A DEFESA CIBERNÉTICA E AS INFRAESTRUTURAS CRÍTICAS NACIONAIS

Paulo Sergio Melo de Carvalho[1]

RESUMO

A impressionante evolução experimentada pela Tecnologia da Informação e Comunicações (TIC), a partir da segunda metade do século passado, trouxe consigo a internet e, com ela, a Era da Informação, que já está cedendo seu lugar à Era do Conhecimento.

Tal situação, não obstante os inquestionáveis benefícios conferidos pela agilização do processo decisório e pela circulação da informação em tempo real e em nível mundial, paradoxalmente, torna as pessoas, as organizações e os Estados-Nação altamente vulneráveis a um novo tipo de ameaça, a cibernética, que desconhece fronteiras e tem potencial para causar grandes prejuízos financeiros, paralisar as estruturas vitais de uma nação e, até mesmo, indiretamente, ceifar vidas.

O espaço cibernético constitui um novo e promissor cenário para a prática de toda a sorte de atos ilícitos, incluindo o crime, o terrorismo e o contencioso bélico entre nações, caracterizado pela assimetria, pela dificuldade de atribuição de responsabilidades e pelo paradoxo da maior vulnerabilidade do mais forte.

O Brasil, como país emergente que busca um lugar de destaque no cenário internacional contemporâneo, não poderia ficar alheio a esse quadro de incertezas que caracteriza a atual conjuntura internacional relativa a esse tema. Assim sendo, a Estratégia Nacional de Defesa (END), de 2008, definiu os três setores considerados de importância estratégica para a defesa nacional, quais sejam: o nuclear, o espacial e o cibernético.

Nesse contexto, a Segurança e a Defesa Cibernéticas surgem naturalmente como imperativos de proteção das infraestruturas críticas da informação associadas às infraestruturas críticas nacionais do Estado brasileiro.

Apresentar a visão do Exército Brasileiro sobre a proteção das infraestruturas críticas nacionais no contexto da Segurança e da Defesa Cibernéticas constitui o objetivo deste artigo.

Palavras-chave: Setor Cibernético, segurança cibernética, defesa cibernética, infraestruturas críticas nacionais, infraestruturas críticas da informação.

[1] O autor é General de Brigada do Exército Brasileiro - 2º Subchefe do Estado-Maior do Exército
(e-mail: psmc_78@hotmail.com)

ABSTRACT

The impressive evolution of Comunications and Information Technology, from the second half of last century on, provided the birth of the internet and the Information Era, which is already yielding to the Knowledge Era.

Such situation, in spite of the unquestionable benefits which were provided by the speeding up of the decision making process and the real time and worldwide circulation of information, paradoxically turns people, organizations and nation-states highly vulnerable to a new kind of threat, that is, the cyber one, which knows no borders and is potentially capable of causing great financial losses, as well as paralyzing a nation's vital structures and even, indirectly, causing deaths.

Cyber Space is a new and promising scenario for all sorts of evil acts, such as crime, terrorism or even international conflicts, which are characterized by asymmetry, difficulty of attribution and the paradox of the greater vulnerability of the stronger.

Brazil, as an emergent country which seeks a place of renown at the current international scenario, could not stand aside from the international trend concerning this issue. Thus, the 2008 National Defense Strategy (END) defined three sectors of strategic importance to the nation, that is, the nuclear, the spatial, and the cyber.

Within this context, Cyber Security, as well as Cyber Defense, emerge natyrally as imperatives to the protection of information critical infrastructures associated with national critical infrastructures of the brazilian state.

The purpose of this paper is to present the Brazilian Army view on the protection of national critical infrastructures within the context of Cyber Security and Cyber Defense.

Key-words: cyber sector, cyber security, cyber defense, national critical infrastructures, information critical infrastructures.

The author is Major General at the Brazilian Army - Chief Information Officer at the Brazilian Army General Staff (e-mail: psmc_78@hotmail.com)

LISTA DE FIGURAS

ÍNDICE

1. **INTRODUÇÃO**

Desde os primórdios da civilização, a informação tem sido um componente indispensável em todas as atividades humanas, principalmente no processo produtivo.

Nos estágios iniciais do desenvolvimento humano, no entanto, não havia a consciência de sua importância nem da necessidade de protegê-la, o que só ocorreu com o surgimento do comércio e da conseqüente competição pelo mercado.

As três grandes revoluções que marcaram a história da humanidade, a agrícola, a industrial e a tecnológica, protagonizaram o gradativo crescimento da importância da informação como insumo básico do processo decisório, culminando com o seu alinhamento entre os fatores clássicos de produção (terra, trabalho e capital), vindo mesmo a superá-los em termos de relevância no cenário econômico mundial.

Em tempos mais recentes, com o advento da Era da Informação[1] e sua sucedânea, a Era do Conhecimento[2], a informação foi alçada à categoria de ativo estratégico para organizações e Estados-Nação, conferindo àqueles que a detém e dela se utilizam, efetiva e oportunamente, uma inquestionável vantagem no ambiente competitivo e nos contenciosos internacionais.

