 1 de setembro de 2001.

_____. Ministério da Defesa. **MD31-D-03: doutrina militar de comando e controle**. 1. Ed. Brasília, DF, 2006b.

_____. Ministério da Defesa. **Diretriz Ministerial nº 14. Integração e Coordenação dos Setores Estratégicos da Defesa**. Brasília, DF, 9 de novembro de 2009.

_____. Ministério da Defesa. **MD31-M-01: doutrina de operações conjuntas**. 1. Ed. Brasília, DF, 2011.

BRASIL. Ministério da Defesa. Portaria nº 3.028, de 14 de novembro de 2012. **Atribui ao Centro de Defesa Cibernética (CDCiber), do Comando do Exército, a responsabilidade pela coordenação e integração das atividades de defesa cibernética, no âmbito do Ministério da Defesa (MD).** Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 20 de novembro de 2012.

BRILL, Alan E. Entrevista concedida ao autor em 10 de maio de 2012, constante do Apêndice E.

CAMPER, A. D. ; DEARTH, D. H. ; GOODDEN, R. T. **Cyberwar: Security, Strategy, and Conflict in the Information Age**. 3. ed. Afcea Intl Pr; 1996. ISBN: 978-0916159269.

CARR, Jeffrey. **Inside Cyber Warfare**. 2. Ed. O'Reilly Media, 2011. ISBN: 978-1-449-31004-2.

CLARKE, R. A.; KNAKE R. K.. **Cyber War: The Next Threat to National Security and What to Do About It**. HarperCollins e-books, 2010. ISBN: 978-0061962240.

DANCHEV, Dancho. **Coordinated Russia vs Georgia cyber attack in progress.** ZDNet, 2008. Disponível em: <http://blogs.zdnet.com/security/?p=1670> Acesso em 31 mar. 2010.

DIMAGGIO, Paul J.; POWELL, Walter W. **A gaiola de ferro revisitada: isomorfismo institucional e racionalidade coletiva nos campos organizacionais**. Revista de Administração de Empresas. V. 45, nº 2, Abr/Jun 2005 (pp. 74 a 89)

EASTWEST INSTITUTE'S WORLDWIDE CYBERSECURITY INITIATIVE. MOSCOW STATE UNIVERSITY'S INFORMATION SECURITY INITIATIVE. **Russia – U.S. Bilateral on Cybersecurity : Critical Terminology Foundations**. Issue 1. New York, 2011. Disponível em <http://www.ewi.info/russia-us-bilateral-cybersecurity-critical-terminology-foundations>. Acesso em: 30 abr. 2011

ESTADOS UNIDOS DA AMÉRICA. Army. Department of the Army. **FM 3-13: information operations: doctrine, tactics, technics and procedures**. Washington, DC, 2003.

_____. Army. Department of the Army. **Army activates network warfare unit**. Army.mil, 2008. Disponível em: <http://www.army.mil/-newsreleases/2008/07/02/10569-army-activates-network-warfare-unit/>. Acesso em: 31 mar. 2010.

_____. Army. Department of the Army. **Cyberspace Operations Concept Capability Plan 2016-2028**. Army.mil, 22 fev. 2010a. Disponível em: <http://www.tradoc.army.mil/tpubs/pamndx.htm>. Acesso em: 25 nov. 2010.

_____. Army. Department of the Army. **Information Operations Primer**. Army.mil, 19 out. 2011. Disponível em: <http://www.carlisle.army.mil/usawc/dmspo/Publications/Publications.htm>. Acesso em: 15 dez. 2011.

ESTADOS UNIDOS DA AMÉRICA. Air Force. Department of the Air Force. **Air Force Doctrine Document 3-12 Cyberspace Operations**. AF.mil, 15 jul. 2010b. Disponível em: <http://www.e-publishing.af.mil/shared/media/epubs/AFDD3-12.pdf>. Acesso em: 25 nov. 2010.

_____. **The Pentagon's Cyberstrategy, One Year Later: Defending Against the Next Cyberattack**. Foreign Affairs Magazine, 28 set. 2011. Disponível em: < http://www.foreignaffairs.com/articles/68305/william-j-lynn-iii/the-pentagons-cyberstrategy-one-year-later> Acesso em: 10 mai. 2012.

FARRELL, Theo; TERRIFF, Terry. **The Sources of Military Changes: culture, politics, technology.** London: Lynne Rienner Publishers, 2002. ISBN 1-55587-975-6.

GIBSON, William. **Neuromancer**. 4. ed. São Paulo: Aleph, 2008. ISBN 978-85-7657-049-3.

HEICKERÖ, Roland. **Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations**. FOI Swedish Defence Research Agency, Stockholm, mar. 2010. Disponível em: <http://www2.foi.se/rapp/foir2970.pdf> Acesso em 15 jun 2012.

LIANG Quiao; XIANGSUI Wang. Unrestricted Warfare. Beijing: PLA Literature and Arts Publishing House, 1999. Disponível em: <http://www.c4i.org/unrestricted.pdf> Acesso em 1 jun. 2012.

LYNN III, William J. **Defending a new domain: the Pentagon´s Cyberstrategy**. Foreign Affairs Magazine, setembro / outubro 2010. Disponível em: <http://www. foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain#>. Acesso em: 10 mai. 2012.

MANDARINO JÚNIOR, Raphael. **Segurança e Defesa do Espaço Cibernético Brasileiro**. 1. ed. Recife: Cubzac, 2010. ISBN: 978-85-61293-13-0.

MIRANDA, André Luís Novaes. Entrevista concedida ao autor em 6 de junho de 2012, constante do Apêndice E.

MCAFEE. **Virtual Criminology Report – Cybercrime: the next wave**. Santa Clara, Califórnia: 2007. Disponível em <http://www.mcafee.com/us/research/ criminology_report/default.html> Acesso em 17 dez. 2009.

McQUAID, James. **The RBN Operatives Who Attacked Georgia.** 18 ago. 2008. Disponível em: <http://securehomenetwork.blogspot.com.br/2008/08/rbn-operatives-who-attacked-georgia.html> Acesso em 4 jun. 2012.

NORTHROP GRUMMAN. **Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation**. McLean, Virgínia: 2009. Disponível em: <http:// www.uscc.gov/researchpapers/2009/ NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf > Acesso em 20 mar. 2010.

PUFENG, Wang. **Challenge of Information Warfare. Chinese Views of Future Warfare**. Institute for National Strategic Studies, National Defense University. Washington D.C., 1997. National Defense University Press. Disponível em <http://www.au.af.mil/au/awc/awcgate/ndu/chinview/chinacont.html> Acesso em 5 jun. 2012.

RESENDE-SANTOS, João. **Neorealism, States, and the Modern Mass Army**. New York: Cambridge University Press, 2007. ISBN 978-0-511-34293-6.

RUSSIA. Ministério da Defesa. Moscow, 2011. **Visões conceituais sobre as ações das Forças Armadas da Federação da Rússia no espaço de informação**. Disponível em: < http://www.ens.mil.ru/science/publications/more.htm?id=10845074 @cmsArticle>. Acesso em 15 abr. 2012.

SHAKARIAN, Paulo. **Análise da Campanha Cibernética da Rússia Contra a Geórgia, em 2008**. MILITARY REVIEW Edição Brasileira Novembro-Dezembro 2011. Disponível em: <http://usacac.army.mil/CAC2/MilitaryReview/Archives/ Portuguese/MilitaryReview_20111231_art011POR.pdf>. Acesso em: 27 mai. 2012.

SILVA, Carlos Alberto Pinto. **Guerra Assimétrica: adaptação para o êxito militar**. Padeceme nº 15. Rio de Janeiro: Escola de Comando e Estado-Maior do Exército, 2007.

SILVA, M. M. ; TARANTI, C. G. R. **Ameaça Cibernética e Segurança da Informação**. São José dos Campos, 2003. Disponível em: <http:// www.defesanet.com.br/docs/cgsi.pdf>. Acesso em: 15 dez. 2009.

SMITH, Rupert. **The Utility of Force: the Art of War in the Modern World**. New York: Alfred A. Knopf, 2007. eISBN: 978-0-307-26741-2

THOMAS, Timothy L. **Comparing US, Russian, and Chinese Information Operations Concepts**. Foreign Military Studies Office Fort Leavenworth, KS, 2004. Disponível em: <http://www.dodccrp.org/events/2004_CCRTS/CD/papers/064.pdf> Acesso em 20 abr. 2012.

THOMAS, Timothy L. **Like Adding Wings to the Tiger: Chinese Information War Theory and Practice**. Foreign Military Studies Office Fort Leavenworth, KS. Disponível em: < http://fmso.leavenworth.army.mil/documents/chinaiw.htm> Acesso em 20 abr. 2012.

THOMAS, Timothy L. The Russian Military Today and Tomorrow. **Russian Information Warfare Theory**: The Consequences of August 2008. Strategic Studies Institute of the U.S. Army War College, 2010. Disponível em: < http://www. strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=997>. Acesso em: 12 nov. 2011.

TOFLER, Alvin. **A Terceira Onda**. 25. ed., São Paulo: Record; 2001, 491p. ISBN: 8501017973.

WEBSTER, Stephen C. **Military's 'persona' software cost millions, used for 'classified social media activities'**. The Raw History. Disponível em: < http://www.rawstory.com/rs/2011/02/22/exclusive-militarys-persona-software-cost-millions-used-for-classified-social-media-activities/>. Acesso em: 07 jul. 2011.

## APÊNDICE A

Memento Comentado de Análise de Guerra Cibernética

(grau de sigilo)

Exemplar Nr ___ de ___cópias
Comando Conjunto ___
Local do Posto de Comando
Grupo Data-Hora (expedição)
Referência de Mensagem: “XXX-XX”

**ANÁLISE DE GUERRA CIBERNÉTICA (MEMENTO COMENTADO)**
(normalmente Adendo X ao Apêndice Y (GUERRA CIBERNÉTICA) ao Anexo Z (PLANO De OPERAÇÕES DE INFORMAÇÃO) ao plano Operacional XXXX

Referências: a. Diretriz (do escalão superior);
b. Mapas e cartas; e
c. Outros documentos relevantes que tenham servido de base ao exame.

### 1. ANÁLISE DA MISSÃO

#### 1.1 Enunciado da missão

Novo enunciado da missão do escalão considerado, retirado da Diretriz de Planejamento do Comandante do Comando Conjunto.

#### 1.2 Intenção do comandante

Retirada da Diretriz de Planejamento do Comandante do Comando Conjunto.

#### 1.3 Premissas

Retiradas do PEECFA correspondente (somente aquelas que afetam o planejamento das ações de Guerra Cibernética).

#### 1.4 Enunciado da missão para a Guerra Cibernética

Missão atribuída à Guerra Cibernética, no contexto das operações militares a serem planejadas pelo Comando Conjunto.

Exemplo:

Executar ações de exploração, ataque e proteção cibernética em apoio às operações militares no TO SAFIRA.

### 2. A SITUAÇÃO E SUA COMPREENSÃO

#### 2.1 Características da área de operações

Aqui são transcritas informações sobre a área de operações que afetam o planejamento de guerra cibernética, retiradas de Levantamentos Estratégicos de Área (LEA), planos e outros documentos de inteligência.

Exemplo:

**a. Centros populacionais**

Relacionar os centros populacionais que, por seu porte, sugerem a possibilidade de serem utilizados como pontos de apoio para possíveis ações cibernéticas hostis.

**b. Instalações estratégicas**

Relacionar as instalações que tenham seu funcionamento baseado em redes de computadores conectadas ou não à *Internet*, passíveis de serem afetadas por ações de Guerra Cibernética que tragam vantagem militar imediata para o Comando Conjunto, tais como refinarias, Sistemas de Radares, instalações que desenvolvam atividades especiais, empresas de transporte e de logística, portos, aeroportos, indústrias de material de defesa, Sistemas de C2 do governo e do Ministério da Defesa adversos, Sistemas de C2 dos comandos das Forças Armadas adversas, Sistemas de C2 desdobrados em apoio às operações militares adversas, dentre outros, que possam ser relacionados como possíveis alvos para as ações de Guerra Cibernética.

**2.2 Forças inimigas**

Relacionar informações sobre a existência de doutrina e estruturas inimigas dedicadas à atividade de Guerra Cibernética, retiradas dos documentos de Inteligência.

**2.3 Nossas forças**

Citar os meios de Guerra Cibernética adjudicados ao Comando Conjunto.

**2.4 Forças amigas**

Citar os meios de defesa cibernética dos comandos da Marinha, do Exército e da Aeronáutica, não empregados no TO.

**3. ANÁLISE**

**3.1 Possibilidades do inimigo**

Relacionar as possibilidades do inimigo no que diz respeito à Guerra Cibernética, com base nos documentos de Inteligência.

**3.2 Nossas linhas de ação**

Descrever o emprego das ações de Guerra Cibernética para cada linha de ação operacional elaborada.

Exemplo:

**a. Linha de Ação Nr 1**

[...]

**b. Linha de Ação Nr 2**

**1) Numa primeira fase**

Desde já.

Empregar o Destacamento Conjunto de Guerra Cibernética (Dst Cj G Ciber) para:

- realizar ações de proteção cibernética das redes computacionais que dão suporte ao sistema de C2 do Comando do TO SAFIRA;

- contribuir para a proteção cibernética das infraestruturas críticas nacionais localizadas no interior do TO SAFIRA, com o propósito de buscar a garantia de sua segurança e de seu funcionamento;

- realizar ações de exploração cibernética para identificar vulnerabilidades nas redes de computadores dos sistemas militares e das infraestruturas críticas do inimigo, de interesse para a missão do TO SAFIRA, com vistas ao planejamento das ações de ataque cibernético; e

- realizar ações de exploração e ataque cibernéticos em proveito das campanhas de operações psicológicas, dentro do contexto das operações de informação.

- apoiar as atividades de Com Soc, Op Psc e Inteligência realizando a coleta e monitoração de sites, redes sociais e serviços da Internet de interesse por intermédio de ferramentas especializadas.

**2) Numa segunda fase**

a) Mediante ordem, empregar o Dst Cj G Ciber para realizar ações de ataque cibernético, colaborando com o esforço de interdição e com a conquista da superioridade aérea, em alvos de interesse do TO SAFIRA.

b) Continuar empregando o Dst Cj G Ciber para:

- realizar ações de proteção cibernética das redes computacionais que dão suporte ao sistema de C2 do Comando do TO SAFIRA;

- contribuir para a proteção cibernética das infraestruturas críticas nacionais localizadas no interior do TO SAFIRA, com o propósito de buscar a garantia de sua segurança e de seu funcionamento; e

- realizar ações de exploração cibernética para identificar vulnerabilidades nas redes de computadores dos sistemas militares e das infraestruturas críticas do inimigo, de interesse para a missão do TO SAFIRA, com vistas ao planejamento das ações de ataque cibernético.

- apoiar as atividades de Com Soc, Op Psc e Inteligência realizando a coleta e monitoração de sites, redes sociais e serviços da Internet de interesse por intermédio de ferramentas especializadas.

**3) Numa terceira fase**

a) Mediante ordem, empregar o Dst Cj G Ciber para realizar ações de ataque cibernético em alvos de interesse das ações ofensivas da FTC, em apoio à conquista dos objetivos impostos.

b) Continuar empregando o Dst Cj G Ciber para:

- realizar ações de proteção cibernética das redes computacionais que dão suporte ao sistema de C2 do Comando do TO SAFIRA ;

- contribuir para a proteção cibernética das infraestruturas críticas nacionais localizadas no interior do TO, com o propósito de buscar a garantia de sua segurança e de seu funcionamento; e

- realizar ações de exploração cibernética para identificar vulnerabilidades nas redes de computadores dos sistemas militares e das infraestruturas críticas do inimigo, de interesse para a missão do TO SAFIRA, com vistas ao planejamento das ações de ataque cibernético.

- apoiar as atividades de Com Soc, Op Psc e Inteligência realizando a coleta e monitoração de sites, redes sociais e serviços da Internet de interesse por intermédio de ferramentas especializadas.

**4) Numa quarta fase**

Iniciar a desmobilização do Dst Cj G Ciber.

**c. Linha de Ação Nr 3**

[...]

### 3.3 Análise

Analisar o emprego das ações de Guerra Cibernética para cada linha de ação operacional elaborada, tendo como parâmetros a quantidade e a complexidade das ações a serem realizadas.

Exemplo:

**a. Linha de Ação Nr 1**

[…]

**b. Linha de Ação Nr 2**

Esta Linha de Ação é dividida em 4 (quatro) fases. Na primeira fase, o Dst Cj G Ciber é empregado, desde já, para realizar ações de proteção cibernética das redes computacionais que dão suporte ao sistema de C2 do Comando do TO SAFIRA e para contribuir para a proteção cibernética das infraestruturas críticas nacionais localizadas no interior do TO. É empregado, também, para realizar ações de exploração cibernética para identificar vulnerabilidades, com vistas ao planejamento das ações de ataque cibernético, além de realizar ações de exploração e de ataque cibernéticos em proveito das campanhas de operações psicológicas.

Numa segunda fase, mediante ordem, o Dst Cj G Ciber é empregado para realizar ações de ataque cibernético, colaborando com o esforço de interdição e com a conquista da superioridade aérea, em alvos de interesse do TO SAFIRA. O Dst Cj G Ciber continua sendo empregado para realizar ações de proteção cibernética das redes computacionais que dão suporte ao sistema de C2 do Comando do TO SAFIRA e para contribuir para a proteção cibernética das infraestruturas críticas nacionais localizadas no interior do TO. Continua sendo empregado, também, para realizar ações de exploração cibernética para identificar vulnerabilidades, com vistas ao planejamento das ações de ataque cibernético.

Numa terceira fase, mediante ordem, o Dst Cj G Ciber é empregado para realizar ações de ataque cibernético em alvos de interesse das ações ofensivas da FTC, totalizando 3 (três) objetivos. O Dst Cj G Ciber continua sendo empregado para realizar ações de proteção cibernética das redes computacionais que dão suporte ao sistema de C2 do Comando do TO SAFIRA e para contribuir para a proteção cibernética das infraestruturas críticas nacionais localizadas no interior do TO. Continua sendo empregado, também, para realizar ações de exploração cibernética

para identificar vulnerabilidades, com vistas ao planejamento das ações de ataque cibernético e apoiar as atividades de Com Soc, Op Psc e Inteligência realizando a coleta e monitoração de sites, redes sociais e serviços da Internet de interesse por intermédio de ferramentas especializadas.

Numa quarta fase, tem início a desmobilização do Dst Cj G Ciber.

**c. Linha de Ação Nr 3**

[...]

**3.4 Conclusão parcial**

Tirar conclusões sobre as linhas de ação elaboradas para o emprego das ações de Guerra Cibernética, quanto à sua complexidade.

Exemplo:

A Linha de Ação Nr 2 é a mais complexa, não apenas por ser dividida em 4 (quatro) fases, mas também por envolver o planejamento e a execução de um maior número de ações cibernéticas, particularmente ações de ataque cibernético em apoio à conquista de 3 (três) objetivos em direções distintas, que são ações mais críticas e dependem do sucesso das ações de exploração cibernética.

## 4. CONCLUSÕES

**4.1 Priorização das linhas de ação para a Guerra cibernética**

Relacionar as linhas de ação operacionais, na ordem de prioridade, quanto ao emprego das ações de guerra cibernética.

**4.2 Lista preliminar de possíveis alvos para ações de exploração e de ataque cibernéticos**

Relacionar os possíveis alvos para as ações de exploração e de ataque cibernéticos, existentes no interior do TO, com base no estudo realizado (Características da Área de Operações).

