



Cyber War – A Nova Guerra

Parte III – Medidas de Proteção do Estado

Por Leonardo SANTOS Silva (022/2007)

1 - Introdução

Como vimos nos dois textos anteriores, os ataques às redes de computadores evoluíram de um momento onde os atacantes queriam mostrar sua capacidade técnica, realizando pichações em sites de internet, para um contexto muito mais elaborado, no qual os alvos passam a ser instituições bancárias privadas ou, até mesmo, instalações governamentais. Hoje, o usuário caseiro não é mais um alvo, mas sim um agente intermediário nesses ataques. Pequenas forças, sejam elas ligadas a um Estado ou não, conduzem verdadeiros ataques às grandes nações, num verdadeiro exemplo de guerras de 4ª geração, ou as guerras assimétricas.

As Nações são cada vez mais dependentes de sistemas complexos e de tecnologia da informação. Em muitos casos, as tecnologias de informação e comunicação (TIC) são vitais para a segurança econômica e nacional e estão sujeitas à interrupção por uma série de fatores que podem ser provenientes de dentro ou fora do país. Líderes do governo e do setor privado estão cada vez mais preocupados com a incerteza sobre os ciber riscos e suas vulnerabilidades. Esta incerteza deriva da complexidade e interconectividade da tecnologia em evolução utilizada para apoiar os sistemas críticos. Para garantir a segurança e vitalidade da economia, as nações devem gerir a segurança cibernética de acordo com suas próprias considerações de ordem econômica, social e política.

Em junho de 2009, o Departamento de Defesa Norte-americano (*DoD*) instituiu o *United States Cyber Command* (USCYBERCOM), unidade militar subordinada ao Comando Estratégico Norte-americano que tem como objetivo a condução de operações militares de defesa e, quando autorizados, de ataque aos inimigos, no âmbito do espaço virtual. O USCYBERCOM é composto por unidades das seguintes forças:



Figura 1 Logo do USCYBERCOM

- Comando Cibernético do Exército/2º Exército
- Comando Cibernético da Frota/10ª Frota Naval
- Comando Cibernético da Força Aérea/24ª Força Aérea
- Comando Cibernético do Corpo de Fuzileiros Navais

Após a sua criação, observou-se uma motivação de outras nações realizarem o mesmo. Em Dezembro do mesmo ano, a Coreia do Sul criou o Comando de Guerra Cibernética¹. Em resposta, a Coreia do Norte criou a Unidade de Guerra Cibernética. A Inglaterra iniciou as



Associação dos Diplomados da Escola Superior de Guerra

Delegacia no Estado de Minas Gerais

“Conhecer o Brasil para melhor servi-lo”



atividades de sua Força Cibernética através do GCHQ (Quartel General de Comunicações Governamentais, em Inglês)ⁱⁱ. E em 2010, a China inaugurou seu primeiro departamento dedicado à defesa de guerra cibernéticaⁱⁱⁱ.

E o que acontece no Brasil? Estamos preparados?

.2 – A Doutrina da ESG

Para entendermos a posição das Forças Armadas no Brasil atuando na guerra cibernética, precisamos dar um passo atrás e voltar nos fundamentos da Doutrina da ESG e o que ela fala sobre Segurança e Forças Armadas.

“**Segurança** é a sensação de garantia necessária e indispensável a uma sociedade e a cada um de seus integrantes, contra ameaças de qualquer natureza.”

Esse é um dos conceitos definidos pela ESG no que se refere à segurança: a capacidade que o homem, a comunidade, a nação e a coletividade têm para sentir que todas as suas necessidades serão atendidas, sem que óbices interfiram. Como isso é uma sensação, não pode ser mensurada. Uma vez que nos sentimos seguros, isto significa que não existe ameaça.

“**Defesa** é um ato ou um conjunto de atos realizados para obter ou resguardar as condições que proporcionam a sensação de **Segurança**.”

Quando uma ameaça se apresenta frente a uma garantia de segurança, é pela defesa que eliminamos esta ameaça, trazendo de volta a sensação de estar seguro. Neste ponto, quando a defesa se apresenta de maneira efetiva o **Poder Nacional**, com intuito de neutralizar as ameaças, se caracteriza enquanto uma **Defesa Nacional**.