A internet, proporcionando conectividade em tempo real e com abrangência mundial, trouxe consigo um crescimento sem precedentes no volume de informações disponíveis aos modernos decisores, dificultando seu gerenciamento e ensejando o aparecimento de uma nova área de atividade, a Gestão do Conhecimento[3]. Por outro lado, sua grande vulnerabilidade, aliada à existência de novos atores de funestas intenções no cenário internacional, fez crescer a preocupação com a proteção da informação que por ela trafega, dando origem à Segurança da Informação.

O espaço cibernético, neologismo gerado pela Era da Informação, desafia conceitos tradicionais, entre eles o de fronteiras geopolíticas ou mesmo organizacionais, constituindo um novo território, ainda inóspito, a ser desbravado pelos bandeirantes do século XXI.

---

1. Também conhecida como Era Digital, corresponde ao período pós-Era Industrial, mais especificamente após a década de 1980, embora suas bases remontam ao início do século XX e, particularmente, na década de 1970, com invenções tais como o microprocessador, a rede de computadores, a fibra óptica e o computador pessoal.
2. Considera o conhecimento como sendo a informação contextualizada.
3. Refere-se à criação, identificação, integração, recuperação, compartilhamento e utilização do conhecimento dentro de uma organização.

A inexistência de marcos legais que disciplinem a disputa pelo seu domínio transforma esse espaço no "velho oeste" dos dias atuais, com potencial para suscitar conflitos de proporções e conseqüências mais danosas à humanidade do que a própria arma nuclear.

O Brasil, como nação soberana de inquestionável relevância e completamente inserida no cenário internacional contemporâneo, não poderia ficar à margem desse vertiginoso processo de transformação pelo qual o mundo moderno vem passando.

Constitui, portanto, objetivo estratégico do Estado brasileiro marcar presença nas discussões relativas ao controle do espaço cibernético como protagonista e não como coadjuvante. Nesse sentido, ressalta-se a clarividência do poder público brasileiro ao alçar o Setor Cibernético como um dos setores estratégicos da defesa, conforme estabelece a Estratégia Nacional de Defesa (END)[4].

O presente artigo pretende apresentar a visão do Exército Brasileiro (EB) sobre a proteção das infraestruturas críticas nacionais no contexto da Segurança e da Defesa Cibernéticas.

Para a consecução desse objetivo, far-se-á, inicialmente, uma apresentação dos conceitos básicos considerados indispensáveis à compreensão do tema, ressaltando-se que ainda não há consenso sobre alguns deles, seja no meio acadêmico, seja no militar. É importante destacar que, embora já tenha havido menção a tais conceitos na presente introdução, optou-se por não explicá-los em nota de rodapé, uma vez que eles serão apresentados posteriormente.

Em seguida, abordar-se-á a inserção do Setor Cibernético na END, passando-se à sua estruturação no Ministério da Defesa (MD), sua implantação no EB e, finalmente, serão tecidas considerações sobre a proteção das infraestruturas críticas nacionais no contexto da Segurança e da Defesa Cibernéticas, tópico esse que constitui o cerne do presente artigo.

4. Brasil. Ministério da Defesa. Estratégia Nacional de Defesa. Brasília, 2008. p.12

2. CONCEITOS BÁSICOS

A compreensão do presente artigo não pode prescindir da recordação de alguns conceitos básicos, já consagrados em literatura oficial ou concebidos especificamente para a consecução de seus propósitos, os quais serão, a seguir, apresentados.

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/Forças Armadas (MD/FA). No campo da Defesa Nacional, inclui os recursos informatizados que compõem o Sistema Militar de Comando e Controle (SISMC^2)[5] , bem como os sistemas de armas e de vigilância.

2.2 Espaço Cibernético[6]: espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam e são processadas e/ou armazenadas. As ações no espaço cibernético classificam-se em ofensivas, exploratórias ou de proteção, sendo que as ofensivas podem impactar, até mesmo, a segurança nacional.

2.3 Ativos de Informação[7]: 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.

2.4 Infraestruturas Críticas Nacionais (ICN)[8]: 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.

2.5 Infraestrutura Crítica da Informação (ICI)[9]: subconjunto dos ativos de informação que afeta diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade.

---

5. Conjunto de instalações, equipamentos, comunicações, doutrina, procedimentos e pessoal essenciais para o comandamento, em nível nacional, de crises e dos conflitos (MD 35-G-01. Glossário das Forças Armadas. p. 242)
6. Brasil. Ministério da Defesa. Exército Brasileiro. Estado-Maior do Exército. Minuta de Nota de Coordenação Doutrinária relativa ao I Seminário de Defesa Cibernética do Ministério da Defesa. Brasília, 2010. p.9
7. Mandarino Jr, Raphael. Um estudo sobre a Segurança e Defesa do Espaço Cibernético Brasileiro. Brasília, 2009. p.19
8. Mandarino Jr, Raphael. Segurança e Defesa do Espaço Cibernético Brasileiro. Brasília, 2010. p.38
9. Mandarino Jr, Raphael. Segurança e Defesa do Espaço Cibernético Brasileiro. Brasília, 2010. p. 37 e 38

2.6 Segurança da Informação e Comunicações (SIC)[10]: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

2.7 Segurança Cibernética: termo que se refere à proteção e garantia de utilização de ativos de informação estratégicos, principalmente os ligados às infraestruturas críticas da informação (redes de comunicações e de computadores e seus sistemas informatizados) que controlam as infraestruturas críticas nacionais. Também abrange a interação com órgãos públicos e privados envolvidos no funcionamento das infraestruturas críticas nacionais, especialmente os órgãos da Administração Pública Federal (APF).