**4.3 Sistemas de C2 e infraestruturas críticas a serem protegidas**

Relacionar os nossos sistemas de C2 e infraestruturas críticas, existentes no interior do TO, que necessitam ser protegidos por ações de proteção cibernética.

## 5. NECESSIDADES DE INTELIGÊNCIA

Levantar as necessidades de conhecimento, a respeito do inimigo, sobre doutrina, estruturas inimigas dedicadas à atividade de Guerra Cibernética e possíveis alvos (sistemas e infraestruturas) para as ações de exploração e ataque cibernético, dentre outros.

Esse levantamento deverá ser informado à Seção de Inteligência, para que seja incluído como Necessidade de Inteligência (NI) no Plano de Obtenção de Conhecimentos (POC) do Comando Conjunto.

# APÊNDICE B

Exemplo de Análise de Guerra Cibernética

(grau de sigilo)

Exemplar Nr ___ de ___cópias
Comando Conjunto SAFIRA
ESMERALDA/MO
Grupo Data-Hora (expedição)
Referência de Mensagem:
"XXX-XX"

## ANÁLISE DE GUERRA CIBERNÉTICA (UM EXEMPLO)

Referências: a. Diretriz de Planejamento do Comandante do TO SAFIRA;
b. Mapas Operação SAFIRA escala 1:2.400.000; e
c. Anexo de Inteligência ao Plano Operacional SAFIRA.

## 1. ANÁLISE DA MISSÃO

### 1.1 Enunciado da missão

Mediante ordem do Comandante Supremo, realizar operações militares no TO SAFIRA, a fim de garantir a soberania nacional, o patrimônio, a integridade territorial brasileira e a salvaguarda das pessoas, dos bens e dos interesses brasileiros na área de conflito.

### 1.2 Intenção do comandante

Tenho a intenção de:

**- durante a crise**, ampliar a presença na faixa de fronteira com o País VERDE, aumentar o controle aéreo e fluvial na região fronteiriça e intensificar ações de inteligência e Operações psicológicas;

**- durante o conflito armado**, proteger os nacionais em território verdense, próximos à faixa de fronteira; neutralizar as forças inimigas que possam interferir nas ações; produzir o menor número de baixas aos militares, minimizar os danos colaterais à população civil e ao meio ambiente; preservar, sempre que possível, o funcionamento das infraestruturas críticas verdenses e terminar o conflito em curto prazo, com o menor esforço de guerra possível; e

**- no restabelecimento da paz**, participar, no que for possível, na reconstrução das áreas afetadas pelo conflito.

### 1.3 Premissas

a. Minimizar os danos colaterais à população civil.

b. Garantir a segurança e o funcionamento das infraestruturas críticas nacionais no interior do TO.

c. Preservar, sempre que possível, o funcionamento das infraestruturas críticas do País VERDE no interior do TO.

**1.4 Enunciado da missão para a Guerra Cibernética**

Executar ações de exploração, ataque e proteção cibernética em apoio às operações militares no TO SAFIRA.

## 2. A SITUAÇÃO E SUA COMPREENSÃO

### 2.1 Características da área de operações

**a. Centros populacionais**

Importantes centros populacionais podem ser citados na região fronteiriça, no território País VERDE, como pontos de apoio a possíveis ações cibernéticas hostis: as cidades de PEDRA/POMBA, a cidade de ROCHA/BICA e a cidade de PORTO BELO/DOURADO.

**b. Instalações estratégicas**

**1) Refinarias**

- Refinaria "Amendoeira"
- Refinaria de Boqueirão (PETROVERDE)
- Refinaria da Mata
- Refinaria "Molusco"
- Refinaria "Rocha"
- Refinaria "Violeta"

**2) Sistema de Radares e de Defesa**

**a) Zona Norte de Defesa**

- Base Áerea de ADANS
- Base Aérea de PUMA
- Base Aérea de BOQUEIRÃO
- Base Aérea de MUMO

**b) Zona Central de Defesa**

- Base Aérea de PALMEIRA
- Aeroporto Internacional "Bento Carneiro"

**c) Zona Sul de Defesa**

- Base Aérea de JOIALA
- PATIMA
- ARROIO VELHO
- RIO MORTO
- Base Aérea de CERRADO

**3) Instalações especiais**

- Base Aeroespacial "Marisco", localizada em RATUNA, ao S de VENTURA.

- Estação de recebimento de sinais de satélite, localizada no distrito de SANTA CLARA, próximo de MINEIRO/CABALA.

- Estações de radar em FONTANA/POMBA, instalada pelos norte-austrais para controle do tráfego aéreo na região.

- Centro Nuclear de Matagal, em CAVALINHO, a 42 km de VENTURA.

**4) Linhas de transporte e de suprimento**

**a) Estatais que atuam no setor de transportes**

- Corporação Verdense de Aeroportos e Aviação Comercial (CORVAC) que é a empresa encarregada da supervisão e administração da infraestrutura aeroportuária.

- Empresa Nacional de Portos de Verde (ENAPO VERDE S/A), encarregada do controle e administração da infraestrutura portuária.

**b) Modal ferroviário**

- Consórcio Ferrovia Central Corubense.
- Ferrovia Transcorubense, operada pela Verde Rail.
- Empresa Planaltense.
- Empresa estatal ENAPO.

**c) Modal dutoviário**

- Operadora do Oleoduto Planaltino.

**d) Modal aquaviário**

- Consórcio Verdense S.A.
- PWZ.
- Calamares S.A.
- Mundial Transportes Marítimos.

**e) Portos fluviais**

- PEDRA na Região de POMBA.
- ROCHA, em BICA.
- FONTANA, em SÃO JOSÉ.
- BELA (DOURADO).

**f) Porto lacustre**

- PONTÃO, no CHIXICOCO.

**g) Portos marítimos**

- BOQUEIRÃO, em PUMA.
- PATUQUE, em PUMA.
- BAÍA NEGRA, em PUMA.
- TICUNA, em NOVA LIBERDADE.
- DUMBO, em SÃO JOÃO.
- CABALA, em VENTURA.
- SÃO JOSÉ, em TEBAS.
- DANDARA, em VENTURA.
- DAMIÃO, em ARARAS.
- RIO MORTO, em MUQUECA.

**h) Aeroportos**

- Aeroporto Internacional Bento Carneiro, em VENTURA.

- Aeroportos de QUINDIM, ARARAS, PATIMA, MOLA e PORTO BELO.

**5) Indústria Militar de Defesa**

- EXPLOVERDE S.A.
- FAPOLVE (Fábrica de Pólvora de Verde S.A.).
- MANASA (Manutenção Naval S.A.).
- TECSERVICE (Serviços Técnicos S.A.).
- FAMAVE (Fábrica de Armas Verdense).

**c. Alvos militares ou ligados à defesa**

- Sistemas de C2 do governo e do Ministério da Defesa verdenses.
- Sistemas de C2 dos comandos das Forças Armadas verdenses.
- Sistemas de C2 desdobrados em apoio às operações militares verdenses.

**2.2 Forças inimigas**

a. Não existem informações sobre a existência de doutrina e estruturas inimigas dedicadas à atividade de Guerra Cibernética.

b. O inimigo possui baixo nível tecnológico para conduzir atividades de comando e controle, comprometendo sua capacidade de realizar ações cibernéticas de forma organizada.

**2.3 Nossas forças**

a. Existe a necessidade de organizar um Destacamento de Guerra Cibernética (Dst Cj G Ciber), integrado por militares das três Forças, tendo por base o 19º Centro de Telemática de Área (19º CTA), possuindo capacidade de realizar Exploração, Ataque e Proteção Cibernética, para apoiar em Guerra Cibernética o TO SAFIRA.

b. O Dst Cj G Ciber deverá ser desdobrado junto ao Comando do TO SAFIRA, em um grande centro urbano, como a cidade de ESMERALDA/MO, tendo em vista a necessidade de estar localizado em um local que possua as condições técnicas necessárias para a execução das ações de Guerra Cibernética.

c. O Dst Cj G Ciber precisa estar diretamente subordinado ao Comandante do TO SAFIRA, em razão da necessidade de centralização da decisão quanto às ações de ataque cibernético e de que sua execução seja determinada pela maior autoridade do TO.

d. Sugere-se que o Dst Cj G Ciber possua a seguinte constituição organizacional mínima:

1) Comandante;
2) Estado-Maior;
3) Seção de Inteligência Cibernética;
4) Seção de Operações Cibernéticas;

e. O detalhamento da estrutura e o efetivo do Dst Cj G Ciber deverá ser definido e proposto após estudo específico elaborado por seu comandante.

f. O Dst Cj G Ciber poderá contar, a critério do seu comandante e da disponibilidade, com elementos de outras agências do Governo e/ou especialistas civis para operação assistida de sistemas computacionais e outras funções especializadas julgadas necessárias.

**2.4 Forças amigas**

a. Meios de defesa cibernética dos comandos da Marinha, do Exército e da Aeronáutica, não empregados no TO SAFIRA.

b. É importante que seja estabelecida ligação, com a finalidade de coordenação, com o Departamento de Segurança da Informação e Comunicações (DSIC) do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), órgão responsável, no nível político, pela Segurança da Informação e Comunicações (SIC), bem como pela Segurança Cibernética, abrangendo a Administração Pública Federal (APF), direta e indireta, além das infraestruturas críticas da informação nacionais dos setores público e privado.

## 3. ANÁLISE

**3.1 Possibilidades do inimigo**

Não foram identificadas doutrina, estrutura ou capacidades de Guerra Cibernética pelo inimigo. No entanto, podem ocorrer tentativas isoladas e não sistematizadas de realizar ações cibernéticas (exploração, proteção e ataque) em nossos sistemas de C2 e infraestruturas críticas cujo funcionamento seja baseado em redes de computadores, dentro ou fora do TO.

**3.2 Nossas linhas de ação**

**a. Linha de Ação Nr 1**

**1) Numa primeira fase**

Desde já.

Empregar o Destacamento de Guerra Cibernética (Dst Cj G Ciber) para:

- realizar ações de proteção cibernética das redes computacionais que dão suporte ao sistema de C2 do Comando do TO SAFIRA;

- contribuir para a proteção cibernética das infraestruturas críticas nacionais localizadas no interior do TO SAFIRA, com o propósito de buscar a garantia de sua segurança e de seu funcionamento;

- realizar ações de exploração cibernética para identificar vulnerabilidades nas redes de computadores dos sistemas militares e das infraestruturas críticas do inimigo, de interesse para a missão do TO SAFIRA, com vistas ao planejamento das ações de ataque cibernético; e

- realizar ações de exploração e ataque cibernéticos em proveito das campanhas de operações psicológicas, dentro do contexto das operações de informação.

- apoiar as atividades de Com Soc, Op Psc e Inteligência realizando a coleta e monitoração de sites, redes sociais e serviços da Internet de interesse por intermédio de ferramentas especializadas.

**2) Numa segunda fase**

a) Mediante ordem, empregar o Dst Cj G Ciber para realizar ações de ataque cibernético, colaborando com o esforço de interdição, em alvos de interesse do TO SAFIRA.

b) Continuar empregando o Dst Cj G Ciber para:

- realizar ações de proteção cibernética das redes computacionais que dão suporte ao sistema de C2 do Comando do TO SAFIRA;

- contribuir para a proteção cibernética das infraestruturas críticas nacionais localizadas no interior do TO, com o propósito de buscar a garantia de sua segurança e de seu funcionamento; e

- realizar ações de exploração cibernética para identificar vulnerabilidades nas redes de computadores dos sistemas militares e das infraestruturas críticas do inimigo, de interesse para a missão do TO SAFIRA, com vistas ao planejamento das ações de ataque cibernético.

- apoiar as atividades de Com Soc, Op Psc e Inteligência realizando a coleta e monitoração de sites, redes sociais e serviços da Internet de interesse por intermédio de ferramentas especializadas.

**3) Numa terceira fase**

Iniciar a desmobilização do Dst Cj G Ciber.

**b. Linha de Ação Nr 2**

**1) Numa primeira fase**

Desde já.

Empregar o Destacamento de Guerra Cibernética (Dst Cj G Ciber) para:

- realizar ações de proteção cibernética das redes computacionais que dão suporte ao sistema de C2 do Comando do TO SAFIRA;

- contribuir para a proteção cibernética das infraestruturas críticas nacionais localizadas no interior do TO SAFIRA, com o propósito de buscar a garantia de sua segurança e de seu funcionamento;

- realizar ações de exploração cibernética para identificar vulnerabilidades nas redes de computadores dos sistemas militares e das infraestruturas críticas do inimigo, de interesse para a missão do TO SAFIRA, com vistas ao planejamento das ações de ataque cibernético; e

- realizar ações de exploração e ataque cibernéticos em proveito das campanhas de operações psicológicas, dentro do contexto das operações de informação.

- apoiar as atividades de Com Soc, Op Psc e Inteligência realizando a coleta e monitoração de sites, redes sociais e serviços da Internet de interesse por intermédio de ferramentas especializadas.

**2) Numa segunda fase**

a) Mediante ordem, empregar o Dst Cj G Ciber para realizar ações de ataque cibernético, colaborando com o esforço de interdição e com a conquista da superioridade aérea, em alvos de interesse do TO SAFIRA.

b) Continuar empregando o Dst Cj G Ciber para:

- realizar ações de proteção cibernética das redes computacionais que dão suporte ao sistema de C2 do Comando do TO SAFIRA;

- contribuir para a proteção cibernética das infraestruturas críticas nacionais localizadas no interior do TO SAFIRA, com o propósito de buscar a garantia de sua segurança e de seu funcionamento; e

- realizar ações de exploração cibernética para identificar vulnerabilidades nas redes de computadores dos sistemas militares e das infraestruturas críticas do inimigo, de interesse para a missão do TO SAFIRA, com vistas ao planejamento das ações de ataque cibernético.

- apoiar as atividades de Com Soc, Op Psc e Inteligência realizando a coleta e monitoração de sites, redes sociais e serviços da Internet de interesse por intermédio de ferramentas especializadas.

**3) Numa terceira fase**

a) Mediante ordem, empregar o Dst Cj G Ciber para realizar ações de ataque cibernético em alvos de interesse das ações ofensivas da FTC, em apoio à conquista dos 3 (três) objetivos impostos.

b) Continuar empregando o Dst Cj G Ciber para:

- realizar ações de proteção cibernética das redes computacionais que dão suporte ao sistema de C2 do Comando do TO SAFIRA;

- contribuir para a proteção cibernética das infraestruturas críticas nacionais localizadas no interior do TO, com o propósito de buscar a garantia de sua segurança e de seu funcionamento; e

- realizar ações de exploração cibernética para identificar vulnerabilidades nas redes de computadores dos sistemas militares e das infraestruturas críticas do inimigo, de interesse para a missão do TO SAFIRA, com vistas ao planejamento das ações de ataque cibernético.

- apoiar as atividades de Com Soc, Op Psc e Inteligência realizando a coleta e monitoração de sites, redes sociais e serviços da Internet de interesse por intermédio de ferramentas especializadas.

**4) Numa quarta fase**

Iniciar a desmobilização do Dst Cj G Ciber.

**c. Linha de Ação Nr 3**

**1) Numa primeira fase**

Desde já.

Empregar o Destacamento de Guerra Cibernética (Dst Cj G Ciber) para:

- realizar ações de proteção cibernética das redes computacionais que dão suporte ao sistema de C2 do Comando do TO SAFIRA;

- contribuir para a proteção cibernética das infraestruturas críticas nacionais localizadas no interior do TO SAFIRA, com o propósito de buscar a garantia de sua segurança e de seu funcionamento;

- realizar ações de exploração cibernética para identificar vulnerabilidades nas redes de computadores dos sistemas militares e das infraestruturas críticas do inimigo, de interesse para a missão do TO SAFIRA, com vistas ao planejamento das ações de ataque cibernético; e

- realizar ações de exploração e ataque cibernéticos em proveito das campanhas de operações psicológicas, dentro do contexto das operações de informação.

- apoiar as atividades de Com Soc, Op Psc e Inteligência realizando a coleta e monitoração de sites, redes sociais e serviços da Internet de interesse por intermédio de ferramentas especializadas.

**2) Numa segunda fase**

a) Mediante ordem, empregar o Dst Cj G Ciber para realizar ações de ataque cibernético, colaborando com o esforço de interdição e com a conquista da superioridade aérea, em alvos de interesse do TO SAFIRA.

b) Continuar empregando o Dst Cj G Ciber para:

- realizar ações de proteção cibernética das redes computacionais que dão suporte ao sistema de C2 do Comando do TO SAFIRA;

- contribuir para a proteção cibernética das infraestruturas críticas nacionais localizadas no interior do TO SAFIRA, com o propósito de buscar a garantia de sua segurança e de seu funcionamento; e

- realizar ações de exploração cibernética para identificar vulnerabilidades nas redes de computadores dos sistemas militares e das infraestruturas críticas do inimigo, de interesse para a missão do TO SAFIRA, com vistas ao planejamento das ações de ataque cibernético.

- apoiar as atividades de Com Soc, Op Psc e Inteligência realizando a coleta e monitoração de sites, redes sociais e serviços da Internet de interesse por intermédio de ferramentas especializadas.

**3) Numa terceira fase**

a) Mediante ordem, empregar o Dst Cj G Ciber para realizar ações de ataque cibernético em alvos de interesse das ações ofensivas da FTC, em apoio à conquista do objetivo imposto.

b) Continuar empregando o Dst Cj G Ciber para:

- realizar ações de proteção cibernética das redes computacionais que dão suporte ao sistema de C2 do Comando do TO SAFIRA A;

- contribuir para a proteção cibernética das infraestruturas críticas nacionais localizadas no interior do TO SAFIRA, com o propósito de buscar a garantia de sua segurança e de seu funcionamento; e

- realizar ações de exploração cibernética para identificar vulnerabilidades nas redes de computadores dos sistemas militares e das infraestruturas críticas do inimigo, de interesse para a missão do TO SAFIRA, com vistas ao planejamento das ações de ataque cibernético.

- apoiar as atividades de Com Soc, Op Psc e Inteligência realizando a coleta e monitoração de sites, redes sociais e serviços da Internet de interesse por intermédio de ferramentas especializadas.

**4) Numa quarta fase**

Iniciar a desmobilização do Dst Cj G Ciber.

## 3.3 Análise

**a. Linha de Ação Nr 1**

Esta Linha de Ação é dividida em 3 (três) fases. Na primeira fase, o Dst Cj G Ciber é empregado, desde já, para realizar ações de proteção cibernética das redes computacionais que dão suporte ao sistema de C2 do Comando do TO SAFIRA e para contribuir para a proteção cibernética das infraestruturas críticas nacionais localizadas no interior do TO. É empregado, também, para realizar ações de exploração cibernética para identificar vulnerabilidades, com vistas ao planejamento das ações de ataque cibernético, além de realizar ações de exploração e de ataque cibernéticos em proveito das campanhas de operações psicológicas, dentro do contexto das operações de informação.

Numa segunda fase, mediante ordem, o Dst Cj G Ciber é empregado para realizar ações de ataque cibernético, colaborando com o esforço de interdição. O Dst Cj G Ciber continua sendo empregado para realizar ações de proteção cibernética das redes computacionais que dão suporte ao sistema de C2 do Comando do TO SAFIRA e para contribuir para a proteção cibernética das infraestruturas críticas nacionais localizadas no interior do TO. Continua sendo empregado, também, para realizar ações de exploração cibernética para identificar vulnerabilidades, com vistas ao planejamento das ações de ataque cibernético e para apoiar as atividades de Com Soc, Op Psc e Inteligência realizando a coleta e monitoração de sites, redes sociais e serviços da Internet de interesse por intermédio de ferramentas especializadas.

