Presidência da República
Secretaria de Assuntos Estratégicos

DESAFIOS ESTRATÉGICOS PARA A

SEGURANÇA E DEFESA CIBERNÉTICA

1ª Edição
Brasília - 2011

DESAFIOS ESTRATÉGICOS PARA A SEGURANÇA E DEFESA CIBERNÉTICA

Presidência da República
Presidenta Dilma Rousseff

Secretaria de Assuntos Estratégicos
Ministro Wellington Moreira Franco

Secretaria de Assuntos Estratégicos
Bloco O – 7º, 8º e 9º andares
CEP: 70052-900 Brasília, DF
http://www.sae.gov.br

PRESIDÊNCIA DA REPÚBLICA
SECRETARIA DE ASSUNTOS ESTRATÉGICOS

DESAFIOS ESTRATÉGICOS PARA A SEGURANÇA E DEFESA CIBERNÉTICA

1ª EDIÇÃO
BRASÍLIA, 2011

Coordenação
Maj Brig R1 Whitney Lacerda de Freitas

Organizadores
Cel Cav Otávio Santana do Rêgo Barros
TC Inf Ulisses de Mesquita Gomes

Projeto gráfico e diagramação
Rafael W. Braga
Bruno Schurmann

Revisão
Luis Violin
Sarah Pontes

Imagem de Capa
© Centro de Comunicação Social do Exército

Tiragem
2.000 exemplares

Catalogação na fonte Biblioteca da Presidência da República.

D313
Desafios estratégicos para segurança e defesa cibernética / organizadores Otávio Santana Rêgo Barros, Ulisses de Mesquita Gomes, Whitney Lacerda de Freitas. – Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011.
216 p.

ISBN 978-85-85142-32-2

1. Cibernética – segurança. 2. Cibernética – defesa. I. Barros, Otávio Santana Rêgo. II. Gomes, Ulisses de Mesquita. III. Freitas, Whitney Lacerda de.

CDD 001.53
CDU 007

Os organizadores desta publicação gostariam de agradecer a fundamental colaboração das seguintes pessoas no processo que deu origem a este livro: João Roberto de Oliveira, Paulo Sergio Melo de Carvalho, Paulo Martino Zuccaro, Raphael Mandarino Junior, José Eduardo Portella Almeida, Otávio Carlos Cunha da Silva, Sérgio Luiz Ribeiro e José Eduardo Malta de Sá Brandão.

SUMÁRIO

PAINEL 2: SISTEMA DE SEGURANÇA E DEFESA CIBERNÉTICA NACIONAL

CONCLUSÃO

APRESENTAÇÃO

Com vistas a cumprir sua atribuição de realizar estudos e pesquisas destinados a promover o planejamento de longo prazo governamental e contribuir para a implementação da Estratégia Nacional de Defesa, a Secretaria de Assuntos Estratégicos (SAE) criou o programa "Encontros da SAE".

No âmbito desse programa, a SAE promove reuniões técnicas, seminários e oficinas de trabalho visando a aprofundar o entendimento de temas considerados estratégicos para o desenvolvimento socioeconômico e para a segurança nacional. Entre os assuntos examinados ao longo de 2010, estão: a segurança da Amazônia e da "Amazônia Azul"; o planejamento das políticas nuclear, espacial e de tecnologia da informação e comunicação; o aperfeiçoamento da doutrina naval brasileira; a cooperação sul-americana na área de defesa e o X Encontro Nacional de Estudos Estratégicos.

Este livro compila os artigos elaborados com base nas apresentações realizadas durante a Reunião Técnica sobre Segurança e Defesa Cibernética, desenvolvida no dia 16 de dezembro de 2010, na cidade de Brasília-DF. Ela foi organizada pela Secretaria de Assuntos Estratégicos em parceria com o Comando do Exército, por meio do Estado-Maior do Exército.

O evento buscou atingir dois objetivos principais. O primeiro foi proporcionar aos servidores do governo federal conhecimentos sobre as atividades de segurança e defesa cibernética, identificando o papel desenvolvido pelas Forças Armadas e de outras instituições do Estado brasileiro na área, bem como de outros órgãos públicos e privados envolvidos ou relacionados com o tema. O segundo objetivo consistiu em contribuir para capacitar os órgãos públicos a propor políticas públicas que considerem a indissolubilidade do binômio defesa–desenvolvimento, permitindo ao País estabelecer um sistema de segurança e defesa cibernética que envolva também os sistemas de informação ligados às infraestruturas críticas.

O evento teve cerca de 110 participantes, oriundos de ministérios, de autarquias, das Forças Armadas e de órgãos que têm interesse no tema e competência na formulação de políticas públicas. A reunião foi estruturada na forma de painéis e contou com a presença do ministro de Assuntos Estratégicos, Samuel Pinheiro Guimarães, e do secretário-executivo, Luiz Alfredo Salomão.

Os painéis abordaram temas transversais relativos à segurança e à defesa cibernética no País. Foram apresentados diagnósticos dos assuntos em debate e os desafios mais relevantes no que tange aos seguintes aspectos: a formulação de políticas públicas e de marco legal para o uso efetivo do espaço cibernético, especialmente no que concerne à manutenção das infraestruturas críticas do País; o estabelecimento de medidas que contribuam para a gestão da segurança da informação e comunicações e para a produção do conhecimento de inteligência; o estímulo das atividades de pesquisa e desenvolvimento para atender às necessidades do setor; a retenção de talentos; e o estabelecimento do perfil da carreira que deve ser de estado.

Na conclusão do livro, os organizadores apresentam um documento de trabalho com vistas a contribuir na orientação do planejamento estratégico para a Segurança e Defesa Cibernética e na fundamentação das políticas públicas nesse domínio. Tal documento é uma proposta, com sugestões para a criação e a implementação de um grupo de trabalho do Setor Estratégico Cibernético, a ser constituído pela Secretaria de Assuntos Estratégicos, em parceria com o Ministério da Defesa, especialmente no que tange à criação do Sistema de Segurança e Defesa Cibernético brasileiro. Para essa proposta, tomou-se por base as apresentações da Reunião Técnica e os artigos produzidos pelos palestrantes.

Assessoria de Defesa da
Secretaria de Assuntos Estratégicos

CONFERÊNCIA DE ABERTURA

CONFERÊNCIA DE ABERTURA: O SETOR CIBERNÉTICO NAS FORÇAS ARMADAS BRASILEIRAS

*Paulo Sergio Melo de Carvalho**

Resumo

A impressionante evolução experimentada pela Tecnologia da Informação e Comunicação (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 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.

* General-de-Brigada, exerce o cargo de 2º subchefe do Estado-Maior do Exército. Em sua carreira militar, realizou os cursos da Academia Militar das Agulhas Negras, de Manutenção de Comunicações, de Aperfeiçoamento de Oficiais, de Comando e Estado-Maior, Avançado de Inteligência e de Política, Estratégia e Alta Administração do Exército. Realizou, ainda, o Curso de Economia de Defesa, no Centro Hemisférico para Estudos de Defesa, nos EUA, e os cursos de pós-graduação MBA Executivo e MBA em Administração Estratégica de Sistemas de Informação, ambos da Fundação Getúlio Vargas. Desempenhou as seguintes funções: instrutor da Aman e da Escola de Comunicações, integrou a Cooperação Militar Brasileira no Paraguai, comandou o 4º Batalhão de Comunicações, serviu no Ministério da Defesa e comandou a 7ª Brigada de Infantaria Motorizada.

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.

Nesse contexto, 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.

O Ministério da Defesa, cumprindo o que prescreve a END, resolveu dar início à Consolidação do Setor Cibernético no âmbito da Defesa, cuja descrição constitui objetivo deste artigo.

Palavras-chave: setor cibernético, espaço cibernético, defesa cibernética, segurança cibernética.

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 consequente 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 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 abrangência mundial, trouxe consigo crescimento sem precedentes no volume de informações disponíveis aos modernos decisores, dificultando seu gerenciamento e ensejando o aparecimento de 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.

[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 20 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 informação contextualizada.

[3] Refere-se à criação, à identificação, à integração, à recuperação, ao compartilhamento e à utilização do conhecimento em uma organização.

O espaço cibernético, neologismo gerado pela Era da Informação, desafia conceitos tradicionais, entre eles o de fronteiras geopolíticas ou mesmo os organizacionais, constituindo novo território, ainda inóspito, a ser desbravado pelos bandeirantes do século 21.

A inexistência de marcos legais que disciplinem a disputa pelo domínio desse espaço cibernético transforma-o no "velho oeste" dos dias atuais, com potencial para suscitar conflitos de proporções e consequências 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 ao patamar de um dos setores estratégicos da Defesa, conforme estabelece a END.[4]

Este artigo pretende apresentar uma visão geral do estágio atual dos estudos iniciais para a Consolidação do Setor Cibernético no âmbito da Defesa, decorrentes da designação do Exército Brasileiro (EB), pelo ministro da Defesa, como coordenador e força líder na condução das atividades desse setor estratégico no Ministério da Defesa (MD).

[4]Cf. < https://www1.defesa.gov.br/eventos_temporarios/2009/estrategia/arquivos/estrategia_defesa_nacional_portugues.pdf >. Acesso em: 17 dez. 2010.

Conceitos básicos

A compreensão deste 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.

- 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 (SISMC),[5] bem como os sistemas de armas e de vigilância.

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

- Ativos de Informação[7] – Meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso (computadores, equipamentos de comunicação e de interconexão), os sistemas utilizados para tal, os sistemas de informação de modo geral, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

- Infraestruturas Críticas (IC)[8] – Instalações, serviços, bens e sistemas que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional e à segurança do Estado e da sociedade.

[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.

- 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

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

- Segurança Cibernética – 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).

- 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.

[9] MANDARINO JR., Raphael. Segurança e Defesa do Espaço Cibernético Brasileiro. Brasília, 2010. p. 37 e 38.

[10] BRASIL. Presidência da República. Gabinete de Segurança Institucional da Presidência da República. Instrução Normativa GSI/PR n. 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.

O setor cibernético na Estratégia Nacional de Defesa

A END, aprovada pelo Decreto nº 6.703, 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.

A END enfatiza que os setores cibernético e espacial devem permitir que as Forças Armadas, em conjunto, possam atuar em rede.

Todas as instâncias do Estado deverão contribuir para o incremento do nível de segurança nacional, com particular ênfase nos seguintes aspectos do Setor Cibernético:

a. as medidas para a segurança das áreas de infraestruturas críticas; e

b. 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 que o Setor Cibernético, na visão da END, não se restringe às atividades relacionadas à Segurança e Defesa Cibernética, mas abrange, também, a Tecnologia da Informação e Comunicação (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:

a. estrutura de comando, controle, comunicações, computação e inteligência (C&I) para a atuação operacional e o funcionamento administrativo das Forças Armadas;

b. recursos de TIC; e

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

A consolidação do setor cibernético na defesa

Órgãos de estado e de governo[12]

Em nível político (Estado ou governo), as atividades relacionadas ao Setor Cibernético são tratadas pelos órgãos a seguir apresentados.

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, que tem sua secretaria-executiva exercida pelo ministro-chefe do Gabinete de Segurança Institucional da Presidência da República (GSI-PR).

CÂMARA DE RELAÇÕES EXTERIORES E DEFESA NACIONAL (Creden)

A Creden é um órgão de governo para assessoramento do presidente da República nos assuntos pertinentes às relações exteriores e à defesa nacional.

Sua presidência cabe ao ministro-chefe do GSI-PR e, entre suas atribuições, encontra-se a segurança da informação, atividade essa que se insere no escopo do Setor Cibernético.

CASA CIVIL DA PRESIDÊNCIA DA REPÚBLICA

Entre as atribuições da Casa Civil da Presidência da República, merece destaque, por sua inequívoca relação com o Setor Cibernético, a aquela relacionada com a execução das políticas de certificados e 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), uma autarquia federal vinculada à Casa Civil da Presidência da República, que tem o objetivo de manter a ICP-Brasil, da qual é a primeira autoridade na cadeia de certificação, ou seja, é a Autoridade Certificadora Raiz (AC Raiz).

[12] MANDARINO JR., Raphael. *Segurança e Defesa do Espaço Cibernético Brasileiro*. Brasília, 2010. p. 109-115.

GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA (GSI-PR)

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

No tocante às infraestruturas críticas nacionais, foram selecionadas seis áreas prioritárias, a saber: energia, telecomunicações, transportes, água, finanças e informação. Esta última permeia todas as anteriores, pois as ICs dependem cada vez mais de redes de informação para a sua gerência e controle.

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

DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (DSIC)

O DSIC tem como atribuição operacionalizar as atividades de Segurança da Informação e Comunicações (SIC) na APF, nos seguintes aspectos:

a. regulamentar a SIC para toda a APF;

b. capacitar os servidores públicos federais, bem como os terceirizados, sobre SIC;

c. realizar acordos internacionais de troca de informações sigilosas;

d. representar o País junto à Organização dos Estados Americanos (OEA) para assuntos de terrorismo cibernético; e

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

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), que busca promover a pesquisa científica e tecnológica aplicada a projetos de segurança das comunicações.

Premissas básicas para a consolidação do setor cibernético na defesa

Analisando-se a mencionada Diretriz Ministerial nº 014/2009, pode-se extrair do seu texto as seguintes premissas básicas, que devem orientar a Consolidação do Setor Cibernético no âmbito da Defesa:

a. atender às prioridades estabelecidas pela END;

b. capacitar pessoal para as ações de médio e longo prazos;

c. interagir e cooperar com outras áreas governamentais e de pesquisa;

d. realizar os trabalhos conjuntamente com representantes do MD e das Forças Armadas;

e. considerar trabalhos e projetos em andamento e sistemas existentes no âmbito do MD;

f. realizar intercâmbio de pesquisadores em projetos das Forças Armadas;

g. criar ambientes laboratoriais específicos;

h. considerar que não existem tratados e controles internacionais sobre o tema cibernético;

i. estudar a criação de um centro de coordenação e supervisão das atividades do setor em questão; e

j. concentrar militares das três Forças em um mesmo ambiente de atuação.

Visualização do setor cibernético da defesa

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 Consolidação do Setor Cibernético na Defesa, enfatizando-se a sua integração e o trabalho conjunto.

Analisando essa figura, verifica-se que a capacitação de recursos humanos constitui a atividade prioritária na consolidação do setor em tela, uma vez que ela 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.

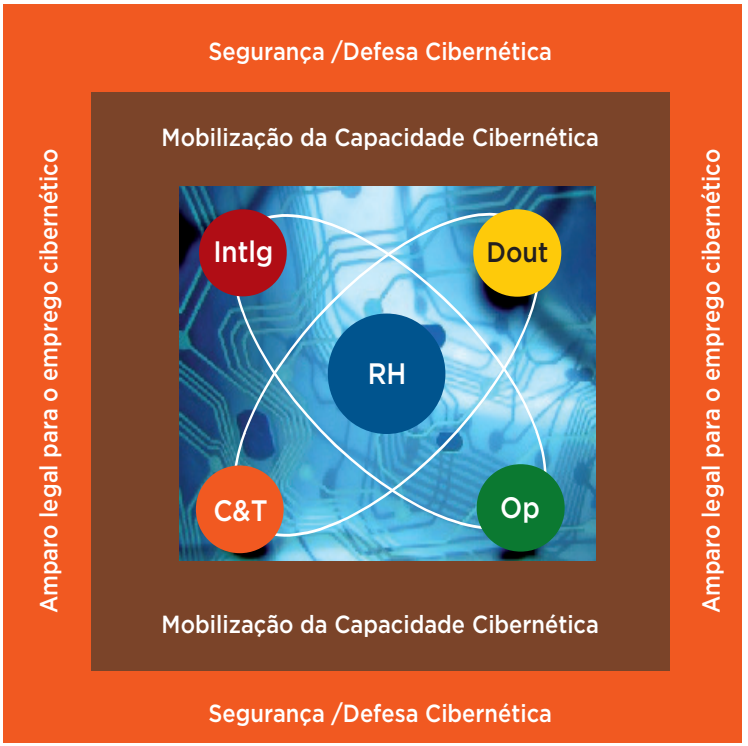

Figura 1 – Visualização do Setor Cibernético na Defesa

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, esta faz parte dessa visualização porque o MD dela participa, como órgão da APF, coordenado pelo GSI-PR.

Principais atividades no Ministério da Defesa

Como atividades recentes, no âmbito do MD, relacionadas à Consolidação do Setor Cibernético naquele ministério, pode-se citar a expedição da mencionada Diretriz Ministerial nº 014/2009, a realização do I Seminário de Defesa Cibernética do Ministério da Defesa, a criação do Centro de Defesa Cibernética do Exército e a ativação de seu núcleo, bem como o prosseguimento da capacitação de talentos humanos.

O Ministro da Defesa atribuiu ao EB a coordenação do Setor Cibernético no âmbito da Defesa e dividiu os seus estudos iniciais com vista à sua consolidação em duas fases, definindo, respectivamente, as seguintes tarefas a serem realizadas em cada uma delas:

a. primeira fase: definição da abrangência do tema e dos objetivos setoriais; e

b. segunda fase: detalhamento das ações estratégicas, adequabilidade das estruturas existentes nas três Forças Armadas e proposta de alternativas e soluções, se for o caso.

Os documentos contendo a solução aos quesitos das 1ª e 2ª fases, relativos ao Setor Cibernético, foram elaborados por um Grupo de Trabalho Inter-Forças, coordenado pelo Estado-Maior do Exército (EME), e encaminhados ao MD, respectivamente, em janeiro e julho de 2010, os quais foram analisados e aprovados com pequenas ressalvas.

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, de representantes de infraestruturas críticas nacionais, dos setores público e privado, das Forças Armadas e do MD, versando, basicamente, sobre Segurança Cibernética. Destinou-se a prover uma base de conhecimentos para a fase seguinte.

A segunda fase, denominada "Perspectivas Estratégica e Operacional-Militar", teve participação restrita ao MD e às Forças Armadas. Iniciou-se com palestras específicas sobre a situação do Setor Cibernético em cada Força Armada e continuou 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 Inter-Forças, 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 que sejam obtidas lições aprendidas que sirvam de subsídios para a atuação de outro GT Inter-Forças, que pode ser constituído pelo MD, com a missão de elaborar a Doutrina Militar de Defesa Cibernética.

O MD e as Forças Armadas participam das atividades coordenadas pelo GSI-PR, particularmente a SIC e a Segurança Cibernética. Em face da 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.

Para isso, visualiza-se a implantação do Sistema Brasileiro de Defesa Cibernética, cujo organograma encontra-se na Figura 2.

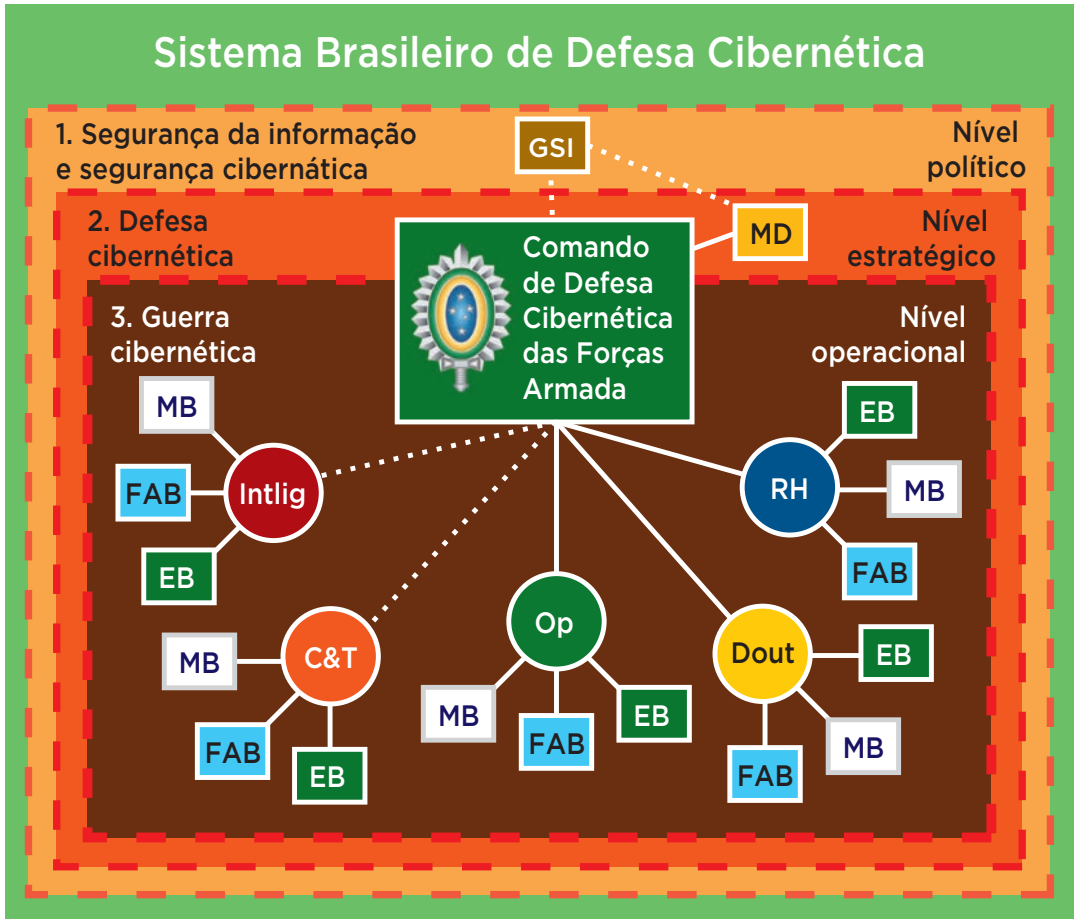

Figura 2 – Sistema Brasileiro de Defesa Cibernética

Observando-se a Figura 2, 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 Forças Armadas (Níveis Operacional e Tático – Guerra Cibernética), com vista a engajar toda a sociedade na defesa dos interesses nacionais dentro do espaço cibernético.

Trata-se de um objetivo ambicioso, que deve ser perseguido. Sua consecução constitui condição *sine qua non* para a defesa das infraestruturas críticas nacionais contra ataques cibernéticos, a qual se insere na missão constitucional das Forças Armadas, 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 ela perceba que é vantajoso cooperar com o esforço nacional de Defesa Cibernética.