2.8 Defesa Cibernética[11]: conjunto de ações defensivas, exploratórias e ofensivas, no contexto de um planejamento militar, realizadas no espaço cibernético, com as finalidades de proteger os nossos sistemas de informação, obter dados para a produção de conhecimento de inteligência e causar prejuízos aos sistemas de informação do oponente. No contexto do preparo e emprego operacional, tais ações caracterizam a Guerra Cibernética.

Além dos conceitos apresentados, cabe mencionar, ainda, que, para fim de Defesa Nacional, as ações no espaço cibernético enquadram-se nos níveis de decisão previstos na Estrutura Militar de Defesa[12] conforme o quadro abaixo:

NÍVEL	DENOMINAÇÃO	ÓRGÃO DE COORDENAÇÃO
Político	Segurança da Informação e Comunicações (SIC) Segurança Cibernética	Gabinete de Segurança Institucional da Presidência da República (GSI-PR)
Estratégico	Defesa Cibernética	Ministério da Defesa
Operacional	Guerra Cibernética	Forças Armadas
Tático		

10. Brasil. Presidência da República. Gabinete de Segurança Institucional da Presidência da República. Instrução Normativa GSI/PR Nr 1, de 13 de Junho de 2008. Brasília, 2008.
11. Brasil. Ministério da Defesa. Exército Brasileiro. Estado-Maior do Exército. Minuta de Nota de Coordenação Doutrinária relativa ao I Seminário de Defesa Cibernética do Ministério da Defesa. Brasília, 2010. p.9
12. Brasil. Ministério da Defesa. Estado-Maior de Defesa. Estrutura Militar de Defesa. Brasília, 2005. p.17

3. O SETOR CIBERNÉTICO NA ESTRATÉGIA NACIONAL DE DEFESA

A END, aprovada pelo Decreto Nr 6703, de 18 de dezembro de 2008, considera que existem três setores estratégicos da defesa, o nuclear, o cibernético e o espacial.

O mencionado dispositivo legal também estabelece que as capacitações cibernéticas incluirão, como parte prioritária, as tecnologias de comunicações entre todos os contingentes das Forças Armadas, de modo a assegurar sua capacidade de atuar em rede, enfatizando que os setores cibernético e espacial devem, em conjunto, viabilizar tal capacidade.

Também estabelece que todas as instâncias do Estado deverão contribuir para o incremento do nível de segurança nacional, com particular ênfase, no tocante ao Setor Cibernético, aos seguintes aspectos:

- As medidas para a segurança das áreas de infraestruturas críticas nacionais.

- 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.

Verifica-se, portanto, que o Setor Cibernético, na visão da END, não se restringe às atividades relacionadas à Segurança e Defesa Cibernéticas, abrangendo, também, a Tecnologia da Informação e Comunicações (TIC), ferramenta básica para a implementação de redes de computadores.

Nesse contexto, podem-se listar os seguintes componentes básicos do Setor Cibernético para a sua atuação em rede:

- Estrutura de comando, controle, comunicações, computação e inteligência (C4I) para a atuação operacional e o funcionamento administrativo das Forças Armadas.

- Recursos de TIC.

- Arquitetura matricial que viabilize o trânsito de informações em apoio ao processo decisório em tempo quase real.

4. ESTRUTURAÇÃO DO SETOR CIBERNÉTICO NO MINISTÉRIO DA DEFESA

4.1 AMBIENTE EXTERNO

A estruturação do Setor Cibernético no MD insere-se num contexto externo em que atuam alguns órgãos da APF, cujas designações e principais atribuições serão, a seguir, apresentadas.

4.1.1 ÓRGÃOS DE ESTADO E DE GOVERNO

No nível político (Estado ou governo) as atividades relacionadas ao Setor Cibernético são tratadas pelos órgãos a seguir apresentados.

4.1.1.1 CONSELHO DE DEFESA NACIONAL (CDN)

Trata-se de um órgão de consulta do Presidente da República nos assuntos relacionados à soberania nacional e à defesa do Estado democrático de direito. Constitui um órgão de Estado e não de Governo, com sua secretaria executiva sendo exercida pelo Ministro-Chefe do GSI-PR.

4.1.1.2 CÂMARA DE RELAÇÕES EXTERIORES E DEFESA NACIONAL (CREDEN)

A CREDEN é um órgão de assessoramento do Presidente da República nos assuntos pertinentes às relações exteriores e à defesa nacional, tratando-se de um órgão de governo.
Sua presidência cabe ao Ministro-Chefe do Gabinete de Segurança Institucional da Presidência da República (GSI-PR) e, dentre suas atribuições, encontra-se a Segurança da Informação, atividade essa que se insere no escopo do Setor Cibernético.