Numa terceira fase, tem início a desmobilização do Dst Cj G Ciber.

**b. Linha de Ação Nr 2**

Esta Linha de Ação é dividida em 4 (quatro) fases. Na primeira fase, o Dst Cj G Ciber é empregado, desde já, para realizar ações de proteção cibernética das redes computacionais que dão suporte ao sistema de C2 do Comando do TO SAFIRA e para contribuir para a proteção cibernética das infraestruturas críticas nacionais localizadas no interior do TO. É empregado, também, para realizar ações de exploração cibernética para identificar vulnerabilidades, com vistas ao planejamento das ações de ataque cibernético, além de realizar ações de exploração e de ataque cibernéticos em proveito das campanhas de operações psicológicas, dentro do contexto das operações de informação.

Numa segunda fase, mediante ordem, o Dst Cj G Ciber é empregado para realizar ações de ataque cibernético, colaborando com o esforço de interdição e com a conquista da superioridade aérea, em alvos de interesse do TO SAFIRA. O Dst Cj G Ciber continua sendo empregado para realizar ações de proteção cibernética das redes computacionais que dão suporte ao sistema de C2 do Comando do TO SAFIRA e para contribuir para a proteção cibernética das infraestruturas críticas nacionais localizadas no interior do TO. Continua sendo empregado, também, para realizar ações de exploração cibernética para identificar vulnerabilidades, com vistas ao planejamento das ações de ataque cibernético.

Numa terceira fase, mediante ordem, o Dst Cj G Ciber é empregado para realizar ações de ataque cibernético em alvos de interesse das ações ofensivas da FTC, totalizando 3 (três) objetivos. O Dst Cj G Ciber continua sendo empregado para realizar ações de proteção cibernética das redes computacionais que dão suporte ao sistema de C2 do Comando do TO SAFIRA e para contribuir para a proteção cibernética das infraestruturas críticas nacionais localizadas no interior do TO.

Continua sendo empregado, também, para realizar ações de exploração cibernética para identificar vulnerabilidades, com vistas ao planejamento das ações de ataque cibernético e apoiar as atividades de Com Soc, Op Psc e Inteligência realizando a coleta e monitoração de sites, redes sociais e serviços da Internet de interesse por intermédio de ferramentas especializadas.

Numa quarta fase, tem início a desmobilização do Dst Cj G Ciber.

**c. Linha de Ação Nr 3**

Esta Linha de Ação é dividida em 4 (quatro) fases. Na primeira fase, o Dst Cj G Ciber é empregado, desde já, para realizar ações de proteção cibernética das redes computacionais que dão suporte ao sistema de C2 do Comando do TO SAFIRA e para contribuir para a proteção cibernética das infraestruturas críticas nacionais localizadas no interior do TO. É empregado, também, para realizar ações de exploração cibernética para identificar vulnerabilidades, com vistas ao planejamento das ações de ataque cibernético, além de realizar ações de exploração e de ataque cibernéticos em proveito das campanhas de operações psicológicas, dentro do contexto das operações de informação.

Numa segunda fase, mediante ordem, o Dst Cj G Ciber é empregado para realizar ações de ataque cibernético, colaborando com o esforço de interdição e com a conquista da superioridade aérea, em alvos de interesse do TO SAFIRA. O Dst Cj G Ciber continua sendo empregado para realizar ações de proteção cibernética das redes computacionais que dão suporte ao sistema de C2 do Comando do TO SAFIRA e para contribuir para a proteção cibernética das infraestruturas críticas nacionais localizadas no interior do TO. Continua sendo empregado, também, para realizar ações de exploração cibernética para identificar vulnerabilidades, com vistas ao planejamento das ações de ataque cibernético.

Numa terceira fase, mediante ordem, o Dst Cj G Ciber é empregado para realizar ações de ataque cibernético em alvos de interesse das ações ofensivas da FTC, totalizando 1 (um) objetivo. O Dst Cj G Ciber continua sendo empregado para realizar ações de proteção cibernética das redes computacionais que dão suporte ao sistema de C2 do Comando do TO SAFIRA e para contribuir para a proteção cibernética das infraestruturas críticas nacionais localizadas no interior do TO. Continua sendo empregado, também, para realizar ações de exploração cibernética para identificar vulnerabilidades, com vistas ao planejamento das ações de ataque cibernético e apoiar as atividades de Com Soc, Op Psc e Inteligência realizando a coleta e monitoração de sites, redes sociais e serviços da Internet de interesse por intermédio de ferramentas especializadas.

Numa quarta fase, tem início a desmobilização do Dst Cj G Ciber.

## 3.4 Conclusão parcial

A Linha de Ação Nr 1 é a mais simples de ser apoiada, não apenas por ser dividida em apenas 3 (três) fases, mas também por envolver o planejamento e a execução de menos ações cibernéticas, particularmente ações de ataque cibernético, que são ações mais críticas e dependem do sucesso das ações de exploração cibernética.

A Linha de Ação Nr 2 é a mais complexa, não apenas por ser dividida em 4 (quatro) fases, mas também por envolver o planejamento e a execução de um maior número de ações cibernéticas, particularmente ações de ataque cibernético em

apoio à conquista de 3 (três) objetivos em direções distintas, que são ações mais críticas e dependem do sucesso das ações de exploração cibernética.

A Linha de Ação Nr 3 possui complexidade menor que a Linha de Ação Nr 2. Apesar de também ser dividida em 4 (quatro) fases, envolve o planejamento e a execução de um menor número de ações cibernéticas em relação à Linha de Ação Nr 2, particularmente ações de ataque cibernético em apoio à conquista de 1 (um) objetivo.

## 4. CONCLUSÕES

### 4.1 Priorização das linhas de ação para a Guerra cibernética

a. Primeira prioridade: Linha de Ação Nr 1.
b. Segunda prioridade: Linha de Ação Nr 3.
c. Terceira prioridade: Linha de Ação Nr 2.

### 4.2 Lista preliminar de possíveis alvos para ações de exploração e de ataque cibernéticos

É necessário que se faça um levantamento e identificação dos possíveis alvos para as ações de exploração e de ataque cibernéticos, existentes no interior do TO SAFIRA. Dentre tais, foram levantados, preliminarmente, os seguintes:

a. Sistemas de vigilância e alerta aéreo;
b. Empresas de geração e de distribuição de energia;
c. Empresas de produção e de distribuição de combustíveis;
d. Empresas de telefonia fixa e móvel;
e. Provedores de acesso à internet;
f. Sistemas militares de C2;
g. Sistemas de radares e de defesa;
h. Corporação Verdense de Aeroportos e Aviação Comercial (CORVAC), empresa encarregada da supervisão e administração da infraestrutura aeroportuária;
i. Empresa Nacional de Portos de Verde (ENAPO VERDE S/A), encarregada do controle e administração da infraestrutura portuária;
j. Empresas de transporte aeroviário, rodoviário, ferroviário e dutoviário;
k. Empresas de transporte maritimo;
l. Sistemas de C2 do governo e do Ministério da Defesa verdenses;
m. Sistemas de C2 dos comandos das Forças Armadas verdenses; e
n. Sistemas de C2 desdobrados em apoio às operações militares verdenses.

### 4.3 Sistemas de C2 e infraestruturas críticas a serem protegidas

É necessário que se faça um levantamento e identificação dos nossos sistemas de C2 e infraestruturas críticas, existentes no interior do TO SAFIRA, que necessitam ser protegidos. Dentre tais, foram levantados, preliminarmente, os seguintes:

a. Sistema de Controle do Tráfego Aéreo dos principais aeroportos;
b. Sistema de fornecimento de energia;
c. Sistema de fornecimento de água;
d. Sistemas de Comunicações (fixa e móvel, dados e voz);
e. Sistema de Proteção Espartana (SIPE);
f. Sistema de Comunicações Militares por Satélite (SISCOMIS);
g. Redes internas das Forças Armadas;

h. Sistemas relacionados às instituições bancárias; e
i. Sistemas relacionados à produção e distribuição de combustíveis.

**5. NECESSIDADES DE INTELIGÊNCIA**

5.1 Identificação e localização das capacidades inimigas de defesa cibernética, de nível estratégico.

5.2 Identificação da capacidade de guerra cibernética do inimigo, nos níveis operacional e tático.

5.3 Identificação das infraestruturas críticas verdenses, que sejam do interesse das operações militares no TO SAFIRA, tais como empresas distribuidoras de energia, combustíveis, serviços de telecomunicações, serviços aeroportuários e de transporte, dentre outras, cujo funcionamento seja baseado no emprego de redes de computadores, cujos serviços, se interrompidos ou degradados, representem vantagem militar imediata.

5.4 Levantamento e identificação das estruturas voltadas à proteção das redes de computadores dedicadas ao Sistema de C2 adverso.

5.4 Levantamento e identificação das estruturas voltadas à proteção das redes de computadores dedicadas ao Sistema de C2 adverso.

5.5 Levantamento das demandas das Op Psc quanto a (ao):

a. Rastreamento cibernético de elementos envolvidos em ataques cibernéticos;

b. Relatórios que descrevam ataques cibernéticos com informações sobre conteúdo das mensagens, ideologia dos grupos atacantes, elementos ou grupos alvo e outras informações julgadas úteis;

c. “Modus operandi” dos ataques;

## APÊNDICE C

Memento Comentado de Apêndice de Guerra Cibernética

(grau de sigilo)

Exemplar Nr ___ de ___cópias
Comando Conjunto ___
Local do Posto de Comando
Grupo Data-Hora (expedição)
Referência de Mensagem: “XXX-XX”

**APÊNDICE “X” (GUERRA CIBERNÉTICA) ao ANEXO “Y” (OPERAÇÕES de INFORMAÇÃO) ao PLANO OPERACIONAL ZZZZ**
**(MEMENTO COMENTADO)**

Referências: listar documentos e cartas utilizados no planejamento.

### 1. SITUAÇÃO

#### 1.1 Forças inimigas

Relacionar as informações sobre as forças inimigas, levantadas por ocasião da elaboração da Análise de Guerra Cibernética.

#### 1.2 Nossas forças

Relacionar as informações sobre as nossas forças, levantadas por ocasião da elaboração da Análise de Guerra Cibernética.

#### 1.3 Forças amigas

Relacionar as informações sobre as forças amigas, levantadas por ocasião da elaboração da Análise de Guerra Cibernética.

#### 1.4 Meios recebidos e retirados

Relacionar as informações sobre os meios recebidos e retirados, levantadas por ocasião da elaboração da Análise de Guerra Cibernética.

### 2. MISSÃO

Transcrever o enunciado da missão para a Guerra Cibernética, obtido por ocasião da elaboração da Análise de Guerra Cibernética.

### 3. EXECUÇÃO

#### 3.1 Premissas de emprego

Relacionar as premissas de emprego extraídas do PEECFA, levantadas por ocasião da elaboração da Análise de Guerra Cibernética.

#### 3.2 Exploração Cibernética

a. Explicitar todas as orientações que se façam necessárias para o planejamento das ações de exploração cibernética, levantadas por ocasião da elaboração da Análise de Guerra Cibernética, para o elemento de Guerra Cibernética do Comando Conjunto e para os elementos de Guerra Cibernética das Forças Componentes.

b. Levantar o relacionamento dessas ações com as operações de informação e com a Atividade de Inteligência.

**3.3 Ataque Cibernético**

Explicitar todas as orientações que se façam necessárias para o planejamento das ações de ataque cibernético, levantadas por ocasião da elaboração da Análise de Guerra Cibernética, para o elemento de Guerra Cibernética do Comando Conjunto e para os elementos de Guerra Cibernética das Forças Componentes.

**3.4 Proteção Cibernética**

a. Explicitar todas as orientações que se façam necessárias para o planejamento das ações de proteção cibernética, levantadas por ocasião da elaboração da Análise de Guerra Cibernética, para o elemento de Guerra Cibernética do Comando Conjunto e para os elementos de Guerra Cibernética das Forças Componentes.

b. Levantar o relacionamento dessas ações com a adoção de medidas de proteção cibernética por parte das infraestruturas críticas nacionais localizadas no interior do TO, com o propósito de buscar a garantia de sua segurança e de seu funcionamento, se for o caso.

**3.5 Lista preliminar de possíveis alvos para ações de exploração e de ataque cibernéticos**

Relacionar os possíveis alvos para as ações de exploração e de ataque cibernéticos, existentes no interior do TO, com base no levantamento realizado por ocasião da elaboração da Análise de Guerra Cibernética (Características da Área de Operações).

**3.6 Lista preliminar de sistemas de C2 e infraestruturas críticas a serem protegidas**

Relacionar os nossos sistemas de C2 e infraestruturas críticas, existentes no interior do TO, que necessitam ser protegidos por ações de proteção cibernética.

**3.7 Concepção geral de emprego**

Descrever a linha de ação de emprego das ações de guerra cibernética adotada, após a decisão, para o cumprimento da missão atribuída ao Comando Conjunto.

**4. LOGÍSTICA**

Citar os assuntos de logística de interesse para a guerra cibernética ou referenciar o Anexo de Logística, conforme o caso.

**5. DEMANDAS**

Transcrever as necessidades de conhecimento, a respeito do inimigo, sobre doutrina, estruturas inimigas dedicadas à atividade de Guerra Cibernética e possíveis alvos (sistemas e infraestruturas) para as ações de exploração e ataque

cibernético, dentre outros, identificadas por ocasião da elaboração da Análise de Guerra Cibernética e ainda não atendidas.

## 6. PRESCRIÇÕES DIVERSAS

### 6.1 Eventos de Coordenação e de Tomada de Decisão

a. Relacionar os eventos de coordenação e de tomada de decisão planejados pelo Comando Conjunto, dos quais o Comandante do elemento de Guerra Cibernética deva participar, tais como as reuniões do Estado-Maior Conjunto (EMC) previstas no Manual de Procedimentos de Comando e Controle para Operações Conjuntas (MD31-M-04).

b. Cabe destacar que na Reunião de Coordenação de Operações de Informação serão coordenadas as ações do elemento de Guerra Cibernética do Comando Conjunto e dos elementos de Guerra Cibernética das Forças Componentes, com o propósito de otimizar o emprego dos meios e evitar a duplicidade de esforços.

### 6.2 Integração com as Operações de Informação

Relacionar as prescrições relativas à realização de ações de guerra cibernética que poderão ser executadas em proveito das operações de informação.

### 6.3 Integração com a Atividade de Inteligência

Relacionar as prescrições quanto à realização de ações de guerra cibernética orientadas ao atendimento das Necessidades de Inteligência (NI), constantes do Plano de Obtenção de Conhecimentos (POC) do Comando Conjunto, que deverão ser solicitadas mediante a formalização de um Pedido de Inteligência (PI) pela Seção de Inteligência do Comando Conjunto, exclusivamente, não podendo, em hipótese alguma, serem realizadas por iniciativa do elemento de Guerra Cibernética.

### 6.4 Coordenação com o nível político

a. Relacionar prescrições a respeito do relacionamento com o nível político, que afetem o planejamento das ações de Guerra Cibernética, se for o caso.

b. Não existindo assunto para ser inserido neste parágrafo, ele deverá ser suprimido.

### 6.5 Outras prescrições

a. Relacionar outras prescrições que afetem o planejamento das ações de Guerra Cibernética, não abordadas nos parágrafos anteriores, se for o caso.

b. Não existindo assunto para ser inserido neste parágrafo, ele deverá ser suprimido.

(Assinatura)
Nome e Posto
Comandante do Comando Conjunto

AUTENTICAÇÃO:

LISTA DE DISTRIBUIÇÃO:

(grau de sigilo)

**APÊNDICE D**
Exemplo de Apêndice de Guerra Cibernética

(grau de sigilo)

Exemplar Nr ____ de ____ cópias
Comando Conjunto SAFIRA
ESMERALDA/MO
Grupo Data-Hora (expedição)
Referência de Mensagem: "XXX-XX"

**APÊNDICE "X" (GUERRA CIBERNÉTICA) ao ANEXO "Y" (OPERAÇÕES de INFORMAÇÃO) ao PLANO OPERACIONAL SAFIRA**
**(UM EXEMPLO)**

Referências: a. Análise de Guerra Cibernética referente à Operação SAFIRA; e
b. Mapas Operação SAFIRA escala 1:2.400.000.

## 1. SITUAÇÃO

### 1.1 Forças inimigas

a. Não existem informações sobre a existência de doutrina e estruturas adversas dedicadas à atividade de Guerra Cibernética.

b. O inimigo possui baixo nível tecnológico para conduzir atividades de comando e controle.

### 1.2 Nossas forças

a. Será organizado, para apoiar em Guerra Cibernética o TO SAFIRA, um Destacamento de Guerra Cibernética (Dst Cj G Ciber), integrado por militares das três Forças, tendo por base o 19º Centro de Telemática de Área (19º CTA), possuindo capacidade de realizar Exploração, Ataque e Proteção Cibernética.

b. O Dst Cj G Ciber será desdobrado junto ao Comando do TO SAFIRA, tendo em vista a necessidade de estar localizado em um local que possua as condições técnicas necessárias para a execução das ações de Guerra Cibernética.

c. O Dst Cj G Ciber ficará diretamente subordinado ao Comandante do TO SAFIRA, em razão da necessidade de centralização da decisão quanto às ações de ataque cibernético e de que sua execução seja determinada pela maior autoridade do TO.

d. Sugere-se que o Dst Cj G Ciber possua a seguinte constituição organizacional mínima:

1) Comandante;
2) Estado-Maior;
3) Seção de Inteligência Cibernética;
4) Seção de Operações Cibernéticas;

e. O detalhamento da estrutura e o efetivo do Dst Cj G Ciber deverá ser definido e proposto após estudo específico elaborado por seu comandante.

f. O Dst Cj G Ciber poderá contar, a critério do seu comandante e da disponibilidade, com elementos de outras agências do Governo e/ou especialistas civis para operação assistida de sistemas computacionais e outras funções especializadas julgadas necessárias.

**1.3 Forças amigas**

a. Meios de defesa cibernética dos comandos da Marinha, do Exército e da Aeronáutica, não empregados no TO SAFIRA.

b. Departamento de Segurança da Informação e Comunicações (DSIC) do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), órgão responsável, no nível político, pela Segurança da Informação e Comunicações (SIC), bem como pela Segurança Cibernética, abrangendo a Administração Pública Federal (APF), direta e indireta, além das infraestruturas críticas da informação nacionais dos setores público e privado.

**1.4 Meios recebidos e retirados**

Não é o caso.

**2. MISSÃO**

Executar ações de exploração, ataque e proteção cibernética em apoio às operações militares no TO SAFIRA.

**3. EXECUÇÃO**

**3.1 Premissas de emprego**

a. Minimizar os danos colaterais à população civil.

b. Garantir a segurança e o funcionamento das infraestruturas críticas nacionais no interior do TO.

c. Preservar, sempre que possível, o funcionamento das infraestruturas críticas do País VERDE no interior do TO.