Visualiza-se a criação do Comando de Defesa Cibernética das Forças Armadas, o qual poderá realizar a supervisão, a coordenação e a orientação técnica e normativa das atividades do Sistema Brasileiro de Defesa Cibernética, 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 Ministério da Defesa com o GSI-PR, para fins de participação na Segurança Cibernética e de obtenção da indispensável cooperação dos setores público e privado e da comunidade acadêmica no esforço nacional de Defesa Cibernética.

Desafios do setor cibernético no âmbito da defesa

A efetivação das ações estratégicas, listadas e detalhadas no documento referente aos quesitos previstos para a 2ª fase na Diretriz Ministerial nº 014/2009, constitui o grande desafio à Consolidação do Setor Cibernético na Defesa, uma vez que óbices de natureza diversa dificultam a sua concretização.

Entre esses óbices, merecem destaque os seguintes:

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

b. necessidade de conscientização de governantes e da sociedade como um todo em relação ao tema, decorrente do óbice anterior, que dificulta a obtenção da indispensável mobilização para a participação nas atividades de Segurança e Defesa Cibernéticas;

c. escassez de recursos financeiros ou não priorização do setor na alocação de recursos financeiros, também, em parte, decorrente dos óbices anteriores;

d. caráter sensível da atividade, dificultando a aquisição de conhecimento vindo do exterior; e

e. integração e atuação colaborativa incipientes dos diversos atores envolvidos.

Entre as citadas ações estratégicas, as julgadas mais relevantes como desafios à consolidação do Setor Cibernético na Defesa serão listadas e detalhadas a seguir.

Assegurar o uso efetivo do espaço cibernético pelas Forças Armadas e impedir ou dificultar sua utilização contra interesses da defesa nacional

a. Criar o Comando de Defesa Cibernética das Forças Armadas, com a participação de civis e militares das três Forças, para executar os objetivos do Sistema Brasileiro de Defesa Cibernética.

b. Elaborar a Política de Defesa Cibernética.

c. Propor a criação de uma estrutura de Defesa Cibernética subordinada ao Estado-Maior Conjunto das Forças Armadas para inserir o tema nos planejamentos militares conjuntos.

d. Levantar as ICIs associadas ao Setor Cibernético para formar a consciência situacional necessária às atividades de Defesa Cibernética.

e. Levantar critérios de riscos e sua gestão para reduzir a probabilidade e o impacto de ameaças cibernéticas nas ICIs de interesse da Defesa Nacional.

Capacitar e gerir talentos humanos para a condução das atividades do setor cibernético na defesa

a. Criar cargos e funções específicos e mobiliá-los com pessoal especializado.

b. Identificar e cadastrar pessoal com competências ou habilidades nos ambientes interno e externo das Forças Armadas.

c. Estabelecer critérios para a mobilização e desmobilização de pessoal.

d. Capacitar, de forma continuada, pessoal para atuar no Setor Cibernético, aproveitando as estruturas existentes nas Forças Armadas.

e. Viabilizar a participação de pessoal envolvido com o Setor Cibernético em cursos, estágios, congressos, seminários e simpósios.

f. Realizar, periodicamente, o Seminário de Defesa Cibernética de Defesa.

g. Criar um plano de carreira para viabilizar e motivar a permanência do pessoal especializado nas atividades do Setor Cibernético.

h. Realizar parcerias estratégicas e intercâmbio com instituições de interesse.

Desenvolver e manter atualizada a doutrina de emprego do setor cibernético

a. Fomentar o desenvolvimento e o intercâmbio de teses, dissertações e outros trabalhos similares em instituições de ensino superior civis e militares de interesse para as atividades do Setor Cibernético.

b. Promover intercâmbio doutrinário com instituições militares nacionais e nações amigas.

c. Criar a Doutrina de Defesa Cibernética.

d. Inserir a Defesa Cibernética nos exercícios de simulação de combate e nas operações conjuntas.

e. Criar um sistema de gestão de conhecimento de lições aprendidas para composição e atualização da doutrina.

Adequar as estruturas de CT&I dasForças Armadas e implementar atividades de pesquisa e desenvolvimento (P&D) para o setor cibernético

a. Planejar e executar a adequação das estruturas de CT&I, integrando esforços entre as Forças Armadas.

b. Criar comitê permanente, no âmbito da Defesa, constituído por representantes do MD, Forças Armadas, MCT e outros ministérios e agências de fomento para intensificar e explorar novas oportunidades de cooperação em CT&I.

c. Identificar competências em CT&I, no âmbito do MD e dos centros de P&D civis públicos e privados, estabelecendo centros de excelência.

d. Prospectar as necessidades do Setor Cibernético, na área de CT&I, no âmbito da Defesa, para identificar as capacidades científico-tecnológicas necessárias ao desenvolvimento do Setor Cibernético.

e. Criar parcerias e cooperação entre os centros militares de P&D e os centros de P&D civis públicos e privados.

Cooperar com o esforço de mobilização militar e nacional para assegurar as capacidades operacional e dissuasória do setor cibernético

a. Realizar levantamento sistemático de equipamentos, instalações e pessoal passíveis de serem mobilizados.

b. Confeccionar Plano de Mobilização de Equipamento, Instalações e Pessoal, com respectivos custos. Elaborar e manter atualizado um banco de talentos humanos de interesse para a mobilização.

c. Adequar as necessidades de mobilização do setor cibernético ao Sistema Nacional de Mobilização.

d. Propor ao governo federal a realização de campanha nacional de educação sobre Segurança e Defesa Cibernética para elevar o nível de conscientização da sociedade brasileira sobre o tema.

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 neste século, podendo, até mesmo, ser comparado ao domínio dos mares no período das grandes navegações.

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

De modo semelhante ao ocorrido com o colonialismo luso-espanhol das grandes navegações e com o neocolonialismo afro-asiático do final do século 19, vislumbra-se o prenúncio de uma verdadeira corrida rumo ao espaço cibernético, que pode constituir o moderno colonialismo do século 21.

A grande diferença dessa nova forma de colonialismo para as anteriores, no entanto, é que, atualmente, a disputa não fica restrita às grandes potências do momento, diante do 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 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 mais bem 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.

_____. 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.

_____. Presidência da República. Gabinete de Segurança Institucional da Presidência da República. *Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008.* Brasília, 2008.

_____. 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.

_____. *Segurança e defesa do espaço cibernético brasileiro.* Brasília, 2010.

PAINEL 1

TENDÊNCIAS GLOBAIS EM SEGURANÇA E DEFESA CIBERNÉTICA

REFLEXÕES SOBRE SEGURANÇA E DEFESA CIBERNÉTICA

Raphael Mandarino Junior[*]

Resumo

Quase que sem perceber, a moderna sociedade se viu participando do que se convencionou chamar *sociedade da informação*. Essa nova era trouxe um sem-número de benefícios e possibilidades, antes inimagináveis, que introduziram importantes modificações no dia a dia das pessoas, alterando comportamentos sociais, econômicos, culturais, políticos, religiosos e até filosóficos, em razão da modificação na forma de se olhar o mundo. O surgimento da internet, que introduziu novas formas de comunicação e de troca de informações, a velocidades estonteantes, formou uma complexa teia de atores, equipamentos e locais, conjunto ao qual se denomina *espaço cibernético,* ao qual o homem se acostumou e com o qual se interage de forma natural, sem necessariamente conhecer o outro a quem se dirige ou com quem se interage. Expõe sua intimidade, a privacidade, sem saber por onde trafegam suas informações, pressupondo-se que está seguro nesse ambiente virtual. Como toda mudança de comportamento nas práticas diárias, estas também trouxeram consequências não percebidas originalmente. Dentre essas consequências, destaca-se a necessidade de garantir que essa quantidade enorme de informações que trafegam e são armazenadas em volumes crescentes e imensuráveis esteja segura. À medida que a sociedade da informação vai estabelecendo-se em um país, inicia-se o processo de construção de verdadeira *nação* virtual, constituída no que se denomina *espaço cibernético,* em que os três elementos básicos que caracterizam uma nação estão presentes: o povo, caracterizado pelos atores que interagem na própria sociedade da informação; o território, caracterizado pelo próprio es-

[*] Formou-se em Matemática e complementou sua formação com uma série de cursos de extensão e especialização em Informática no Brasil e no Exterior. Atua na área de Informática há mais de 30 anos, em sua maior parte no Distrito Federal, e desempenhou inúmeras funções técnicas e cargos diretivos. Atualmente é diretor do Departamento de Segurança da Informação e Comunicações (DSIC) do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), desde maio 2006; coordenador do Comitê Gestor da Segurança da Informação (CGSI), órgão do Conselho de Defesa Nacional, desde setembro de 2006; e membro do Comitê Gestor da Infraestrutura de Chaves Públicas do Brasil (CG ICP-Brasil), desde abril de 2007.

paço cibernético; e a soberania, capacidade de controlar, de ter poder de decisão sobre esse espaço. À semelhança dos preceitos que obrigam o Estado brasileiro a garantir a segurança e a defesa de sua sociedade na vida como se conhece, deve-se construir estratégias de segurança e defesa cibernéticas para garantir a nação virtual.

Palavras-chave: segurança cibernética, segurança da informação, sociedade da informação.

A sociedade da informação

Vive-se nos tempos da chamada *sociedade da informação*, expressão que ainda carece de definição universalmente aceita, apesar de ter suas primeiras referências na década de 1970, nas discussões sobre como seria construída e o que caracterizaria a "sociedade pós-industrial" (TAKAHASHI, 2002).

Já se encontravam as suas premissas no que Toffler (1980) chamou de a "nova civilização", resultante do terceiro grande fluxo de mudança na história da humanidade – a terceira onda – que impõe um novo código de comportamento: "Essa nova civilização traz consigo novos estilos de família; modos de trabalhar, amar e viver diferentes; uma nova economia; novos conflitos políticos; e além de tudo isso igualmente uma consciência alterada".

Segundo Toffler, a primeira onda ocorreu há cerca de 10 mil anos, quando a espécie humana passou de uma civilização eminentemente nômade para uma civilização sedentária, a partir do domínio das tecnologias agrícolas. E a segunda onda se deu há cerca de 330 anos, quando a espécie humana deixou de ser uma civilização predominantemente agrícola para tornar-se uma civilização industrial, ao dominar novas tecnologias de fabricação de bens de consumo, especialmente as máquinas a vapor.

O autor dá como característica para cada onda o fato de a humanidade se ver diante de novas formas de criar riquezas, sempre acompanhadas de transformações profundas nos modelos sociais, culturais, políticos, filosóficos, econômicos e institucionais – uma verdadeira revolução que alterava o modo de vida, então conhecido de forma tão profunda e ampla.

Está-se vivendo hoje em pleno período de uma dessas revoluções. Embora esteja reservado aos computadores e às telecomunicações um papel importante nessas mudanças revolucionárias, é importante entender que as mudanças não são apenas tecnológicas, mas também: **econômicas**, cuja melhor caracterização se dá pelo surgimento do comércio eletrônico; **sociais**, expressas, por exemplo, nos sítios de relacionamento; **culturais**, ao facilitarem a troca de informações, permitindo o aprofundamento dos conhecimentos sobre usos e costumes entre os povos; **políticas**, ao permitirem um contato direto entre eleitor e eleito; **religiosas**, quando percebemos a especial atenção que igrejas das mais variadas orientações dão às mídias eletrônicas na propagação de sua fé; **institucionais**, cuja melhor expressão talvez esteja nas diversas iniciativas do governo eletrônico, no uso das Tecnologias da Informação e Comunicação (TICs) em proveito do cidadão; e, sem esgotar, até mesmo **filosóficas**, pois mudam a maneira de ver o mundo, o que pode ser exemplificado com a abordagem da obra *Não-lugares,* de Áuge (1994), que discute os impactos antropológicos, "frutos da supermodernidade", advindos dessa revolução que se está vivendo (MANDARINO JUNIOR, 2010).

Essa nova era tem sua melhor caracterização no surgimento da internet, que introduziu novas formas de comunicação e de troca de informações, a velocidades inimagináveis há poucos anos e suportadas por uma miríade de equipamentos e *softwares* distribuídos e operados por pessoas, empresas e governos. Formando uma complexa teia de atores, de equipamentos e de locais aos quais o homem se acostumou e com os quais interage de forma natural, ao realizar atividades cotidianas, tais como assistir à televisão ou a um filme, falar ao telefone ou corresponder-se com amigos, estudar ou fazer pesquisas em bibliotecas, conferir o extrato ou o saldo bancário, pagar tributos ou duplicatas, comprar discos ou livros. Enfim, o homem "conversa", "vai aos bancos", "namora", "trabalha", "compartilha opiniões", para ficar em poucos exemplos, de forma virtual, sem necessariamente conhecer o outro a quem se dirige ou com quem interage. Sem saber por onde trafegam suas informações, expõe sua intimidade, sua privacidade, sua capacidade financeira e econômica, suas atividades profissionais, pressupondo que está seguro nesse ambiente virtual, nesse espaço cibernético.

Toda mudança de comportamento nas práticas diárias trazida pela sociedade da informação fez que fossem aceitas alterações significativas nos valores sociais, profissionais e econômicos, sem uma clara percepção das suas consequências em médio e longo prazo.

A segurança da informação

Dentre essas consequências, destaca-se a necessidade de garantir que essa quantidade enorme de informações que trafegam e são armazenadas em volumes crescentes e imensuráveis esteja segura.

Entretanto, o assunto *segurança da informação* está longe de ser consensual e compreendido em toda a sua abrangência e consequências, seja pela sociedade, seja por profissionais, seja pela academia.

Com o incremento da chamada *internet comercial* em meados da década de 1990, a questão da manipulação de informações e da sua segurança ganha maior ênfase, pois a grande rede e seus protocolos, especialmente a família TCP/IP, foram construídos sem muita preocupação com a confidencialidade, a integridade, a disponibilidade e a autenticidade.

À semelhança do que ocorre em qualquer novo espaço aberto e pouco regulado no mundo físico, como o antigo "velho oeste", as regiões de fronteiras ou as bordas de expansão agrícola, ainda não perfeitamente demarcadas, pessoas mal-intencionadas sempre buscam obter vantagens ilícitas ou socialmente inaceitáveis explorando a falta de regras.

Assim ocorre na internet, ou melhor, no chamado *espaço cibernético,* em que pessoas e grupos, acobertados pela distância e pelo anonimato, tentam burlar a segurança dos equipamentos e dos sistemas informatizados de qualquer empresa, governo ou indivíduo e extrair benefícios indevidos da exploração desse bem chamado *informação*.

A segurança da informação, definida como uma "área de conhecimento dedicada à proteção de ativos de informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade" (SÊMOLA, 2003), surge como nova especialidade, responsável por assegurar que as informações, sejam elas de caráter pessoal, institucional ou corporativo, estejam preservadas.

Como a informação é um bem incorpóreo, intangível e volátil, os ativos de informação tornam-se naturalmente os principais focos de atenção da segurança da informação. São exemplos de ativos de informação: os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso, como computadores, equipamentos de comunicações e de interconexão; os sistemas utilizados para tal; os locais onde se encontram esses meios; e também os recursos humanos

que a eles têm acesso. Os ativos de informação confundem-se, de certa forma, com a própria sociedade da informação.

Pode-se também entender que um subconjunto desses ativos forma a base, a infraestrutura de informação, que suporta a sociedade da informação, se se interpretar o entendimento de Morais Silva (1961) para o termo *infraestrutura* como *estrutura das partes inferiores.*

Com o advento da sociedade da informação, em que as tecnologias de informação e comunicação têm papel preponderante nas infraestruturas de uma nação e na interação entre elas, percebe-se que as infraestruturas de informação são críticas porque não podem sofrer solução de continuidade. Se elas param, a sociedade da informação também para, com graves consequências para a sociedade real.

Há de se considerar ainda que, apesar de essas infraestruturas, por suas características, estarem acessíveis e utilizáveis de forma pulverizada pela sociedade, não cabe apenas aos indivíduos, às empresas ou ao governo protegê-las de forma individualizada e descentralizada, pois se trata de um bem comum.

A definição mais usual de infraestrutura crítica é aquela que, uma vez prejudicada por fenômenos de causas naturais, como terremotos ou inundações ou por ações intencionais de sabotagem ou terrorismo, traz grandes reflexos negativos para toda uma nação e sua sociedade. São exemplos clássicos de infraestruturas críticas: as redes de telefonia; os sistemas de captação e distribuição de água; e as fontes geradoras e as redes de distribuição de energia.[1]

O Gabinete de Segurança Institucional da Presidência da República (GSI/PR), no âmbito de suas atribuições, define como infraestruturas críticas as instalações, os serviços, os bens e os sistemas que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade.

Vale notar que, com relação à proteção da sociedade da informação ou à segurança da informação e comunicações, encontram-se duas visões que se complementam ao se estudar o cenário internacional: a proteção da infraestrutura crítica da informação e a proteção da infraestrutura da informação crítica, que são caracterizadas a seguir.

[1] International Critical Information Infrastructures Protection Handbook 2008/2009. Center for Security Studies, ETH Zurich, p. 36-37. Apud CANONGIA, Claudia, março 2009.

A primeira busca identificar e proteger a infraestrutura: *hardwares, softwares,* dados e serviços, que suportam uma ou mais infraestruturas críticas e, uma vez afetados, causam sérios problemas a essas infraestruturas. Uma definição que reforça essa visão encontra-se em um trabalho publicado pelo Centro de Estudos para a Segurança, de Zurich (2008/2009):

> *Critical Information Infrastructure (CII) is that part of the global or national information infrastructure that is essentially necessary for the continuity of a country's critical infrastructure services. The CII, to a large degree, consists of, but is not fully congruent with, the information and telecommunications sector, and includes components such as telecommunications, computers/software, the internet, satellites, fiber-optics, etc. The term is also used for the totality of interconnected computers and networks and their critical information flows.*

A segunda busca identificar e proteger as informações consideradas críticas de uma infraestrutura crítica, como os planos e a relação de vulnerabilidades. Essa visão foi proposta na lei americana de proteção da infraestrutura crítica de 2002.[2]

> *Critical Infrastructure Information (CII) means information not customarily in the public domain and related to the security of critical infrastructure or protected systems: (A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety; (B) the ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or (C) any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.*

[2] Critical Infrastructure Information (CII) Act 2002, Information Analysis and Infrastructure Protection, Critical Infrastructure Information, H. R. 5005—17. Apud CANONGIA, Claudia, março 2009.

Como no Brasil esse assunto é relativamente novo e pouco estudado e não se conhece, na medida exata, o grau de interdependência e conectividade das infraestruturas críticas da informação, assim também não se pode assegurar que todas as informações críticas a respeito de uma infraestrutura crítica estejam protegidas corretamente. Com base nessa realidade e nas proposições anteriores, defende-se que a infraestrutura crítica da informação é o subconjunto dos ativos de informação que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade.

Espaço cibernético

As informações trafegam por uma infinidade de interconexões entre computadores, servidores, roteadores e *switches* conectados por milhares de quilômetros de fibras óticas, por cabos especiais ou por via satélite, os quais formam uma complexa malha de comunicação. É assim que as residências se conectam aos bancos, às empresas públicas ou privadas e aos diversos níveis de governo, os quais, por sua vez, também interconectados, fazem uso dessa extensa malha que cobre todo o País e se interligam com outros países de todos os continentes.

O conjunto das pessoas, das empresas, dos equipamentos e suas interconexões, dos sistemas de informação e das informações que por eles trafegam pode ser também denominado, no entendimento do autor, de espaço cibernético. Esse espaço, em princípio autorregulado e autônomo, permite a troca de informações das mais variadas formas, por pessoas e equipamentos, pessoas que fazem uso de toda essa infraestrutura crítica de informações, sem muitos conhecimentos técnicos de como essa troca se processa e sem clara percepção das suas consequências, como já referenciado.

À medida que a sociedade da informação vai-se estabelecendo em um país, inicia-se um processo de construção de verdadeira "nação" virtual, constituída no que se denomina de espaço cibernético.

Aqui, a exemplo do espaço real, também são estabelecidas relações sociais e políticas, no tempo e no espaço, a partir das quais o povo passa a tomar decisões sobre como "construir" parte de suas vidas, permitindo que alguns, por exemplo, passem a trabalhar exclusivamente, ou não, nesse novo espaço, desfrutem de suas amizades e gerenciem seus interesses financeiros da forma como entenderem correta.

Assim se percebe que, nesse espaço, convivem três características, chamadas centrais pela maioria dos autores, que são elementos importantes na formação de um Estado: o povo, o território e a soberania.

O povo pode ser caracterizado pela sociedade da informação; o território, pelo próprio espaço cibernético; e a soberania, pela capacidade de controlar, de ter poder de decisão sobre esse espaço.

Como em Martinez (2006):[3]

> Pode-se dizer que é até uma questão de lógica que se defina o Estado a partir das relações estabelecidas entre povo, território e soberania. Pois é preciso que haja um mínimo de organização social e política para que as instituições tenham um sentido claro e vivido, e é óbvio, então, que é por obra desse mesmo povo ou de seus líderes que existem tais instituições. Também é de se esperar que esse povo ocupe ou habite um determinado território.

Segurança e defesa cibernética

O que são a segurança e a defesa cibernética do Estado brasileiro e como se estabelecem os seus limites?

De acordo com o *Glossário das Forças Armadas* (2007), o termo *segurança* pode ser entendido como a "condição que permite ao País a preservação da soberania e da integridade territorial, a realização dos seus interesses nacionais, livre de pressões e ameaças de qualquer natureza, e a garantia aos cidadãos do exercício dos direitos e deveres constitucionais".

O termo *defesa* deve ser entendido como "o ato ou conjunto de atos realizados para obter, resguardar ou recompor a condição reconhecida como de segurança" ou ainda a "reação contra qualquer ataque ou agressão real ou iminente".[4]

[3] Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=8453>. Acesso em: 12 dez. 2010.

[4] BRASIL. Ministério da Defesa. Glossário das Forças Armadas – MD35-G-01. Apresenta definições de termos comuns às Forças Armadas. Acesso em: 19 jul. 2008.

Aplicando os conceitos de segurança e defesa ao espaço cibernético, surgem os conceitos de segurança cibernética e de defesa cibernética.

Entende-se, portanto, que segurança cibernética incorpora as ações de prevenção (incidentes) e repressão enquanto a defesa cibernética abrange ações ofensivas e defensivas.