4.1.1.3 CASA CIVIL DA PRESIDÊNCIA DA REPÚBLICA

Dentre as atribuições da Casa Civil da Presidência da República (PR), merece destaque, por sua inequívoca relação com o Setor Cibernético, a relacionada com a execução das políticas de certificados e de normas técnicas e operacionais aprovadas pelo Comitê Gestor da Infraestrutura de Chaves Públicas Brasileiras (ICP-Brasil). Tal atribuição é da competência do Instituto Nacional de Tecnologia da Informação (ITI), que é uma autarquia federal, vinculada à Casa Civil da Presidência da República, com o objetivo de manter a ICP-Brasil, sendo a sua primeira autoridade da cadeia de certificação, ou seja, a Autoridade Certificadora Raiz (AC Raiz).

4.1.1.4 GSI-PR

O GSI-PR é o órgão da PR encarregado da coordenação, no âmbito da APF, de alguns assuntos estratégicos que afetam a segurança da sociedade e do Estado, quais sejam: Segurança das ICN, SIC e Segurança Cibernética.

No tocante à segurança das ICN, foram selecionadas seis áreas prioritárias, a saber: energia, telecomunicações, transportes, água, finanças e informação, sendo que essa última permeia todas as anteriores, pois as IC dependem cada vez mais de redes de informação para a sua gerência e controle.

Para o cumprimento da atribuição de coordenar as atividades de SIC, o GSI-PR conta, em sua estrutura organizacional, com três órgãos subordinados a seguir apresentados.

4.1.1.5 DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (DSIC)

O DSIC tem como atribuição operacionalizar as atividades de SIC na APF nos aspectos a seguir listados:

- Regulamentar a SIC para toda a APF.

- Capacitar os servidores públicos federais, bem como os terceirizados, sobre SIC.

- Realizar acordos internacionais de troca de informações sigilosas.

- Representar o país junto à Organização dos Estados Americanos (OEA) para assuntos de terrorismo cibernético.

- Manter o Centro de Tratamento e Resposta a Incidentes de Redes da APF (CTIR.Gov).

4.1.1.6 AGÊNCIA BRASILEIRA DE INTELIGÊNCIA (ABIN)

A ABIN é o órgão central do Sistema Brasileiro de Inteligência (SISBIN), que tem como objetivo estratégico desenvolver atividades de Inteligência voltadas para a defesa do Estado democrático de direito, da sociedade, da eficácia do poder público e da soberania nacional.

Dentre suas atribuições, no que interessa especificamente ao Setor Cibernético, destaca-se a de avaliar as ameaças internas e externas à ordem constitucional, entre elas a cibernética.

Conta, em sua estrutura organizacional, com o Centro de Pesquisa e Desenvolvimento de Segurança das Comunicações (CEPESC), o qual busca promover a pesquisa científica e tecnológica aplicada a projetos de segurança das comunicações.

4.2 PREMISSAS BÁSICAS

A Diretriz Ministerial Nr 0014/2009, de 09 de Novembro de 2009, atribuiu ao EB a responsabilidade pela coordenação e integração do Setor Cibernético do MD, orientando no sentido de que os trabalhos afetos à sua estruturação fossem desenvolvidos em duas fases, cujos produtos são os a seguir expostos:

- 1ª Fase – definição da abrangência do tema e dos objetivos setoriais, com prazo de entrega até 15 de Janeiro de 2010.

- 2ª Fase – desdobramento dos objetivos setoriais em ações estratégicas, estudo da adequabilidade das estruturas existentes nas três FA e proposta de alternativas e soluções, havendo necessidade, com prazo de entrega até 31 de Julho de 2010.

O Estado-Maior do Exército (EME) conduziu a elaboração dos supracitados documentos por meio de um grupo de trabalho (GT) interforças, com a participação de representantes do MD, tendo cumprido os prazos estabelecidos.

Com a extinção do Estado-Maior de Defesa e a criação do Estado-Maior Conjunto das Forças Armadas (EMCFA), surgiu um novo ator no cenário da estruturação do Setor Cibernético no MD, com novas diretrizes e orientações, o que ocasionou pequenas alterações no documento já enviado ao MD, prosseguindo os trabalhos no corrente ano.

No corrente ano, os trabalhos do GT interforças foram retomados, tendo havido, em 22 de Março, uma reunião, sob a coordenação do EME, com os oficiais generais das três Forças Armadas e do MD envolvidos com o tema.

Analisando-se a Diretriz Ministerial Nr 014/2009, de 09 de Novembro de 2009, podem-se extrair, do seu texto, as premissas básicas a seguir expostas, as quais devem orientar a Estruturação do Setor Cibernético no MD:

- Atender às prioridades estabelecidas pela END.
- Capacitar pessoal para as ações de médio e longo prazos.
- Interagir e cooperar com outras áreas governamentais e de pesquisa.
- Realizar os trabalhos conjuntamente, com representantes do MD e das FA.
- Considerar trabalhos e projetos em andamento e sistemas existentes no âmbito do MD.
- Realizar intercâmbio de pesquisadores em projetos das FA.
- Criar ambientes laboratoriais específicos.
- Considerar que não existem tratados e controles internacionais sobre o tema cibernético.
- Estudar a criação de um centro de coordenação e integração das atividades a ele afetas.
- Concentrar militares das três Forças Armadas em um mesmo ambiente de atuação.