**3.2 Exploração Cibernética**

a. A exploração cibernética consiste de ações de busca, nos Sistemas de Tecnologia da Informação (TI) de interesse, com o propósito de obter dados, de forma não autorizada para a produção de conhecimento ou para identificar as vulnerabilidades de tais sistemas.

b. As ações de exploração cibernética desencadeadas com o propósito de identificar vulnerabilidades nos sistemas de TI adversos de interesse para a missão do TO SAFIRA serão realizadas sistematicamente, sob a responsabilidade do Dst Cj G Ciber, com vistas a levantar as oportunidades e as possibilidades de emprego das ações de ataque cibernético.

c. As ações de busca relacionadas à produção do conhecimento de Inteligência, a partir de dados oriundos da fonte cibernética, caso estas se façam necessárias, deverão ser solicitadas e coordenadas pela Seção de Inteligência do TO SAFIRA, exclusivamente, não podendo, em hipótese alguma, serem realizadas por iniciativa do Dst Cj G Ciber.

d. O Dst Cj G Ciber deverá, também, realizar a monitoração das redes de computadores estabelecidas pelo Comando do TO SAFIRA e orientar as ações de monitoração das redes estabelecidas pelos elementos subordinados, desdobrados em profundidade no interior do TO, com vistas a identificar e corrigir falhas de segurança.

e. O Dst Cj G Ciber poderá apoiar as atividades de Com Soc, Op Psc e Inteligência realizando a coleta e monitoração de sites, redes sociais e serviços da Internet de interesse por intermédio de ferramentas especializadas.

**3.3 Ataque Cibernético**

a. O ataque cibernético compreende ações para interromper, negar, degradar, corromper ou destruir informações armazenadas em dispositivos, redes computacionais e de comunicações do oponente.

b. As ações de ataque cibernético, uma vez autorizadas, serão direcionadas às redes de computadores e sistemas de informação do oponente, de interesse das operações do TO, explorando as vulnerabilidades identificadas pelas ações de exploração cibernética.

c. Em razão de sua criticidade e dos danos colaterais que possam ocorrer, a decisão de realizar essa ação é da competência exclusiva do Comandante do TO.

d. As ações de ataque cibernético planejadas pelos elementos de Guerra Cibernética das Forças Componentes, sobre alvos táticos, em proveito das operações futuras, poderão ser autorizadas, desde que aprovadas na Reunião de Coordenação de Operações de Informação.

e. Os elementos de Guerra Cibernética das Forças Componentes poderão realizar ações de ataque cibernético sobre alvos táticos imediatos, identificados no desenvolvimento das operações correntes, mediante solicitação ao Comando Conjunto, sem necessidade de coordenação prévia.

**3.4 Proteção Cibernética**

a. A proteção cibernética abrange as ações para neutralizar ataques e exploração cibernética contra os nossos dispositivos computacionais, redes de computadores e de comunicações.

b. O Dst Cj G Ciber desdobrará, no Comando do TO SAFIRA, uma Equipe de de Tratamento de Incidentes de Rede (ETIR).

c. A ETIR tem como responsabilidade realizar a proteção das redes de computadores estabelecidas pelo Comando do TO SAFIRA e orientar as ações de proteção cibernética das redes estabelecidas pelos elementos subordinados, desdobrados em profundidade no interior do TO, bem como realizar a perícia forense computacional operacional nos casos de violação de segurança identificados.

d. Deverá, também, orientar a adoção de medidas de proteção cibernética por parte das infraestruturas críticas nacionais localizadas no interior do TO, com o propósito de buscar a garantia de sua segurança e de seu funcionamento.

**3.5 Lista preliminar de possíveis alvos para ações de exploração e de ataque cibernéticos**

a. Sistemas de vigilância e alerta aéreo.
b. Empresas de geração e de distribuição de energia.
c. Empresas de produção e de distribuição de combustíveis.
d. Empresas de telefonia fixa e móvel.
e. Provedores de acesso à internet.
f. Sistemas militares de C2.
g. Sistemas de radares e de defesa.

h. Corporação Verdense de Aeroportos e Aviação Comercial (CORVAC), empresa encarregada da supervisão e administração da infraestrutura aeroportuária.

i. Empresa Nacional de Portos de Verde (ENAPO VERDE S/A), encarregada do controle e administração da infraestrutura portuária.

j. Empresas de transporte aeroviário, rodoviário, ferroviário e dutoviário.

k. Empresas de transporte marítimo.

l. Sistemas de C2 do governo e do Ministério da Defesa verdenses.

m. Sistemas de C2 dos comandos das Forças Armadas verdenses.

n. Sistemas de C2 desdobrados em apoio às operações militares verdenses.

**3.6 Lista preliminar de sistemas de C2 e infraestruturas críticas a serem protegidas**

a. Sistema de Controle do Tráfego Aéreo dos principais aeroportos.

b. Sistema de fornecimento de energia.

c. Sistema de fornecimento de água.

d. Sistemas de Comunicações (fixa e móvel, dados e voz).

e. Sistema de Proteção Espartana (SIPE).

f. Sistema de Comunicações Militares por Satélite (SISCOMIS).

g. Redes internas das Forças Armadas.

h. Sistemas relacionados às instituições bancárias.

i. Sistemas relacionados à produção e distribuição de combustíveis.

**3.7 Concepção geral de emprego**

**a. Numa primeira fase**

Desde já.

Empregar o Destacamento Conjunto de Guerra Cibernética (Dst Cj G Ciber) para:

- realizar ações de proteção cibernética das redes computacionais do sistema de C2 das forças militares desdobradas no interior do TO SAFIRA;

- contribuir para a proteção cibernética das infraestruturas críticas nacionais localizadas no interior do TO SAFIRA, com o propósito de buscar a garantia de sua segurança e de seu funcionamento;

- realizar ações de exploração cibernética para identificar vulnerabilidades nas redes de computadores dos sistemas militares e das infraestruturas críticas do inimigo, de interesse para a missão do TO SAFIRA, com vistas ao planejamento das ações de ataque cibernético; e

- realizar ações de exploração e ataque cibernéticos em proveito das campanhas de operações psicológicas, dentro do contexto das operações de informação.

**b. Numa segunda fase**

a) Mediante ordem, empregar o Dst Cj G Ciber para realizar ações de ataque cibernético, colaborando com o esforço de interdição, em alvos de interesse do TO SAFIRA.

b) Continuar empregando o Dst Cj G Ciber para:

- realizar ações de proteção cibernética das redes computacionais que dão suporte ao sistema de C2 do Comando do TO SAFIRA;

- contribuir para a proteção cibernética das infraestruturas críticas nacionais localizadas no interior do TO, com o propósito de buscar a garantia de sua segurança e de seu funcionamento; e

- realizar ações de exploração cibernética para identificar vulnerabilidades nas redes de computadores dos sistemas militares e das infraestruturas críticas do inimigo, de interesse para a missão do TO SAFIRA, com vistas ao planejamento das ações de ataque cibernético.

**c. Numa terceira fase**

Iniciar a desmobilização do Dst Cj G Ciber.

## 4. LOGÍSTICA

Deverá ser observado o prescrito no Anexo de Logística a este Plano.

## 5. DEMANDAS

5.1 Identificação e localização das capacidades inimigas de defesa cibernética, de nível estratégico.

5.2 Identificação da capacidade de guerra cibernética do inimigo, nos níveis operacional e tático.

5.3 Identificação das infraestruturas críticas verdenses, que sejam do interesse das operações militares no TO SAFIRA, tais como empresas distribuidoras de energia, combustíveis, serviços de telecomunicações, serviços aeroportuários e de transporte, dentre outras, cujo funcionamento seja baseado no emprego de redes de computadores, cujos serviços, se interrompidos ou degradados, representem vantagem militar imediata.

5.4 Levantamento e identificação das estruturas voltadas à proteção das redes de computadores dedicadas ao Sistema de C2 adverso.

## 6. PRESCRIÇÕES DIVERSAS

### 6.1 Eventos de Coordenação e de Tomada de Decisão

O Comandante do Dst Cj G Ciber deverá participar das seguintes reuniões do Estado-Maior Conjunto (EMC):

a. Reunião Diária de Situação, com o propósito de atualizar o EMC quanto às atividades de Guerra Cibernética em curso;

b. Reunião de Coordenação de Operações, com o propósito de colaborar com a elaboração da versão preliminar da Ordem de Coordenação;

c. Reunião de Coordenação de Operações de Informação, com o propósito de apresentar as necessidades e as possibilidades de atuação do Dst Cj G Ciber, bem como coordenar suas ações e as ações dos elementos de Guerra Cibernética das Forças Componentes;

d. Reunião de Controle da Operação Planejada; e

e. Reunião de Aprovação da Ordem de Coordenação, com o propósito de colaborar com a revisão e aprovação da Lista de Alvos, designando aqueles que podem ser neutralizados por meio de ataque cibernético.

### 6.2 Integração com as Operações de Informação

Mediante autorização do Comandante do TO SAFIRA e coordenado na Reunião de Coordenação de Operações de Informação, poderão ser realizadas ações de exploração e ataque cibernéticos em proveito das campanhas de operações psicológicas, com o objetivo de mobilizar a população verdense contra o conflito armado, por intermédio de invasão e modificação de informações constantes de páginas eletrônicas de organizações de grande credibilidade junto à população verdenses, tais como órgãos governamentais, mídia, redes sociais, dentre outras.

**6.3 Integração com a Atividade de Inteligência**

As ações cibernéticas orientadas ao atendimento das Necessidades de Inteligência (NI) constantes do Plano de Obtenção de Conhecimentos (POC) do Comando Conjunto, serão solicitadas mediante a formalização de um Pedido de Inteligência (PI) pela Seção de Inteligência do TO SAFIRA, exclusivamente, não podendo, em hipótese alguma, serem realizadas por iniciativa do Dst Cj G Ciber.

**6.4 Coordenação com o nível político**

Está autorizada a ligação do Dst Cj G Ciber com o DSIC do GSI/PR, para a orientação das medidas de proteção cibernética a serem adotadas por parte das infraestruturas críticas nacionais localizadas no interior do TO, com o propósito de buscar a garantia de sua segurança e de seu funcionamento.

(Assinatura)
General-de-Exército JOSÉ DA SILVA
Comandante do Comando Conjunto SAFIRA

AUTENTICAÇÃO:

LISTA DE DISTRIBUIÇÃO:

# APÊNDICE E

Transcrição das Entrevistas Realizadas

Entrevista com o Cel Inf André Luís Novaes Miranda, servindo no Escritório de Projetos do Exército – Estado-Maior do Exército, realizada em 06 de junho de 2012.

Antes da entrevista, o Cel Novaes solicitou que fossem expostos os conceitos propostos de Guerra Cibernética, com a finalidade de ambientá-lo e de proporcionar um melhor direcionamento da mesma.

Como a finalidade dessa entrevista era de apreender novos conceitos acerca da evolução das operações militares e de como a cibernética se encaixaria dentro do conceito de Operações de Informação, a mesma foi conduzida de forma semiestruturada, com algumas perguntas previamente preparadas e com um direcionamento para o objetivo proposto. Mesmo assim, optou-se por não solicitar a simples resposta às perguntas formuladas, havendo a preocupação de deixar o entrevistado à vontade para expor os seus pontos de vista, que apresentam a sua visão particular, quebram paradigmas e ainda estão em discussão dentro do Exército Brasileiro. A entrevista está transcrita de maneira fidedigna, sem uma eventual correção de erros na expressão oral e teve a duração aproximada de 53 minutos.

## Transcrição 01

LEGENDA: C – João Marinonio Enke CARNEIRO (entrevistador);
N – Cel Inf André Luís NOVAES Miranda.

C: O senhor poderia declarar o seu nome, por favor ?

N: Cel Novaes, sou do Escritório de Projetos do Exército.

C: O senhor poderia fazer uma breve referência à sua vida profissional, que gerou a experiência que o senhor tem para embasar as suas opiniões?

N: Vamos focar nos últimos anos, que é o mais importante. Desde que eu participei nessas operações internacionais e comecei a me debruçar mais no que

estava realmente acontecendo no mundo, até por participar de algumas delas, e não somente do que estava escrito nos nossos manuais, etc. e que muitos deles refletem uma época que está sendo ultrapassada muito rapidamente no mundo. Então, desde a época do Batalhão Haiti, em 2005, quando eu comandava um Batalhão na Vila Militar e na volta, no Comando do Centro de Instrução de Operações de Paz, que por necessidade a gente tem que estudar os conflitos onde os brasileiros estão, e são vários, eu não sei quanto está hoje, na época a gente tinha brasileiros em doze diferentes missões de vários organismos internacionais em quase todas as guerras do mundo. E como isso variava de uma guerra para outra, a gente era obrigado a acompanhar todas as guerras que estavam acontecendo no mundo e de lá eu fui para os Estados Unidos e eu passei dois anos em um instituto de um organismo que não é americano, é da OEA, mas que estuda segurança e defesa internacional e é um estilo bem americano, é um estilo em que você é obrigado a abrir a sua cabeça porque você debate com palestrantes de todos os viés e todos os backgrounds e experiências etc, então ninguém vem ali te falar o que está escrito no manual que você está seguindo, vem da opinião dele, que são as mais diversas possíveis. Então, esses anos de experiências, esses últimos cinco, seis anos que vem me colocando a tentar entender como é a guerra hoje no mundo e como é a guerra na era do conhecimento, que essa evolução, não só tecnológica, mas da sociedade como um todo vem produzindo reflexos diretos na forma de fazer a guerra.

C: O que o senhor vai falar agora expressa as suas opiniões, então o senhor é livre para falar aquilo que o senhor quiser, sem compromisso com o órgão ao que o senhor serve, o senhor está expressando a sua opinião pessoal. O senhor podia comentar melhor essa parte da evolução da guerra, da parte da saída da forma industrial de se combater para uma nova forma, o senhor poderia comentar isso daí? (2:50)

N: Olha, existem bons autores [citados anteriormente: Alvin Tofler[136] e Rupert Smith[137]] que procuram estudar isso com mais embasamento científico etc. mas esses autores mais ou menos vão coincidir que a guerra da era industrial ela atingiu

[136] TOFLER, Alvin. **A Terceira Onda**. 25. ed., São Paulo: Record; 2001, 491p. ISBN: 8501017973.
[137] SMITH, Rupert. **The Utility of Force: the Art of War in the Modern World**. New York: Alfred A. Knopf, 2007. eISBN: 978-0-307-26741-2

o seu auge no final da segunda guerra mundial onde as batalhas eram decididas por uso da força física que eram caracterizadas naquela época por blindados e apoio de fogo, não só da artilharia mas apoio de fogo naval e força aérea bombardeando, etc. O auge disso foram as bombas atômicas que os Estados Unidos usaram. Elas em si decretaram, bem ou mal, o fim da era em que os países podiam usar ao máximo as suas armas de destruição em massa, o emprego máximo da força. A partir daí, aquilo, segundo esses autores, foi o marco que limitou o uso da força e aquilo veio a partir de então, guerra fria em logo em seguida, o outro lado com a bomba atômica gerando limitações nos conflitos, conflitos de caráter limitado e que gerou a tal da guerra fria, que só foi fria para esses dois países, na realidade essas guerras explodiram em vários países do mundo e ao mesmo tempo acompanhava o avanço tecnológico e o avanço dos meios de comunicação e a informação cada vez mais disponível e os governos com compromissos que antes eles não tinham e com responsabilidades de prestação de contas para os seus eleitores do que estava acontecendo, do que ele estava fazendo efetivamente, essas coisas começaram a ficar muito claras, ninguém mais podia mandar uma tropa para algum lugar para fazer o que ela achava que tinha que fazer lá e no final ele ia para a televisão e para o jornal dizer que ganhou a guerra e quem perdeu e acabou e tudo o que aconteceu nesse meio tempo, não as guerras passaram a ser acompanhadas. Essa coisa começou a evoluir após a queda do muro de Berlim e nos ataques em Nova York e Washington em 2001 isso acelerou completamente então hoje com as redes sociais e com a democracia realmente chegando em quase todo mundo, pelo menos no mundo ocidental, onde nós estamos falando. A guerra passou a ter um foco diferente. A guerra não é ganha mais na força, assim não só a guerra como em qualquer outro campo do conhecimento, passou a ser ganho muito mais com as informações do que com a força propriamente dita. Os primeiros a entender isso, segundo esses autores, e eu concordo com eles, a primeira guerra perdida porque não foi compreendido esse paradigma e foram usados os meios da era industrial em uma época diferente, foi a Guerra da Argélia e, de lá para cá você pode citar várias: Vietnã, a primeira guerra do Afeganistão com os Russos e aí você vê essas outras várias guerras que estão acontecendo hoje, a Primavera Árabe quando nós tivermos entendido melhor esses conflitos, principalmente o do Egito, o da Líbia e, atualmente, o da Síria, dali vão sair muitos ensinamentos para esse tipo de guerra.

C: Porque aí a gente já tem o emprego de redes sociais, e já tem o emprego dessa parte cibernética junto com a guerra, não é só mais o correspondente de guerra, não é mais só o controle da mídia. Na realidade a mídia fugiu de controle, não é?

N: Totalmente. Realmente essas guerras do ano passado para cá ela estão nessa fase da cibernética e das redes sociais. O que antes se conseguia na era industrial com um meio de força, com concentração de fogos em determinado local para você quebrar a vontade do adversário lutar, hoje em dia você não pretende mais quebrar a vontade do adversário lutar, é muito mais fácil você quebrar a vontade ou a liberdade de ação do político de manter a força dele fazendo o que ele vinha fazendo. (6:58)

C: Você vira a opinião pública do povo do país dele.

N: Não é uma novidade isso. Se você pegar os nossos manuais, o manual de Estratégia, por exemplo, ele fala isso, ele fala da liberdade de ação que o político tem ou que qualquer comandante tem de poder empregar os seus meios. Então, na realidade o que estamos falando aqui é uma forma moderna de se conduzir uma vitória. A vitória, ela não é mais rápida como ela era na guerra industrial, ainda que guerras durassem cem anos. A segunda guerra durou aquele tempo todo, mas as guerras eram decididas em batalhas. Uma delas era uma batalha decisiva. As nossas escolas militares, elas focam na batalha decisiva. Se você olhar todas as provas que você fez na EsAO ou na ECEME é uma batalha decisiva, onde você visa cercar e destruir o inimigo e ganhar a guerra naquela batalha. Você traça aquelas linhas de controle, aqueles E Prog, desbordando, desviando, entrando pelo lado mais fraco, cerca e destrói. E aquela guerra termina ali, que ótimo, então a guerra é isso aqui. Você usa blindados para manobrar, com apoio de fogo massivo para você romper em algum lugar, você cerca, destrói o inimigo e ganha a guerra. Essa guerra acabou, a última delas foi em 1973. A última guerra que você tinha cercos, blindados manobrando com apoio de fogo, um cercando o outro, tentando cercar e um destruindo o outro. De lá para cá, cada vez mais a guerra foi lutada com o mais fraco, se não cometer o erro que Saddam Hussein cometeu na primeira guerra do golfo, ele no meio do deserto se enterrar na areia.