A conceituação de Defesa Nacional nos leva ao outro item que, segundo a doutrina da ESG é conhecida como a Expressão Militar do Poder Nacional, caracterizada pelo emprego da força, ou pela capacidade de empregá-la com o objetivo de desencorajar as possíveis ameaças.

As instituições militares são os canais pelo qual a Nação emprega o **Poder Nacional**. São compostos pelas seguintes forças:

1. **Marinha**
2. **Exército**
3. **Aeronáutica**

Esses são os conceitos básicos e apresentados de uma maneira resumida de alguns pontos interessantes da Doutrina da ESG. Para uma relação completa desta doutrina, recomenda-se a leitura do “*Manual Básico Vol I – Elementos Fundamentais*” e o “*Manual Básico Vol II –*



Associação dos Diplomados da Escola Superior de Guerra

Delegacia no Estado de Minas Gerais

“Conhecer o Brasil para melhor servi-lo”



Assuntos Específicos”, ambos de 2009, podendo ser adquiridos gratuitamente no endereço eletrônico da Escola Superior de Guerra^{iv}.

3 – Forças Armadas

Seguindo o posicionamento da ESG, as Forças Armadas tem apresentado esforços para a preparação de uma possível guerra cibernética. Notícias divulgadas na Imprensa e informações divulgadas pelos órgãos oficiais nos mostram o que tem sido feito para a diminuição dos óbices em relação à segurança da informação.

Em Julho de 2010, o Comandante do Exército aprovou a diretriz de implantação do setor Cibernético no Exército, definindo oito projetos. Em Agosto de 2010 é ativado o Núcleo do Centro de Defesa Cibernética do Exército (NuCDCiber) que é responsável pela implantação do Centro de Defesa Cibernética do Exército (CDCiber). Dentre as atividades do NuCDCiber, estão:

- Gestão de Pessoal, responsável pela definição do perfil do pessoal envolvido, identificação de talentos, treinamentos, etc.;
- Estrutura de capacitação e de preparo e emprego operacional;
- Estrutura para produção do conhecimento oriundo da fonte cibernética;
- Arcabouço documental;
- Duas vertentes: definições doutrinárias e adequação normativa;
- Os projetos de implantação do Setor Cibernético no EB;
- Estrutura de pesquisa científica na área cibernética;
- Estrutura de apoio tecnológico e desenvolvimento de sistemas;
- Implantação do Centro de Defesa Cibernética;
- Planejamento e execução da Segurança Cibernética.