4.3 VISÃO INICIAL

A figura 1, a seguir, sintetiza uma visão inicial e geral de como se pretende organizar os diversos projetos fundamentais que possuem áreas e requisitos indispensáveis à Estruturação do Setor Cibernético do MD, enfatizando a sua integração e trabalho em conjunto.

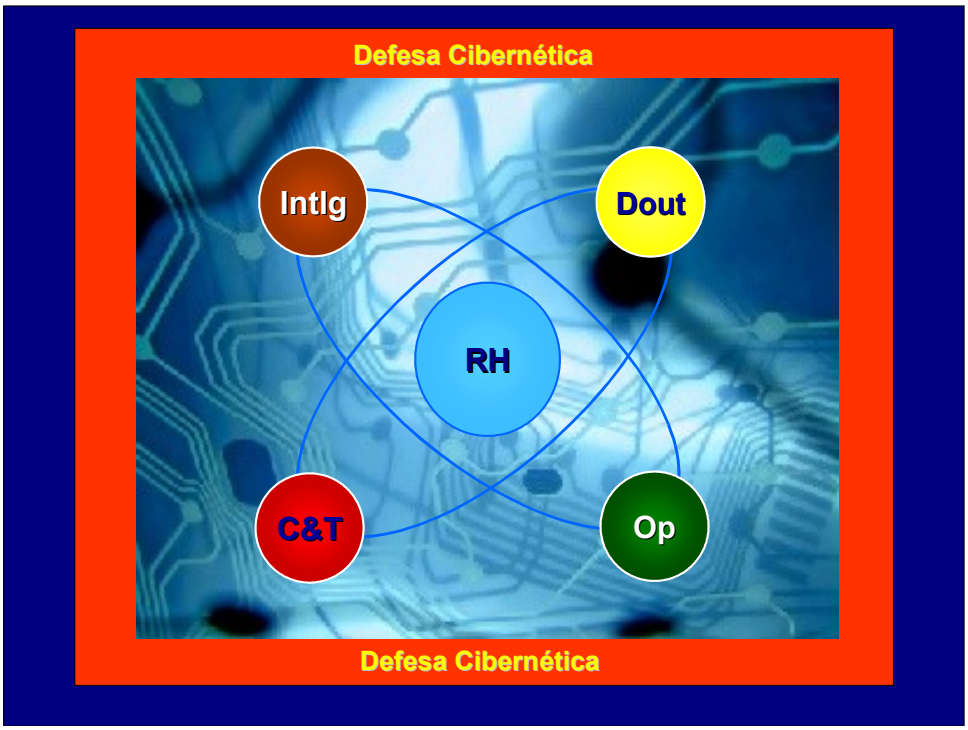

Figura 1 – Visualização da Organização Geral do Setor Cibernético do MD

Analisando-a, verifica-se que a capacitação de recursos humanos constitui a atividade prioritária na estruturação do setor em tela, uma vez que proporciona as capacitações cibernéticas, no dizer da própria END, indispensáveis para mobiliar os quatro vetores que o integram, quais sejam: a Inteligência - a Doutrina - a Ciência, Tecnologia e Inovação - e as Operações.

A mobilização da capacidade cibernética, em nível nacional, atrelada ao amparo legal para a atuação do setor, proporciona os necessários recursos materiais e humanos, com respaldo, para a realização das ações no espaço cibernético que caracterizam a Defesa Cibernética.

Quanto à Segurança Cibernética, ela faz parte dessa visualização porque o MD dela participa, como órgão da APF, coordenado pelo GSI-PR

4.4 ATIVIDADES RECENTES

O I Seminário de Defesa Cibernética do MD foi realizado no período de 21 a 24 de Junho de 2010, cabendo ao EB - condutor do Setor Cibernético no âmbito da Defesa - o seu planejamento, preparação, coordenação, execução e supervisão. O evento abrangeu duas fases a seguir descritas.

A Primeira Fase, denominada de “Perspectiva Político-Estratégica”, aberta ao público convidado, consistiu de uma série de palestras, com a participação da comunidade acadêmica,

representantes de infraestruturas críticas nacionais, dos setores público e privado, das FA e do MD, versando, basicamente, sobre Segurança Cibernética.

A Segunda Fase, denominada "Perspectivas Estratégica e Operacional-Militar", teve participação restrita ao MD e FA, iniciando com palestras específicas sobre a situação do Setor Cibernético em cada FA e continuando com a realização de debates distribuídos em quatro salas temáticas: Gestão de Pessoal; Doutrina; Estruturas; e Ciência, Tecnologia e Inovação (CT&I).