C: Ele traz [a guerra] para dentro dos centros urbanos. (8:45)

N: E essa guerra dos centros urbanos ela é diferente, as pessoas confundem. Ah, realmente, então nós temos que fazer um ataque em localidade, também não é um ataque à localidade. O ataque à localidade da guerra industrial o mais fraco defendia na orla da localidade, aquilo virava um escombro só, progride casa a casa, quarteirão a quarteirão, destruindo tudo, ou seja, a liberdade de ação permitia você usar os meios da era industrial dentro da cidade. A cidade estava evacuada ou semi-evacuada e assim foi Stalingrado. A mudança de fase, ela não foi a partir daqui, acabou essa guerra. Grosny foi assim, no ano 2000, quer dizer, o russo acabou com a cidade, destruiu tudo ali. O americano em Falluja acabou com a cidade, destruiu toda a cidade. Na realidade as pessoas que não entenderam ainda a concepção da guerra de hoje continuam fazendo a mesma coisa e pagando preços altíssimos. Tanto que Falluja foi postergada até a eleição. Quando acabou a eleição nos Estados Unidos, logo em seguida é que se liberou o exército para fazer a operação e eles destruíram a cidade, acabou com a cidade inteira. Bom, eu estava respondendo a sua pergunta dessa passagem de uma fase para outra, da industrial para a era do conhecimento. A era do conhecimento não significa o fim da era industrial na guerra. Todos os países do mundo, responsáveis, não vão mudar os seus exércitos, não vão abandonar os princípios da era industrial.(10:20) Essa é uma coisa importante que, se você não começar explicando bem isso, algumas pessoas vão achar que você está pregando o fim.

C: Já vão reagir violentamente à mudança.

N: Você perdeu o seu argumento naquele momento. E eles têm razão, porque na realidade, não significa abrir mão de um núcleo duro de guerra industrial. Você tem que manter, porque todos os países responsáveis do mundo fazem isso.

C: Até para gerar poder dissuasório.

N: E mantêm esse núcleo duro do tamanho que ele necessita para dissuadir as suas ameaças. Então alguns países como Índia e China, por exemplo, com um

problemaço ali nas fronteiras, vão manter núcleos duros enormes e vão estar dispostos a usar isso quando for necessário. E outros países que têm ameaças, cuja ameaça está na fronteira e tem um problemaço de fronteira não resolvido, continuam mantendo esses núcleos na beira ali prontos para fazer uma ação ali dentro, até para dissuadir o outro lado. E esses países não são a exceção, no mundo inteiro, quase todos os países do mundo têm um problemaço na fronteira que ou foi mal resolvido durante a nossa geração ou, no máximo, na do nossos pais. Então esses países têm uma grande motivação para manter um núcleo duro. Realmente, às vezes, você olha, mas ninguém está se transformando, olha ali para o lado, tem que manter. Nós também temos que manter um núcleo duro proporcional às nossas ameaças do tamanho da dissuasão que a gente tem que manter, isso está totalmente fora de discussão. Mas, mesmo para empregar esse núcleo duro, ou para você fazer a guerra que está acontecendo no mundo, que não é mais essas manobras em deserto, no campo aberto, etc. Mesmo para você empregar o núcleo duro ou para fazer a guerra no meio das cidades, no meio da população, você tem que estar ligado, tem que conhecer a forma como as guerras estão sendo ganhas e perdidas hoje no mundo. O que os mais fracos estão fazendo, já que não podem vencer na força física, eles vão tentar tirar a liberdade de ação de quem está empregando a força. E a guerra ela literalmente está no meio do povo, de qualquer ponto de vista que você olha. Além dela ser lutada no meio do povo, pelo povo, contra o povo, ela vai para dentro de todas as casas, porque os repórteres estão ali dentro e qualquer um do povo com um celular na mão, ele posta no twitter.

C: Por isso que as mídias sociais, as redes, os facebooks, os twitters, e os serviços que permitem fazer isso estão ganhando tanta relevância nisso daí.

N: E daí que vem o que eu considero uma necessidade premente nossa. Nós não podemos deixar essas coisas acontecerem na iniciativa de quem quer que seja, ou pior, que sejam manipuladas e a gente ficar esperando as coisas acontecerem. É uma guerra pelos corações e mentes, de todos os níveis. Ela tem que ser olhada dentro da cidade em que ela está sendo lutada ou daquele bairro, ela tem que ser olhada de forma regional e ela tem que ser olhada nacional e internacionalmente. Em todos esses níveis a gente tem que estar conquistando as opiniões. A gente tem que ter claro qual é o objetivo estratégico da nossa estada ali, da nossa operação

Porque se nós não compreendermos bem esse objetivo, nós vamos confundir emprego de tropa com desdobramento de tropa, que é o normal. Se você pergunta para o político que está ali, vamos empregar a tropa em tal lugar, ele não está pensando no emprego, ele está pensando em mandar uma tropa para lá. Ele mal sabe o porquê ele está mandando a tropa para lá e qual objetivo vai ser conquistado. Mas isso é muito importante para nós entendermos, questionarmos e levarmos esse objetivo claramente, porque aí começa o trabalho das operações de informação. É comunicar esse objetivo. Esse objetivo vai ter que ser comunicado porque ele vai estar se contrapondo a outro.

C: Comunicar envolvendo a população. (14:34)

N: É comunicar para todos. A população é o começo, porque é a população em última instância que vai dar o apoio ao governante ou ao chefe, ao líder, o que quer que seja, ou nosso oponente. Então você tem que comunicar para nossa população, por isso que eu falei que são vários níveis, para a nossa população entender que nós estamos lutando por uma causa mais nobre que a do nosso oponente, que nós estamos usando a força de uma maneira proporcional, que nós não estamos cometendo massacres, que nós não estamos cometendo nenhum ato do qual tenhamos que nos envergonhar ou de responder a eles em nenhum tribunal em nenhuma instância. (15:21)

C: Isso são operações psicológicas ...

N: A operação de informação é tudo. Eu acredito que ela vai variar a predominância dependendo do momento mas, de uma maneira geral, o pivot, a parte visível da operação de informações é a informação pública. Mas a informação pública não vai lá de um forma passiva responder uma pergunta de um repórter. A informação pública tem que estar preparada junto com a Operação Psicológica para transmitir uma mensagem. Essa mensagem começa a ser transmitida antes da operação ser desdobrada e iniciar e ela vai narrando a conquista do objetivo estratégico todos os dias, a todo o momento com proatividade. Então é uma operação de informações públicas? Não é. É a parte visível, mas ela está levando a mensagem da Operação Psicológica e ela está se alimentando da inteligência, que

tem o seu ramo cibernético. Então a inteligência com esse meio cibernético e a parte que tem o seu ramo da Guerra Eletrônica, você ao colocar o seu porta voz no meio dos repórteres que vão fazer aquela notícia chegar a todos os lares, se você chegar lá de uma forma inocente, eu vim aqui responder pergunta, ele vai perder a guerra das informações. Então eu vejo que a operação de informações tem que ser uma coisa muito sincronizada, porque senão você vai matar o seu porta-voz, vai matar a ideia. E aquilo pelo qual você está lutando, vai perder a guerra das informações. Ela vai ser compreendida pelo seu povo, pelo seu exército, pelo oponente, pela população, pelo inimigo, pelo mundo, pelas comunidades internacionais, você vai ser visto como agressor, como desrespeitador de leis internacionais. Então o porta-voz tem que estar muito bem calçado em tudo. E como nós estamos falando de cibernética, cibernética é um troço fundamental porque esse porta-voz não pode chegar ali sem saber quais são as matérias do top 10 do twitter daquele momento que ele está ali, dos minutos anteriores. Se não souber o que está sendo comentado no twitter, que vai ser a pergunta que vão fazer para ele, e vem mais, vem aquela parte que, não sei qual o nível dessa conversa nossa aqui, mas você tem que usar os seus meios dentro de todas as possibilidades, porque a notícia que está no top 10 do twitter pode ser influenciada por você também. Você não pode ficar esperando que isso brote naturalmente dali, porque às vezes não vai brotar. E, às vezes, as que estão ali foram plantadas, e nós temos que ter capacidade de interferir nesse processo de todas as formas. Não é só o porta voz que vai conseguir fazer isso. A nossa tropa tem que estar fazendo algo coerente com isso e os dois apontados para a conquista do objetivo estratégico, que eu não sei qual vai ser, em tese, pode ser apoiar uma eleição num país, você vai ficar meses ali, pode ser o reestabelecimento da ordem, pode ser apoiar uma reforma em um setor de segurança, reconstrução do país. Vai começar com o estabelecimento da ordem e depois você vai ficar meses, anos ali lutando o tempo todo contra isso e o outro lado, se for mais fraco que você, tentando te imputar coisas que você não fez, ou se você fez, teve uma razão para fazer isso. Então essa notícia, você vai ganhar a guerra da informação se você chegar com a sua mensagem ao receptor, que é todo mundo, é a população local, a sua do seu país, da comunidade internacional etc. E ao mesmo tempo, você truncar a comunicação do oponente. Entenda-se por truncar, tudo.

C: Tanto usando guerra eletrônica quanto o meio cibernético...

N: Tanto meios cibernéticos quanto desmentidos pela imprensa, quanto imagens, ou seja, quanto mais rápido a sua imagem chegar por meios cibernéticos em todos os lugares, melhor. Aonde o americano perde a guerra? Ele bombardeia a cidade com artilharia.

C: Ele não está perto...

N: Ele não está perto, ele não controla essa imagem.

C: Ele não tem proximidade para influenciar o controle da imagem.

N: Por isso que a guerra de hoje, eu vejo soldado a pé dentro da cidade. As ações quando você é o mais forte, você está em um país, você está pacificando uma cidade, um bairro, o morro do alemão, o Haiti, a Líbia, sei lá onde nós vamos estar, o mais forte, se ele não ficar muito perto e não usar os meios de letalidade controlada, seletivas e chegar na mesma hora que ele usou a força, ele ser o primeiro a chegar, e ele não fotografar aquilo e ele não der a sua versão imediata, ele já perdeu a guerra da informação. Porque o americano bombardeia, quando ele chega lá, aquilo que ele bombardeou e ele tinha a convicção de que era uma base guerrilheira, se transformou, nas imagens, num casamento, num batizado de criança.(20:35) Já era, não tem mais desmentido, não tem mais. Então isso mostra bem um exemplo do meio da era industrial sendo usado na era do conhecimento. Mais importante do que ele bombardear aquela base terrorista, sei lá o que, ele comunicar isso. Ele provar com imagens etc. que ele realmente eliminou um grupo de oponentes que estava usando a força contra ele, de uma forma proporcional, infelizmente morreram pessoas, foi necessário, nós usamos a força proporcional, estão aqui as imagens, a prova, as pessoas armadas aqui mortas, etc. O americano, toda hora, ele perde isso. Então eu acho que o Brasil aprendeu isso, está fazendo isso bem nos locais. Você não tem um fato como esse no Haiti. Nós usamos a força para valer no Haiti. As pessoas que falam que isso é coisa de polícia, não entenderam a guerra no mundo. A guerra no mundo está sendo assim, volto a dizer, desde 73 as guerras são assim. No Iraque, o que ele fez na invasão do Iraque, ele foi contornando as cidades, definiu aquilo como uma vitória e ficou dez anos atolado nas cidades que ele

desviou, onde ficou a resistência e está até hoje com o mesmo problema no Afeganistão. Saiu do Iraque após redefinir a vitória e vai sair do Afeganistão, talvez no ano que vem, tendo redefinido o objetivo estratégico para o qual ele entrou, para poder dizer que foi uma vitória e vai largar aquilo para trás sem resolver, não conseguiu resolver.

C: Vai buscar uma saída honrosa para tirar o pessoal de lá. Saída honrosa para a população dele.

N: E, lá nos Estados Unidos, eles não perderam a guerra da informação não, lá dentro. Mas numa campanha de informação massiva, massiva. Quem vai ao Estados Unidos e passa ali uma semana ou duas convivendo com o povo americano você vê essa campanha. Essa campanha é um troço impressionante, a campanha de operações psicológicas. Não é nem mais operação psicológica, é a campanha da informação. Volto a dizer, a campanha de informação não pode ser o porta-voz respondendo às perguntas da imprensa, isso não é campanha de informação e nem uma campanha de mídia. Fazer cartaz, isso aí não é campanha de informação. A campanha de informação é a sinergia dos sistemas. O porta-voz é só a parte visível. A população tem que ver naquela pessoa uma pessoa sincera, que acredita no que ela está fazendo, acredita nos objetivos e tem coerência no que ela está falando nas operações que estão acontecendo no terreno. Agora, isso só vai acontecer se essa pessoa estiver apoiada firmemente na operação psicológica, na guerra cibernética, na guerra eletrônica, na inteligência de todas as fontes, inclusive a cibernética. Senão esse cara vai ser desmentido.

C: Ele pode até estar certo, mas a informação dele será manipulada para desmenti-lo.

N: Nada pior do que você ali falar uma coisa e junto, na mesma matéria, ser mostrada uma imagem onde você estava errado. O porta-voz, ele não pode ir para uma situação dessa, e ele tem que ir toda hora, ele tem que estar disponível 24 horas por dia para esse embate e o porta-voz é um narrador da sua conquista do objetivo estratégico. Ele vem narrando dia a dia, momento a momento e o tempo

todo, mas ele não está sozinho, nunca. Agora, a população tem que achar que ele está sozinho. Ele está ali aparentemente sozinho.

C: Porque ele é a parte descartável do sistema. Se queimar o porta-voz, troca o porta-voz. Ele é a ponta do iceberg.

N: Você já não pode queimar nunca os outros sistemas. O porta-voz você queima, ele é descartável, mas o sistema, não. Então os outros sistemas são invisíveis, ele é a ponta do iceberg. O que mantém ele lá em cima são os outros sistemas que estão embaixo. Falando especificamente da cibernética, com esse mundo das redes sociais hoje, no momento de hoje, não sei como vai evoluir isso, mas a cibernética é um dos apoios principais dele. E, se não tiver alguém da cibernética lá, a medida que ele está falando, no mesmo momento, e aquilo não fizer parte de um plano, ele não está falando uma coisa e qualquer pessoa que estiver acompanhando nos seus twitters e nas redes sociais tem que estar vendo aquela notícia sendo confirmada, de alguma forma ou de outra, ou não sendo desmentida. E você vai fazer isso por todos os meios, acho que aí você está entendendo o que estou querendo dizer. Todos os meios que os sistemas podem fazer para que a verdade dele seja a que vai prevalecer tem que ser usados, tem que ser usados. E os sistemas são esses, o que eu falei aqui. Esse é o apoio ao combate de hoje. Quando eu participei da Operação Guanabara em 2008, o Gen Cesário falou uma coisa nas suas diretrizes e eu não entendi, a princípio. Que a gente iria fazer a segurança às eleições. Hoje eu já entendo perfeitamente o que ele falou. Ele falou o seguinte: “Isso pode parecer uma operação de GLO. Tenho certeza que todo mundo está achando que isso é uma operação de GLO, mas não é. Isso é uma operação de informações públicas. Tudo o que você está vendo, essas milhares de pessoas que vão ficar trabalhando dia e noite nessas 27 localidades, isso não é o importante da operação. O mais importante da operação é a informação pública.” Eu hoje já entendo perfeitamente, mas eu vou dar uma outra tradução às palavras dele. Não é uma operação de informações públicas, é uma operação de informações. Aquela operação foi uma que eu tomo como referência de operação como informação. Esses sistemas, menos o cibernético, que não existia, não era operacional à época, estavam funcionado com sinergia. O porta-voz da operação ia, todo o tempo, totalmente junto com o homem que planejou junto com ele a parte de operações

psicológicas. Estavam juntos o tempo todo, iam para a cena conversando dentro do carro. (27:19) E desembarcavam lá conversando. Então todas as outras ações que davam sustentação, elas estavam coerentes. Ele tinha acesso a todos os comandantes da operação com um celular, e ele sabia o que estava acontecendo. Ele não está ali para mentir, ele não pode mentir nunca e nada pode desmentir o porta-voz. O que está acontecendo no terreno não pode desmenti-lo, isso é o pior de tudo. Agora, todas as imagens e fatos, tudo o que poderia desmenti-lo ...

C: Tem que corroborar para aquilo que estava falando...

N: Tudo tem que corroborar. Esse cara é que acelera, ele que cria o “momentum”. Agora, não é ele, basta encontrar uma pessoa que fale bem e não se acanhe na frente das câmeras. O importante é toda a sustentação disso. Esse sistema vai fazer com que ele “não minta”. Tudo o que ele está falando tem que estar sustentado. Ele tem direito de se desculpar e de se corrigir em alguns momentos. Na hora que ele perceber que ele não tem mais condições de fazer isso, ele tem que ser substituído. Ele vai se desculpar, alguém vai entrar, e ele foi substituído e começa um novo processo de conquista da confiança dele. Ele não pode perder a confiança, então tem que entender bem o que eu estou falando e que ele não pode ser desmentido, todos os sistemas tem que ajudar o tempo todo para que ele não seja desmentido, interferindo em tudo o que possa mostrar que ele está mentindo. Porque o fato de ele estar mentindo não significa necessariamente que o que ele fez não aconteceu. (28:50) Não é que ele não possa mentir, porque as vezes ele está falando a verdade, mas o oponente vai postar no twitter uma chuva tão grande de coisas falsas que vai parecer que o que ele falou é mentira. É aí que entra o sistema também. O sistema está ali para não deixa-lo mentir efetivamente e para não deixar que ele seja desmentido por nenhuma forma, principalmente se o que ele está falando é verdadeiramente o fato. Aí é que ele não pode estar mentindo mesmo. E o que acontece se esse sistema não estiver formado ? Quantas vezes nós não vemos você falar uma coisa que é a verdade e você ser desmentido por um fato que foi forjado mas que foi muito bem vendido por um sistema de informação que já está funcionando. (29:40) Então não adianta você chegar com a sua verdade ali se você não estiver com esse sistema montado. Então eu julgo que o sistema de informação é hoje o apoio ao combate, ou seja um multiplicador.

C: Inclusive na opinião do senhor, ele pode subir de status e ganhar o status de um sistema operacional?

N: Eu julgo que sim. Eu julgo que esse deve ser o caminho. Se não acontecer isso, nós não vamos conseguir a sinergia. Porque esses sistemas que nós estamos falando aqui eles ou são um sistema de primeira grandeza ou parte de um outro que não tem nada a ver com aquilo.

C: Então uma ideia é agrupar esses sistemas dentro de um sistema operacional informações para fazer isso ganhar sinergia. Para agrupar e montar uma estrutura para dar sinergia a isso aí.