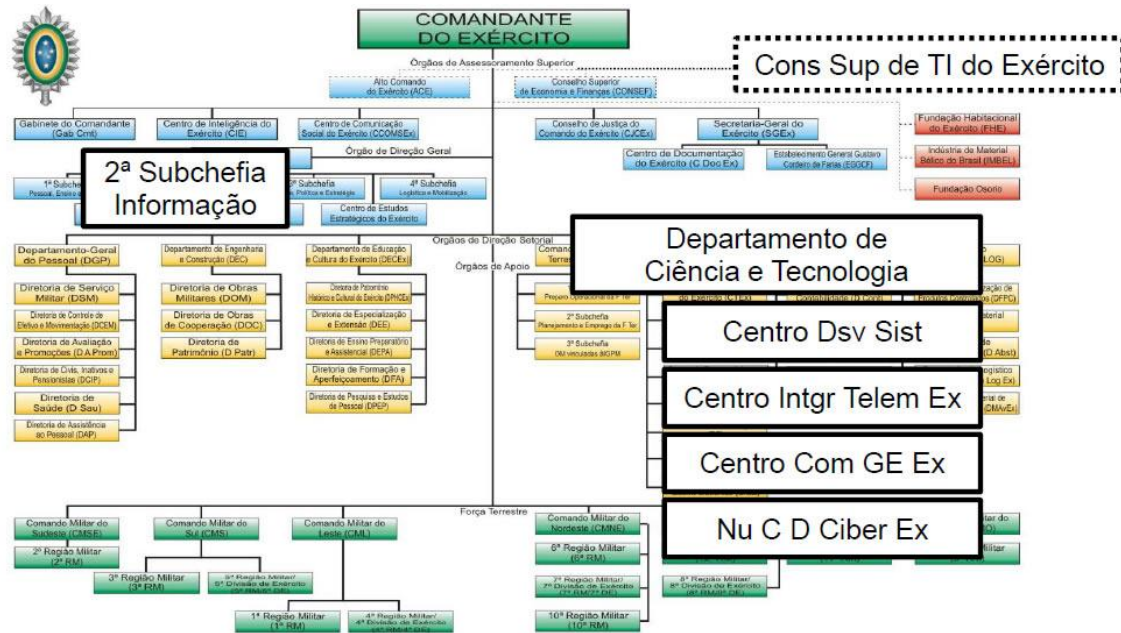


Figura 2 - Estrutura do NuCDCiber no Exército

A Marinha possui o CTIM (Centro de TI da Marinha) que dentro de suas atribuições, é responsável por conduzir as atividades concernentes à Guerra Cibernética, auditoria de segurança e forense computacional, conduzir as atividades concernentes à Guerra Cibernética, auditoria de segurança e forense computacional e implantar, monitorar e manter os ativos da RECIM (Rede de Comunicações Integradas da Marinha) atinentes à segurança da informação digital:

- Proteção da borda da RECIM;
- Proteção das redes locais;
- Antivírus corporativo;
- Atualização de aplicativos e SO;
- Recursos criptológicos da MB.

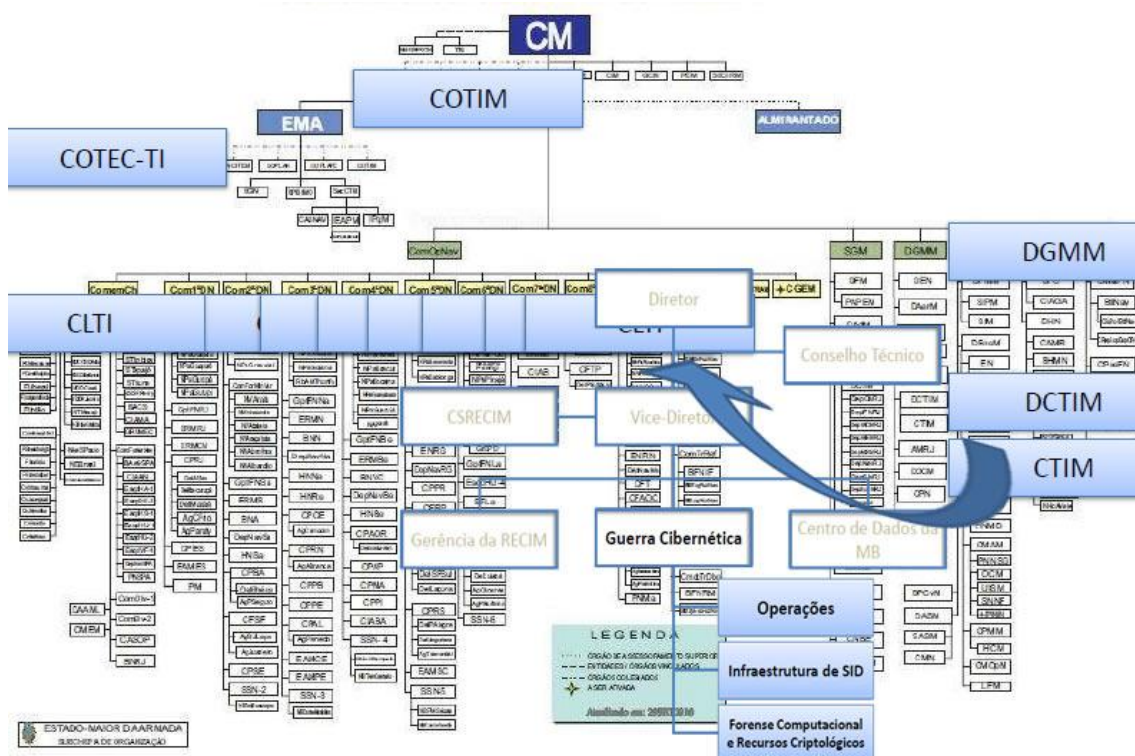


Figura 3 - Estrutura da DCTIM, na Marinha.

Já a Aeronáutica não possui um centro específico para tratar de defesa no espaço cibernético. Existem centros de tecnologia para as atividades de suporte relacionado aos sistemas computacionais, mas nada tem sido divulgado sobre a criação de um núcleo específico para a defesa cibernética.