Quanto aos atores, entende-se que a dimensão *segurança cibernética* se dá dentro do escopo da segurança institucional, cabendo à Polícia Federal a repressão. A dimensão *defesa cibernética* parece já estar estabelecida pela Estratégia Nacional de Defesa (END), que atribuiu ao Exército Brasileiro à preponderância na questão cibernética.

Grosso modo, a segurança cibernética preocupa-se em reduzir ou eliminar vulnerabilidades da sociedade da informação do País e suas infraestruturas críticas da informação e em fazê-las voltar à condição de normalidade em caso de ataque, enquanto a defesa cibernética se preocupa em resguardar de ameaças (externas) e reagir, se for o caso, aos ataques ao "nosso" espaço cibernético.

Dessa forma, do ponto de vista da segurança cibernética, deve-se "adotar ações que assegurem disponibilidade, integridade, confidencialidade e autenticidade das informações de interesse do Estado brasileiro" (MANDARINO JUNIOR, 2010). Deve-se estabelecer uma Estratégia de Segurança Cibernética, que é "a arte de assegurar a existência e a continuidade da sociedade da informação de uma nação, garantindo e protegendo, no espaço cibernético, seus ativos de informação e suas infraestruturas críticas" (id., ibid.).

Uma Estratégia de Segurança Cibernética para a Nação brasileira deve projetar e dimensionar os esforços necessários para proteger seus ativos de informação, suas infraestruturas críticas de informação, suas informações críticas; avaliar riscos; desenhar planos de contingências, para recuperação, ou não, de informações diante de desastres naturais; capacitar recursos humanos para responder, pronta e competentemente, a incidentes nas redes; garantir a privacidade das pessoas e das empresas presentes na sociedade da informação; e, como grande diferencial, ter a capacidade de aprender a desenvolver ferramentas de defesa. E ainda que essa Estratégia de Defesa Cibernética esteja apta a utilizar essas ferramentas e a própria informação como recurso ou arma, para assegurar a preservação do Estado brasileiro.

Considerando que um dos objetivos da defesa é "recompor a condição reconhecida como segurança", pode-se concluir que a atividade de segurança e a de defesa são complementares. Embora esta tenha postura mais enérgica que aquela, a dimensão *segurança* não deve existir sem ser complementada pela dimensão *defesa*.

Conclusão

O Brasil precisa estar preparado para proteger o seu patrimônio de informação, entendido aqui como o somatório de seus ativos de informação, suas informações críticas, seus sistemas de informação, suas infraestruturas críticas, incluindo a de informação, tudo aquilo, enfim, que pode ser identificado como componente da sociedade da informação presente no espaço cibernético. Para tanto, será necessário adotar medidas para a proteção mediante a elaboração de doutrina e a construção de estratégias de segurança e de defesa do espaço cibernético brasileiro, considerando ambos os conceitos complementares.

A Estratégia de Segurança Cibernética deve assegurar, entre outros aspectos, a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações de interesse do Estado e da sociedade brasileira, aspectos da segurança institucional. Nesse caso, identifica-se o Gabinete de Segurança Institucional da Presidência da República, por suas competências legais, como o órgão mais apropriado para articular a sua confecção.

A Estratégia de Defesa Cibernética deve ser entendida como as ações que buscam a prevenção ou a reação contra ataques e hostilidades perpetradas contra as infraestruturas críticas, usando a informação como recurso ou arma. Trata-se, portanto, de ações de defesa nacional.

A manutenção da defesa cibernética é responsabilidade, por atribuição legal, do Conselho de Defesa Nacional, do Ministério da Defesa e das Forças Armadas, uma vez que envolve atividades vinculadas à preservação da soberania nacional.

Entretanto, convém ressalvar que, por serem complementares e de certa forma indissolúveis, essas estratégias devem ser construídas de forma escalonada, a fim de que a segurança do espaço cibernético brasileiro seja o objetivo primeiro a ser buscado por todos, especialmente na Administração Pública

Federal, em que, respeitando-se as atribuições legais, cada órgão e cada servidor público tenham as suas responsabilidades estabelecidas e conhecidas.

Como é necessário o desencadear de atividades de defesa, os órgãos com responsabilidades e atribuições legais específicas já estarão envolvidos e em ação, o que contribuirá para diminuir as possibilidades de solução de continuidade.

É essencial estar preparado para enfrentar esse cenário de ameaças, conhecendo as vulnerabilidades e os riscos existentes sobre a infraestrutura crítica da informação da Administração Pública Federal.

Referências bibliográficas

AUGÉ, Marc. *Não-lugares*: introdução a uma antropologia da supermodernidade. Tradução de Maria Lúcia Pereira. Papirus: Campinas, SP, 1994 (Coleção Travessia do Século).

MANDARINO JUNIOR, Raphael. *Segurança e defesa do espaço cibernético brasileiro*. Cubzac: Recife, 2010.

MORAIS SILVA, Antonio de. *Novo dicionário compacto da língua portuguesa*. José Aguilar: Lisboa, 1961.

SÊMOLA, Marcos. *Gestão da segurança da informação*: uma visão executiva. Campus: Rio de Janeiro, 2003.

TAKAHASHI, Tadao (Org.). *Sociedade da informação no Brasil*: livro verde. Ministério da Ciência e Tecnologia: Brasília, 2000.

TOFFLER, Alvin. *A terceira onda*. Record: Rio de Janeiro, 1980.

TENDÊNCIA GLOBAL EM SEGURANÇA E DEFESA CIBERNÉTICA – REFLEXÕES SOBRE A PROTEÇÃO DOS INTERESSES BRASILEIROS NO CIBERESPAÇO

*Paulo Martino Zuccaro**

Introdução

Como nos recorda Alvin Toffler, o homem combate de forma muito similar àquela que emprega em suas atividades econômicas. Por essa razão, aquele extraordinário autor identificou as três grandes eras ou ondas pelas quais a humanidade já passou e ainda passa: a Era Agrícola, em que se podia observar a evidente similitude entre arados, ancinhos, espadas, lanças e punhais; a Era Industrial, em que a mesma tecnologia e os mesmos processos empregados na produção em massa também eram empregados na destruição em massa; e a Era da Informação, atualmente em plena vigência, na qual o poder econômico se deslocou para associar-se à posse da informação, o que também ocorreu com o poder bélico. Em maior ou menor grau, a disponibilidade de melhores recursos de comando e controle, bem como a posse de armamentos mais "inteligentes" e, em geral, mais eficazes têm representado vantagem decisiva nos campos de batalha, que, na verdade, transformaram-se em espaços multidimensionais de batalha.

Ampliando um pouco mais as ideias do consagrado autor, não apenas na disputa entre Estados, mas também no embate entre grupos sociais nos mais diversos graus de organização, ou mesmo entre

* Contra-Almirante Fuzileiro Naval, exerce o cargo de comandante da Tropa de Reforço da Marinha do Brasil. Na sua carreira militar, concluiu os cursos da Escola Naval, de Aperfeiçoamento de Oficiais, de Estado-Maior para Oficiais Superiores, de Comando de Infantaria de Marinha na Espanha, o Básico da Escola de Guerra Naval, de Comando e Estado-Maior Naval na Argentina, de Política e Estratégia Marítimas, além de MBA em Gestão Internacional pela Coppead/UFRJ. Desempenhou as seguintes funções: instrutor da Escola Naval, comandante do Batalhão de Engenharia de Fuzileiros Navais, chefe do Estado-Maior do Comando da Tropa de Desembarque, comandante do Batalhão Naval, subchefe de Comando e Controle do Estado-Maior de Defesa.

indivíduos e esses grupos, o emprego agressivo de recursos típicos da Era da Informação expandiu-se exponencialmente, produzindo-se diferentes graus de impacto nas coletividades atacadas.

Esses fenômenos da atualidade não têm passado despercebidos pelo governo brasileiro, em todas as suas instâncias. Ao contrário: uma série de iniciativas tem buscado dimensioná-los e identificar ações estratégicas para proteger o País das consequências nefastas do emprego de ativos cibernéticos contra os interesses nacionais, em todo o espectro possível de agressões.

Essas iniciativas devem contribuir para a tomada de consciência sobre a natureza e a dimensão desse campo de ação e sobre a vastidão de estruturas, dados, bens, valores e, em última análise, interesses a serem protegidos, além de não se descartar, *a priori*, o direito ao revide e o uso desses mesmos recursos em caso de conflito armado, até mesmo para lograr-se a aceleração da desarticulação da capacidade de combate de nosso oponente e a obtenção da vitória, com menor cômputo de vidas humanas perdidas por parte de ambos os contendores.

Assim, procurando, ao mesmo tempo, tatear as fronteiras do que, hoje, estamos chamando, genericamente, de "guerra cibernética" e priorizar, dentro do possível, as questões de Defesa propriamente ditas, o autor deste texto pretende apresentar: uma brevíssima resenha histórica sobre a evolução do tema; um diagnóstico sobre a situação corrente, em nível global; e os principais desafios a serem vencidos pela Nação já em curto prazo. Ao final, uma conclusão objetiva procurará sintetizar todo o conteúdo apresentado.

Cumpre ressalvar que este artigo apresenta tão somente algumas reflexões individuais do autor sobre o tema em discussão e não representa, necessariamente, o entendimento do Ministério da Defesa (MD) ou da Marinha do Brasil (MB), instituição esta à qual pertence desde 1975, sobre os assuntos aqui discutidos.

Desenvolvimento

Histórico

Indubitavelmente, a Era da Informação e, portanto, as atividades no espaço cibernético encontram suas raízes na construção dos primeiros computadores, como, por exemplo, o Eniac, uma monstruosa calculadora construída para realizar cálculos balísticos (NUNES, 2010, p. 9). Entretanto, não resta dúvida de que o uso intensivo do que hoje está sendo denominado "ciberespaço", ou o "quinto domínio da guerra", após a terra, o mar, o ar e o espaço exterior (CYBERWAR, 2010, p. 10), somente se expandiu a velocidades espantosas com o advento da internet, derivada da rede Arpanet, concebida pelo Departamento de Defesa norte-americano (NUNES, 2010, p. 9).

Ainda assim, um episódio anterior ao *boom* da internet merece registro. Em junho de 1982, satélites espiões norte-americanos detectaram uma grande liberação de energia na Sibéria. Tratava-se de uma explosão em um gasoduto, atribuída, segundo várias fontes, ao mau funcionamento de seu sistema de controle, comandado por computador. Esse sistema teria sido obtido ilegalmente de uma empresa canadense. Segundo as mesmas fontes, a Agência Central de Inteligência norte-americana (CIA) teria alterado o sistema de modo que, a partir de certo tempo, as bombas e demais mecanismos de controle receberiam instruções para fazer o gasoduto operar com pressões muito mais altas que os limites admitidos para seus componentes, resultando, então, na explosão detectada (WAR, 2010, p. 25).

Não nos é possível asseverar que os fatos ocorridos foram realmente esses. Se o foram, estamos diante de um evento marcante no contexto da guerra cibernética, pois terá sido o primeiro a envolver o ataque a uma infraestrutura crítica mediante o uso de uma "bomba lógica".

Adquiriu muita notoriedade, há poucos anos, a descoberta da existência do que se qualificou como um sistema destinado a realizar escutas eletrônicas em âmbito global e, mediante uma capacidade extraordinária de processamento das informações obtidas, a identificar possíveis ameaças para os Estados Unidos da América (EUA) e seus aliados. É o afamado sistema Echelon. Sua existência teve maior divulgação em 1998, particularmente na perspectiva de constituir uma violação às liberdades individuais e, sob este prisma, passou a ser, e ainda o é, investigado por organizações governamentais e não governamentais. Entretanto, sua existência remonta ao inicio da Guerra Fria, tendo sido idealizado, inicialmente, como uma aliança de inteligência conhecida como Ukusa que atenderia aos interesses de

EUA, Reino Unido, Austrália, Canadá e Nova Zelândia. Levantou-se, também, a suspeita de que estaria sendo usado para beneficiar empresas norte-americanas em concorrências internacionais. Sua força residiria na capacidade de captar sinais de comunicações comerciais por satélite, particularmente dos sistemas Inmarsat e Intelsat, que sustentam grande parte das comunicações civis e governamentais de vários países, bem como em seu módulo Dictionary, que selecionaria automaticamente as mensagens potencialmente relevantes, a partir de datas, localidades, nomes, assuntos e outros dados nelas contidos. (WEBB, 2008, p. 453-457).

A própria existência da National Security Agency (NSA), fundada sigilosamente pelo presidente norte-americano Harry S. Truman em 1952, inicialmente focada em Inteligência de Sinais e Segurança das Comunicações (WEBB, 2008, p. 459), revela que a ação norte-americana de explorar o amplo espectro das comunicações e de tentar impedir que seus oponentes façam o mesmo talvez ainda seja a mais ampla e a mais antiga entre todos os Estados que se lançaram nesse campo. O advento e o crescimento vertiginoso da internet vieram, então, a tornar ainda mais compensadores os esforços despendidos nessa atividade.

Em 1999, no conflito pela autonomia do Kosovo em relação ao governo central da Sérvia, há registros de diversos embates entre *hackers* sérvios e kosovares, durante o período da campanha aérea norte-americana contra alvos da infraestrutura sérvia, a essência estratégica daquele conflito. Após o bombardeio acidental da Embaixada da China em Belgrado, *hackers* chineses também se engajaram em ataques a *sites* do governo norte-americano (MESSMER, 1999).

Em 2000, ocorreu um dos poucos ataques cibernéticos a infraestruturas já efetivamente confirmados. Um ex-funcionário de uma companhia de esgotos na Austrália, inconformado com a preterição para sua promoção, invadiu o sistema de controle de bombas da companhia e causou o derramamento de milhões de litros de esgoto nas ruas da cidade de Maroochy (NUNES, 2010, p. 27).

Durante a Operação Iraqi Freedom, iniciada em 2003, os EUA se abstiveram, segundo relatos oficiais, de empreender ataques cibernéticos ao sistema financeiro iraquiano, por temer que, ao estar aquele sistema fortemente conectado a outros sistemas de igual natureza em outras partes do mundo, principalmente na Europa, e estes últimos, por sua vez, amplamente conectados aos próprios sistemas norte-americanos, os danos causados poderiam se estender para muito além do desejável, resultando em consequências imprevisíveis (WILSON, 2007). A questão relativa à grande dificuldade em se controlar

efetivamente a extensão dos danos provocados por um ataque cibernético é de grande relevância e voltará a ser abordada neste artigo.

Em seis de setembro de 2007, Israel realizou um ataque aéreo à Síria, objetivando destruir uma suposta instalação nuclear denominada al-Kibar, localizada na região de Deir ez-Zor. Algumas fontes afirmam que, para evitar o engajamento de suas aeronaves pelo sofisticado sistema de defesa antiaérea sírio, recém-adquirido da Rússia, este último sofreu um eficaz ataque cibernético que teria mantido o funcionamento aparentemente normal dos equipamentos, que, entretanto, descartaram os contatos gerados pelas aeronaves israelenses (NUNES, 2010, p. 93). Especula-se, inclusive, acerca da existência de uma *kill switch*, uma *back-door* que teria permitido a neutralização remota do sistema (ADEE, 2008). Outras fontes dão conta de que o sistema teria sido neutralizado por meio de mísseis antirradiação e outras supõem que os radares foram postos fora de ação por medidas de guerra eletrônica convencional (FULGHUM, 2007).

Esse episódio, conhecido como a Operação Orchard, ainda permanece obscuro. Israel inicialmente não admitiu a autoria do ataque aéreo, mas, nos dias que se seguiram, algumas declarações de seus líderes demonstraram que, de fato, ele ocorreu. A Síria insiste em que o ataque existiu, mas declara que seu sistema de defesa antiaérea efetivamente engajou as aeronaves atacantes e não reconhece que esteja conduzindo um programa nuclear ou que haja, na área atingida, qualquer construção vinculada a um programa de tal natureza (OPERATION, 2011).

O fato é que o evento indica que a crescente sofisticação dos sistemas de combate acaba por traduzir-se, em alguma medida, em certo aumento de sua vulnerabilidade, particularmente no que concerne aos ataques cibernéticos. Outra constatação é que a fronteira entre a guerra cibernética e a guerra eletrônica quiçá seja mais tênue do que nossa mente cartesiana gostaria de identificar. Talvez, por essa razão, a doutrina de defesa norte-americana, como veremos mais adiante, considera a guerra cibernética, sob o nome de *Computer Network Operations* (*CNO*), parte das operações de informação, que também incluem a guerra eletrônica.

Ainda em 2007, ocorreu um evento marcante no contexto da guerra cibernética. Em represália a uma decisão por parte do governo da Estônia, de remover um memorial de guerra da era soviética no centro de sua capital, Tallinn, ocorreu um ataque coordenado de negação de serviço sobre servidores do governo e dos bancos estonianos, que passou a ser conhecido como a *WW-I*, ou seja, a *Web War I*,

embora tenha-se configurado mais como um "ciber-distúrbio civil" do que propriamente como guerra cibernética (WAR, 2010, p. 28).

No caso da Geórgia, em 2008, embora os recursos tecnológicos usados tenham sido similares, ficou mais evidenciada a participação de um Estado, a Rússia, já que o ataque foi coordenado com o avanço das tropas russas. Cabe recordar, entretanto, que ataques dessa natureza utilizam as chamadas *botnets*, ou redes de zumbis, ou robôs, nas quais computadores "escravizados" em várias partes do mundo passam a participar da agressão, motivo pelo qual é muito difícil caracterizar-se claramente sua autoria verdadeira (WAR, 2010, p. 28).

Não é trivial tentar analisar ou criticar as decisões que levam uma instituição governamental, seja ela militar ou não, uma concessionária de serviços públicos ou uma empresa privada detentora de recursos sensíveis, a lançar agressões cibernéticas na internet, com os mais diversos propósitos. É muito difícil, também, imaginar o grau de isolamento ou proteção existente entre o segmento aberto de sua rede e aquele destinado às suas atividades operacionais, ou, falando de forma mais simples, entre a internet e a sua intranet. Pode-se também questionar, no concernente à intranet, quanto à efetiva separação entre os sistemas administrativos menos sensíveis e os sistemas de missão crítica.

O fato é que, inegavelmente, sistemas de gestão e controle de infraestruturas críticas, sistemas bancários e sistemas de comando e controle militares vêm progressivamente sofisticando-se e utilizando ativos do chamado ciberespaço. Isso representa, por um lado, um incremento alarmante das ameaças aos interesses do Estado. Por outro, e como sempre, enseja oportunidades a serem exploradas, pelos mais capazes, naturalmente.

Diagnóstico

Tomada de consciência da situação corrente

A percepção de que as ameaças cibernéticas vêm-se expandindo exponencialmente com a Internet pode ser corroborada, entre outras formas e fontes disponíveis, pela apreciação do número de incidentes relatados ao Centro de Coordenação do Computer Emergency Readiness Team (CERT/CC), um centro de pesquisa e desenvolvimento na área de segurança de internet, financiado pelo governo norte-americano e operado pela universidade de Carnegie-Mellon. No período de 1990 a 2003, esse número elevou-se de 252 a 137.529, dos quais 55.435 ocorreram em 2003 (KNAPP; BOULTON, 2008, p. 18; CERT, 2009).

O gráfico a seguir, produzido com dados desse centro referentes ao número de incidentes anualmente relatados, demonstra cabalmente a assertiva.

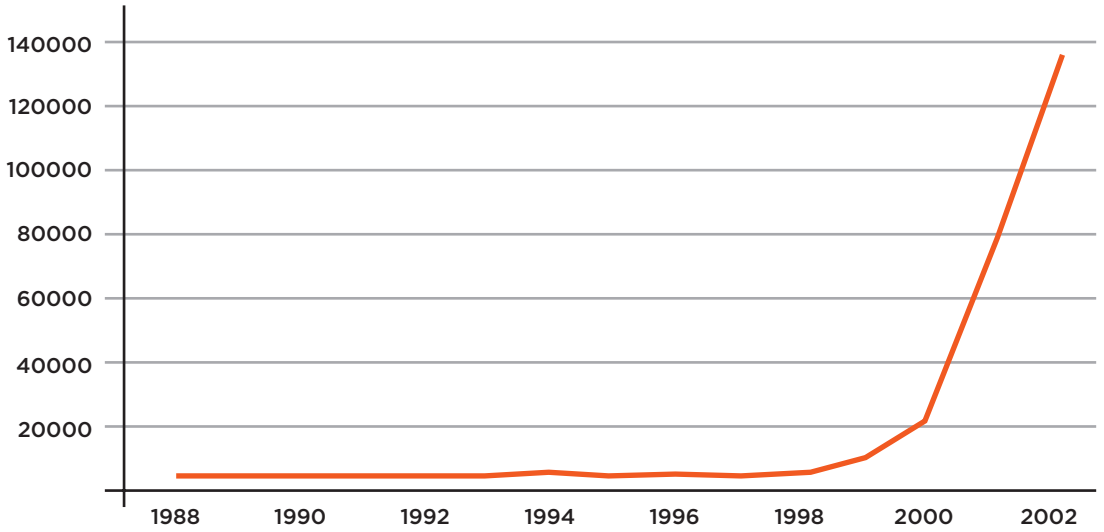

Figura 1 – Estatística anual de incidentes cibernéticos

Fonte: CERT (2009).

Essa constatação nos remete à conhecida "Lei de Metcalfe", atribuída a Robert Melancton Metcalfe, coinventor do padrão Ethernet e um dos fundadores da empresa 3Com, cujo enunciado estabelece que "o valor de um sistema de comunicação cresce na razão do quadrado do número de usuários do sistema" (LEI DE METCALFE, 2011).

Parece ser, portanto, que, se o valor da internet está crescendo com o quadrado do número de usuários, as ameaças também estão acompanhando, *grosso modo*, essa proporção.

Aliás, até 2015, estima-se que, aproximadamente, 28% da população mundial tenha-se tornado usuária da internet, algo na ordem de dois bilhões de pessoas (NUGENT; RAISINGHANI, 2008, p. 28). Quantas terão conhecimento para se tornarem *ciberguerreiros*, qualquer que seja a causa ou motivação? Quantos computadores poderão ser "escravizados" para empreenderem ataques cibernéticos, à revelia de seus proprietários?