N: Exatamente. E isso tinha que estar replicado, não basta fazer isso em Brasília, aqui nesse QG. Se isso não estiver replicado, porque não dá tempo. Tem que estar perto de tudo o que está acontecendo. E não interessa o que está acontecendo, volto a dizer, o importante é a versão que todo mundo está lendo nesse momento. Porque todo mundo que tiver um celular na mão, esteja onde estiver no mundo, ele vai estar lendo o que está acontecendo. Então aqui de Brasília você não vai controlar isso. Brasília tem que dar a direção geral, como tudo no Exército, para as coisas estarem alinhadas e tem que trabalhar a informação no nível nacional e mundial. E o nível regional é trabalhado lá embaixo, eu não sei quem. Eu acredito que esse dispositivo nós tínhamos que ter pelo menos um igual a ele, com tropas constituídas, que eu não sei se seriam pelotões, companhias ou batalhões nas Divisões de Exército que, para mim, tinham que ter esse caráter. De maneira que cada Comando Militar quando um batalhão fosse empregado, uma companhia, qualquer coisa que estiver acontecendo... hoje nós temos 81 operações acontecendo no Exército. Estou dando um dado da semana passada. Quantas dessas operações estão sob esse guarda-chuva das operações de informação? O que deve estar acontecendo hoje? Nós estamos perdendo oportunidade de comunicar 81 ações que devem estão acontecendo nesse momento. Se nós tivermos esses sistemas acontecendo, pelos canais técnicos, como já acontece hoje, você teria a imprensa local, a imprensa não, as pessoas, porque não é só a opinião publicada, porque a imprensa é só uma parte. Antigamente você tinha que controlar

a imprensa, hoje em dia acabou isso. Você controla a imprensa, o governo controla, ou muitos governos controlam pelo menos parte das suas imprensas mas quem controla um twitter? Quem controla uma rede social? O governo pode controlar parte delas, pelo menos é o que a imprensa está noticiando. O governo está pagando, porque aí você vê quem controla e vê quem são os patrocinadores daquele site, daquele blog, você vê Banco do Brasil, Caixa Econômica, etc., então você está vendo quem está patrocinando. Na realidade o governo pode controlar parte das redes sociais mas a rede social tem um espaço infinito, que não tem limites, para qualquer um interferir, inclusive nós. (33:05) Então, se nós estivermos, localmente tem que ter alguém fazendo alguma coisa. E, ao mesmo tempo, naquilo que vale a pena ou naquilo que precisa ser reforçado, no nível nacional, tem que estar reforçado daqui de Brasília, na imprensa nacional. O Globo, no Rio de Janeiro, tem que publicar isso, os twitters do Rio de Janeiro tem que estar comentando isso. A rede social do Rio de Janeiro tem que comentar tal assunto? Então vai comentar. Nós vamos ter que botar isso no ar, lá, comentado. Nós vamos ter que jogar isso lá ar. Algumas coisas não podem ser oficiais, porque se entrar com chapa branca ninguém vai ler. Algumas coisas vão ter que entrar por outro caminho, mas tem que estar no twitter das pessoas. Não sei que caminho vai ser esse aí que vocês vão ter que descobrir, mas acho que tem que estar. E quem controla isso? Brasília. O troço aconteceu na Amazônia, mas se tem interesse que seja do nível nacional, vai ter que repercutir nos grandes centros, para que aquilo chegue na imprensa dos grandes centros. E algumas coisas vão ter que sair daqui. Vai ter que chegar no mundo, vai ter que entrar na imprensa internacional. Quais são os sintomas de quando você começa a perder a guerra da informação? Começa nos twitters, nas redes sociais, imprensa, protestos de rua, recomendações nos organismos internacionais, até chegar na condenação pelos organismos internacionais, até chegar na Resolução. (34:35) Esses são os passos. Se o governo não mudar de opinião antes, de interromper uma operação antes, ele tem várias oportunidades de interromper. Quando ele começa a perceber na opinião publicada, depois nos movimentos de rua, depois nas recomendações, a Síria acabou de perder embaixadores no mundo, várias pessoas expulsando os seus embaixadores fruto dessa opinião pública que está virando, na hora que isso chegar ao nível de Resolução do Conselho de Segurança, acabou, não tem mais jeito. Aí, só se for loucura se ele quiser manter aquilo.

C: E aí você tem o emprego do meio da força justificado.

N: Aí você vai justificar a operação da era industrial contra você. Então eu acredito que a operação de informação ela tem que estar... e nós temos que começar a treinar isso quando sai o pelotão para vacinar cachorro, quando sai o pelotão para ver a situação da dengue.

C: Isso é uma mudança de paradigma muito grande. Mas eu também acredito que é um caminho muito plausível.

N: Temos que pensar nisso. Senão nós não estamos entendendo o que é a rede social, o que é a opinião pública. Nós não podemos achar que as pessoas vão entender o que nós estamos fazendo, só porque a gente está fazendo. Nós temos que estar nos comunicando. Se não fizermos isso, o outro lado vai se comunicar. E vai ficar valendo só o dele. E aí nós vamos ser reativos. Eu acho que o sistema de informações públicas ou de comunicação social, aí depende de como vai se chamar, eu não digo que ele tem que ser o central, porque aí eu vou estar desprezando outros sistemas que cada hora um vai prevalecer. Eu digo que ele é o visível, a ponta do iceberg. (36:20) E não é mais importante que nenhum deles.

C: Tem que ter o pessoal trabalhando em torno.

N: Esse cara não pode ficar na berlinda. E o sistema de informação vai escolher um, e esse cara é a cara conhecida. Todos os repórteres tem celular dele e ele tem o celular de todos os repórteres. Ele sabe quem publica o que, ele sabe como chegar até a imprensa.

C: A engrenagem trabalha para ele. Na realidade, ele é a parte visível da engrenagem.

N: Essa cara tem que estar disponível 24 horas com o celular dele. Nós não podemos receber uma consulta e no dia seguinte dar a resposta. Isso não adianta nada, isso não é informação. A operação de informação tem que ser uma coisa ágil.

Eu já vi exemplo, o Exército já deu exemplos bons disso. A operação Guanabara em 2008 foi um exemplo muito bom disso. A gente não tinha ideia do que era aquilo ainda, pelo menos eu.

C: O senhor era o porta-voz ...

N: Era o porta-voz, mas por acaso. Eu estou falando assim porque eu vivi de dentro. Mas não foi uma operação do porta-voz. A operação psicológica estava o tempo todo junto. Quando eu estava falando uma coisa em uma comunidade daquela, aquele "carro da pamonha" lá estava falando a mesma coisa ali atrás, com aquele alto-falante e os repórteres viam o que estava acontecendo. O sistema estava impedindo que eu fosse desmentido. E a inteligência me dizia o tempo todo o que eles sabiam e o que deveria ser contado, inclusive, porque eu tenho que ter a proatividade.

C: O senhor não tinha só o dado, o senhor tinha o trabalho de inteligência, a análise feita também.

N: Exatamente. Então eu julgo que essa operação foi uma das operações que eu vejo assim, top de linha. E aí eu dou esse exemplo. Eu acho que a Divisão de Exército é o escalão melhor para isso estar montado. Não a Divisão de Exército de hoje. Eu me refiro ao Centro de Operações (C Op). Porque a Divisão de Exército de hoje está presa numa estrutura da era industrial. Aquilo enxuto, sem aqueles dispositivos mais um General de Divisão experiente, com um Estado-Maior parrudo o que você vai economizar descontinuando essas ações da era industrial, mantendo o número de divisões que o Exército achar que tem que manter mas não se deve criar um C Op onde já existe uma DE. Aí são duas estruturas para fazer a mesma coisa. Então, aonde já tem uma DE, é esse o escalão. E ela não pode ter aquela ideia da era industrial que ela está aí para coordenar de duas a cinco brigadas. Não interessa se tem uma companhia única trabalhando. Se tiver uma companhia, todas as missões que saem do quartel, essa estrutura tem que estar junto. Ela tem que treinar, "brifar" o Capitão que irá comandar a operação, "brifar" com ele, às vezes o próprio Capitão é o iceberg, não precisa estar o porta-voz. O próprio Capitão vai ser. Ele vai numa coisa muito localizada, mas ele tem que ser "brifado".

C: Dá inclusive a credibilidade porque ele é o cara que está fazendo, não é um cara de fora.

N: Esse Capitão vai ser “brifado” e vai ser o tempo todo alimentado por esse sistema. A cibernética, enquanto esse Capitão está cumprindo essa missão, está lendo tudo o que puder ler em relação a aquilo. E ela tem que estar medindo com um painel de controles. Você está vendo os ponteirinhos ali. Então é um painel de avião. O setor de informação é um painel, é aquele monte do botõezinhos. De repente algum começa a entrar no vermelho, estamos perdendo a guerra da informação em tal área em tal posição por isso e aquilo. Estou vendo aqui o que está saindo na mídia, no twitter, o que está comentando. E o comandante da operação com o seu estado-maior, em todos os níveis, ele está lá na rua sentindo a temperatura, ele está passando isso para o sistema. Isso aí não é desprezado, isso aí continua acontecendo. O que vai acontecer, o desavisado olha para aquilo e acha que não tem nada diferente. Não mudou nada na guerra, não mudou nada realmente, os sistemas continuam ali. (40:30) Eu não estou falando de GLO, isso tem que ficar claro, isso pode estar acontecendo durante a batalha principal da guerra pesada, mas mesmo aquela batalha precisa de uma estrutura dessa. É um sistema a mais. Isso não quer dizer que os outros sistemas todos não têm que estar funcionando, todos tem que estar funcionando. Todos os que se aplicam àquela operação estão funcionando, inclusive os típicos da guerra da era industrial, vão ser usados se for necessário e o comandante decidir. Mas se o comandante decidir usar um meio duro desse da guerra industrial é bom que o sistema de informações, com pró-atividade já comece a preparar. Já começa a jogar na opinião pública que está pintando a necessidade de uma ação dura, porque o oponente está fazendo isso, está fazendo aquilo, está abusando, está matando, matou a criança, matou não sei aonde, já prepara, porque ele entrar como entrou agora nessa cidade síria, faz uma semana, que entrou com carro de combate e morteiros, com arma curva, não sei se foi morteiro ou artilharia. Mas quando ele entrou com carro de combate, eu fiquei impressionado que a imprensa brasileira chamou de carro de combate, não chamou nem de tanque nem de blindado, quando ela chamou de carro de combate e estava atirando de artilharia na cidade, ele perdeu a guerra da informação. Perdeu ali já,

não adianta o que vai acontecer lá. Pode acontecer o que for, ele entrou com carro de combate e ele não conseguiu comunicar porque ele fez isso.

C: Não conseguiu justificar o emprego daquilo ali.

N: Você lê a notícia e lá no último parágrafo ele vai dizer o que estava acontecendo dentro da cidade, o que o outro lado estava fazendo, você vê, perdeu a guerra da informação, e perdeu mesmo. Tanto que, por causa daquilo, já tem uma comissão independente da ONU entrando, já foram expulsos embaixadores de vários países e o cerco deu uma estrangulada muito grande por causa daquela ação, que foi típica de excesso de força ou de força mal comunicada.

C: A mídia, a primeira coisa que fez, foi alinhar os corpos das crianças e fotografar.

N: Eu não diria que foi a mídia que fez isso. Eu diria que foi o sistema de informação do oponente que montou, botou o corpo da criança do lado do adulto, enrolados por pano. Não sei nem se havia corpos ali embaixo, e isso é irrelevante. A comissão independente da ONU é que vai dizer isso, sei lá quando. Ali tinha alguma coisa que pareciam adultos e depois alguma coisa que pareciam crianças. Inclusive era estranho porque as crianças estavam todas alinhadinhas, parecia que todas as crianças eram do mesmo tamanho, para chamar atenção realmente que todas eram crianças realmente. O que será que tinha ali embaixo? O fato é que foi aquela a imagem que eu vi, que você viu, todo mundo aqui viu. E eles não tiveram a capacidade de mostrar as outras imagens que fizessem a contraposição disso, e mostrar que o objetivo estratégico dele estava certo. Vamos analisar o caso da Síria, um minutinho para falar da Síria. Não interessa o que está acontecendo lá. Parece que a Síria acha que a guerra é ganha na força, como ela foi ganha por muito tempo. Então ele ou não está conseguindo realmente decolar com o sistema de informação dele ou está interpretando a guerra como ela deveria ser ganha na era industrial. Não é só a Síria, o americano fez isso, agora, acabou de fazer recentemente. As pessoas que não entendem o novo paradigma continuam insistindo no anterior, continuam usando força. (44:14) Agora põe mais força, agora põe mais força ainda, e vai aumentando, o americano vai escalando. Ele está lá no Iraque, não está

resolvendo, o que ele faz? Ele não bota mais sistemas de informação, ele bota mais tropas. E aí ele bota mais tropas ainda, e aí ele bota mais tropas ainda, até ele achar “bom, agora eu resolvi”. Ele abafou tudo, na realidade, e quando ele começa a tirar as tropas, o problema começa a voltar de novo, porque ele não resolveu o problema. Ele simplesmente enfiou mais brigadas, e mais brigadas, e mais brigadas. Ele precisa fazer isso. Ele tem que fazer isso. Então é um problema interno deles lá. A Síria está resolvendo uma guerra da era da informação, em 2012, usando os meios da era industrial. Ele está colocando carros de combate dentro da cidade. Para que ele colocou carros de combate naquela cidade? Tinha carros de combate do adversário ali? Ia ter uma guerra de blindados ali dentro? Por que não foi lá a pé naquela cidade? Ele não ia ter aquela imagem. Aquela imagem ele teria negado. Para que ele enfiou carros de combate? Para que ele atirou de morteiro dentro da cidade? Ele acertou o que com aqueles tiros de morteiro ali dentro? O que ele ganhou com aquele tiro ali? Ele não ganhou nada. Para que você usa esse tipo de arma? Você usa para vencer uma resistência pontual, numa área, negar. Você vê lá para que você usa apoio de fogo e vai na cartilha ali. Para que ele usou aquele troço ali dentro? Não entendi para que ele usou aquilo. Perdeu a guerra da informação ao utilizar dois meios que eram os mais nobres da guerra industrial e vão continuar sendo importantes na guerra industrial. Onde eles se aplicam. Onde você justifica. Usar esse troço dentro da cidade, está perdendo a guerra. Cidade é lugar para tropa a pé, com proteção mecanizada para as primeiras fases, eu me refiro a um carro como o Guarani, por exemplo, a infantaria mecanizada. Tão logo que aquela primeira resistência armada tenha sido eliminada, é a pé. É tropa a pé, não tem que botar mais nada ali dentro, com sniper nos pontos mais altos. A pé, pulando o muro, entrando e operações de informações. Esses outros meios, se você botar na cidade, você está dando um tiro no pé. O israelense faz isso, o americano fez isso lá. Ele tinha o carro de combate, fazer o que com aquilo? Botava na cidade. O que o carro de combate estava fazendo? Apoiando a operação urbana. Caramba, precisava de um carro de combate? É um subemprego de um carro de combate.

C: Um carro mecanizado fazia isso...

N: Fazia isso. Com a vantagem de que dentro de um carro mecanizado tem nove pessoas. Ou sete, oito, depende do país.

C: A guarnição do carro de combate não desembarca...

N: Não desembarca. Então o que ele está fazendo com aquele carro ali? O carro de combate era usado, você emassava, rompia, manobrava e cercava ou destruía ou perseguia, num E Prog, num eixo grande, ou seja, feito para outro tipo de guerra. Ele dentro de uma cidade, não agrega muito valor. Não dá para eliminar essa possibilidade aqui, sentado nessa mesa. Os fatores da decisão vão indicar, mas essa guerra no meio da população é guerra para tropa a pé.

C: Numa cidade não evacuada ...

N: Isso. A cidade está normal. A cidade continua funcionando, o comércio está aberto, tem aula. Suspende a aula num dia, no dia seguinte a escola abre de novo, as crianças vão para a escola. Você está ali no meio daquela confusão e as escolas estão funcionando. É assim, você viu isso aí. A coisa funciona assim. A operação nossa no morro do alemão em 2008, as escolas todas funcionaram. E nós tínhamos ali dois ou três mil soldados armados com munição real. Não sei quantos bandidos estavam ali dentro e as escolas funcionando.

C: E as professoras achando ótimo, porque tinha segurança.

N: É, eu olhando aquilo, os repórteres falando “Coronel, nunca tinha vindo aqui. Nunca tinha vindo. Eu tinha vindo até três quarteirões para baixo ali, uma vez que o BOPE veio. Para chegar ali trocou tiro pra caramba, nós conseguimos chegar até ali. Aqui eu nunca tinha pisado, vou aproveitar para tirar fotos aqui.” As pessoas às vezes falam em cidade e raciocinam logo com combate em localidade. Eu não sei qual foi o último combate em localidade. Talvez tinha sido Falluja ou Grosny, não sei, clássico. Então, a guerra de hoje, não é combate em localidade. As pessoas não podem confundir a guerra de hoje com combate em localidade, que é a primeira associação que a nossa mente, treinada para guerra industrial faz. É combate no meio das pessoas na cidade que está com a sua vida normal. Isso é guerra, isso não é operação de polícia, é guerra. Porque está normal hoje e amanhã tem um tiroteio daqueles de 10 mil tiros e de durar 3 horas como aconteceu várias vezes no Haiti. E,

no final da tarde, aquela mesma tropa que participou daquele tiroteio, descansaram um pouco, vai fazer um ACISO no mesmo bairro, no mesmo bairro, dois quarteirões para lá. Essa é uma guerra, falar que isso não é guerra, caramba, o que faltou para aquilo no Haiti ser considerado guerra? Faltaram minas e morteiro, artilharia.

C: Apoio de fogo por parte do oponente...

N: O oponente tinha armas anticarro, tinha granadas, tinha fuzil para caramba, tinha munição a suficiente para sustentar horas de tiroteio. Então falar “isso não é guerra, é operação tipo polícia”, então eu não sei o que é guerra. Quer dizer, eu sei o que é guerra, mas essa guerra que a gente está querendo não tem ocorrido e a probabilidade dela ocorrer aqui, no nosso teatro é muito pequena. Agora, essa outra guerra, está acontecendo todos os dias. Hoje, se não estou enganado, são 21 guerras no mundo, conflitos né? Então nessas 21, se nós dermos um zoom agora nas 21 guerras e também no morro do alemão, você não vai saber o que é o que. Talvez você consiga adivinhar por causa dos tipos de construção ou pelas pessoas. Se você der um zoom em todas as 21 guerras de hoje e mais o alemão que não está computado nessa aí, eu duvido que nós consigamos ver o que está muito diferente dali. Não vai ter muita diferença. O Haiti está hoje na fase normal. Nós vivemos lá de 2005 a 2007 muito combate ali dentro, muito combate.

C: Era interessante, cada contingente foi conquistando um pedaço do terreno até chegar no mar.

N: E sem nunca ter perdido a confiança da população. Agora, esses sistemas de informação no Haiti, não existiam no começo. O 3º contingente não tinha nada. O primeiro destacamento de forças especiais foi criado no 4º contingente. Operações psicológicas foi no 5º ou no 6º, ou seja, a função de Estado-Maior específica da relação civil-militar foi criada no 9º contingente. Aliás isso estava fazendo falta naquela minha lista que eu estava tentando. A base do sistema de informação, também está ali em baixo a cooperação e coordenação civil-militar, a CIMIC. Até hoje nós ainda não chegamos a esse objetivo.

C: O problema foi o terremoto, que impediu os avanços. Coronel, muito obrigado e espero ter trocado algumas experiências com o senhor.

N: Eu agradeço, aprendi muito naquela parte inicial e acho que isso é fundamental, nós precisamos colocar essas coisas em debate, vai ser difícil porque tem uma resistência muito grande ainda de pessoas de alguns sistemas que querem continuar a prevalecer. Todos continuam sendo importantes.

## Transcrição 02

Entrevista com o Major (R/1) Alan E. Brill[138], do Exército Americano, atualmente *Senior Managing Director* da *Kroll Advisory Solutions*, realizada em 10 de maio de 2012.

Mr. Brill foi palestrante convidado pelo Centro de Excelência – Defesa Contra o Terrorismo (COE-DAT) da OTAN, em Ankara – Turquia para ministrar dois módulos e conduzir o painel de discussão final do curso de Terrorismo Cibernético realizado pelo autor de 07 a 11 de maio de 2012. Com larga experiência em segurança da informação, proteção cibernética e análise forense, Mr. Brill foi um dos responsáveis pela proteção cibernética da campanha presidencial de Barack Obama e John McCain nas eleições americanas de 2008.