Como resultado do evento, foi constituído um Grupo de Trabalho Interforças, coordenado pelo EME, o qual elaborou uma Nota de Coordenação Doutrinária.

Prevê-se que, a partir do próximo ano, essa nota seja empregada em operações conjuntas, de modo a obter-se lições aprendidas que sirvam de subsídios para a atuação de um outro GT Inter-forças, que pode ser constituído pelo MD, com a missão de elaborar a Doutrina Militar de Defesa Cibernética.

4.5 SISTEMA MILITAR DE DEFESA CIBERNÉTICA (SMDC)

O MD e as FA participam das atividades coordenadas pelo GSI-PR, particularmente a SIC e a Segurança Cibernética. Face à crescente importância do domínio do espaço cibernético, em nível mundial, faz-se necessário ampliar o escopo de sua atuação de modo a abranger, também, a Defesa Cibernética.

Observando-se a Figura 2 (SMDC), depreende-se que o sistema visualizado poderá ter abrangência nacional e capilaridade desde o nível político (Nível Político - GSI-PR e APF - Segurança da Informação e Cibernética), passando pelo MD (Nível Estratégico - Defesa Cibernética) até os mais baixos escalões de comando no âmbito das FA (Níveis Operacional e Tático - Guerra Cibernética), com vista a engajar toda a sociedade na defesa dos interesses nacionais dentro do espaço cibernético.

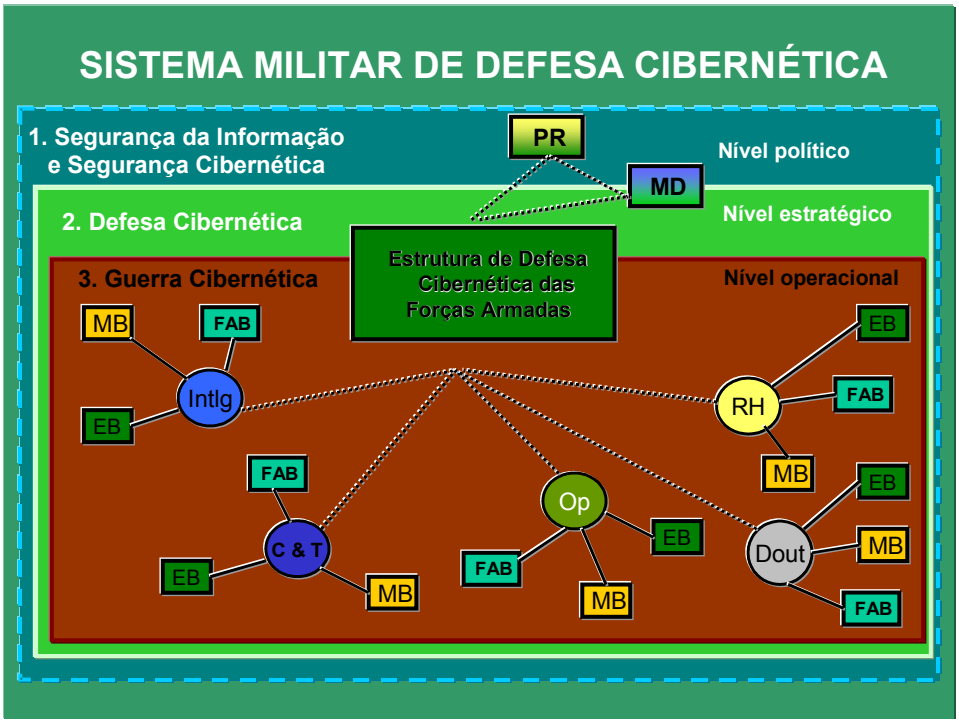

Figura 2 – Sistema Militar de Defesa Cibernética

Trata-se de um objetivo ambicioso, mas que deve ser perseguido. Sua consecução constitui condição "si ne qua non" para a defesa das ICN contra ataques cibernéticos, a qual se insere na missão constitucional das FA, com o apoio da sociedade civil.

Para isso, é imprescindível a realização de campanhas de sensibilização e conscientização, expondo os prejuízos decorrentes de ataques cibernéticos contra infraestruturas críticas nacionais, de modo que a sociedade perceba que é vantajoso cooperar com o esforço nacional de Defesa Cibernética.

Visualiza-se a criação do Comando de Defesa Cibernética das FA, o qual poderá realizar a supervisão, a coordenação e a orientação técnica e normativa das atividades do SMDC, particularmente no tocante aos seguintes aspectos: capacitação de talentos humanos; doutrina; operações; inteligência; e ciência, tecnologia e inovação.

Poderá, ainda, encarregar-se da interação do MD com o GSI-PR, para fins de participação na Segurança Cibernética e obtenção da indispensável cooperação dos setores público e privado e da comunidade acadêmica no esforço nacional de Defesa Cibernética.

A efetivação das ações estratégicas, listadas e detalhadas no documento solução referente aos quesitos previstos para a 2ª Fase na Diretriz Ministerial Nr 014/2009, constitui o grande desafio à

estruturação do Setor Cibernético do MD, uma vez que óbices de naturezas diversas dificultam a sua concretização.