Cabe ressaltar que, diferentemente do que ocorre com a espionagem humana, física, sua correspondente cibernética é, além de muito difícil controle, tacitamente aceita, à medida que o impedimento do acesso aos conteúdos colocados em computadores conectados à rede mundial é, fundamentalmente, responsabilidade daqueles que optaram por arquivá-los em um meio que pode, ao menos teoricamente, ser perscrutado de qualquer parte do mundo. Friamente falando, a prática nos tem demonstrado que é muito difícil imputar responsabilidades a invasões de privacidade, à apropriação de conteúdo protegido por direitos autorais ou comerciais e até mesmo de material sensível à segurança nacional, quando o alvo da ação se encontra armazenado em computadores conectados à rede mundial.

> Espiões humanos tradicionais se arriscam a perder a vida procurando surrupiar cópias de documentos físicos. Hoje, um espião virtual não corre tal risco. Ademais, enquanto um espião pode, no máximo, conseguir alguns livros, sua versão virtual pode conseguir a biblioteca inteira e, se as prateleiras forem reabastecidas, ele roubará tudo outra vez (WAR, 2008, p. 26, tradução nossa).

Isto sem mencionar o fato de que tudo pode acontecer sem que o proprietário das informações dê falta delas ou saiba que elas foram copiadas.

Existe, inclusive, um caso conhecido em que a atividade de varredura do espectro cibernético não é apenas admitida, mas amparada por lei. Trata-se de uma provisão legal norte-americana, datada de 1994, cujo propósito é facilitar as ações de *law enforcement* (imposição da lei). Alavancada pelo Federal Bureau of Investigation (FBI), o *Calea*, acrônimo de *Communications Assistance for Law Enforcement Act*, é, mais precisamente, uma emenda ao Código dos EUA,[1] que já dava legalidade ao emprego do conhecido "grampo" telefônico, quando em uso por autoridades policiais. O *Calea* estende o campo de atuação dessas investigações policiais à internet, impondo aos provedores de banda larga a obrigação de facultar o acesso dos órgãos incumbidos de *law enforcement*, especialmente o FBI, aos dados transmitidos, sem que os proprietários das informações tenham ciência disso (COMMUNICATIONS, 2011).

O *Calea* resulta do reconhecimento de que a internet também é amplamente usada com fins ilícitos. Em particular, o advento da tecnologia *Voice Over IP* (*VOIP*) havia tornado os grampos tradicionais praticamente inúteis. O *Calea* é operacionalizado mediante a inclusão de itens de *hardware* e *software* na estrutura desses provedores, de forma a facilitar o acesso aos dados transmitidos por parte dos órgãos de imposição da lei. Recordando que não há como definir claramente fronteiras no ciberespaço, existe uma possibilidade razoável de que esses órgãos acessem, rotineiramente, dados em outros países, desde que, em princípio, haja um fim legal por detrás de tal intrusão, ao menos sob a ótica do Estado norte-americano. Isso posto, possivelmente, os algoritmos criptográficos existentes nos roteadores fabricados em conformidade com o *Calea* sejam inertes no caso dessas investigações.

Indo mais além, é virtualmente impossível impedir as atividades ou imputar autoria e responsabilidade de qualquer natureza às ações daqueles especialistas que, sem realizar qualquer agressão cibernética imediata, se dedicam a vasculhar redes e outros ativos pertencentes a potenciais oponentes, sejam eles Estados, empresas, grupos, organizações ou mesmo indivíduos, na busca de conhecer e registrar suas vulnerabilidades, preparando-se para, quando necessário, explorá-las em sua plenitude.

Muitos países já consideram a formação de guerreiros cibernéticos como "estratégia de Estado", como, por exemplo, EUA, China, Rússia, Canadá, Alemanha, Reino Unido, Austrália e Índia, mas, certamente, China e Rússia ocupam posição de destaque nesse cenário (ALVAREZ, 2010). A propósito, no que diz respeito à admissão do uso de meios cibernéticos contra outros Estados, é fato marcante a publicação

[1] Compilação e codificação das leis federais gerais e permanentes norte-americanas.

do trabalho, que hoje já possui considerável fama, dos coronéis chineses Qiao Liang e Wang Xiangsui, cujo título traduzido ao português seria *Guerra além dos limites*, cuja versão para o inglês ficou conhecida como *Unrestricted Warfare*. Nesse trabalho, os autores levantam a possibilidade do uso da guerra cibernética e de outros meios pouco convencionais para que a China possa, futuramente, confrontar-se com os EUA (KILROY JR., 2008, p. 443).

Além das ameaças lógicas em ação no ciberespaço, há de se preocupar, também, com as ameaças físicas à própria estrutura material que consubstancia esse espaço. À guisa de exemplo, verifica-se que mais de 90% do tráfego da internet passa por fibras óticas em cabos submarinos, os quais, ao longo de seus trajetos, por vezes se concentram perigosamente em alguns pontos de estrangulamento, como, por exemplo, ao largo de Nova Iorque, no Mar Vermelho e no Estreito de Luzon, nas Filipinas (WAR, 2010, p. 25). No Brasil, embora não sejam propriamente estrangulamentos, são importantes as águas próximas às cidades do Rio de Janeiro, de Santos e de Fortaleza.

Figura 2 – Distribuição dos cabos submarinos de fibra ótica
Fonte: WAR (2010, p. 26).

Ainda tratando de questões mais relacionadas com o mundo real do que com o virtual, não há unanimidade acerca da real vulnerabilidade dos sistemas que controlam instalações industriais, os chamados *SCADA – Supervisory Control and Data Acquisition* (WAR, 2010, p. 28). Entretanto, se esses sistemas estiverem, de alguma forma, conectados à internet ou logicamente acessíveis a potenciais agressores, o risco de acesso de agressores torna-se bastante concreto. Os episódios da explosão do gasoduto na Sibéria, partindo-se da suposição de que a causa foi realmente a modificação do *software* de controle, e do vazamento de esgoto na Austrália demonstram a potencialidade desse risco, que deve ser alvo da máxima atenção por parte de empresas e instituições que têm sob sua responsabilidade elementos pertencentes ao conjunto de infraestruturas críticas, com destaque para oleodutos, gasodutos, linhas de transmissão, usinas de produção de energia das mais diversas fontes, plataformas de produção de petróleo, redes de transmissão de dados e telefonia, portos, aeroportos e outros.

Aliás, a proteção dessas infraestruturas, embora não seja prerrogativa imediata ou exclusiva das estruturas de defesa cibernética do MD, deve, certamente, contar com seu apoio, já que é líquido e certo seu emprego na mobilização nacional para um conflito armado, sem o que nem ao menos será possível lograr-se o desdobramento das forças já disponíveis (KILROY JR., 2008, p. 440).

Questões legais

Alguns fatos e aspectos levantados na breve resenha histórica e no tópico dedicado à tomada de consciência já nos permitiram antever as grandes dificuldades para a construção de um marco legal para pautar a conduta de Estados e de outros atores supraestatais ou infraestatais na eventualidade de um conflito cibernético.

De imediato, deve-se recordar que, entre outras características do ciberespaço, merece especial consideração o fato de ali não existirem fronteiras perfeitamente controladas (NUNES, 2010, p.20).

Como corolário, há de se reconhecer que iniciativas de construção de um arcabouço jurídico de âmbito nacional terão muito pequena efetividade no que se refere à proteção cibernética do Estado, pois seus potenciais agressores provavelmente não estarão sob a égide de seu direito interno. Poderão, contudo, ter utilidade para prevenção, limitação e punição de crimes cibernéticos realizados em território nacional.

Devemos recordar, ainda, que as ações de inteligência no ciberespaço não são consideradas agressão (NUNES, 2010, p. 16), ou seja, conforme já mencionado, nenhum ator, estatal ou não, pode ser moral ou juridicamente questionado por fazer pesquisas acerca das vulnerabilidades dos inúmeros sistemas atualmente conectados à internet, desde que não sejam perpetrados ataques explorando essas vulnerabilidades. Naturalmente, esses ataques seriam desferidos após o início do conflito propriamente dito, quando questionamentos jurídicos acerca de ações cibernéticas seriam considerados absolutamente irrelevantes, em meio a um quadro de hostilidades e agressões materiais das mais diversas naturezas por parte de todos os contendores.

Algumas pessoas ainda advogam pelo afastamento dos Estados das ações ofensivas cibernéticas e pela autolimitação às ações de defesa cibernética. Essas mesmas pessoas tendem a propor a construção de um marco jurídico progressivamente restritivo às atividades cibernéticas governamentais que não sejam de defesa *stricto sensu*. Talvez caiba recordar, se não impomos restrições de qualquer ordem e até mesmo incentivamos o desencadeamento de ações ofensivas de guerra eletrônica, quando associadas à manobra das forças militares, por que não poderíamos fazer o mesmo com a guerra cibernética? Indo um pouco mais além, se, no caso de um conflito armado, podemos atacar fisicamente determinado alvo legítimo à luz do Direito Internacional, por que não poderíamos atacá-lo ciberneticamente, talvez com menor perda de vidas humanas para ambos os contendores?

A propósito, alguns autores afirmam que as Convenções de Genebra e seus Protocolos Adicionais, se devidamente interpretados, conformariam o marco legal necessário e suficiente para reger as ações no ciberespaço ante a eventualidade de um conflito interestatal. Por outro lado, outros tantos, incluindo este autor, têm posição oposta e consideram imperfeita tal aplicação ao ambiente cibernético, mesmo que, no jargão jurídico, *mutatis mutandis*, pois, entre outros, existem os seguintes óbices:

- dificuldades para estabelecer a distinção entre combatentes e não combatentes;
- impossibilidade prática de o dano limitar-se ao alvo selecionado; e
- dificuldades para garantir a legitimidade dos alvos, ou seja, classificá-los como inequivocamente militares.[2]

[2] Cabe a ressalva de que a História é farta em exemplos de pesados ataques físicos a cidades e a infraestruturas civis de beligerantes, como forma de reduzir, indiretamente, sua capacidade de combate, abater o moral nacional e, se possível, alcançar a vitória sem o enfrentamento direto. Londres, Dresden, Hiroshima, Nagasaki e, para não deixar de citar um exemplo pós-Convenções de Genebra, Kosovo são alguns desses exemplos.

Uma taxonomia

A existência, ou não de uma estratificação para determinado campo de ação ou de pesquisa não chega a ser determinante para o estabelecimento de políticas ou estratégias objetivando sua exploração, menos ainda quando se trata do interesse da Nação, mas é certo que a construção de uma ordenação de ideias e, melhor ainda, de uma taxonomia para o campo em questão nos ajuda a entendê-lo e a delinear posturas e procedimentos. Até onde alcança a investigação procedida por este autor, seria possível propor um primeiro *approach* para uma taxonomia das ameaças cibernéticas, basicamente uma consolidação de diversas estratificações propostas encontradas em fontes bibliográficas. Assim, podem ser visualizados três grandes blocos:

- Guerra Cibernética – É focada em conflito interestatal. Independentemente de métodos e executantes, o que estará por trás das ações, de forma velada, ou não, será a agressão de um Estado a outro na busca da redução de poder nacional, que pode estar associada a outros métodos de ataque, inclusive os físicos. Bom exemplo pode ser a ação desencadeada a partir do território russo contra a Geórgia, embora nunca tenha havido uma efetiva admissão por parte do governo russo da autoria dos ataques.

- Terrorismo Cibernético – Neste caso, os interesses a serem alcançados têm motivação política, como, naturalmente, também é o caso da guerra cibernética. A diferença fica por conta do fato de que seus autores, normalmente, serão grupos não estatais. As agressões, em geral, serão dirigidas aos Estados cuja ação ou postura política seja contrária aos interesses ou à visão de mundo daqueles grupos. Também podem ser atacadas instituições ou empresas que possuam ponderável carga simbólica em relação ao Estado ou grupo de Estados a ser agredido, como, por exemplo, uma grande multinacional de uma potência econômica ocidental.

- Crime Cibernético – Quanto a este último bloco, geralmente as motivações serão de indivíduos ou de pequenos grupos, com fins privados e egoísticos. Na maioria dos casos, são ilícitos com objetivo de ganhos econômicos, como, por exemplo, o roubo de senhas bancárias, fraudes com cartões de créditos e outros afins.

Também se encontram menções a determinado tipo de ameaça, chamada "Elemento Interno", considerada como aquela desencadeada no interior da própria organização por, como o nome bem o revela,

pessoa ou grupo de seus próprios quadros. Salvo melhor juízo, como a presente taxonomia se baseia nas motivações, normalmente esse tipo de ameaça enquadrar-se-á em uma daquelas anteriormente definidas.

Alguns autores ainda defendem a existência de outro tipo de ameaça, conhecida como "Ativismo Cibernético", ou *"Hacktivism"*, em que grupos de pessoas vinculadas a determinada causa, sem entrar aqui em considerações acerca de sua legitimidade, realizam ataques cibernéticos a instituições que constituam alvo de sua revolta, como forma de chamar a atenção do público a seu pleito ou mesmo de provocar-lhes perdas para induzi-los a uma reavaliação de suas decisões.

Um caso recente e perfeitamente consistente com tal perfil foram os ataques realizados por ativistas em resposta às ações norte-americanas dirigidas contra o *site* Wikileaks e seu criador, Julian Assange.

Assim, em linhas gerais, as ameaças cibernéticas poderiam ser classificadas conforme os três grandes eixos principais, a saber, guerra cibernética, terrorismo cibernético e crime cibernético, admitindo-se, ainda, uma quarta modalidade, que seria o ativismo cibernético, que, no entanto, representa uma ameaça de menor monta.

A esta altura, é essencial fazer duas importantes ressalvas sobre o embrião de taxonomia aqui apresentado. A primeira delas consiste no fato de que se trata de uma estratificação baseada em motivação, o que, em si, já nos impõe duas reflexões. Ora, as motivações podem ser diferenciadas, mas a relativa homogeneidade do espaço cibernético, particularmente após o advento da internet e de seu *Internet Protocol* (IP), conduzirá para o emprego de recursos e métodos de agressão idênticos ou muito similares. Assim, o intercâmbio de conhecimentos, tecnologias e ideias entre as instituições governamentais e privadas que estejam orientadas à capacitação cibernética da Nação tem de ser fluido, contínuo e incansavelmente perseguido.

Em segundo lugar, o aspecto motivacional, embora desconsiderando recursos e métodos de ataque e defesa, pode ser útil na definição de esferas de competência. Desse modo, não restariam muitas dúvidas de que a contraposição às ameaças classificáveis como "guerra cibernética" e mesmo o desenvolvimento de capacitações ofensivas para a exploração do ciberespaço estarão a cargo da Defesa Nacional, conforme ditarem os interesses da Nação.

Tampouco haverá dúvida de que o crime cibernético será primordialmente combatido tanto por setores especializados das instituições de segurança pública como por grupo, público ou privado, que tenha ativos financeiros ou outros conhecimentos passíveis de constituírem alvo para a cobiça de indivíduos ou grupos dispostos a obtê-los ilicitamente.

Já o terrorismo cibernético exige uma análise menos superficial do que esta que vem sendo conduzida neste artigo, mas, no mínimo, pode-se dizer que, assim como o terrorismo clássico termina, geralmente, por ameaçar o Estado em uma ou várias de suas dimensões (população, território, governo), o terrorismo cibernético também tende a ser multidimensional. Assim, a proteção do Estado contra tal ameaça também tende a ser multidimensional, devendo envolver, no mínimo, os setores dedicados à sua segurança institucional e à sua defesa material. Na atualidade organizacional do governo brasileiro, estamos falando, respectivamente, do Gabinete de Segurança Institucional da Presidência da República (GSI-PR) e do MD.

A complicar esta incursão taxonômica está o fato de que o terrorismo não está perfeitamente tipificado na legislação penal brasileira, ou seja, um ato terrorista acabaria sendo enquadrado e julgado por seus efeitos, não por sua motivação. Por exemplo, se um terrorista for preso por um ato que resultou na morte de algumas pessoas, ele será julgado por homicídio, e não por terrorismo. Não seria de se estranhar, portanto, o fato de que outros órgãos, além do MD e do GSI, venham a envolver-se em um possível combate ao terrorismo cibernético. Seria o caso do Ministério da Justiça, mais especificamente, do Departamento de Polícia Federal (DPF).

Cumpre ressaltar que qualquer divisão de responsabilidades baseada em taxonomias, seja a que foi estipulada neste artigo, seja outra qualquer, tão boa ou tão deficiente quanto esta, deve ser considerada como absolutamente primária e restrita ao tempo de paz e normalidade. Em caso de conflito ou ante a sua iminência, é necessário um engajamento integrado e coordenado, porém é impróprio considerar que não haverá uma série de intercorrências a desafiar os tênues limites de competência de cada ator.

Por exemplo, é óbvio que, para um país em estado de beligerância com outro, será altamente compensador produzir o caos financeiro em seu oponente. Ademais, em uma situação como essa, algum tipo de cooperação no recrutamento e no emprego de recursos humanos qualificados deverá ocorrer, principalmente porque os conflitos da atualidade tendem a ser do tipo *come as you are* (venha como estiver), mas é temerário imaginar que haverá tempo suficiente para grandes mobilizações, particular-

mente na preparação de recursos humanos de qualidades muito especiais e de capacitação demorada, como é o caso de *ciberguerreiros*.

Ademais, os ataques cibernéticos têm duas características marcantes, já comentadas, que nos impõem ação coordenada para a proteção da Nação: a extrema dificuldade de prever e controlar a extensão dos danos provocados; e a possibilidade de ocultação de sua real autoria, se este for o desejo de seu autor ou autores. Desse modo, se a autoria não está clara, tampouco estará sua motivação e, portanto, qualquer divisão de responsabilidades nela baseada.

Talvez seja por esse motivo, no concernente à divisão de tarefas na defesa cibernética norte-americana, que se optou por dividi-las não segundo a natureza das ameaças, mas em correspondência ao espaço cibernético a ser defendido ou explorado. Assim, ficou decidido que o recém-criado US Cyber Command, com *status* de comando combatente[3] e, como tal, subordinado diretamente à Autoridade de Comando Nacional[4] e ocupado em regime de rodízio entre oficiais-generais de todas as Forças, encarregar-se-á somente de proteger o domínio ".mil", enquanto o ".gov" e o ".com" serão defendidos pelo Department of Homeland Security e pelas empresas privadas, respectivamente (CYBERWAR, 2010, p. 28).

Uma particularidade relevante e que merece menção reside no fato de que, no plano puramente militar, a doutrina conjunta norte-americana não considera a guerra cibernética isolada em si mesma, mas integrante das Operações de Informação – *Information Operations*, integrada pela guerra eletrônica, operações em rede de computadores, operações psicológicas, simulação militar e segurança das operações. O foco é colocado para influenciar, destruir, corromper ou usurpar o processo decisório do oponente, ao mesmo tempo que se procura proteger o próprio processo decisório dessas mesmas ações (INFORMATION, 2006).

Nesse caso, o que se visará diretamente é afetar a capacidade de comando e controle do oponente, particularmente seu processo decisório contínuo, hoje conhecido no meio militar como ciclo de Boyd ou ciclo OODA (Observação-Orientação-Decisão-Ação), que também guarda correspondência com o ciclo *PDCA (Plan-Do-Check-Act)*, conhecido no meio empresarial.

[3] Tradução direta de *combatant command*, que, no contexto da defesa norte-americana, são comandos conjuntos organizados permanentemente. Em geral, cada comando combatente é responsável pelas operações militares correntes e futuras em determinada região do globo terrestre, mas alguns têm vinculação a um tipo específico de ação militar, como são os casos do US Cyber Command e do US Special Operations Command.

[4] National Command Authority, composta pelo presidente da República e pelo secretário de Defesa.

O desafio brasileiro no campo cibernético

Indubitavelmente, o grande desafio para o Brasil na exploração e na defesa de seus interesses no ciberespaço é o estabelecimento de adequadas políticas públicas que assegurem um mínimo de racionalização de esforços e o fomento ao desenvolvimento nacional, em um campo que se caracteriza pela forte tendência ao descontrole, à ocorrência de eventos de previsibilidade baixa e dinâmica exponencial. Tudo isso na presença de múltiplos atores, alguns desconhecidos, todos eles lutando por objetivos geralmente conflitantes entre si, pouco explícitos e, por vezes, ocultos.

Ao buscar-se o estabelecimento de uma política pública, normalmente são visualizados horizontes de planejamento mais dilatados. Entretanto, para o campo em questão, em que as incertezas sobrepujam, muito, as certezas, faz-se mister, inicialmente, dar os primeiros passos e colocar em marcha um conjunto de iniciativas que, ao mesmo tempo, procurem compensar o pequeno, porém comprovado atraso do Brasil diante de outros países mais avançados em sua exploração e, também, aumentar o nível de conhecimento mútuo e de coordenação de empreendimentos isolados ora em execução ou em concepção.

Portanto, este autor entende que, com o transcurso do tempo e com a maturação de, ao menos, parte desses empreendimentos, será possível aprimorar essas políticas e reorientar esforços, razão pela qual as sugestões que se apresentam, a seguir, estão mais orientadas a ações de curto prazo, quiçá de desencadeamento imediato, embora algumas delas dificilmente produzam efeitos imediatos. Ainda assim, a percepção de urgência parece-nos inquestionável.

Divisão de tarefas e atribuição de responsabilidades

Talvez seja inviável lograr um ordenamento rígido das atividades de exploração do ciberespaço por parte do governo brasileiro, dadas as supracitadas características desse campo de ação. Ademais, mesmo que exequível, é muito provável que tal rigidez resulte indesejável para o desenvolvimento nacional no campo em análise, uma vez que tenderia a tolher iniciativas e a restringir a liberdade de ação de cada órgão ou instituição, que, aliás, tem, no mínimo, o direito e a obrigação de defender seus ativos de informação de agressões cibernéticas, qualquer que seja sua natureza ou motivação.

Considerando, então, por um lado, o caráter quase caótico do espaço cibernético e, por outro, a relativa homogeneidade tecnológica desse ambiente, ao menos no que se refere à internet, o modelo de colaboração em rede parece ser o mais efetivo para a ampliação do conhecimento e para o intercâmbio de soluções.