Como a finalidade dessa entrevista era de apreender novos conceitos acerca do que a OTAN chama de terrorismo cibernético e sua aplicação na doutrina de defesa cibernética, aproveitando o passado militar do palestrante e sua experiência em lidar com proteção cibernética, a mesma foi conduzida de forma semi-estruturada, com algumas perguntas previamente preparadas e com um direcionamento para o objetivo proposto. Mesmo assim, optou-se por não realizar a simples resposta às perguntas formuladas, havendo a preocupação de deixar o entrevistado à vontade para expor os seus pontos de vista, que apresentam uma visão realista das ameaças que estão ocorrendo, integrando visões do setor militar e da iniciativa privada. Como a entrevista foi concedida na língua inglesa, a transcrição representa uma tradução livre da entrevista concedida, com pequenas adaptações em termos e expressões idiomáticas empregadas. A entrevista teve a duração

[138] Informações mais detalhadas sobre Alan Brill: http://www.krolladvisory.com/professionals/alan-brill/

aproximada de 34 minutos e foi concedida um dia antes do final do curso do COE-DAT em Ankara – Turquia.

LEGENDA: C – João Marinonio Enke CARNEIRO (entrevistador);
B – Mr Alan E. BRILL

C: Qual é o seu nome ?

B: Alan E. Brill

C: O senhor poderia comentar a sua experiência profissional relacionada ao setor cibernético ?

B: Eu sou Diretor de Gerenciamento Sênior de uma companhia privada chamada "*Kroll Advisory Solutions*". É uma companhia que está no mercado em torno de 40 anos e nós provemos assistência a governos e corporações na área de segurança cibernética. Eu tenho um grau de bacharelado e mestrado na Universidade de Nova York e me graduei no "*US Army Command and General Staff College*" (equivalente à ECEME) e me graduei no *National Security Management Program* no *Industrial College of the Armed Forces da National Defense University* em Washington. Eu fiz também todo o curso de doutorado, menos a tese na Universidade de Pace em Nova York. Eu escrevi duas teses de doutorado, mas vendi as mesmas para a editora Prentice-Hall, como livros texto.

C: Então isso foi mais lucrativo ?

B: Foi muito mais lucrativo. Então estou no ramo da segurança da informação, em tempo integral desde 1974. 24 anos na Kroll, parte dos quais fui diretor de sistemas de informação e segurança das informações do departamento de investigação da cidade de Nova York e parte dos quais eu fui subinspetor geral da cidade de Nova York. Eu passei três anos em uma organização de pesquisa chamada Yourdon, iniciada por Ed Yourdon. Ed foi o matemático que desenvolveu a programação, análise e design estruturado e eu trabalhei com ele por três anos, implementando características de segurança e controle em sistemas que foram

desenhados utilizando a sua metodologia e escrevi alguns livros sobre isso. Antes disso, eu trabalhei na Ernest & Young como consultor de segurança da informação. Eu servi no governo 3 vezes, na primeira na cidade de Nova York, como militar eu fui Major do Exército Americano e na Reserva do Exército Americano e passei para a reserva com 38 anos de serviço comissionado. Antes disso, eu estava no grupo de desenvolvimento de sistemas da NASA, desenvolvendo softwares para o sistema de suporte de solo do programa Apolo, de pouso na Lua. Escrevi 67 livros, várias centenas de artigos. O que posso fazer, se você achar útil, é fornecer para você o meu portfólio com as publicações nos últimos anos.

C: O desenvolvimento de Doutrina Militar de Defesa Cibernética está em progresso na maioria dos países. A maioria dos países está conduzindo operações e então irá escrever uma doutrina. O senhor acha que essa abordagem é adequada?

B: Eu realmente não acho. Se você olhar a situação que se apresenta para a maioria dos militares, e para a maioria dos governos, você tem gastar... bem, o que eu descobri ao longo dos anos é que uma organização militar ou governamental tende a não aproveitar o conhecimento do setor privado tanto quanto ela provavelmente pagou por isso. Nem toda área das operações militares têm uma contraparte civil, mas segurança da informação é uma das áreas que estão sob a responsabilidade tanto dos militares quanto de outros setores do governo. Há uma comparação quase direta entre o que as corporações multinacionais têm que fazer. Eu acho que se colocarem os planejamentos juntos, examinarem os padrões que são seguidos no setor privado, isso iria fornecer informações para servir de base para os planejamentos [militares]. Se você está em uma situação onde estão ocorrendo operações e então você sai para escrever um plano, o problema com o qual você tem que lidar é que, até que você tenha um planejamento ao menos aprovado preliminarmente, é que cada um está fazendo o que acha correto por sua conta. Eles estão fazendo da sua maneira. Em segurança das informações, ter as coisas sendo feitas por conta do que cada especialista acha certo pode não ser uma boa coisa. Você precisa de uniformidade no programa. Em contrapartida, o problema é que algumas vezes é difícil de mudar, difícil de manter e de ter todas as mudanças finalizadas. Vou dar um exemplo: se eu estivesse escrevendo um livro de operações de informação alguns anos atrás eu provavelmente diria: tenham foco no perímetro

da rede e mantenham os atacantes fora. Mas hoje eu não diria mais isso. Eu diria para focar no perímetro e fazer tudo o que for possível e razoável para manter os atacantes fora, mas entenda que eles provavelmente vão conseguir entrar na sua rede, porque há pontos de falha demais. Hardware, software, redes, humanos. Pessoas cometem erros. Então eu acho que a doutrina muda do “mantenham os atacantes fora”, para “tentem manter os atacantes fora, mas gastem os recursos necessários para reconhecer quando um oponente penetrou a sua segurança da informação e está agora operando de dentro da sua rede”. A habilidade de vê-los e de perceber que algo de errado está acontecendo é absolutamente vital. (7:45). Deixe-me fazer uma pergunta: você já leu os dois artigos escritos pelo Subsecretário de Defesa Americano William J. Lynn III na revista Foreign Affairs ?

C: Ainda não.

B: Eu recomendo fortemente a leitura desses artigos. O primeiro eu creio que foi publicado por volta de Setembro ou Outubro de 2010[139]. Nesse artigo, o secretário Lynn revela um vazamento massivo de informações nos sistemas militares americanos, o pior na história do país. Alguém colocou um pen drive infectado em um computador no Oriente Médio. Aquela infecção se espalhou tanto em sistemas de caráter ostensivos quanto sigilosos tal como um incêndio sem controle. Ninguém sabia o que estava acontecendo durante meses. (8:53) Como o secretário Lynn falou na revista, este é o cenário da pior hipótese. O seu adversário está dentro do seu sistema, acessando o que você está fazendo, quase em tempo real, e você nem ao menos sabia que ele estava lá. Quando eles descobriram isso, como você pode imaginar, houve uma reação massiva dos militares americanos. Havia a intenção de fechar os sistemas e tentar descobrir o que havia acontecido. Se você olhar na revista Foreign Affairs, no ano passado (2011) foi publicado outro artigo[140] no qual eles falam nas lições que foram aprendidas decorrentes dessa intrusão e como a doutrina americana mudou para dizer: “não entre !”. Você pode

[139] LYNN III, William J. **Defending a new domain: the Pentagon´s Cyberstrategy**. Foreign Affairs Magazine, September / October 2010. Disponível em: <http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain#>. Acesso em: 10 mai. 2012.

[140] LYNN III, William J. **The Pentagon's Cyberstrategy, One Year Later: Defending Against the Next Cyberattack**. Foreign Affairs Magazine, 28 set. 2011. Disponível em: < http://www.foreignaffairs.com/articles/68305/william-j-lynn-iii/the-pentagons-cyberstrategy-one-year-later> Acesso em: 10 mai. 2012.

notar se o seu sistema tem a resiliência necessária para identificar o fato de que alguma coisa está errada, se você tiver a tecnologia de investigação necessária para descobrir o que está acontecendo, mantenha-se operando e permita-se evoluir com a segurança de acordo com as mudanças na tecnologia.

C: Então o foco mudou de “mantenha os oponentes fora” para “melhore a resiliência do seu sistema”?

B: Você continua tentando mantê-los fora, tentando fazer tudo o que você pode fazer em relação a isso. Mas, quando você faz o pequeno salto do “eu preciso mantê-los fora a todo custo” para “não importa o que eu fizer, eles conseguirão entrar em algum ponto”, isto representa uma mudança muito importante na doutrina. Se eu tiver uma pequena quantidade de dinheiro para a defesa cibernética e sempre há uma pequena quantidade de dinheiro para a defesa cibernética, não importa em qual país. E agora, deve-se pensar em dividir aquela torta de uma forma diferente. Então, ao invés de gastar o que eu costumava gastar na defesa do perímetro, agora eu vou gastar dinheiro em prevenção de intrusão, detecção de intrusão e sistemas de proteção contra vazamento de dados. Eu vou me preocupar muito mais em como meus logs (registros) funcionam e colocar mecanismos em lugares para consolidar e analisar os logs para transforma-los de um conjunto grande de dados (big data) para inteligência efetiva. E a evolução disso também aponta como você organiza uma organização militar para lidar com isso. Você tem uma responsabilidade difusa em manter esses sistemas funcionado e seguros ou você centraliza isso em um Centro de Operações de Segurança que consolida os logs, tem os melhores especialistas e tem condições de fazer alguma coisa e respeito.

C: Quais são as principais preocupações acerca da defesa cibernética nos dias de hoje?

B: Eu vou falar isso na minha palestra que será ministrada amanhã, onde irei discorrer sobre os 10 itens que estão se tornando os mais importantes. Então, eu acho que a coisa que mais assusta as pessoas no nosso campo é a velocidade que as mudanças ocorrem. Se nós olharmos como os sistemas eram desenvolvidos alguns anos atrás nós iriamos ver as pessoas utilizando ferramentas como Java, C++, .Net, provavelmente, Oracle, talvez SQL, mas o que é mais impressionante é

que isso está mudando muito rapidamente. Hoje você tem grande possibilidade de ver grandes volumes de dados (big data) usando algo como Hadoop[141], você pode ver os programadores escrevendo código em algo como “Ruby on Rails”[142] (13:40)

C: Essa é uma linguagem de programação muito nova.

B: Muito nova. Bem, inicialmente era somente Ruby então evoluiu para Ruby on Rails mas, obviamente, quando você olha para ela, percebe que a mesma traz grandes vantagens para construir sistemas modernos, então os programadores amam essa linguagem. E, você sabe, há hoje toda uma “biosfera” desenvolvendo em torno do Ruby. Mas, tanto quanto eu posso dizer, a maioria dos governos e seus militares não pensam muito nisso. O problema é: será que nós sabemos que os sistemas estão sendo desenvolvidos nessas linguagens e ferramentas ou está simplesmente acontecendo e ninguém está percebendo isso? Toda a vez que você insere uma nova ferramenta nessa situação, você tem que determinar que questões de segurança ela traz consigo e como você é capaz de lidar com isso. E isso representa uma questão muito séria. Eu acho que a evolução e a habilidade de evoluir o modelo de segurança rápido o suficiente para mantê-lo atualizado com a realidade. Qual é a realidade da segurança lá fora, o que os hackers estão fazendo, o que os governos estão fazendo, já que muitos estão desenvolvendo capacidades cibernéticas defensivas e ofensivas.

C: Então, o senhor está dizendo que uma doutrina deve ser mais genérica para lidar com todas essas mudanças e para que ela não necessite de grandes atualizações toda a vez que pequenas mudanças ocorram.

B: É exatamente isso que estou falando, Coronel. Se nós construirmos a nossa doutrina tão especificamente, a única coisa que podemos garantir é que ela ficará obsoleta rapidamente. Eu acho que uma doutrina deve enfatizar princípios e aspectos de longo prazo. E você então pode implementar a sua doutrina com

---

[141] http://hadoop.apache.org/ é uma biblioteca de software que permite o processamento distribuído de grandes bases de dados, utilizando clusters de computadores usando um modelo de programação simples. É feito para tornar escaláveis aplicações de poucos servidores para milhares de máquinas, cada uma oferecendo poder computacional local e armazenamento.

[142] http://rubyonrails.org/

políticas e procedimentos que podem ser, obviamente, muito mais específicos. Mas a questão é que, com qual frequência você deseja voltar e reescrever aquela doutrina básica? Eu creio que a resposta seja “não com muita frequência”. Você sabe, a frequência pode ser o nosso pior inimigo. De alguma forma pode ser simples escrever uma doutrina, mas não uma que cubra todos os aspectos em todos os detalhes. Eu diria que os aspectos não devem ser aprofundados em muitos detalhes para que ela possa se tornar flexível, porque ela deve ser capaz de interoperar com as leis nacionais dos locais que você tiver que utiliza-la, ela deve ser congruente com os padrões adotados para a segurança da informação, deve utilizar as ferramentas apropriadas, que devem ser licenciadas e as suas licenças mantidas. É uma esfera complicada mas eu acho que você deve listar os princípios, aqueles que não mudam tanto.

C: Princípios, categorizar ações, por exemplo, o início da doutrina cibernética no Brasil categoriza três ações: Proteção Cibernética, Exploração Cibernética e Ataque Cibernético. É uma divisão bem simples.

B: Então você pode dividir cada uma dessas categorias. Proteção Cibernética pode ser dividida em vigilância cibernética, monitoração ativa, gerenciamento de redes e gerenciamento de dados. Uma das grandes evoluções no aspecto dos dados é o que eles chamam de “big data”[143]. As leis que estão sendo aprovadas relacionadas a dados, leis de privacidade, leis relacionadas à requisição de notificar pessoas quando os seus dados são perdidos estão claramente se espalhando por todo o mundo. Mas se você olhar as coisas que aconteceram nos últimos anos na área legal, todo o assunto de descoberta eletrônica que está em cada ação cível onde as partes brigam por dados levou as pessoas a se darem conta de quanto valem os dados para as corporações. Eu mantenho uma grande percentagem dos dados que existem na minha companhia, talvez quase tudo. Não ajuda. É só um risco. Onde nós estamos envolvidos em fazer análises de segurança nós olhamos para essas coisas. Isso é o que é visto hoje, em nosso mundo. Mas a doutrina deve

[143] Em tecnologia da informação, “big data” se trata de um conceito, no qual o foco é o grande armazenamento de dados e maior velocidade. O software de “big data” recolhe todos os dados que uma organização gera e permite que os administradores e analistas se preocupem em como usa-los mais tarde. Neste sentido são mais escaláveis do que os bancos de dados tradicionais e os “datas warehouses”.

ser razoavelmente de alto nível. E as suas referências mais detalhadas, colocadas em instruções. O que é interessante é que eu fiz alguns trabalhos envolvendo um padrão de segurança da informação que foi implementado pela Associação de Química Americana e que, para certificar esse programa, foi necessário deixar que as coisas fossem examinadas e conversar com as pessoas mas eles também queriam ser aderentes às séries de normas ISO 27000[144] e outras normas americanas. O que nós dissemos a eles foi que nós descobrimos que a maioria dos controles têm muitas partes sobrepostas. E nós viemos com algumas ferramentas que permitiam que você visse a sobreposição e possibilitavam que você tomasse as decisões uma vez, não sendo necessário tomar cinco vezes a mesma decisão. Mas quando você precisa tomar as decisões em ambientes mais amplos, você precisa de mais inteligência, você tem uma probabilidade maior de tomar a decisão certa. (21:10) Nós não somos uma empresa de pesquisas nesse sentido, mas eu suspeito que eu possa ver entre 100 e 150 violações de dados por ano, eu realmente olho para eles, examino as fontes da violação e tentamos fornecer aos clientes e amigos informações de como poderá ser o próximo ataque.

C: Então, quando você analisa esses ataques, há alguma diferença entre ataques conduzidos por Estados-Nações ou outros tipos de grupos?

B: Essa é uma pergunta realmente boa. E a resposta é: algumas vezes. Estados-Nações tendem a ter recursos para gerar mais ataques tipo “zero-day”[145] do que uma organização terrorista. Não estou dizendo que uma organização terrorista não pode utilizar um software muito, muito específico. Eles podem. Somente é necessário uma ou duas pessoas para escrever essas coisas. Você não precisa recrutar todo mundo. Mas quando você olha para isso, um ataque patrocinado por um Estado pode ter um conjunto de ferramentas mais sofisticado sendo utilizado e mais pessoas em torno do seu desenvolvimento do que vemos todos os dias no setor privado. Se você é compatível com a ISO 27000 e também tenta ser compatível com cinco outros padrões, pessoas cometem o erro de tentar construir

[144] As normas ISO da série 27000 tratam de padrões para segurança da informação. Podem ser encontradas em http://www.27000.org/.

[145] O ataque zero-day (ou zero-hour, 0day ou zero day) é uma ameaça de computador que tenta explorar vulnerabilidades nas aplicações ou sistema operacional do computador que estão desconhecidos ainda até pelos próprios fabricantes do software, reservadas apenas para o hackers, ou para as quais não ainda não há correção de segurança disponível.

suas operações pelo padrão. Nós dizemos para comparar os padrões e achar os pontos em comum e aí utiliza-los.

C: Desde que esses tipos de ataque podem ser conduzidos por Estados-Nações, grupos terroristas, indivíduos ou gangues criminosas com diferentes motivações...

B: Crime cibernético é terrorismo cibernético com motivações diferentes. Você não tem que ter uma base ideológica para o que está fazendo.

C: Então nós estamos olhando para algum tipo de operação dual. Você tem Estados-Nações com mais recursos, utilizando ferramentas mais avançadas ou de desenvolvimento mais recente e outros grupos, indivíduos, terroristas ou criminosos cibernéticos. Você acha que é importante do desenvolvimento de parcerias amplas com universidades, centros de estudos, para lidar com essa situação? Por exemplo, no Brasil, o setor bancário é muito forte. Eles possuem pessoas muito capacitadas para lutar contra o crime cibernético, lutar protegendo as suas redes do crime cibernético. O que você acha do estabelecimento desse tipo de parceria?

B: Eu acho que isso se torna inevitável. O que nós estamos vendo é que o setor público está perdendo investigadores cibernéticos e especialistas. O setor público está terceirizando os especialistas para realizar os trabalhos. Por exemplo: alguns anos atrás o governo fazia todas as credenciais de segurança. Não faz mais. Eles terceirizaram para algumas poucas empresas diferentes. Quando alguém procura o governo para realizar algo e fornecem o número do seguro social como referência, eles são checados.

C: Esse tipo de situação leva para uma outra coisa. Por exemplo, se eu preciso conduzir uma operação militar com características sigilosas, eu devo contratar alguém, um especialista, ou eu poderia mobilizar um e dar a ele uma patente?

B: O que o governo americano fez quando eles necessitaram um aumento, eles criaram um programa chamado “*Advanced Degree Lieutenant*” (tenente de grau avançado) onde pessoas tinham somente uma função no serviço. Essencialmente

eram recrutados para aquela posição. Primeiro se negociava as qualificações necessárias. Mas eu acho que a coordenação entre as partes civis e militares tornaram-se mais importantes. Sem o setor público, será muito difícil para o governo atingir as suas necessidades.

C: Como deveriam ser os esforços de coordenação entre os militares e o setor privado?

B: É sempre um problema quando os militares precisam transferir informações para fontes na iniciativa privada para que isso não seja tornado público. Não é a minha especialidade mas você precisa saber o que é realmente importante.

C: O quão importante é este tipo de operações ser conduzido como uma operação militar? Por exemplo, eu deveria tratar esse tipo de ação de proteção cibernética ou eu preciso conduzir uma exploração cibernética ou ataque cibernético como uma operação militar ou como uma operação clandestina junto, o Brasil não tem isso, com o Serviço Secreto ou a CIA?