Dentre eles, merecem destaque os seguintes:

- Óbices de natureza cultural, associando as ações cibernéticas a atividades ilícitas de intrusão, quebra de privacidade das pessoas, roubo de dados etc.

- Necessidade de conscientização de governantes e da sociedade como um todo em relação ao tema, decorrente do óbice anterior, dificultando a obtenção da indispensável mobilização para a participação nas atividades de Segurança e Defesa Cibernéticas.

- Escassez de recursos financeiros ou não priorização do setor na alocação de recursos financeiros, também, em parte, decorrente dos óbices anteriores.

- Caráter sensível da atividade, dificultando a aquisição de conhecimento vindo do exterior.

- Integração e atuação colaborativa incipientes dos diversos atores envolvidos.

5. IMPLANTAÇÃO DO SETOR CIBERNÉTICO NO EXÉRCITO BRASILEIRO

Conforme já citado, a END menciona, como setores estratégicos da Defesa, o Nuclear, o Espacial e o Cibernético. A fim de colocar em prática tal prescrição, o EB, no que lhe compete, adotou algumas iniciativas, as quais serão, a seguir, mencionadas.

O Cmt Ex, em 22 JUN 10, aprovou a Diretriz de Implantação do Setor Cibernético no EB, que abrange oito projetos, a saber: Organização do Centro de Defesa Cibernética do Exército (CDCiber), Planejamento e Execução da Segurança Cibernética, Estrutura de Apoio Tecnológico e Desenvolvimento de Sistemas, Arcabouço Documental, Estrutura de Capacitação e de Preparo e Emprego Operacional, Estrutura para Produção do Conhecimento oriundo da Fonte Cibernética, Estrutura de Pesquisa Científica na Área Cibernética e Gestão de Pessoal.

Em 4 AGO 10, o Cmt Ex criou o CDCiber, estabelecendo-se que a sua subordinação seria regulada em diretriz a ser expedida pelo EME. Pela Portaria Nr 667, de mesma data, foi ativado o Núcleo do Centro de Defesa Cibernética do Exército (Nu CDCiber), subordinado ao Departamento de Ciência e Tecnologia (DCT), que tem, em suas atribuições, a gerência e supervisão dos projetos relativos ao Setor Cibernético do EB.

O Chefe do EME designou os Gerentes dos Projetos inerentes à implantação do Setor Cibernético no EB, a saber: para o Projeto de Estrutura de Capacitação e de Preparo e Emprego Operacional, o Comandante do Centro de Comunicações e Guerra Eletrônica do Exército (CCOMGEx), para o Projeto de Planejamento e Execução da Segurança Cibernética, o Chefe do Centro Integra-

do de Telemática do Exército (CITEx), para os Projetos de Estrutura de Apoio Tecnológico e Desenvolvimento de Sistemas; e de Estrutura de Pesquisa Científica na Área Cibernética, o Chefe do Centro de Desenvolvimento de Sistemas (CDS), para os Projetos de Gestão de Pessoal; de Arcabouço Documental; de Estrutura para Produção do Conhecimento oriundo da Fonte Cibernética; e de Organização do Centro de Defesa Cibernética do Exército, o Chefe do NuCDCiber.

6. A SEGURANÇA/DEFESA CIBERNÉTICA E AS INFRAESTRUTURAS CRÍTICAS NACIONAIS

As ICN constituem preocupação permanente dos órgãos de Estado e de governo envolvidos na segurança e na defesa nacionais, uma vez que, conforme expressa seu próprio conceito, sua destruição, ou mesmo a interrupção de seu funcionamento, ainda que temporariamente, provoca sério impacto social, econômico, político, internacional ou na segurança do Estado e da sociedade. Foram eleitas seis áreas prioritárias a serem protegidas, quais sejam: energia, telecomunicações, transportes, água, finanças e informação, enfatizando essa última por caracterizar as ICI.

A dependência crescente de sistemas de informação controlados por redes de computadores e com aplicativos expostos à internet, onde o risco de exploração de eventuais vulnerabilidades por ameaças cibernéticas é uma realidade, torna a proteção das ICI que controlam a operação das ICN o foco da ações de Segurança e de Defesa Cibernéticas.

Tais ICI, no entanto, são administradas, operadas e mantidas por órgãos civis, não havendo, no arcabouço legal vigente no país, nenhum dispositivo que autorize qualquer forma de atuação coercitiva em relação a elas, o que, é importante frisar, é totalmente coerente com o Estado de direito em uma sociedade democrática.

Assim sendo, o grande desafio para a estratégia governamental relativa à Segurança e à Defesa Cibernéticas consiste na realização de uma campanha de sensibilização e conscientização, em nível nacional, envolvendo todos os setores da sociedade e todos os níveis educacionais, que viabilize a formação de uma cultura nacional de atuação colaborativa para com o MD/FA e demais órgãos governamentais envolvidos no tema. Tal campanha deve, necessariamente, comportar a interação constante entre o MD/FA, o GSI-PR e as ICN inseridas nos setores público e privado. Nesse contexto, avulta de importância o papel do GSI-PR como grande coordenador e articulador, realizando a interface entre o MD/FA e a sociedade civil. No tocante ao setor

empresarial, é importante, inclusive, incutir a idéia de uma relação custo-benefício altamente positiva decorrente da atuação colaborativa.