Ao observar estas estruturas, vemos que apenas o Exército tem um núcleo formalmente voltado para a Guerra Cibernética, embora esteja em seu estado inicial. Pelo Decreto Presidencial 6.703 (18 de dezembro de 2008)^v, o Brasil dará prioridade a três setores decisivos para a Defesa Nacional: Cibernético, Espacial e Nuclear. Entretanto, pela própria definição da doutrina da ESG, é o exército que estará à frente do gerenciamento deste novo aparato de guerra^{vi}.

Coube então ao Exército a estruturação do Núcleo que irá coordenar, juntamente com o GSI, as ações de defesa e ataques cibernéticos. Lembrando que, segundo a Doutrina da ESG, o Exército possui dentre entre suas atividades:

- ✓ *Atuar de modo preventivo ou repressivo contra qualquer forma de ameaça ou agressão que, apoiadas ou não do exterior, comprometam a lei, a ordem e os fundamentos do Estado Democrático de Direito (no ambiente interno);*
- ✓ *Prevenir e dissuadir atividades hostis e ameaças externas aos interesses vitais da Nação (no ambiente externo);*



- ✓ *Atuar contra o inimigo externo, impedindo ou repelindo qualquer forma de ameaça ou agressão aos interesses vitais da Nação (no ambiente externo).*

Segundo o comandante do CDCiber, o Gen. Div. José Carlos dos Santos, a estratégia a ser usada será a da Defesa-Ativa, isto é, o Brasil, poderá atacar e neutralizar forças cibernéticas que possam surgir como uma ameaça. A ideia do Centro é contar com 100 militares altamente capacitados, com equipamentos avançados e um ambiente para simular ataques virtuais. Atualmente o centro está em funcionamento e conta com 20 militares (não foi divulgado se esses são apenas do Exército ou das três Forças). Até o final do ano, está previsto o primeiro exercício de Guerra cibernética. Além disto, o Centro terá um Gabinete de Crise, que irá orientar as ações de defesa ativa juntamente com outros órgãos. Segundo o General, parte da equipe sairá do IME (Instituto Militar de Engenharia), já que este possui cursos específicos na área. Outra fonte de capital humano poderá vir da contratação de civis especialistas, como consultores ou prestadores de serviço, mas esse assunto ainda não está definido.

4 – O Livro Verde^{vii}

O Governo Brasileiro publicou em 2010, o Livro Verde – Segurança Cibernética no Brasil. A publicação foi feita pelo Grupo Técnico de Segurança Cibernética (GT SEG CIBER), cujo objetivo é propor diretrizes e estratégias de Segurança Cibernética. O GT é composto pelos seguintes órgãos:

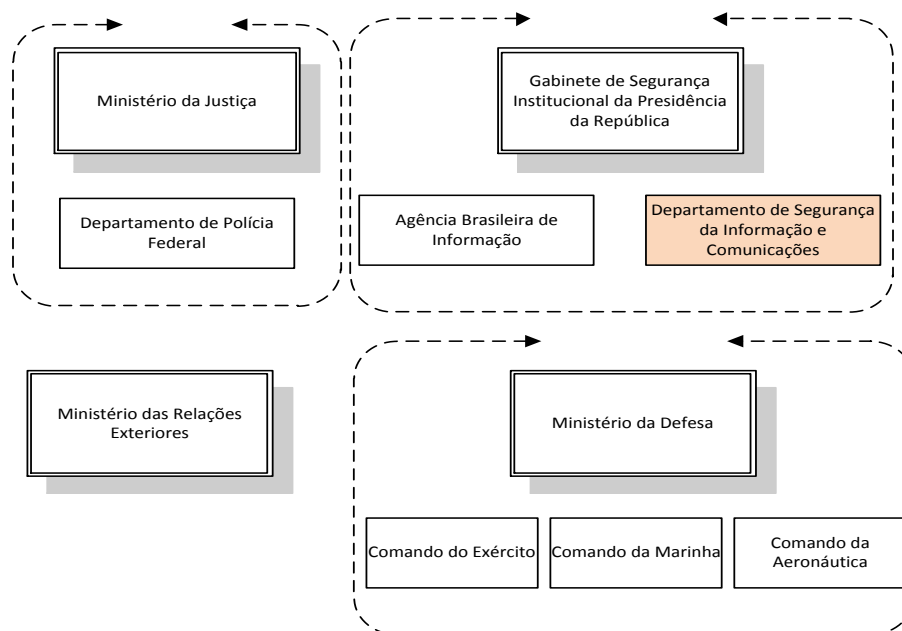


Figura 4 Participantes do Livro Verde



Associação dos Diplomados da Escola Superior de Guerra

Delegacia no Estado de Minas Gerais

“Conhecer o Brasil para melhor servi-lo”