B: Isso depende do tipo de operação. Há algumas operações que devem ser conduzidas em coordenação com as estruturas militares. Interdição de comunicações, você sabe que em muitos lugares estas as pessoas estão se comunicando por meio de telefones celulares, interferindo em redes de telefones celulares. Mas o ponto chave está em como você quer fazer com que isso se pareça. Todos estão fazendo da mesma forma. Eu sou um grande fã da centralização e dos padrões.

C: O senhor acha que se essas operações forem conduzidas por militares você terá padrões e procedimentos mais claros?

B: Eu acho que deveria, mas o problema é se irá ocorrer. Ter um padrão não ajuda se as pessoas não acreditarem nele. Elas não o seguirão. Minha preocupação é, quando você está conduzindo uma operação, você precisa pensar em quais serão as consequências informacionais. Nós teremos que bloquear comunicações? Pense sobre interdição da internet. O que o outro lado vai fazer? Eles vão nos atacar

utilizando a cibernética? Isso muda a forma de como você vai planejar. Nós temos a determinação para fazer isso? Eu não sei. Eu vi os Estados Unidos cometendo uma série de erros ao longo dos anos por não utilizar mais tempo para planejar corretamente. E partir para a execução correndo porque algum General deu a ordem para fazer. Isso não deveria ocorrer mais.

C: Você tem mais alguma ideia ou ponto para destacar?

B: O que nós iremos conversar amanhã durante a minha apresentação está perfeitamente alinhado com o que você está falando. Se você olhar para as dez questões que eu identifiquei. Eu acho que essas questões devem ser levadas em consideração no estabelecimento de uma metodologia de planejamento e elas poderão falar por mim amanhã.

C: Muito obrigado senhor Brill, eu apreciei bastante a sua entrevista.

B: Eu agradeço e espero que tenhamos a oportunidade de trabalhar juntos novamente em breve.

**ANEXO A**

Composição da Central de Monitoramento Cibernético da Rio+20

**CENTRAL DE MONITORAMENTO CIBERNÉTICO (C Mon Ciber) – Op Rio+20**

| Função | Nome | OM/Força | Observações |
|---|---|---|---|
| **CMDO (03) (Cel XXX )** | | | |
| **Comandante** | Cel | CD Ciber | Coor G Ass |
| **Subcomandante** | Cel | CD Ciber | |
| **O Lig com o CCOp Rio+20** | Cel | 2ª SCh EME | |
| **O Com Soc** | Maj | CD Ciber | Ass Com Soc |
| **Seção de Operações (16)** | | | |
| **Chefe** | Cel | CD Ciber | Ass Op (SCmt) |
| | Cel | CD Ciber | Ass Seg Ciber |
| | Ten Cel | CD Ciber | |
| **Adjuntos** | Ten Cel | CComGEx | Ass Def Atv |
| | 2 Of MB | MB | |
| | 2 Of FAB | FAB | |
| | Maj | 2º CTA | |
| **Auxiliares** | ST | CD Ciber | |
| | 1º Sgt | CD Ciber | |
| | 2 SO/Sgt MB | MB | |
| | 2 SO/Sgt FAB | FAB | |
| | 3º Sgt | CITEx | |
| **Seção de Inteligência (05)** | | | |
| **Chefe** | Ten Cel | CIE | Ass Intlg |
| **Adjuntos** | Ten Cel | CD Ciber | |
| | Maj | CIE | |
| | Maj | CIE | |
| **Auxiliar** | ST | CD Ciber | |
| **Seção Polícia Federal (04)** | | | |
| **Chefe** | Delegado | PF | |
| **Adjuntos** | Perito criminal | PF | |
| | Perito Criminal | PF | |
| | Agente | PF | |

| Função | Nome | OM/Força | Observações |
|---|---|---|---|
| **Seção de Sistemas/BD (06)** | | | |
| **Chefe** | Cap QCO | CD Ciber | Ass Sistemas/BD |
| **Adjuntos** | 1º Ten QCO | CD Ciber | |
| | ST | DCT | |
| **Auxiliares** | Sgt | DCT | |
| | Sgt Mnt Com | CD Ciber | |
| | Cb | CD Ciber | |
| **Seção de C2 (10)** | | | |
| **Chefe** | Ten Com | BEsCom | |
| **Adjunto** | Ten Com | BEsCom | |
| | Sgt Com | BEsCom | |
| | Sgt Com | BEsCom | |
| | Sgt Com | BEsCom | |
| | Sgt Com | BEsCom | |
| | Sgt Com | BEsCom | |
| | Sgt Com | BEsCom | |
| | Sgt Com | BEsCom | |
| | Sgt/Cb/Sd | BEsCom | |
| | Cb/Sd | BEsCom | |
| **Seção de Logística (03)** | | | |
| **Chefe** | TC | CD Ciber | Ass log |
| **Auxiliares** | 1º Sgt | CD Ciber | |
| | Sd | CD Ciber | |
| **Outros (3)** | | | |
| Ch CDCiber | Gen | CD Ciber | |
| SCh CDCiber | Cel | CD Ciber | |
| EMP | Ten | CD Ciber | |
| | | | |
| **EFETIVO DESTACAMENTO – 50 homens** | | | |

1. Participação do Ch CDCiber e EMP no período de 17 a 23 jun
2. Participação do SCh no período de 05 a 17 jun
3. Motoristas civis contratados: **3 civis**
4. Funcionários civis prestando serviço de Operação Assistida: 06 **civis.**

**ANEXO B**

Fluxo de Informações da Central de Monitoração Cibernética da Rio+20

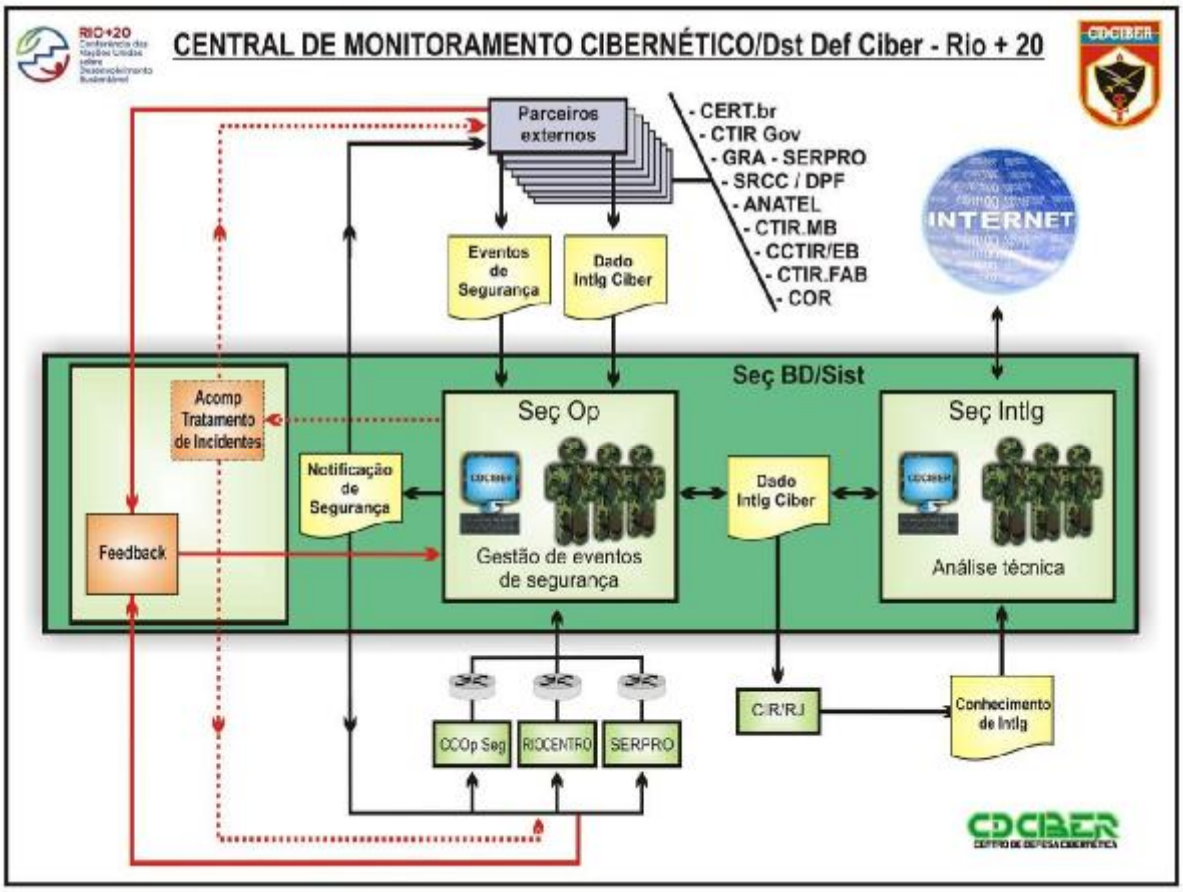



Figura 10 – Fluxo de Informações da Central de Monitoração Cibernética da Rio + 20

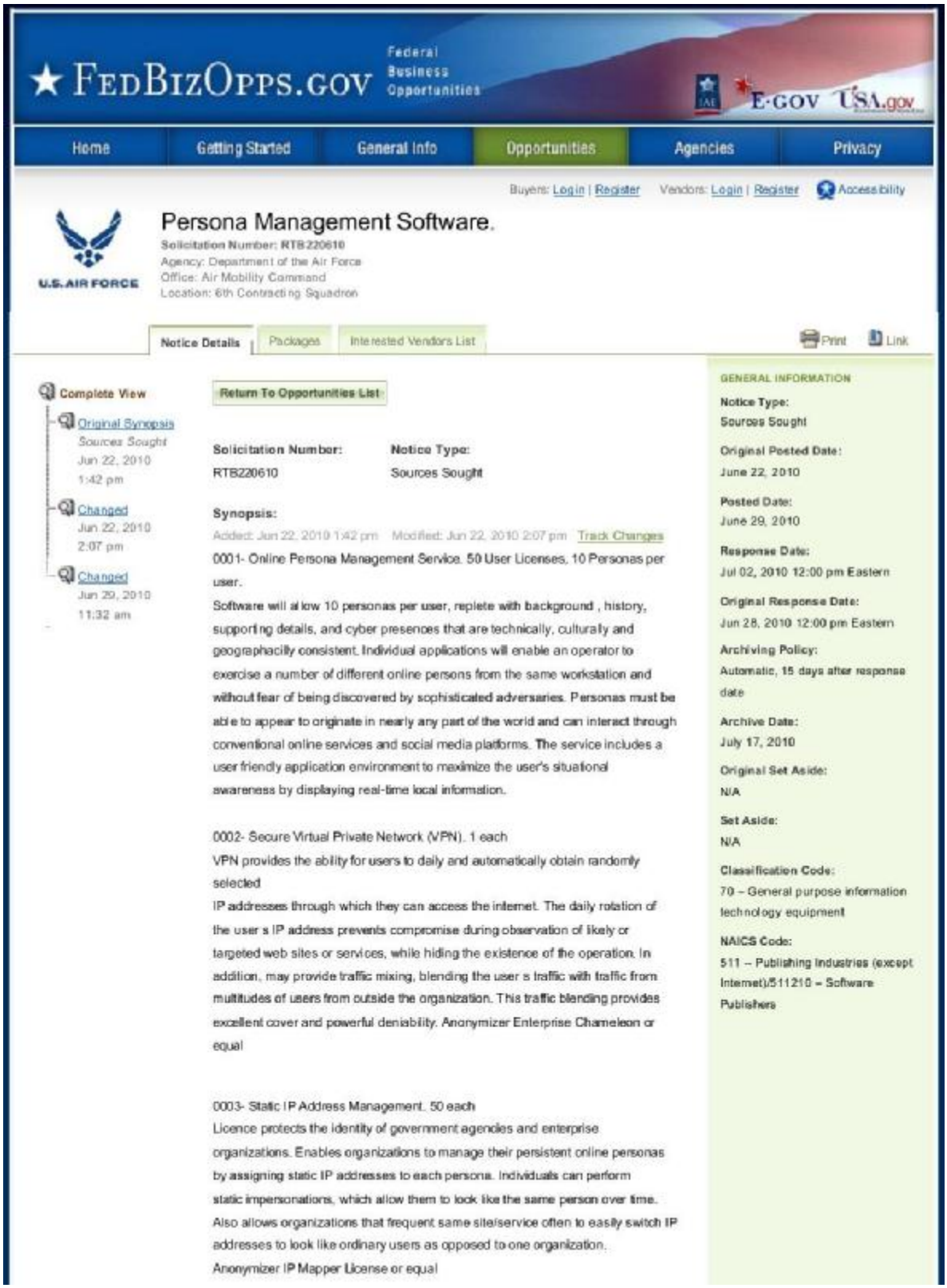
Fonte: Centro de Defesa Cibernética

Legenda:

| | |
|---|---|
| CERT.br | O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil |
| CTIR Gov | Centro de tratamento de incidentes de rede do governo federal |
| GRA | Grupo de Resposta a ataques do SERPRO |
| SRCC / DPF | Serviço de Repressão ao Crime Cibernético do Departamento de Polícia Federal |
| ANATEL | Agência Nacional de Telecomunicações |
| CTIR MB | Centro de Tratamento de Incidentes de Redes da Marinha do Brasil |
| CTIR FAB | Centro de Tratamento de Incidentes de Redes da Força Aérea Brasileira |
| COR | Centro de Operações Rio |
| CCOp Seg | Centro de Coordenação de Operações de Segurança |
| CIR / RJ | Centro de Incidentes de Rede do Rio de Janeiro |

**ANEXO C**

Edital para aquisição de software para gerenciamento de Persona Cibernética



FEDBIZOPPS.GOV Federal Business Opportunities

E-GOV USA.gov

Home | Getting Started | General Info | Opportunities | Agencies | Privacy

Buyers: Login | Register  Vendors: Login | Register  Accessibility

U.S. AIR FORCE

# Persona Management Software.

**Solicitation Number: RTBZ20610**
Agency: Department of the Air Force
Office: Air Mobility Command
Location: 6th Contracting Squadron

Notice Details | Packages | Interested Vendors List  Print  Link

Complete View
- Original Synopsis — *Sources Sought* — Jun 22, 2010 1:42 pm
- Changed — Jun 22, 2010 2:07 pm
- Changed — Jun 29, 2010 11:32 am

Return To Opportunities List

**Solicitation Number:** RTBZ20610

**Notice Type:** Sources Sought

**Synopsis:**
Added: Jun 22, 2010 1:42 pm  Modified: Jun 22, 2010 2:07 pm  Track Changes

0001- Online Persona Management Service. 50 User Licenses, 10 Personas per user.
Software will allow 10 personas per user, replete with background , history, supporting details, and cyber presences that are technically, culturally and geographically consistent. Individual applications will enable an operator to exercise a number of different online persons from the same workstation and without fear of being discovered by sophisticated adversaries. Personas must be able to appear to originate in nearly any part of the world and can interact through conventional online services and social media platforms. The service includes a user friendly application environment to maximize the user's situational awareness by displaying real-time local information.

0002- Secure Virtual Private Network (VPN). 1 each
VPN provides the ability for users to daily and automatically obtain randomly selected
IP addresses through which they can access the internet. The daily rotation of the user s IP address prevents compromise during observation of likely or targeted web sites or services, while hiding the existence of the operation. In addition, may provide traffic mixing, blending the user s traffic with traffic from multitudes of users from outside the organization. This traffic blending provides excellent cover and powerful deniability. Anonymizer Enterprise Chameleon or equal

0003- Static IP Address Management. 50 each
Licence protects the identity of government agencies and enterprise organizations. Enables organizations to manage their persistent online personas by assigning static IP addresses to each persona. Individuals can perform static impersonations, which allow them to look like the same person over time. Also allows organizations that frequent same site/service often to easily switch IP addresses to look like ordinary users as opposed to one organization.
Anonymizer IP Mapper License or equal

GENERAL INFORMATION

**Notice Type:** Sources Sought

**Original Posted Date:** June 22, 2010

**Posted Date:** June 29, 2010

**Response Date:** Jul 02, 2010 12:00 pm Eastern

**Original Response Date:** Jun 28, 2010 12:00 pm Eastern

**Archiving Policy:** Automatic, 15 days after response date

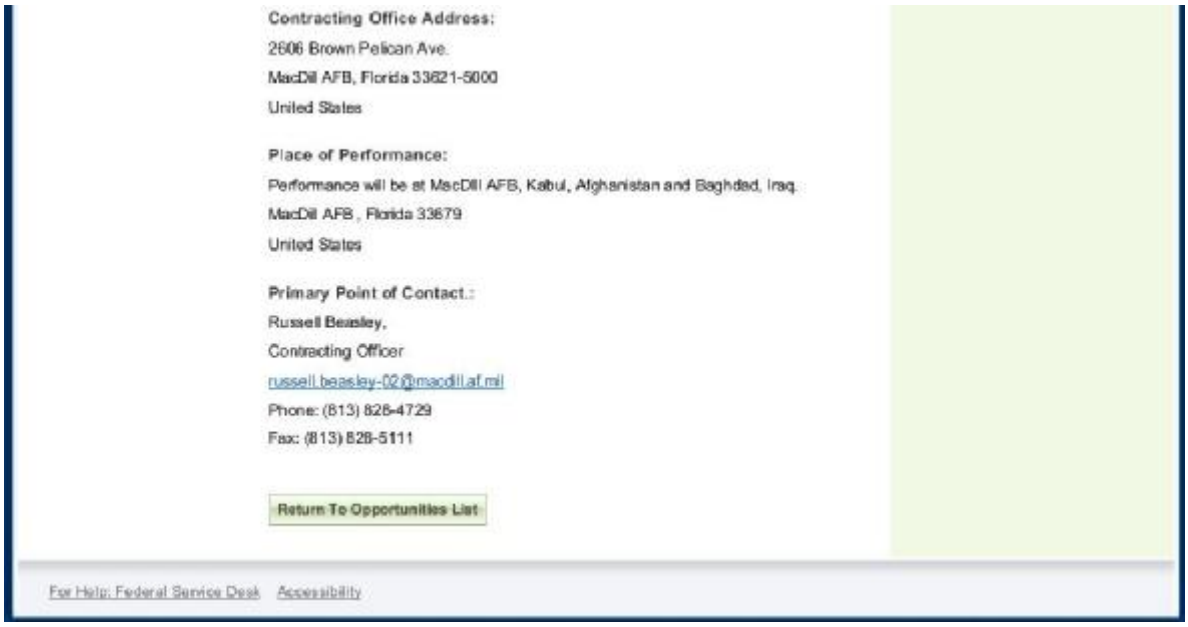
**Archive Date:** July 17, 2010

**Original Set Aside:** N/A

**Set Aside:** N/A

**Classification Code:** 70 – General purpose information technology equipment

**NAICS Code:** 511 – Publishing Industries (except Internet)/511210 – Software Publishers




Detalhe ampliado da solicitação de serviço de gerenciamento de persona cibernética online:

**Synopsis:**

Added: Jun 22, 2010 1:42 pm Modified: Jun 22, 2010 2:07 pm Track Changes

0001- Online Persona Management Service. 50 User Licenses, 10 Personas per user.

Software will allow 10 personas per user, replete with background , history, supporting details, and cyber presences that are technically, culturally and geographacilly consistent. Individual applications will enable an operator to exercise a number of different online persons from the same workstation and without fear of being discovered by sophisticated adversaries. Personas must be able to appear to originate in nearly any part of the world and can interact through conventional online services and social media platforms. The service includes a user friendly application environment to maximize the user's situational awareness by displaying real-time local information.