Observa-se, também, uma tendência mundial crescente em destacar e priorizar a proteção das ICN de um modo geral, e, em particular, das ICI a elas inerentes, no contexto da Segurança e Defesa Nacional, mediante campanhas de conscientização e atuação colaborativa entre órgãos governamentais e a sociedade em geral.

7. CONCLUSÃO

Nas últimas décadas, o conhecimento na área cibernética tem crescido exponencialmente e a uma velocidade sem precedentes na história da humanidade.

O espaço cibernético é um ambiente ainda desconhecido, mal definido, sem fronteiras nem leis, constituindo uma verdadeira terra de ninguém, com grande potencial para se tornar palco de mais uma disputa de poder no cenário internacional.

Seu domínio constitui-se em grande desafio para a humanidade no presente século, podendo-se, até mesmo, compará-lo ao domínio dos mares no período das grandes navegações.

Como era o mar para os navegadores portugueses e espanhóis, o espaço cibernético é, para o mundo contemporâneo, um grande desconhecido e, para sua conquista, não existem referências nem modelos.

De modo semelhante ao ocorrido com o colonialismo luso-espanhol das grandes navegações e o neocolonialismo afro-asiático do final do século XIX, vislumbra-se o prenúncio de uma verdadeira corrida rumo ao espaço cibernético, que pode constituir o moderno colonialismo do século XXI.

A grande diferença dessa nova forma de colonialismo para as anteriores, no entanto, é que, nela, a disputa não fica restrita às grandes potências do momento, face ao caráter de assimetria do contencioso cibernético que pode beneficiar atores menos aquinhoados de poder.

O paralelo com as armas nucleares é inevitável, pois já se pensa em um Tratado de Não-Proliferação de Armas de Informação, à semelhança do Tratado de Não Proliferação de Armas Nucleares.

Fazendo-se uma analogia com o princípio do “uti possidetis”, que legitimou as conquistas decorrentes das grandes navegações, o país que tiver fincado sua bandeira no espaço cibernético, certamente, estará em grande vantagem nas discussões com vistas ao estabelecimento de um marco legal que discipline a atuação no espaço cibernético.

Nesse contexto, o Brasil, pelo menos, aparentemente, encontra-se em boa situação, pois alguns dos protagonistas das discussões já em curso, particularmente a Rússia, têm elogiado o alegado potencial brasileiro para atuação no espaço cibernético. Os Estados Unidos da América também têm buscado o diálogo e apresentando propostas de cooperação e parceria.

Faz-se mister ressaltar, no entanto, que os países mais desenvolvidos, por se sentirem mais vulneráveis, têm buscado ampliar seu leque de parcerias internacionais, pois sabem que sua defesa depende do estabelecimento de laços de cooperação com os demais países.

Assim sendo, pode-se afirmar, sem sombra de dúvida, que as medidas recentemente adotadas pelo Brasil, seja em nível de Governo (END), seja no âmbito do MD (Consolidação do Setor Cibernético), são muito pertinentes e oportunas, não apenas no contexto da afirmação da capacidade brasileira perante o mundo, mas também para preparar o país para defender seus interesses no espaço cibernético e proteger suas infraestruturas críticas nacionais contra ataques cibernéticos.

Em síntese, pode-se afirmar que estamos no caminho certo e que, em termos de conhecimento e talentos, não ficamos a dever a nenhum dos países melhor situados econômica e tecnologicamente.

Caso sejamos competentes na adoção das medidas que se fazem necessárias para fincarmos nossa bandeira no espaço cibernético e se conseguirmos motivar, conscientizar e mobilizar a população brasileira para a importância do tema e para a relação custo-benefício altamente positiva da cooperação nos esforços de Segurança e Defesa Cibernética, não correremos o risco de ficarmos alijados do seleto clube de países detentores de capacidade de atuar com desenvoltura e liberdade de ação nesse novo ambiente de atividade humana.

REFERÊNCIAS BIBLIOGRÁFICAS

Brasil. Ministério da Defesa. MD31-D-03. Doutrina Militar de Comando e Controle. Brasília, 2006.

Brasil. Ministério da Defesa. Exército Brasileiro. Estado-Maior do Exército. Minuta de Nota de Coordenação Doutrinária relativa ao I Seminário de Defesa Cibernética do Ministério da Defesa. Brasília, 2010.

Brasil. Presidência da República. Gabinete de Segurança Institucional da Presidência da República. Instrução Normativa GSI/PR Nr 1, de 13 de Junho de 2008. Brasília, 2008.

Brasil. Ministério da Defesa. MD 35-G-01. Glossário das Forças Armadas. Brasília, 2009.

MANDARINO Jr, Raphael.Um estudo sobre a segurança e a defesa do espaço cibernético brasileiro. Brasília, 2009.

MANDARINO Jr, Raphael. Segurança e Defesa do Espaço Cibernético Brasileiro. Brasília, 2010.