Avançando um pouco mais na questão da divisão de tarefas e atribuição de responsabilidades, pode-se constatar que o estabelecimento de uma taxonomia não proporciona grande contribuição para uma possível divisão de tarefas, mesmo no âmbito defensivo. Dessa forma, é provável que, de modo semelhante ao adotado pelo governo norte-americano, produza bons resultados a atribuição de responsabilidades na proteção dos ativos de informação governamental brasileiros segundo os diversos domínios, cabendo ao MD e às Forças Armadas a proteção dos domínios ".mil.br" e "defesa.gov.br" e ao GSI dos demais ".gov.br".

Nunca é demais lembrar que cada órgão ou instituição tem o dever de, independentemente de coordenação ou subordinação, proceder à defesa de seus ativos. Isso também vale para o setor privado (".com"), especialmente, conforme já mencionado, para aqueles grupos e aquelas companhias detentores de infraestruturas críticas de interesse nacional, os quais deverão demandar atenção diferenciada e a busca de coordenação mais estreita por parte dos órgãos governamentais.

Quanto às possíveis ações ofensivas no ciberespaço, o mais indicado é que elas sejam uma prerrogativa do MD e das Forças Armadas, que, em tempo de paz, devem limitar-se a desenvolver capacidades para que, ante a inevitabilidade de algum conflito, possam ser eficazmente utilizadas para acelerar a derrota de nosso oponente e restringir os danos de seu emprego ao mínimo possível.

A atribuição de responsabilidades anteriormente proposta é perfeitamente compatível com a Lei nº 10.683, de 28 de maio de 2003, que dispõe sobre o funcionamento da Presidência da República e dos Ministérios, e dá outras providências (BRASIL, 2003). Nesse diploma legal, inciso IV, artigo 6º, fica estabelecida a responsabilidade do GSI na segurança da informação, que pode ser interpretada como a proteção do domínio do governo federal, exceto a do segmento militar, que, naturalmente, está ao encargo do MD e das Forças Armadas, por tratar-se de assunto da Defesa Nacional, portanto, afeto ao MD, conforme estipulado no artigo 27 da mencionada lei.

No concernente ao segmento militar, releva mencionar a importância atribuída ao campo cibernético pela Estratégia Nacional de Defesa (BRASIL, 2008), que o considera um dos setores estratégicos do País, com o nuclear e o espacial.

Em 2009, o ministro da Defesa, por meio da Diretriz Ministerial nº 14, decidiu designar uma força responsável para cada setor estratégico, com o propósito de coordenar as ações em cada um dos mencionados setores (BRASIL, 2009). Assim, coube à Marinha o setor nuclear, ao Exército o cibernético e à Aeronáutica o espacial. No momento, cada Força responsável está consolidando a definição da abrangência do setor e os objetivos setoriais identificados, bem como traçando as estratégias setoriais e avaliando a adequabilidade das estruturas já existentes.

Em qualquer um dos setores estratégicos, a coordenação dos trabalhos exigirá, do responsável designado, grande dedicação, capacidade de articulação e certa dose de desprendimento, a fim de permitir que sejam contemplados os interesses e as necessidades de todas as Forças e da Administração Central do MD. No setor cibernético, esses atributos serão ainda mais exigidos, pois inexiste uma proeminência determinante da Força responsável perante as demais, diferentemente do que ocorre nos setores nuclear e espacial. Ademais, as três Forças, cumprindo o que delas sempre se espera, foram ágeis e zelosas na adoção de um sem-número de medidas para a proteção de suas informações, requerendo-se, portanto, inteligência e flexibilidade para o máximo aproveitamento possível dos investimentos já realizados e das estruturas físicas e organizacionais já erigidas.

É, de qualquer forma, bastante alvissareiro o fato de que, na área da Defesa Nacional, passos importantes foram dados no robustecimento da proteção dos sensíveis ativos de informação sob sua guarda e na busca do insistentemente recomendado intercâmbio de conhecimento e tecnologia.

Marco legal

Uma simples reflexão sobre as questões legais já abordadas neste artigo não deixa margem à dúvida de que não deveria haver, pelo menos no presente, um interesse maior por parte do Brasil em construir um rígido marco regulatório internacional para as ações governamentais no espaço cibernético, principalmente porque a tendência natural seria a consolidação ou mesmo a ampliação das vantagens alcançadas pelos países situados mais à vanguarda neste campo de ação sobre os demais. Conforme já

mencionado, o Brasil, não obstante o grande esforço para a acumulação de conhecimento nesta área, está mais para o segundo grupo do que para o primeiro.

Ademais, dadas as grandes dificuldades para o efetivo estabelecimento de responsabilidades por ações perpetradas no ciberespaço, seria muito simples para um país agressor participar e ser signatário de diversos acordos e mecanismos multinacionais orientados à imposição de limitações ao uso deste espaço, ao mesmo tempo em que realiza seus ataques por intermédio de "renegados" e refuta sua autoria.

Não se pode olvidar, tampouco, que, ante a conformação de um estado de beligerância entre o Brasil e outro país, nenhum acordo internacional nos protegerá das ameaças cibernéticas produzidas por nosso oponente, pois, como vimos, são recursos que, dependendo da eficácia com que são utilizados, abreviam o conflito e permitem o ataque a alvos que, se fossem engajados por meio de armas tradicionais, provavelmente produziriam ainda mais mortes e destruição. Que tribunal internacional vai condenar esses ataques cibernéticos? Mais ainda: mesmo se condenasse, de que isso adiantaria se não impedisse, como não deve impedir, que soframos as consequências dessas agressões?

Assim, é recomendável extrema cautela para que não haja precipitação em aderir-se a marcos regulatórios que visem ao estabelecimento de limitações quanto à exploração e ao uso do ciberespaço, porquanto, à luz do atual estágio de conhecimento acumulado, eles seriam, provavelmente, incipientes e prematuros.

Isso não quer dizer que o Brasil não deva participar de todas as discussões sobre esse assunto, em nível internacional. Ao contrário: é fundamental que o País esteja presente nos foros em que a questão cibernética seja tratada, não apenas na condição de observador, mas como ator protagonista. Mais à frente, quando se atingir um amadurecimento tal que permita a conformação de um marco regulatório consistente e, sobretudo, aplicável, teremos alcançado uma posição de destaque e de conhecimento que não possuímos hoje.

Este autor atreve-se a afirmar que a atual dificuldade em se estabelecer um rígido marco legal no uso do ciberespaço não é propriamente danosa ao País. Devemos, pois, evitar, a todo custo, a assunção de compromissos bilaterais ou multilaterais que possam tolher as pesquisas e as iniciativas ora em curso, as quais, futuramente, poderão fazer muita falta à defesa e, *lato sensu*, da Nação.

Por outro lado, no campo do direito interno, é natural que se deva buscar um contínuo fortalecimento do arcabouço jurídico que respalde o firme combate ao crime cibernético. Nesse caso, já existe toda uma institucionalização a definir direitos e obrigações dos cidadãos e coletividades, bem como uma série de instrumentos apropriados à sua imposição. Além disso, na maioria dos crimes cibernéticos do tipo fraude ou apropriação indébita, sua autoria acaba sendo, cedo ou tarde, determinada. Também há de se considerar que é interesse de todo Estado minimamente organizado, a ponto de merecer esta denominação, criar um ambiente de segurança jurídico-financeira para que sua vida econômica possa prosperar de forma pujante.

Estímulo à Pesquisa & Desenvolvimento

Preliminarmente, os dois "celeiros" naturais para o desenvolvimento de conhecimento e tecnologia no campo cibernético, bem como para a identificação e o aperfeiçoamento de talentos nesse mister seriam as empresas e as universidades. No caso brasileiro, até onde alcança o conhecimento deste autor, não há nenhuma empresa que tenha alcançado papel proeminente nesse setor, ao menos a ponto de rivalizar com as grandes empresas estrangeiras que têm explorado comercialmente essa atividade, particularmente no segmento de proteção (antivírus, *firewalls*, entre outros). Isso não quer dizer que não possam existir no futuro. À guisa de exemplo, uma empresa relativamente nova que vem disputando espaço com as mais tradicionais do setor é de origem espanhola, país cuja capacidade na área da tecnologia da informação não era notória até pouco tempo atrás.

Isso posto, a universidade alinha-se como grande opção para a criação de polos de pesquisa e desenvolvimento nesse setor, proporcionando força de trabalho para o setor privado e, principalmente, para os órgãos governamentais que pretendam atuar no campo cibernético.

Para tanto, será de todo conveniente que esses órgãos, sejam eles da área da Defesa, de segurança institucional ou pública, fomentem, mediante diversas formas de atuação, a criação desses polos nas universidades. Esses lugares poderão conformar-se como ambientes apropriados para o desenvolvimento de tecnologias e para o surgimento de futuros *ciberguerreiros*. Desses, uma pequena parte poderá ser rotineira e gradualmente incorporada ao serviço público. A esse pessoal seria oferecida uma carreira de Estado e sua principal atribuição seria conduzir a exploração do ciberespaço e a defesa dos

ativos de informação de interesse governamental em situação de normalidade. Ante a eventualidade de ameaça potencial, particularmente em situação de guerra cibernética, poderia ser empreendida uma mobilização em grande escala dos recursos humanos disponíveis nesses polos.

Recorda-se, entretanto, que a mobilização de *hackers*, se for o caso, implica a assunção de riscos e a adoção de medidas de contrainteligência e, mais especificamente, de segurança orgânica (NUNES, 2010, p. 29).

Carreira de Estado e retenção de talentos

A preocupação com a retenção de talentos, qualquer que seja o campo de atividade e o segmento a explorá-lo, é invariavelmente pertinente. Em se tratando do campo cibernético existente no segmento governamental, tal preocupação é ainda mais justificada. O segmento empresarial é bastante atrativo, particularmente nas empresas estrangeiras, que drenam uma parte considerável dos brasileiros de alta competência nesse campo.

Essa é uma, entre muitas outras, das manifestações do fenômeno *brain drain*, magistralmente descrito por Merle (1981) em sua obra. Melhores salários, qualidade de vida, condições de trabalho e pesquisa são os principais fatores que explicam a migração de pessoas de qualificação diferenciada dos países em desenvolvimento para os efetivamente desenvolvidos.

Cabe a ressalva de que, mais recentemente, tem-se observado certa inversão nesses fluxos. Nos últimos anos, tem ocorrido a chegada de estrangeiros buscando colocação no mercado nacional, tanto nas posições mais modestas quanto naquelas de maior nível, e o que tem chamado mais a atenção é o influxo de pessoal mais qualificado. Esse fenômeno se deve, provavelmente, às crises econômicas de considerável porte que têm atingido as principais economias do mundo, particularmente as europeias. Essas crises tiveram efeitos muito mais discretos no Brasil, que, embora não ostente o crescimento pujante de China, Índia e mais algumas outras economias ascendentes, tem podido manter uma taxa de crescimento razoável, sem a ocorrência de grandes sobressaltos. A indústria do petróleo e toda a cadeia produtiva em seu entorno também têm contribuído sobremaneira para atrair estrangeiros.

O impacto dessa inversão é mais perceptível nas carreiras de caráter mais industrial do que cibernético (engenharias civil, mecânica, elétrica, produção e outras), mas, de qualquer forma, não contribui para facilitar o trabalho de captação de talentos do campo cibernético para o serviço público. Ao contrário. De modo geral, sempre que a economia se encontra aquecida, a atratividade do serviço público, tanto militar como civil, acaba sendo reduzida, em todos os campos de atividades.

Compensar esse déficit de atratividade não é tarefa simples, mas, no caso dos quadros governamentais, pode-se afirmar que, também nos últimos anos, as condições de trabalho têm-se tornado mais positivas. Remunerações razoáveis, estabilidade e, em muitos casos, expectativas de crescimento profissional e salarial mediante a existência de uma carreira institucionalizada são atributos que, devidamente explorados, podem atrair jovens de boa capacitação para a ocupação de cargos na estrutura do governo federal, tanto na área militar quanto na civil.

Cabe-nos, então, criar esses cargos e fazer que aqueles talentos gerados nos polos universitários se interessem por eles. Não é fácil criar novos cargos, civis ou militares, na administração pública federal, mas não é impossível. Ademais, ante a improvável impossibilidade absoluta de criação de, digamos, novas matrículas, poder-se-ia, paulatina e limitadamente, substituir algumas funções já existentes por novas no campo da exploração do espaço cibernético. Cabe a importante ressalva de que a natureza dessa atividade não requer grandes massas de mão de obra, mas tão somente alguns poucos especialistas que possam desenvolver trabalhos e pesquisas de forma sistêmica e rotineira e recorrer, na iminência de grande conflito, àqueles repositórios de pessoal qualificado existentes nas universidades.

Uma vez captados esses talentos para o serviço público, deve-se buscar, incessantemente, mantê-los estimulados para a continuação de seus trabalhos e de sua qualificação. Isso implica a existência de bons laboratórios, de equipamentos no estado da arte, de cursos, a participação em eventos da área, outras oportunidades de aprimoramento e, sobretudo, a sua permanência na atividade para a qual foram recrutados. Esta permanência parece ser uma observação tão óbvia, estéril e inócua que não mereceria sequer ser apresentada, mas nunca é demais recordar que, no serviço público, e mesmo no segmento empresarial, existe forte tendência para, no curso das carreiras, "empurrar" o funcionário para atividades cada vez mais administrativas e menos técnicas. No caso de um *ciberguerreiro*, isso pode constituir um desestímulo fatal.

Assim, a manutenção desses talentos o máximo possível na atividade técnica propriamente dita é fundamental e transforma-se em considerável desafio. Algumas empresas de porte na área de tecnologia da informação têm tentado criar e sustentar carreiras técnicas, nas quais alguns funcionários mais talentosos têm prolongado sua permanência no campo tecnológico propriamente dito e com acesso aos mesmos incrementos salariais daqueles que migram mais cedo para a média e a alta gerência.

Nas carreiras militares, tal artifício é de difícil implementação, mas não nas carreiras civis governamentais. Por outro lado, na área militar, já existem, nas três Forças Armadas, os diversos corpos e quadros de engenheiros e técnicos, que tornam possível incorporar pessoal para trabalhar na exploração do espaço cibernético. Existem, inclusive, engenheiros de computação e de telecomunicações já disponíveis para emprego imediato. Como foi dito anteriormente, é uma questão de prioridade e, indiscutivelmente, as Forças já estão fazendo a sua parte.

Conclusão

Após ter discorrido sobre os principais aspectos que compõem o instigante tema deste artigo, será, enfim, apresentada uma breve síntese conclusiva.

Conforme percebido, o Brasil, decerto, não está incluído entre os países de maior desenvolvimento no campo cibernético. Não obstante, é perfeitamente possível vencer esse hiato hoje existente, mediante grande determinação e a execução de um conjunto de ações perfeitamente factíveis, algumas delas apontadas neste texto.

Se por um lado devemos ter pressa na execução dessas medidas de edificação de nossas capacidades cibernéticas, por outro devemos ser bastante cautelosos e moderados na busca do desenvolvimento de um marco legal internacional de exploração do espaço cibernético. É de se ressaltar, uma vez mais, que tal desenvolvimento, mais do que nos proteger, tenderia a nos desprover de recursos e oportunidades que poderão demonstrar seu valor ante a ocorrência de contencioso com outra nação que, desafortunadamente, deságue em um conflito armado.

Conforme defendido, isso não significa que o País deva afastar-se dos foros internacionais de discussão do tema, mas deles participar progressivamente fortalecido para que seja um ator de peso a influenciar o curso das discussões e as eventuais decisões tomadas, não apenas um mero espectador privilegiado.

Relembre-se, também, de que, no âmbito nacional, a postura deve ser outra e tender ao fortalecimento do marco regulatório, a fim de contribuir para o combate ao crime cibernético.

Como se viu, a comparação da guerra cibernética com a guerra eletrônica é bastante elucidativa e nos alerta para duas principais reflexões:

- Não podemos privar o País da possibilidade de empregar ações cibernéticas ofensivas que abreviem os conflitos armados e, potencialmente, reduzam a ocorrência de perdas humanas, em relação não apenas à nossa população, mas também à população de nosso oponente.

- Diante da ocorrência de conflito armado e, uma vez tendo-se optado por explorar ofensiva e defensivamente o ciberespaço, o que, aliás, tende cada vez mais a ser uma imposição e não uma opção, a combinação das ações cibernéticas com os ataques convencionais, realizando-se aquelas no limiar do desencadeamento destes, parece ser a forma mais eficaz de alcançar uma vitória rápida e decisiva.

Quanto ao estabelecimento de uma taxonomia, tal como a que foi apresentada – guerra cibernética, terrorismo cibernético, crime cibernético e, em plano inferior, o ativismo cibernético –, a sua utilidade é limitada, já que, em geral, as armas são as mesmas e as motivações em que ela se baseia somente serão identificadas se assim desejar nosso oponente.

Por outro lado, ela nos chama a atenção para a importância de grande intercâmbio de conhecimentos no campo cibernético. Governo, em seus setores militar e civil, empresas e universidades devem promover encontros e trabalhos conjuntos que potencializem essa troca de informações e de experiências, apontando-se, assim, para um modelo colaborativo em rede.

É de se relembrar, contudo, que cada grupo, órgão ou empresa deve buscar, incessante e obstinadamente, o robustecimento de sua própria capacidade de defesa cibernética. Não se pode esperar que uma única instituição possa responder pelas necessidades cibernéticas de todas as outras, mormente

porque, como se pode constatar, o crescimento das ameaças das ameaças é exponencial e, mesmo havendo considerável coincidência nos tipos mais comuns de ameaças, as estruturas e os ativos de informação a defender são muito variados.

Cada ator nacional deve fazer a sua parte e isso, certamente, inclui empresas e prestadoras de serviços públicos, principalmente as que lidam com grandes volumes de dados sobre ativos financeiros, como os bancos e as bolsas, as que ostentam grande peso no conjunto das infraestruturas críticas nacionais, como na produção e transmissão de todas as formas de energia, de telecomunicações, as infovias, as indústrias estratégicas e assim por diante.

Quanto a uma possível divisão de tarefas, especialmente quanto ao uso defensivo do espaço cibernético, parece ser desejável que haja uma atribuição primária por domínios, cabendo ao MD e às Forças Armadas a proteção dos domínios ".mil.br" e "defesa.gov.br"; ao GSI os demais ".gov.br"; e a cada órgão, empresa ou instituição o seu próprio domínio. Tudo isso sem olvidar-se da propugnada colaboração em rede.

No concernente à exploração ofensiva do ciberespaço, a sugestão natural é que ela seja prerrogativa do MD e das Forças Armadas, que devem desenvolver as capacidades necessárias para tal desde o tempo de paz, limitando-se a empregar tais recursos somente em situação de conflito. Não parece ser aceitável admitir a participação de empresas ou de outros órgãos governamentais nessa forma de exploração do espaço cibernético, a não ser ante o envolvimento do Brasil em conflito de maiores proporções e a decorrente necessidade de mobilização em larga escala.

Finalmente, qualquer que seja a divisão de tarefas e responsabilidades a ser adotada, cada instituição tem a prerrogativa e, mais ainda, o dever de investir tempo, dinheiro, pessoal e atenção gerencial à defesa de seus bens infoativos de informação. Esse dever se justifica não apenas pela defesa de seus interesses específicos, mas também pela garantia dos interesses nacionais no espaço cibernético, e, à luz da ponderável gama de conhecimentos já disponíveis, pode-se afirmar que as ameaças são reais e o perigo que elas representam, imediato, assim como são também reais e imediatas as oportunidades que a exploração positiva do espaço cibernético nos oferece, sempre no único e exclusivo interesse da Nação.

Referências bibliográficas

ADEE, S. *The hunt for the kill switch*. IEEE Spectrum, 2008. Disponível em: <http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch>. Acesso em: 3 dez. 2010.

ALVAREZ, T. *Guerra e defesa cibernética*. Rio de Janeiro: Blog SegInfo, 2010. Disponível em: <http://www.seginfo.com.br/guerra-e-defesa-cibernetica>. Acesso em: 22 nov. 2010.

BRASIL. Decreto nº 6.703, de 18 de dezembro de 2008. Aprova a Estratégia Nacional de Defesa, e dá outras providências. *Diário Oficial da União*, Poder Executivo, Brasília, DF, 19 dez. 2008.

_____. 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 União*, Congresso Nacional, Brasília, DF, 29 mai. 2003.

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

CERT Statistics. *Software Engineering Institute*, 2009. Disponível em: <http://www.cert.org/stats>. Acesso em: 5 dez. 2010.

COMMUNICATIONS Assistance for Law Enforcement Act. *Wikipedia*, 2011. Disponível em: <http://en.wikipedia.org/wiki/Communications_Assistance_for_Law_Enforcement_Act>. Acesso em: 5 nov. 2010.

CYBERWAR – It is time for countries to start talking about arms control on the internet. *The Economist.* Londres, 3 jul. 2010, ed. 3 a 9 jul., p. 11-12.

FULGHUM, D. A.; BARRIE, D. *Israel used electronic attack in air strike against Syrian mystery target,* Aviation Week, 2007. Disponível em: <http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/aw100807p2.xml&headline=Israel%20used%20electronic%20attack%20in%20air%20strike%20against%20Syrian%20mystery%20target>. Acesso em: 3 dez. 2010.

INFORMATION Operations. *Joint Staff*, 2006. Disponível em: <http://www.fas.org/irp/doddir/dod/jp3_13.pdf>. Acesso em: 25 nov. 2010.

KILROY JR., R. J. The U.S. Military Response to Cyber Warfare. In: COLARIK, A. M.; JANCZEWSKI, L. J. *Cyber Warfare and Cyber Terrorism*. Nova Iorque, EUA: Information Science Reference, 2008. Cap. 51.

KNAPP, K. J.; BOULTON W. R. Ten Information Warfare Trends. In: COLARIK, A. M.; JANCZEWSKI, L. J. *Cyber warfare and cyber terrorism*. Nova Iorque, EUA: Information Science Reference, 2008. Cap. 3.

LEI DE METCALFE. *Wikipedia*, 2011. Disponível em: <http://pt.wikipedia.org/wiki/Lei_de_Metcalfe>. Acesso em: 5 nov. 2010.

MERLE, M. *Sociologia das relações internacionais*. Brasília: Editora UnB, 1981. 384p.

MESSMER E. *Kosovo cyber-war intensifies*. Network World Fusion, 1999. Disponível em: <http://www.networkworld.com/news/1999/0512kosovo.html>. Acesso em: 5 nov. 2010.