A coordenação do grupo é exercida pela DSIC, Departamento de Segurança da Informação e das Comunicações, órgão vinculado ao Gabinete de Segurança Institucional da Presidência da República. Dentre as suas missões, duas são de destaque e relativas a este texto:

- Planejar e coordenar a execução das atividades de segurança cibernética e de segurança da informação e comunicações na administração pública federal;
- Operacionalizar e manter centro de tratamento e resposta a incidentes ocorridos nas redes de computadores da administração pública federal.

Para o GT, está claro que uma das funções do Estado é a segurança cibernética necessária para assegurar as infraestruturas críticas da Nação, como energia, defesa, transporte, telecomunicações e finanças. Os objetivos do Livro Verde corrobora a preocupação do Estado com a Segurança Cibernética e traça algumas diretrizes estratégicas de curto (2 a 3 anos) médio (5 a 7 anos) e longo prazo (10 a 15 anos). Na segunda parte do livro, são apresentados os vetores, com foco na segurança cibernética, mostrando as oportunidades e desafios. Os vetores são caracterizados por:

- Político Estratégico;
- Econômico;
- Social & Ambiental;
- Comunicação, Tecnologia e Informação;
- Educação;
- Legal;
- Cooperação Internacional;
- Segurança das Infraestruturas Críticas;

Finalmente, na terceira parte, são apresentadas as diretrizes estratégicas para uma Política Nacional de Segurança Cibernética. Das ações enumeradas, algumas estão de acordo com as áreas consideradas de foco para os países membros da OECD (Organização para o Desenvolvimento e Cooperação Econômica, do inglês):

- Combate ao crime cibernético;
- Criação de CERT /CIRT em nível nacional;
- Aumento da cultura de segurança;
- Promoção da educação.

5 – Conclusão

Tendo em vista as ações estabelecidas no Brasil e os acontecimentos mundiais que nos chamam a atenção para uma política de segurança de informação mais efetiva, temos poucos insumos para crer que existe uma proteção cibernética plausível no Brasil. Estamos no início de



Associação dos Diplomados da Escola Superior de Guerra

Delegacia no Estado de Minas Gerais

“Conhecer o Brasil para melhor servi-lo”



um caminho longo e tortuoso, onde o inimigo, que não conhece fronteiras, está se preparando e atuando furtivamente há anos. A estrutura de defesa cibernética proposta ainda precisa de amadurecimento, pessoal qualificado e muito investimento, pois corre-se o risco de todas essas ações serem ineficazes, caso esbarrem na burocracia governamental. O Livro Verde é uma boa ferramenta para guiar os próximos passos, mas a falta de uma legislação específica para a área pode tornar muitas destas diretrizes impossíveis de serem implantadas. E como será feita a integração entre as empresas e corporações consideradas como de infraestrutura crítica com os centros de defesa cibernéticos? Precisaremos ver os próximos capítulos para saber como esse contexto irá se desenvolver.

Sobre o Autor



Leonardo Santos Silva (LeoSantos@LeonardoSantos.com.br) é Administrador, com MBA em Gestão Executiva e Adesguiano da turma de 2007. Já atuou em diversas empresas como especialista em Segurança da Informação, possuindo vários certificados na área e realizando análises de risco, criando Plano de Continuidade de Negócios, Política de Segurança da Informação, Infraestrutura de Chaves Públicas, Análises Criptográficas e Defesa em Perímetro.

<http://www.LeonardoSantos.com.br>

ⁱ http://www.koreatimes.co.kr/www/news/nation/2009/12/205_56502.html

ⁱⁱ <http://www.dodbuzz.com/2009/06/29/stratcom-plows-ahead-on-cyber/>

ⁱⁱⁱ <http://www.guardian.co.uk/world/2010/jul/22/chinese-army-cyber-war-department>

^{iv} <http://www.esg.br/cursos/>

^v

http://www.defesa.gov.br/projetosweb/estrategia/arquivos/estrategia_defesa_nacional_portugues.pdf

^{vi} <http://www.defesanet.com.br/cyberwar/noticia/1677/Governo-brasileiro-planeja-nucleo-de-seguranca-on-line>

^{vii} <http://dsic.planalto.gov.br/>