NUGENT, J. H.; RAISINGHANI, M. Bits and bytes vs Bullets and bombs: a new form of warfare. In: COLARIK, A. M.; JANCZEWSKI, L. J. *Cyber warfare and cyber terrorism*. Nova Iorque, EUA: Information Science Reference, 2008. Cap. 4.

NUNES, L. A. R. *Guerra cibernética*: está a MB preparada para enfrentá-la? Rio de Janeiro, 2010. 98f. Trabalho de Conclusão de Curso (Curso de Política e Estratégia Marítimas, Escola de Guerra Naval, 2010).

OPERATION Orchard. *Wikipedia,* 2011. Disponível em: <http://en.wikipedia.org/wiki/Operation_Orchard>. Acesso em: 3 nov. 2010.

WAR in the fifth domain – Are the mouse and keyboard the new weapons of conflict? *The Economist*. Londres, 3 Jul. 2010, ed. 3 a 9 jul., p. 25-28.

WEBB, D. C. ECHELON and the NSA. In: COLARIK, A. M.; JANCZEWSKI, L. J. *Cyber warfare and cyber terrorism.* Nova Iorque, EUA: Information Science Reference, 2008. Cap. 53.

WILSON, C. *Information operation, electronic warfare, and cyberwar*: capabilities and related policy issues. Congressional Research Service, 2007. Disponível em: <http://www.fas.org/sgp/crs/natsec/RL31787.pdf>. Acesso em: 3 dez. 2010.

A TENDÊNCIA MUNDIAL PARA A DEFESA CIBERNÉTICA

*José Eduardo Portella Almeida**

Resumo

As nações estão percebendo a velocidade assustadora com que a informática está preenchendo espaços no cotidiano da humanidade.

Em 2005, a Federação Russa, preocupada com o uso malicioso de ferramentas informacionais, propôs à Organização das Nações Unidas (ONU) a formação de um grupo de peritos governamentais para considerar a regulamentação de emprego de armas cibernéticas. A preocupação russa relacionava-se com a possibilidade de alguns efeitos produzidos por essas armas serem catastróficos, chegando aos de armas de destruição em massa.

Durante as reuniões, a delegação americana não aceitou nenhuma restrição ou regulamentação ao emprego de armas cibernéticas por nações em conflito ou em guerra.

Em 2010, em uma nova rodada de reuniões do mesmo grupo de trabalho, os representantes de todos os países concordaram em assinar uma resolução com uma série de recomendações aos países, sobre a ameaça provocada pelo uso de armas cibernéticas.

* Coronel Aviador da reserva da Força Aérea, atualmente trabalha como consultor independente. Na sua carreira militar, concluiu os cursos de: Formação de Oficiais Aviadores, Aperfeiçoamento de Oficiais, superior de Comando e Estado-Maior, promoção a oficial general em Portugal e Administração Estratégica de Sistemas de Informação pela Fundação Getúlio Vargas. Desempenhou as seguintes funções: comandante do 1º Grupo de Defesa Antiaérea, chefe do Centro de Guerra Eletrônica do Comando Geral de Operações Aéreas e vice-chefe do Centro de Comando e Controle de Operações Aéreas e chefe interino do Estado-Maior Combinado do Comando de Defesa Aeroespacial Brasileiro.

Várias ocorrências, provavelmente, provocaram a mudança de postura dos Estados Unidos da América (EUA) em relação à ameaça cibernética.

Em função disso, os EUA e outros países desenvolvidos criaram uma série de instituições nacionais e privadas que podem servir de exemplo para o planejamento estratégico brasileiro, no campo da Defesa Cibernética.

Palavras-chave: guerra cibernética, ataque cibernético, Defesa Cibernética.

Introdução

O objetivo deste trabalho é apresentar aspectos relevantes de uma experiência vivida em um grupo de trabalho que desenvolveu suas atividades na sede da ONU, durante a última reunião do Grupo de Peritos Governamentais em Desenvolvimento no Campo da Informação e Telecomunicações no Contexto da Segurança Nacional, em 2005, a fim de estabelecer subsídios para a indicação de algumas boas práticas que estão sendo desenvolvidas por governos estrangeiros, na área da Defesa Cibernética.

O assunto foi abordado sob a premissa de que as nações mais desenvolvidas e detentoras de capacidades tecnológicas diferenciadas não se submetem aos apelos da comunidade mundial, a não ser que se sintam ameaçadas. A experiência relatada ilustra bem esse fato diante de uma ameaça assimétrica que, se bem conduzida, pode levar pequenos grupos ou mesmo nações com poucos recursos a perpetrarem ações de consequências catastróficas.

Há vários trabalhos que comumente abordam o mesmo tema, exceto o exemplo da experiência vivida na ONU, que é singular por razões óbvias. Grande parte dessas obras está disposta na internet e um bom *site* de busca poderá trazê-las ao interessado, desde que seja de seu conhecimento a correta nomenclatura dos termos informáticos nos idiomas que deseja procurar.

O tema foi indicado por interesse da Secretaria de Assuntos Estratégicos e, devido ao tempo destinado à consecução do trabalho, a pesquisa foi realizada em documentos de propriedade do autor e em buscas na internet. Foi utilizado o método dedutivo, com recurso à pesquisa documental.

O resultado final esperado são indicações de boas iniciativas tomadas em países que estão mais afetos à Defesa Cibernética, para que possam servir de exemplo para os elaboradores de planejamento de longo prazo do Estado brasileiro.

Reunião na ONU – 2005

Em 2005, o Brasil foi convidado a participar de um grupo de trabalho na ONU, com o objetivo de estudar conceitos internacionais relevantes, voltados ao fortalecimento da segurança global dos sistemas de informações e de telecomunicações. Esse foi o motivo para se reunirem peritos de 15 países, em três reuniões (a primeira e a terceira em Nova Iorque e a segunda em Genebra), os quais, mais sinteticamente, discutiram acerca do perigo representado pela ameaça cibernética.

Preparando-se para a última reunião, o Ministério da Defesa (MD) orientou que fosse feita a análise de uma proposta enviada pelo grupo de peritos da Rússia, cujo chefe da comissão havia sido eleito, na primeira reunião, condutor dos trabalhos do grupo.

Na verdade, o grupo de trabalho na ONU foi formado por solicitação da Rússia, que alegava que as ações cibernéticas nas guerras deveriam ser reguladas por uma norma própria, pois o uso de armas cibernéticas, se não devidamente controlado, poderia ter consequências muito graves às nações e regiões mais despreparadas e mais dependentes de sistemas de controle.

O objetivo de analisar a proposta russa era, inicialmente, compor um parecer sobre o teor dos argumentos citados pelos russos, para assessorar um possível alinhamento do Brasil com a proposta. Com a aprovação do MD, o parecer seria enviado ao Ministério das Relações Exteriores (MRE), para se tornar a contribuição do Brasil aos trabalhos da última reunião.

Foram analisados muitos documentos para compor a assessoria, tais como: *Contribuição Russa, Contribuição da França, Contribuição da Alemanha, Contribuição dos Estados Unidos, Contribuição da China, Contribuição da Venezuela, Contribuição do México* e um documento russo muito interessante, semelhante a um manual, que abordava, de forma doutrinária, a guerra cibernética: *Desafios da Informação para a Segurança Nacional e Internacional – 2001*.

A *Contribuição Russa* era, por larga margem, a mais completa de todos e trazia conceitos muito interessantes, que foram sumarizados, para que fosse possível constituir a assessoria necessária ao MD. Além disso, o "manual" explicava como se poderia utilizar o potencial das armas cibernéticas na guerra e dividia em fases esse emprego, como coleta de informação, defesa e ataque.

Na introdução, vários conceitos eram citados e alguns trouxeram surpresa pelo fato de, à época, não se estar lidando com aquele tipo de pensamento. Uma das citações relacionava os efeitos do uso de armas cibernéticas aos do uso de armas de destruição em massa. Parecia um tanto catastrófico fazer este tipo de comparação e buscaram-se explicações que pudessem ilustrar melhor essa afirmação.

No documento que abordava de forma doutrinária a guerra cibernética, havia um exemplo que melhorava a compreensão da citação catastrófica da introdução. Dizia que, caso um *hacker* invadisse o computador de controle de uma estação de distribuição de energia elétrica, na Sibéria, durante o período do inverno, e desligasse o fornecimento de energia durante a noite, o efeito poderia ser comparável ao do emprego de uma arma de destruição em massa.

Ainda durante as citações iniciais do documento, havia muitas referências a "armas cibernéticas" que não se sabia exatamente como classificá-las e foram simplificadas como a utilização de vírus e *worms* que invadem e afetam o funcionamento dos computadores e, naturalmente, dos sistemas por eles controlados ou assistidos.

Outro aspecto interessante da *Contribuição Russa* era a organização das ideias e a sequência em que elas foram apresentadas. Percebe-se uma ordem de apresentação orientadora, quase educativa. Em sequência, o documento aborda o que deve ser protegido, as principais ameaças, as fontes dessas ameaças, princípios que devem ser seguidos para a segurança das informações e, finalmente, propostas de ações.

Os russos demonstraram com suas contribuições que haviam refletido bastante sobre o contexto da guerra cibernética, mas deixaram escapar o reconhecimento de que, tecnicamente, não dominavam o assunto tanto quanto seus potenciais adversários, pois ofereceram sugestões que uma potência militar nunca colocaria em pauta para tratamento das Nações Unidas, se tivesse hegemonia naquela área de atividade.

A *Contribuição do Brasil*, resultante de toda essa análise, foi cautelosa e equilibrada e, depois de aprovada pelo MRE, foi incorporada ao processo estabelecido pela criação do grupo de trabalho.

A *Contribuição Russa* e o documento *Desafios da Informação para a Segurança Nacional e Internacional – 2001,* também russo, foram as fontes que melhor prepararam a equipe brasileira para as discussões em Nova Iorque. Entretanto, a suspeita de que os russos estavam querendo, além de estabelecer uma ordem mundial para a ameaça cibernética, proteger-se de adversários mais poderosos foi confirmada no decorrer das reuniões, como será visto a seguir.

A reunião ocorreu em duas semanas de julho de 2005, num típico verão de Nova Iorque, com muito calor e dias longos.

O grupo reunia-se todos os dias, desde as 8h até as 18h, numa sala do subsolo do prédio principal da ONU. Os países que participaram do grupo de trabalho foram: Bielorrússia, Brasil, China, França, Alemanha, Índia, Jordânia, Malásia, Mali, México, Coreia do Sul, Rússia, África do Sul, Reino Unido e Estado Unidos da América.

A maior comitiva era a da Rússia e várias possuíam apenas um único representante. Havia tradução simultânea para as línguas oficiais da ONU e as comitivas eram dispostas por ordem alfabética num retângulo de mesas, exceto a da Rússia, que tomava assento na cabeceira mais próxima da entrada da sala, por ter sido o seu delegado escolhido como *chairman*[1] do grupo de trabalho.

As reuniões foram sempre orientadas pelo *chairman* e visaram à busca de um texto que representasse o consenso dos países em relação a "desenvolvimentos no campo da informação e telecomunicações no contexto da segurança nacional", que, como já dito anteriormente, resumiam-se ao risco da ameaça cibernética em atos de terrorismo, conflitos e guerras. Vale dizer que esse grupo de peritos já se reunia seguidamente, desde 1999, sempre por iniciativa da Rússia.

Inicialmente, ficou clara a pouca percepção e, como consequência, a pouca participação de alguns representantes. Mas havia grandes discussões e muitos pontos importantes eram colocados em pauta, os

[1] Pessoa que preside um comitê ou reunião.

quais, por vezes, surpreendiam pelo ineditismo de suas abordagens e por representarem traços culturais muito distantes da nossa realidade ocidental do novo mundo.

Uma das mais marcantes dessas "viagens" foi uma acalorada discussão entre os representantes da China e do Reino Unido, em que o chinês citava a liberdade de distribuição da internet como origem de um problema social em seu país. O inglês tratou o assunto com pouco caso e o relacionou ao regime político adotado na China, voltando-se aos outros participantes com ar de deboche. O representante chinês fez uma longa pausa, parecendo procurar entender exatamente o que o inglês havia dito, por meio da tradução simultânea, e subiu o tom de sua voz na resposta. Disse, em resumo, que a internet forçava a entrada da cultura ocidental nas famílias chinesas e que isso não era aceitável, alegando que a cultura chinesa tinha origem há milhares de anos e não poderia ser modificada por sistema de comunicação intruso. Depois de dizer isso aos gritos, o chinês calou-se, e restou ao inglês pedir-lhe desculpas pela forma descortês que tratou o assunto.

Aos poucos, percebeu-se a formação de subgrupos com opiniões alinhadas entre as comitivas. A Rússia, o Brasil, a China, a Malásia e a Bielorrússia alinharam-se pela opinião de que a ameaça cibernética poderia gerar efeitos catastróficos em guerras e deveria ser tratada com a atenção devida pela ONU, em especial pelo Conselho de Segurança. A França, a Alemanha, a Coreia do Sul, a Índia e a África do Sul não concordaram com a inserção do termo "catastrófico", mas entenderam que o assunto deveria ser tratado com atenção pela ONU e aceitaram alguma regulamentação acerca do tema. Esse grupo influenciou as representações que demonstravam menos conhecimento sobre a matéria.

Um terceiro e último grupo, formado por EUA, Reino Unido e, inicialmente, México, considerou que nenhuma regulamentação deveria ser promulgada e os acordos internacionais que regiam os conflitos armados e guerras eram suficientemente abrangentes para regular o emprego de armas cibernéticas.

A partir dessas três opiniões, o grupo como um todo buscou redigir um texto que expressasse a opinião de todos os presentes, o que, naturalmente, pendeu para a eliminação das opiniões mais extremas. O grupo do qual o Brasil participava passou a aceitar termos menos fortes para os efeitos que seriam gerados pelo emprego de armas cibernéticas em conflitos armados. O grupo conduzido pela França e Alemanha aceitou algumas ponderações do grupo do Brasil e da Rússia e incrementou algumas de suas recomendações para serem abordadas pela Assembleia Geral, mas ainda recusou o fato de que o assunto deveria ser levado ao Conselho de Segurança. A delegação do México aceitou os termos que

estavam sedo discutidos pela maioria e começou a apoiar a hipótese de se alarmarem os países ao se tratar dessa questão na Assembleia Geral.

Os delegados dos EUA e do Reino Unido, sentados lado a lado, conversavam paralelamente às discussões e tinham sempre a mesma opinião: não havia nada a ser melhorado nos dispositivos reguladores dos conflitos, por influência da entrada, nos teatros de operações, das armas cibernéticas.

Sendo relatado resumidamente, pode parecer que o trabalho foi-se resolvendo com facilidade, mas cada linha de cada tentativa de se compor um texto comum demorava, às vezes, horas ou dias para ser construída. As opiniões eram muitas e diversas e até mesmo a interpretação do que estava sendo escrito era trabalhada para ter o sentido exato do que o grupo queria expressar. Depois das apresentações iniciais de opiniões e das divagações comentadas anteriormente, que levaram mais da metade da primeira semana, o grupo passou a trabalhar com afinco em um texto que representasse a opinião de todos. O primeiro deste tipo de texto foi proposto pelo representante da Malásia, um general do Exército, que o apresentou na segunda-feira da segunda semana.

O representante do Reino Unido participava dos debates, mas, quando contrariado, reagia com deboche. Todas as vezes que um texto era apresentado, antes de emitir a sua opinião, ele falava em voz baixa com a representante dos EUA e, via de regra, discordava. A representante dos EUA praticamente não participava. Não emitia um ruído sequer durante as discussões. Lia, tomava notas e raramente olhava diretamente para algum dos participantes, a não ser para o do Reino Unido.

Em conversas informais entre os representantes das delegações russa e brasileira, que ficaram todo o tempo muito próximas em suas opiniões, procurou-se entender o motivo do comportamento da representante dos EUA, e algumas coisas interessantes foram comentadas. Os EUA, segundo os russos, tinham um conhecimento enorme sobre a capacidade de se protegerem de infiltrações e de ataques cibernéticos ou, pelo menos, achavam que possuíam. A regulamentação das ações cibernéticas em guerra ou em conflito poderia restringir sua liberdade de agir para enfraquecer e mesmo para atacar o adversário com armas cibernéticas. Os representantes dos EUA e do Reino Unido concordavam com todo tipo de proposta de regulamentação sobre crime ou terrorismo cibernético, quer dizer, sobre a ação deliberada de indivíduos contra sistemas públicos ou privados que viessem a prejudicar o funcionamento ou expor a segurança dos mesmos sistemas, auferindo vantagens ou não por essas ações.

Mas, quando se falava em conflito entre nações, não aceitavam nenhuma sugestão acerca de regulamentação.

Na quarta-feira da segunda semana, havia um texto considerado aceitável por quase todas as delegações. Apenas EUA e Reino Unido discordavam. Com algum trabalho mais próximo e contando com a curiosidade do inglês, conseguiu-se convencê-lo a aceitar o texto com pequenas ressalvas sugeridas por ele mesmo. A americana nada comentou até o fim do dia.

Na quinta-feira, todos se sentaram certos de que o árduo trabalho tinha resultado em um texto de aceitação comum. A representante dos EUA, nesse dia, estava fazendo as unhas, enquanto os últimos ajustes eram feitos no texto final, que foi lido para todos. Próximo ao horário do almoço, ela tomou a palavra e disse:

> Estamos perdendo tempo. Acho que vocês ainda não entenderam o ponto de vista dos EUA. Os EUA não vão concordar com nenhum texto que contenha alguma citação à necessidade de qualquer comissão da ONU ouvir, analisar ou regulamentar algo que diga respeito à ameaça cibernética no conflito entre nações. Estamos aqui há duas semanas e ainda não tivemos tempo de visitar os *shoppings*. Eu proponho que encerremos agora e tenhamos tempo à tarde para irmos às compras. Amanhã, voltamos aqui e assinamos um *report* de uma folha, informando que não chegamos a um consenso.

Todos ficaram calados por um tempo, olhando para ela, que voltou a fazer as unhas. O *chairman* encerrou a reunião e, no dia seguinte, todos os delegados assinaram um *report* dizendo que, "devido à complexidade dos assuntos envolvidos, nenhum consenso foi alcançado para a preparação do *report final*", o qual está disponível em: <http://disarmament.un.org/Library.nsf/c0996f411fc369518525704c00502170/e67ac010a7a643498525708800716e75/$FILE/exgr60.202.pdf>.

Durante as conversas com os russos, um assunto foi abordado e tratado como de grande relevância. Em quase todos os computadores vendidos ao redor do mundo, o sistema operacional já instalado pela fábrica é o Windows. Somente a NSA,[2] nem mesmo a Microsoft, possui o algoritmo de *backdoor*[3] do Windows. Segundo os russos, isso permite que a NSA acesse qualquer computador ligado à internet,

[2] National Security Agency.

[3] É um método de contornar a autenticação normal, permitindo o acesso remoto a um computador.

direta ou indiretamente, o que traz grande segurança às forças dos EUA, no caso de uma ação cibernética. Disseram que alguns países estão protegendo-se contra essa ameaça, desenvolvendo sistemas operacionais nacionais que controlam todos os computadores públicos. Citaram a França e a China como dois dos países que possuem sistemas próprios.

Como pôde ser visto, o Grupo de Peritos Governamentais em Desenvolvimento no Campo da Informação e Telecomunicações no Contexto da Segurança Nacional, formado em 2005, parecia ter sido um fracasso total, mas o fracasso era apenas aparente. O trabalho do grupo de peritos continuou em 2008, 2009 e 2010, sempre solicitado pela Rússia. O *report* final de 2010 assemelha-se muito ao texto produzido ao fim da reunião de julho de 2005 e será comentado a seguir.

Report Final – 2010

O primeiro ponto importante a se notar no report final de 2010 é que o *chairman* era o mesmo representante russo da reunião em 2005 e a representante dos EUA era, também, a mesma pessoa, texto que se encontra disponível em: <http://www.reachingcriticalwill.org/political/1com/1com10/reports/201.pdf>.

Logo no sumário está escrito que "(...) a potencial ameaça no âmbito da segurança da informação é o mais sério desafio do século 21 (....)". Isso caracteriza uma mudança radical de posição das nações participantes, em especial dos EUA. E continua "(...) Há um aumento de reports de que Estados estão desenvolvendo ICT (Tecnologias de Informação e Comunicações) como instrumentos de guerra e inteligência, e para propósitos políticos ...)". Essa afirmação seria impensável, no *report* final de 2005, mesmo para países que se mostraram mais moderados, como a França e a Alemanha.

A estrutura do documento traz um capítulo sobre ameaças, riscos e vulnerabilidades, onde se pode destacar que "(...) A variedade de graus de capacidade em ICT e segurança entre os diferentes Estados aumenta a vulnerabilidade da rede global (...)". Daí, infere-se que as grandes potências entenderam que a ameaça cibernética, muitas vezes, não deixa caminho rastreável até o inimigo.

Em seguida, há um capítulo sobre cooperação, que chega a dizer que, "Como as atividades irregulares usando tecnologias de informação e comunicações tendem a ser mais complexas e perigosas, é óbvio que **nenhum Estado é capaz de tratar dessas ameaças sozinho**" (grifo nosso), numa clara aceitação de que nenhuma nação, nem mesmo as mais desenvolvidas e detentoras de tecnologias dominantes em TI, sente-se segura com relação à sua capacidade de se defender de um ataque cibernético.

Em cinco anos, a percepção de segurança cibernética mudou muito. O que aconteceu? Há necessidade de uma reflexão de como evoluíram as atividades de guerra cibernética nos últimos anos, principalmente nos países mais desenvolvidos e envolvidos em conflitos.

Ocorrências mundiais

A origem da guerra cibernética remonta às primeiras ações de espionagem pela internet, ainda nos anos 1980, quando os espiões descobriram que podiam recolher dados sigilosos pela rede mundial, sem que corressem nenhum risco pessoal.

Mas a tecnologia na sociedade informacional evolui de forma espantosa. Ainda nos anos 1990, os casos mais famosos foram relacionados ao crime cibernético, tal como a invasão das intranets da GE e da rede de televisão NBC, que imobilizou vários postos de trabalho dessas gigantes e causaram milhões de dólares de prejuízos, em novembro de 1994.

Em 1997, o Departamento de Defesa dos EUA encomendou um experimento de codinome *Eligible Receiver*. O principal objetivo do exercício era ver se um grupo de *hackers* poderia infiltrar-se nos computadores do Pentágono e ter acesso aos sistemas de defesa. Os resultados foram preocupantes. De acordo com John Hamre, secretário-adjunto da Defesa na época, passaram-se apenas três dias para que alguém no Pentágono percebesse que os sistemas de computador estavam sob ataque. Os *hackers* ganharam o controle do Pentágono e dos sistemas de comando e controle militares. Um verdadeiro ataque poderia ter desligado os sistemas. Ainda mais desconfortável foi o pensamento de que os atacantes poderiam ter tido acesso e roubado informações. O curioso é que, um ano depois, um ataque cibernético real foi deflagrado contra computadores do Pentágono, da Nasa e de outros órgãos governamentais. Esse ataque foi descoberto por acaso, em 2000, e teve como provável origem a Rússia.

Em 1999, o satélite militar inglês Skynet foi posto fora de ação. A agência Reuters reportou: "*Hackers* supostamente tomaram o controle de um dos satélites militares da Grã-Bretanha e enviaram ameaças de chantagem". A notícia correu o mundo e chegaram a dizer que os "sequestradores" estavam pedindo um resgate.

Na guerra do Kosovo, registrou-se a primeira ação cibernética de um exército regular contra outro, visando a vantagem em combate. Os EUA usaram ataques baseados em computador para comprometer os sistemas de defesa aérea da Sérvia. Os ataques distorciam as imagens geradas pelos sistemas, dando informações incorretas às forças sérvias durante a campanha aérea.

Mike McConnell, antigo diretor da National Intelligence, disse ao presidente Bush, em maio de 2007, que, se os terroristas do 11 de Setembro tivessem escolhido como armas computadores em vez de aviões e tivessem empreendido enorme assalto a um banco dos EUA, as consequências econômicas teriam sido de "uma ordem de grandeza maior" do que aquelas causadas pelo ataque físico no World Trade Center.

O Centro de Estudos Estratégicos e Internacionais dos EUA divulgou um relatório sobre Segurança Cibernética para a 44ª Presidência dizendo que a segurança cibernética é um grande problema de segurança nacional para os Estados Unidos e que apenas uma compreensão estratégica do que é segurança cibernética tornará os EUA mais seguros. O relatório afirma que os Estados Unidos enfrentam um desafio de longo prazo no ciberespaço contra agências de inteligência estrangeiras civis e militares, criminosos e outros e que perder essa luta vai causar sérios danos para a economia e para a segurança nacional.

O presidente Obama disse, em discurso na Universidade de Purdue, em 16 de julho de 2008, que

> [...] cada americano depende, direta ou indiretamente, de nosso sistema de redes de informação. Elas são, cada vez mais, a espinha dorsal da nossa economia e da nossa infraestrutura, a nossa segurança nacional e o nosso bem-estar pessoal. Mas não é nenhum segredo que os terroristas poderiam usar as redes de computadores para nos dar um duro golpe. Nós sabemos que as ocorrências de espionagem cibernética e de crime cibernéticos comuns estão em crescimento. E ainda, enquanto países como a China têm sido rápidos em reconhecer essa mudança, nos últimos oito anos nós estamos nos arrastando.

Além disso, o presidente Obama afirmou que "nós precisamos ter a capacidade de identificar, isolar e responder a qualquer ataque cibernético".

Em 2008, na intervenção armada da Rússia na Geórgia, vários computadores do governo da Geórgia foram invadidos e ficaram sob controle externo, pouco tempo antes de as tropas russas entrarem em território da Geórgia. Barack Obama, na época candidato à Presidência dos EUA, pediu ao governo russo para cessar os ataques cibernéticos.

Em 2010, um consultor independente do governo dos EUA, chamado Joshua Pollack, registrou que "nos últimos anos, tornou-se quase um rito entre os funcionários federais americanos terem suas redes de computadores parcialmente interrompidas por dias ou semanas, depois de uma invasão, geralmente (mas não sempre), atribuída à China".

Em 2010, o Lt Gen Wallace Gregson, assessor do secretário de Defesa dos EUA para a segurança da Ásia e do Pacífico, fez a seguinte afirmação: "O exército chinês está fazendo progressos significativos no desenvolvimento de conceitos de guerra cibernética, que variam da defesa das redes chinesas à realização de operações ofensivas contra as redes adversárias". Essa realização de operações ofensivas, segundo ele, é vista pelo Pentágono como uma parcela de um esforço mais amplo por parte de Pequim para desenvolver uma capacidade avançada de guerra de informações, para estabelecer o controle do fluxo de informações de um adversário e manter o domínio do campo de batalha.

Além dessas, outras várias reportagens com alertas sobre a vulnerabilidade das estruturas governamentais estão à disposição na internet. Autoridades, americanas em sua maioria, alardeiam, nos EUA e, por consequência, no mundo a possibilidade de catástrofes geradas por ataques cibernéticos.

Mas, ainda, será que "catástrofe" ou "efeito de arma de destruição em massa" não seriam expressões exageradas? Há duas ocorrências muito recentes que podem servir de exemplo para uma avaliação.

Ocorrências recentes

O primeiro caso é o vazamento de dados sigilosos da diplomacia mundial pelo *site* WikiLeaks. Quanto trabalho de coleta, análise e mesmo de diplomacia não foi perdido por falta de conhecimento sobre os perigos da internet. Um diplomata americano avaliou o escândalo como catastrófico para a diplomacia americana, o qual porém não foi mais grave graças ao teor das matérias. De qualquer maneira, a diplomacia americana ficou manchada e certamente o serviço diplomático e até a economia dos EUA vão sofrer revezes que poderiam ser evitados.

O outro caso, mais grave, ocorreu em junho de 2010 e chegou ao Brasil no fim de novembro, numa breve reportagem do *Jornal Nacional*. Stuxnet foi o nome dado a um *worm* que pode ter danificado as instalações da usina nucelar iraniana de Natanz e atrasou o início das operações na usina nuclear iraniana de Bushehr. É o primeiro *worm* descoberto que espiona e reprograma sistemas industriais. No caso, foi especialmente desenvolvido para afetar o sistema de controle industrial Scada, da Siemens, que é utilizado no Irã. Segundo alguns analistas, o *worm* poderia ter causado um mau funcionamento nos sistemas de segurança da usina e permitido a elevação da temperatura do reator ao ponto de uma fratura, o que poderia gerar uma catástrofe regional. O Stuxnet, provavelmente, foi inserido por meio de um *pendrive*, num ato claro de guerra cibernética.

Não resta dúvida de que a sensação de segurança cibernética das nações está bastante afetada. Há quem diga que a maior proteção contra ataques cibernéticos será a consciência do atacante de que a arma poderá causar mal a si próprio. Nesse aspecto, há pensadores que veem semelhança entre o ataque cibernético e o nuclear.

Há várias medidas a serem tomadas para reagir à sensação de insegurança cibernética. Uma das mais produtivas é conscientizar a população, desde seus líderes políticos e militares até os trabalhadores das classes sociais mais baixas, sobre a possibilidade de estarem sendo alvo de levantamentos de dados, que podem comprometer indivíduos ou mesmo nações, ou de ataques, que podem ter efeitos gravíssimos. As potências mundiais têm investido muito em informar seus povos para reconhecer a ameaça cibernética, além de preparar suas defesas para reagir a contento. Algumas das instituições criadas nos últimos anos serão apresentadas a seguir.

Boas práticas

Ao se preparar para seguir para Nova Iorque, em 2005, o grupo de peritos do Brasil confrontou-se com uma notícia espantosa. O exército dos EUA já possuía dois batalhões cibernéticos. O curioso foi conhecer como esses batalhões foram formados. Obviamente, reuniram-se os militares de melhor capacitação técnica na área de informática, mas voluntários também foram convocados. *Hackers* sob processo judicial ou mesmo condenados foram convocados para servir o exército, com a promessa de alguns benefícios jurídicos.

Um conceito oportuno de ser citado com relação à guerra cibernética é a possibilidade de grupos ou nações adquirirem grande potencial de destruição, sem possuírem armas poderosas e caras. Esse é um dos conceitos fundamentais da guerra assimétrica.

Não é pretensão deste trabalho esgotar a apresentação de instituições que abordam a segurança cibernética criadas nos últimos anos. A intenção aqui é tão somente mostrar algumas iniciativas que possam servir de exemplo para os pensadores do Estado brasileiro, a fim de colaborar com o planejamento nacional de longo prazo.

Os EUA anunciaram, em maio de 2010, a criação do Comando Cibernético, que é comandado pelo atual chefe da National Security Agency (NSA) e está subordinado ao Comando Estratégico, apesar de ser um comando de general de quatro estrelas. É um Comando Conjunto, isto é, tem a participação de pessoal e de unidades operacionais das três Forças Armadas (nos EUA são quatro, com os Marines). A criação desse comando reflete a importância que os EUA estão dando ao desenvolvimento da capacidade de Defesa Cibernética e quanto essa área da guerra representa para a defesa dos interesses dos norte-americanos. O USCYBERCOM está criando uma unidade que vai gerenciar um estande de treinamento para as atividades relacionadas com a Defesa Cibernética. (http://en.wikipedia.org/wiki/United_States_Cyber_Command).

O Centro de Crime Cibernético do Departamento de Defesa dos EUA é outra iniciativa interessante. Trata-se de um centro que auxilia investigações que estejam relacionadas com crimes cibernéticos, abrangendo atos terroristas, contrainteligência e fraudes. As investigações preparam os efetivos da defesa para lidar com as técnicas utilizadas pelas organizações criminosas e terroristas, com a clara intenção de manter seus colaboradores atualizados (http://www.dc3.mil/).

Os Profissionais para a Defesa Cibernética é uma instituição criada em 2002, a partir de uma carta enviada ao presidente dos EUA, em que 54 profissionais com experiência em segurança cibernética alertavam-no sobre a possibilidade de os EUA sofrerem um ataque cibernético, cujas consequências poderiam ser devastadoras para a psique do povo e para a economia do país. Assessores do presidente enviaram às pessoas que assinaram a carta o documento *Estratégia Nacional para Segurança Cibernética*, para que ele fosse revisado, antes de ser apresentado para aprovação presidencial. Daí nasceu a organização, que tem como missão defender, aconselhar e servir de porta-voz da política de defesa cibernética dos EUA (http://www.uspcd.org/).

A Agência de Defesa Cibernética é uma empresa privada de consultoria e de pesquisa, nos EUA. Oferece dez diferentes cursos que abrangem desde Estratégias para a Defesa Cibernética até cursos para *hackers* que testam as defesas das empresas e organizações (http://www.cyberdefenseagency.com/).

A Agência Nacional da Segurança dos Sistemas de Informação da França é outro bom exemplo de organização ao serviço da Defesa Cibernética. Foi criada, em 2009, com a missão de desenvolver uma capacidade de detecção precoce de ataques a computadores, a utilização crescente de produtos e redes de alto nível e estabelecer um conjunto de competências em benefício das administrações e dos operadores das infraestruturas críticas (http://www.ssi.gouv.fr/site_article185.html).

Em se tratando de documentos que regem as iniciativas de um Estado, o melhor exemplo disponível é o Ato sobre Segurança Cibernética 2009, proclamado pelo Congresso dos EUA. Sua primeira observação diz o seguinte: "A falha da América em proteger o espaço cibernético é um dos mais urgentes problemas nacionais do país". O ato possui cunho de planejamento do Estado, para atender à demanda das instituições que tratam da segurança cibernética, incluindo orçamento previsto. É, sem dúvida, uma demonstração de que os parlamentares americanos possuem uma consciência bastante elevada sobre as ameaças cibernéticas (http://cdt.org/security/CYBERSEC4.pdf).

Conclusão

As novas armas quase sempre precederam os conflitos. A evolução da informática está introduzindo uma dependência a um recurso material, no cotidiano do ser humano, jamais experimentada na história da humanidade.

Os países mais belicosos perceberam a oportunidade advinda do emprego de armas cibernéticas nos teatros de operação. Entretanto, alguns pensadores vislumbraram que a possibilidade de serem gerados efeitos catastróficos derivados do emprego dessas armas poderia existir, o que requeria a atenção das Nações Unidas.

Inicialmente, as nações que possuíam maior desempenho tecnológico no setor cibernético reagiram, mas, ao longo do tempo e com as ocorrências mundiais danosas ao desenvolvimento mútuo em franco crescimento, aceitaram a possibilidade de regulamentação sobre o uso dessas armas.

O Brasil, nação que passa por um período de grande desenvolvimento social e econômico, precisa atentar e acreditar na possibilidade de ser alvo, em futuro próximo, de ataques cibernéticos, que poderão gerar grandes perdas materiais, quando não catástrofes político-sociais ou humanas.

É preciso iniciar um programa sério, voltado à preparação das instituições nacionais para enfrentar as ameaças cibernéticas, o qual abranja a educação não só das autoridades que vão regular os procedimentos e processos, mas de técnicos capazes de proteger as infraestruturas críticas da Nação, bem como a criação de instituições públicas e privadas voltadas para o conhecimento, a pesquisa e o assessoramento em âmbito nacional.

Referências bibliográficas

ALMEIDA, José E. P. *Relatório de Missão - Grupo de Peritos Governamentais em Desenvolvimento no Campo da Informação e Telecomunicações no Contexto da Segurança Nacional*. Comando-Geral de Operações Aéreas. Brasília, 2005.

BRUNO, Greg. *The evolution of cyber warfare*. Council on Foreign Relations. Disponível em: <http://www.cfr.org/publication/15577/evolution_of_cyber_warfare.html>. Acesso em: 6 dez. 2010.

CAMPBELL, Duncan. *Cyber sillies*. The Guardian. Disponível em: <http://www.guardian.co.uk/uk/1999/may/20/military.defence>. Acesso em: 6 dez. 2010.

DoD. *DoD Cyber Crime Center*. Department of Defense. Disponível em: <http://www.dc3.mil/>. Acesso em: 6 dez. 2010.

Gregson, Wallace. *Chinese buildup of cyber, space tools worries U.S*. Defense News. Disponível em: <http://www.defensenews.com/story.php?c=ASI&s=TOP&i=4452407>. Acesso em: 6 dez. 2010.

KENDALL, Paul. *Cyber attacks could be new weapons of mass destruction*. Disponível em: <http://www.ourherald.com/news/2010-02-11/Columns/Cyber_Attacks_Could_Be_New_Weapons_of_Mass_Destruc_001.html>. Acesso em: 6 dez. 2010.

POLLACK, Joshua. *Is the cyber threat a weapon of mass destruction?* Bulletin of the Atomic Scientists. Disponível em: <http://www.thebulletin.org/web-edition/columnists/joshua-pollack/the-cyber-threat-weapon-of-mass-destruction>. Acesso em: 6 dez. 2010.

SCHNEIER, Bruce. *Did NSA put a secret backdoor in new encryption standard?* Wired. Disponível em: <http://www.wired.com/politics/security/commentary/securitymatters/2007/11/securitymatters_1115>. Acesso em: 6 dez. 2010.

SENATE and House of Representatives of the United States of America. *Cybersecurity act of 2009*. Disponível em: <http://cdt.org/security/CYBERSEC4.pdf>. Acesso em: 6 dez. 2010.

STRICKLAND, Jonathan. *Is cyberwar coming?* How stuff works. Disponível em: <http://computer.howstuffworks.com/cyberwar.htm/printable>. Acesso em: 6 dez. 2010.

ULLMAN, Harlan. *Worms of mass destruction*. Daily Times. Disponível em: <http://www.dailytimes.com.pk/default.asp?page=2010%5C10%5C14%5Cstory_14-10-2010_pg3_5>. Acesso em: 6 dez. 2010.

Anexo A – Resumo da colaboração russa

Dados gerais

- A informação é o mais importante recurso da riqueza de um país.
- A expansão da informação global pode ser usada com propósitos inconsistentes com a estabilidade e segurança dos países.
- A TI aumenta significativamente o potencial militar de um país.
- Estamos vivendo uma transição para novos métodos de controle de forças armadas e armas em todos os níveis.
- Existe a possibilidade de, nos próximos conflitos, os desenvolvimentos científicos e tecnológicos no campo da TI e das comunicações liderarem a corrida armamentista.
- Há uma grande preocupação de que o desenvolvimento e a disseminação de armas cibernéticas incrementem o crime e o terrorismo (cibernéticos) e de que o uso dessas armas por exércitos possa causar catástrofes globais, com efeitos de armas de destruição em massa.
- O uso de armas cibernéticas em atos de terrorismo internacional põe em perigo a vida e o bem-estar dos indivíduos, além da paz e a segurança dos Estados.
- Atualmente, a maioria dos métodos tradicionais de combate inclui aspectos da guerra da informação, mas está nascendo uma nova geração de armas que combina características das guerras da informação e cibernéticas.
- A vulnerabilidade da área da informação e as características das armas cibernéticas são atrativos à evolução dos cenários de guerra. Por outro lado, não há padronização internacional para a aplicação de leis a respeito, e o uso dessas armas continua desregulamentado.

- Devido ao que foi dito anteriormente, garantir a segurança das informações em âmbito internacional torna-se muito complicado.

- Em razão disso, há necessidade urgente de regulamentação internacional sobre leis, metodologias e tecnologias, em âmbito civil e militar, para garantir a segurança das informações.

Objetos da segurança da informação

1 – Nacional:

- sistemas de apoio a decisão;
- infraestrutura de informação civil;
- infraestrutura de informação para a defesa;
- mídia de massa; e
- consciência da população.

2 – Internacional:

- organizações internacionais – ONU;
- sistemas de administração internacionais;
- redes abertas de informação; e
- consciência individual e da massa – PSYOPS.

Potenciais ameaças cibernéticas no campo da segurança das informações:

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

Fontes de ameaças:

- o ambiente (desastres naturais etc.);
- indivíduos, incluindo criminosos e terroristas;
- organizações criminosas e terroristas; e
- nações.

Princípios para a segurança

1º princípio

- As atividades na área de segurança em TI têm de ser conduzidas para o desenvolvimento social e econômico geral, mantendo a estabilidade global e a garantia dos direitos soberanos de cada Estado.

- Devem ser consistentes com o direito de cada cidadão receber e disseminar informações e ideias, respeitando a lei e a ordem para proteger a segurança e os interesses dos Estados.

- Cada Estado e as organizações internacionais devem ter direito igual para proteger seus recursos de TI, apoiados pela comunidade internacional.

2º princípio

- Os Estados deverão restringir as ameaças no âmbito da segurança internacional às definidas neste documento.

3º princípio

- A ONU deve promover a cooperação internacional, limitando as ameaças e criando uma base legal para:
    - identificar e classificar as características da guerra cibernética;
    - identificar e classificar as armas e ferramentas cibernéticas;
    - restringir o desenvolvimento, a disseminação e o uso das armas cibernéticas;
    - prevenir da ameaça de uma guerra cibernética;
    - reconhecer o perigo do uso das armas cibernéticas, comparável ao perigo de uma arma de destruição em massa;
    - criar condições para um intercâmbio equilibrado e seguro entre as nações;
    - prevenir o uso de TI por organizações terroristas;
    - estabelecer procedimentos para notificação mútua de ataques;
    - desenvolver mecanismos para verificação dos compromissos assumidos;

- desenvolver mecanismos para resolver situações de conflito;
- desenvolver sistemas para testar as tecnologias de informação contra ameaças;
- desenvolver sistemas de cooperação internacional para garantir o funcionamento de agências de aplicação das leis;
- criar uma atmosfera de confiança nas relações internacionais (na área de TI); e
- harmonizar as legislações nacionais de forma voluntária.

4º princípio

- Orientar a responsabilidade internacional para as atividades na área de TI, carreadas nos países membros.

5º princípio

- As disputas entre os países deverão ser resolvidas por procedimentos estabelecidos.

Proposta de plano de ação

- Continuar estudos conjuntos.
- Manter o trabalho sob a égide da ONU.
- Os esforços têm de se concentrar na adoção de resoluções da ONU.
- Desenvolver princípios internacionais (código de conduta das nações).
- Desenvolver um regime legal internacional mútuo.
- Regular ações que tenham como obrigações:
  - restringir ações voltadas para infligir danos nas redes de informações;
  - proibir o uso de armas cibernéticas contra determinados alvos; e
  - criar condições para a disseminação segura das informações e da TI.

- Analisar as possibilidades de:
    - desenvolver procedimentos para notificação mútua e prevenir a disseminação não autorizada de informações;
    - estabelecer um sistema internacional de monitoramento;
    - estabelecer um sistema internacional de teste de sistema de TI;
    - fortalecer a cooperação internacional entre as agências de aplicação das leis cibernéticas; e
    - prover assistência internacional a países vítimas de ataques ou agressões cibernéticas.

PAINEL 2

SISTEMA DE SEGURANÇA E DEFESA CIBERNÉTICA NACIONAL

SISTEMA DE SEGURANÇA E DEFESA CIBERNÉTICA NACIONAL: ABORDAGEM COM FOCO NAS ATIVIDADES RELACIONADAS À DEFESA NACIONAL

*João Roberto de Oliveira**

Resumo

O presente trabalho apresenta inicialmente uma visão geral sobre como a expressão *Segurança e Defesa Cibernética* vem sendo tratado no Brasil e no mundo, privilegiando a análise dos programas, estruturas e processos que vêm sendo estabelecidos, para, ao fim, indicar sugestões que poderão ser úteis na organização e na consolidação de um sistema de segurança e defesa cibernética nacional.

Palavras-chave: Cibernética, Segurança, Defesa.

* General-de-Divisão da Reserva, exerce o cargo de assessor especial do comandante do Exército para o Setor Cibernético. É graduado em Administração de Empresas. Na sua carreira militar, além dos cursos da Academia Militar das Agulhas Negras, de Aperfeiçoamento de Oficiais e de Comando e Estado-Maior, possui o Curso de Política, Estratégia e Alta Administração do Exército e o Curso de Estado-Maior do Exército Britânico. Desempenhou as seguintes funções: comandante do 4º Batalhão de Comunicações de Exército; oficial de ligação do Exército Brasileiro junto ao Centro de Armas Combinadas nos EUA; diretor de Material de Comunicações, Eletrônica e Informática; comandante da 11ª Região Militar; comandante da 4ª Região Militar e 4ª Divisão de Exército; e secretário-executivo do Gabinete de Segurança Institucional da Presidência da República.

Introdução

Tratar de assunto relacionado ao tema Cibernética requer espírito imaginativo e dedutivo bastante aprofundado, considerando a conotação não consolidada e a dinâmica evolutiva bastante acentuada que o termo sugere.

Entretanto, ao associá-lo aos conceitos de segurança e defesa, a imprevisibilidade e a incerteza inicialmente afloradas se tornam menos inquietantes e nos remetem a possibilidades mais concretas de visualizarmos contornos viáveis para um sistema de segurança e defesa cibernética nacional, para um horizonte temporal de aproximadamente uma década à frente.

Não se trata, porém, de idealizar algo totalmente novo, inusitado, mas sim, partindo-se de organizações e instrumentos que já existem e que já trabalham nesse tema tão atual, procurar chegar-se a uma estrutura que proporcione funcionamento sistêmico a conjuntos que hoje se encontram um tanto dispersos e com objetivos, em boa parte, individualizados.

A obtenção de atitudes sinérgicas nesse campo não é tarefa fácil, pois envolve interesses públicos e privados de características e intensidades bastante variadas. Apesar dos óbices, porém, o foco deve estar voltado para a superação de eventuais divergências setoriais, em prol do interesse coletivo e, num patamar mais elevado, para a cooperação visando à consecução dos lídimos interesses nacionais no sentido de se obter uma situação consolidada de bem-estar social, prosperidade, desenvolvimento sustentável e de preservação da soberania nacional.

O presente trabalho tem por objetivo apresentar ideias sobre como poderia estar estruturado um sistema de segurança e defesa cibernética no Brasil, ao fim da segunda e início da terceira década do presente século.

Talvez esse horizonte temporal seja demasiado longo para um assunto inserido num campo de intensa mutabilidade e o contorno estrutural a ser sugerido já tenha que ser repensado e adequado daqui a três ou quatro anos ou, até mesmo, antes disso. Entretanto, é possível supor que as ideias básicas da proposta permaneçam válidas e possam sustentar prováveis adequações.

O ponto de partida é o entendimento atual sobre o tema e como ele vem sendo tratado no Brasil e em outros países, principalmente, naqueles de maior projeção no cenário internacional.

É preferível falar em entendimento, pois pode ser prematura a apresentação de conceitos nesse ambiente extremamente dinâmico e que envolve áreas interdependentes e, muitas vezes, superpostas, como a segurança da informação e das comunicações e a segurança das infraestruturas críticas.

A partir desta base inicial, da análise de experiências que vêm sendo desenvolvidas em outras partes do mundo e, principalmente, dos frutos que já vêm sendo colhidos, provenientes dos esforços de coordenação de atividades correlatas no nível nacional e da estruturação do Setor Cibernético no ambiente de Defesa Nacional é que será desenvolvido o trabalho, para, ao fim, chegar-se a ideias que possam ser úteis na organização e na consolidação de um sistema de segurança e defesa cibernética nacional.

Tendo em vista o destaque dado ao tema, por sua inserção na Estratégia Nacional de Defesa, aprovada pelo Decreto nº 6.703, de 18 de dezembro de 2008, e em razão das ações que já vêm sendo implementadas no âmbito das Forças Armadas, a abordagem a ser feita no presente trabalho privilegiará os aspectos relacionados à Defesa Nacional.

Desenvolvimento

O ambiente cibernético e as ameaças à sociedade e ao Estado

Na atualidade, o termo *cibernética* é utilizado com variadas conotações, normalmente procurando estabelecer as relações entre o homem e a máquina e seus efeitos nos ambientes das diversas atividades humanas.

Sua origem vem do termo grego *kybernetike*, que significa condutor, governador, piloto, ou aquele que tem o leme ou o timão. Recebendo um tratamento mais científico no século passado, o seu emprego procurou caracterizar o estudo do controle e da comunicação nos seres vivos e nas máquinas, sob o enfoque da transmissão da informação nesses ambientes.

Com a evolução tecnológica, que acelerou, em velocidade vertiginosa, a capacidade de processamento automatizado de dados, o termo vem sendo usado, cada vez mais, como referência ao uso de redes de computadores e de comunicações para intercâmbio de informações entre pessoas e instituições.

A esse ambiente de interação entre pessoas, empresas e instituições públicas e privadas, nacionais e internacionais, utilizando modernos recursos de Tecnologia da Informação e das Comunicações (TIC), convencionou-se chamar de ambiente ou espaço cibernético.

Se, por um lado, o uso dessas modernas tecnologias computacionais e de comunicações, que caracterizam a cibernética trouxe grandes benefícios à humanidade, facilitando o trânsito de informações, a interação e a aproximação entre indivíduos, grupos sociais, políticos e econômicos e até entre nações, por outro lado, possibilitou o aparecimento de ferramentas de intrusão nesses sistemas utilizados pelas pessoas no desenvolvimento de suas atividades particulares e profissionais.

No mais diversos níveis da gestão pública ou da gestão de negócios privados de interesse público, esses recursos informatizados são utilizados em atividades diversas, inclusive nos sistemas de controle de setores estratégicos de uma nação, como são as infraestruturas críticas de energia, telecomunicações, transportes, abastecimento de água, finanças e defesa, entre outras.

Nos campo da Defesa, tem-se que considerar, também, os recursos informatizados que controlam a utilização dos modernos equipamentos militares, que compõem os sistemas de comando e controle, de armas e de vigilância.

Nesse contexto, ações adversas de ataques cibernéticos contra redes de computadores e de comunicações utilizadas em sistemas estratégicos podem impactar até a segurança nacional, na medida em que podem interromper ou degenerar o funcionamento de estruturas essenciais à sociedade e ao Estado, como é o caso da estrutura militar de defesa.

Ações no ambiente cibernético, a Estratégia Nacional de Defesa e a missão constitucional das Forças Armadas

A Estratégia Nacional de Defesa (END) estabelece alguns parâmetros para a atuação das Forças Armadas, no que concerne às ações a serem realizadas no ambiente cibernético, guardando consonância com sua missão prevista na Constituição Federal.

A seguir são transcritos os trechos da END que mais se relacionam ao tema tratado no presente trabalho:

- Diretrizes da END:

> [...] 6. Fortalecer três setores de importância estratégica: o espacial, o cibernético e o nuclear.
>
> Esse fortalecimento assegurará o atendimento ao conceito de flexibilidade.
>
> Como decorrência de sua própria natureza, esses setores transcendem a divisão entre desenvolvimento e defesa, entre o civil e o militar.
>
> Os setores espacial e cibernético permitirão, em conjunto, que a capacidade de visualizar o próprio país não dependa de tecnologia estrangeira e que as três Forças, em conjunto, possam atuar em rede, instruídas por monitoramento que faça também a partir do espaço [...] (BRASIL. Decreto nº 6.703, de 18 de dezembro de 2008. Aprova a Estratégia Nacional de Defesa, e dá outras providências).

- Os setores estratégicos: o espacial, o cibernético e o nuclear:

> [...] 1. Três setores estratégicos – o espacial, o cibernético e o nuclear – são essenciais para a defesa nacional.
>
> 2. Nos três setores, as parcerias com outros países e as compras de produtos e serviços no exterior devem ser compatibilizadas com objetivo de assegurar espectro abrangente de capacitações e de tecnologias sob domínio nacional. [...]

[...] 4. As capacitações cibernéticas se destinarão ao mais amplo espectro de usos industriais, educativos e militares. Incluirão, como parte prioritária, as tecnologias de comunicação entre todos os contingentes das Forças Armadas de modo a assegurar sua capacidade para atuar em rede. Contemplarão o poder de comunicação entre os contingentes das Forças Armadas e os veículos espaciais. No setor cibernético, será constituída organização encarregada de desenvolver a capacitação nos campos industrial e militar.[...] (Id., Ibid.).

- As ações estratégicas para implementar a END:

[...] Segurança Nacional

Contribuir para o incremento do nível de Segurança Nacional.

Todas as instâncias do Estado deverão contribuir para o incremento do nível de Segurança Nacional com particular ênfase sobre:

- o aperfeiçoamento de processos para o gerenciamento de crises;
- a integração de todos os órgãos do Sistema Brasileiro de Inteligência (Sisbin).
- a prevenção de atos terroristas e de atentados massivos aos Direitos Humanos, bem como a condução de operações contra-terrorismo, a cargo dos Ministérios da Defesa e da Justiça e do Gabinete de Segurança Institucional da Presidência da República (GSI/PR);
- as medidas para a segurança das áreas de infraestruturas críticas, incluindo serviços, em especial no que se refere à energia, transporte água e telecomunicações, a cargo dos Ministérios da Defesa, das Minas e Energia, dos Transportes, da Integração Nacional e das Comunicações, e ao trabalho de coordenação, avaliação, monitoramento e redução de riscos, desempenhado pelo Gabinete da Segurança Institucional da Presidência da República (GSI/PR);[...]

[...] - 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, a cargo da Casa Civil da Presidência da República, dos Ministérios da Defesa, das Comunicações e da Ciência e Tecnologia, e do GSI/PR;[...] (Id., Ibid.).

Da análise dessas transcrições da END pode-se inferir que, para as Forças Armadas, caracterizam-se duas grandes vertentes de atuação no que se refere ao Setor Cibernético:

- a configuração de uma estrutura de Tecnologia da Informação e Comunicações (TIC) para atuação em rede; e

- a configuração de uma estrutura de atuação no ambiente cibernético, quer seja nas situações de paz ou normalidade institucional, nas situações de crise ou na evolução para situações que caracterizam o estado de beligerância ou conflito armado.

Na primeira vertente, as Forças Armadas, utilizando-se de recursos de TIC, devem buscar o aperfeiçoamento de sua capacidade de C^4I (Comando, Controle, Comunicações, Computação e Inteligência), para que atendam ao imperativo de atuação em rede.

Isso implica o estabelecimento de uma estrutura intra e inter-forças, que permita o compartilhamento de informações, em tempo quase real, para o apoio à decisão e ao emprego dos atuadores operacionais, desde o tempo de paz ou normalidade institucional.

Na segunda vertente, as Forças Armadas devem buscar o aperfeiçoamento de suas estruturas, de modo que participem efetivamente do esforço nacional de proteção contra as potenciais ameaças cibernéticas, bem como para adquirirem capacidade de atuação eficaz no ambiente cibernético, visando ao cumprimento de suas atribuições constitucionais.

No primeiro caso, as ações se enquadram no campo de Segurança Cibernética, envolvendo a proteção das redes de comunicações e de computação da própria estrutura militar de defesa, bem como a interação permanente com os órgãos públicos e privados, visando colaborar efetivamente com o esforço de proteção das infraestruturas críticas nacionais.

No segundo caso, as ações se inserem no campo que se vem convencionando internacionalmente chamar de Defesa Cibernética, envolvendo ações defensivas e de resposta ativa, mormente nas situações de crise, estendendo-se ao uso mais abrangente de ações ofensivas nas situações de conflito armado, o que caracteriza, no ambiente militar, o emprego de atividades de guerra cibernética, associadas às de guerra eletrônica.

As atividades de Defesa Cibernética a serem desenvolvidas pelas Forças Armadas, como parte de suas atribuições funcionais, devem obedecer a salvaguardas e controles que resguardem os direitos e garantias constitucionais, de maneira similar ao previsto na END para as atividades de inteligência. Além dos preceitos constitucionais, também devem ser obedecidos aqueles estabelecidos na Lei Complementar n° 97, de 9 de junho de 1999, e em suas atualizações posteriores.

As ações cibernéticas e a atividade de inteligência

A atividade de inteligência exerce papel fundamental nos ambientes de Segurança, Defesa e Guerra Cibernética. Ela é essencial na busca de informações, empregando todas as fontes disponíveis, para identificar e prevenir ameaças cibernéticas e proporcionar respostas adequadas, com oportunidade. Além disso, os profissionais que atuam no Setor Cibernético devem desenvolver atitude arraigada de contrainteligência, a fim de proteger o conhecimento e as informações inerentes às suas atividades.

A proposta de Política Nacional de Inteligência, elaborada por um Grupo de Trabalho interministerial de alto nível, organizado em 2009, elenca os ataques cibernéticos com uma das prioridades a serem consideradas nas atividades do Sistema Brasileiro de Inteligência (Sisbin). O assunto é abordado da seguinte forma, na referida proposta:

> [...] 6.5 Ataques Cibernéticos
>
> Referem-se a ações deliberadas com o emprego de recursos da Tecnologia da Informação e Comunicações (TIC) que visem interromper, penetrar, adulterar ou destruir redes utilizadas por setores públicos e privados essenciais à sociedade e ao Estado, a exemplo daqueles pertencentes à infraestrutura crítica nacional.
>
> Os prejuízos das ações no espaço cibernético não advêm apenas do comprometimento de recursos de TIC. Decorrem, também, da manipulação de opiniões, mediante ações de propaganda ou de desinformação.

> Há países que buscam abertamente desenvolver capacidade de atuação na denominada guerra cibernética, ainda que os ataques dessa natureza possam ser conduzidos não apenas por órgãos governamentais, mas também por grupos e organizações criminosas; por simpatizantes de causas específicas; ou mesmo por nacionais que apóiem ações antagônicas aos interesse de seus países.[...] (BRASIL. Decreto nº 6.703, de 18 de dezembro de 2008. Aprova a Estratégia Nacional de Defesa, e dá outras providências).

Portanto, os órgãos de inteligência do Sisbin devem cumprir atividades importantes, dentro do pretendido Sistema Nacional de Segurança e Defesa Cibernética.

A ameaça cibernética e as iniciativas de resposta em vários países

A mídia tem noticiado, particularmente nos últimos dez anos, várias tentativas importantes de intrusão em redes estratégicas de diversos países do globo.

Abstendo-se de eventuais exageros, é possível aquilatar o elevado potencial de danos que podem ser causados a um país que seja alvo de um bem orquestrado ataque cibernético, que não encontre defesas apropriadas para contê-lo.

Na área militar, a "arma cibernética" já vem sendo considerada como uma nova dimensão no combate moderno, ao lado das dimensões representadas pelo combate nos ambientes terrestre, aéreo, marítimo e espacial. Dessa forma, o combate no "espaço cibernético" já é considerado como a quinta dimensão no conflito atual.

A ameaça cibernética já é colocada, por alguns países, em níveis semelhantes à ameaça nuclear, com a vantagem (se assim pode-se dizer) de poder causar consideráveis danos econômicos, políticos, militares ou sociais a um oponente real ou potencial sem que seja necessário disparar um só tiro ou diretamente causar a morte de uma só pessoa.

Trata-se de uma ameaça assimétrica, pois nem sempre o ator que pode causar maior dano é o mais capaz tecnologicamente, ou o ator que detém melhores recursos tecnológicos seja o menos vulnerável.

Alguns episódios são apresentados a seguir para ilustrar o grau de ameaça que pode representar o uso da "arma cibernética". Esses episódios nem sempre são reconhecidos oficialmente pelos países alvos e, obviamente, não são admitidos pelos possíveis atores.

- De 2003 a 2006: nesse período, diversas instalações estratégicas dos Estados Unidos da América (EUA), como laboratórios de pesquisa voltados a inovações tecnológicas, foram alvos de tentativas de penetração em seus sistemas informatizados, provavelmente com o intuito de apropriar-se de conhecimento sensível.

- Abril/maio de 2007: ocorrências de ataques massivos a redes estratégicas da Estônia, causando degeneração no seu funcionamento. Esse episódio ocasionou a instalação de um Centro de Defesa Cibernética, pela Organização do Tratado do Atlântico Norte (Otan), no território estoniano.

- Setembro de 2007: suposta ação de "apropriação" do controle do sistema de defesa aérea da Síria, antecedendo ao bombardeio aéreo israelense contra instalações em construção naquele país, que seriam destinadas a apoiar o processo de produção de armas nucleares (CLARKE, 2010, p. 1-9).

- Agosto de 2008: ocorrências de ataques massivos a redes estratégicas da Geórgia, inclusive de Defesa, antecedendo a ação de tropas russas no território da Ossétia do Sul.

- Julho de 2009: ataques a sítios eletrônicos importantes dos EUA e da Coreia do Sul e suposta tentativa de penetração no sistema de controle de fornecimento de energia elétrica norte-americano.

- Setembro/outubro de 2010: ataques aos sistemas de controle de infraestruturas nucleares do Irã e a sistemas estratégicos de outros países, utilizando o sofisticado software (*worm*) denominado *Stuxnet*.

No Brasil, não se tem notícia oficial de ataques cibernéticos efetuados com finalidade precípua de degeneração de sistemas estratégicos. A mídia, inclusive internacional, chegou a especular que o chamado "apagão elétrico", ocorrido no fim de 2009, tenha sido ocasionado, também, por ataques cibernéticos, o que, efetivamente, não foi comprovado.

Entretanto, isso não significa afirmar que o País não possa ser afetado por ações dessa natureza, já que interesses diversos podem motivar tentativas de penetração em redes importantes e trazer consequências danosas imprevisíveis.

A ameaça cibernética vem ocasionando iniciativas de sistematização de ações para contê-la em várias partes do mundo.

Principalmente nos países de maior visibilidade internacional, tem-se buscado o fortalecimento de suas estruturas nacionais e a cooperação com outros Estados, sempre incluindo os sistemas de Defesa entre suas prioridades.

Essas iniciativas incluem atitudes com variadas denominações, que causam uma considerável confusão e mascaram as verdadeiras intenções por trás das estruturas e processos que são implementados.

Essa confusão é propagada por intermédio da mídia, com a utilização indiscriminada de termos diferentes, na maioria com significados semelhantes, como Segurança da Informação e das Comunicações, Segurança Cibernética, Defesa Cibernética e Guerra Cibernética.

Os entendimentos comumente tidos como os mais apropriados para os referidos termos são os seguintes:

- Segurança da Informação e das Comunicações e Segurança Cibernética: Normalmente refere-se à proteção de redes de comunicações e de computadores de sistemas públicos e privados, de caráter estratégico.

- Defesa Cibernética: é frequentemente utilizado para caracterizar a defesa, pura e simples, contra ataques cibernéticos, mas o seu sentido mais amplo envolve medidas de resposta ativa e até atitudes ofensivas de caráter preventivo, empregadas principalmente no contexto de ações em prol da Defesa Nacional;

- Guerra Cibernética: frequentemente utilizado como referência ao "conflito cibernético" (Ataque x Defesa), entretanto, seu significado mais adequado refere-se à utilização de todo o espectro de

recursos cibernéticos, no ambiente de preparo e emprego operacional de frações militares, num sentido semelhante ao utilizado para caracterizar a Guerra Eletrônica.

Como já dito anteriormente, vários países vêm aperfeiçoando suas estruturas para lidar com essa hodierna e potente ameaça.

Notícias diversas têm sido veiculadas, tais como: China e Israel estabeleceram seus Centros de Defesa Cibernética e Rússia vem tratando o assunto com seus órgãos estratégicos de mais elevado nível na esfera de segurança nacional.

Também tem sido noticiado que o Reino Unido está em via de pôr em operação o seu Centro de Operações de Segurança Cibernética, com a missão principal de monitorar o espaço cibernético para detectar ameaças às infraestruturas estratégicas nacionais, atribuindo especial atenção às atividades ligadas à Defesa e à Inteligência.

As informações mais comumente disponíveis referem-se aos Estados Unidos da América, que recentemente ativaram o seu Comando Cibernético, o qual constitui o órgão de mais elevado nível no âmbito do Departamento de Defesa (Department of Defense)[1] para o trato das atividades cibernéticas.

No desempenho de suas atribuições, o Comando Cibernético interage com vários parceiros governamentais, principalmente do Departamento de Segurança Interna (Department of Homeland Security) e outros do setor privado, de interesse da Defesa.

No âmbito do Departamento de Defesa, a interação do Comando Cibernético é mais intensa com:

- os comandos cibernéticos das Forças Armadas;
- a Agência de Inteligência de Defesa (Defense Intelligence Agency);
- a Agência do Sistema de Informações de Defesa (Defense Information Systems Agency), encarregada de planejar, instalar, operar e manter, com segurança, a estrutura de Tecnologia da Informação e Comunicações necessária para apoiar as operações conjuntas das Forças Armadas, líderes

nacionais e outras missões envolvendo parcerias internacionais (coalizões), em todo o espectro de ações militares; e

- a Agência de Segurança Nacional (NSA – National Security Agency), responsável pelas atividades de Inteligência do Sinal nos EUA, as quais enquadram, também, as atividades de inteligência da área cibernética.

Cumpre ressaltar que no nível político do país, as atividades cibernéticas são tratadas no âmbito do Conselho de Segurança Nacional (National Security Council) e existem programas governamentais para tratar o assunto, como a Comprehensive National Cybersecurity Initiative e a National Initiative for Cybersecurity Education.

A primeira iniciativa reúne várias agências governamentais, estendendo suas ações a organizações privadas de interesse, a fim de buscar protegê-las de tentativas de intrusão e antecipar-se a prováveis ameaças.

A segunda abrange ações de capacitação, sensibilização e outras necessárias para se ter profissionais adequadamente preparados para o exercício de funções inerentes ao setor cibernético, assim como manter o cidadão educado a respeito da ameaça cibernética.

A coordenação nacional do Programa é encargo do National Institute for Science and Technology e as coordenações específicas são encargos dos seguintes órgãos:

- Department[1] of Homeland Security, para as ações visando obter um estado de prontidão nacional face às ameaças cibernéticas às infraestruturas críticas do país;

- Department of Education e Office of Science and Techonology Policy, para as ações relativas à educação formal do cidadão a respeito da ameaça cibernética, em todos os níveis, e com diferentes graus de intensidade;

[1] Nos EUA, o termo "*Department*" corresponde a Ministério, no Brasil.

- Office of Personnel Management, para a conscientização dos servidores públicos federais, no que se refere ao seu papel no combate às ameaças cibernéticas; e

- Department of Defense, Department of Homeland Security e Director of National Intelligence, para a capacitação e o adestramento profissional em Segurança e Defesa Cibernética.

Situação no Brasil referente à Segurança e Defesa Cibernética

Segurança Cibernética e assuntos conexos

No Brasil, os assuntos relacionados à Segurança da Informação e das Comunicações, Segurança Cibernética e Segurança das Infraestruturas Críticas vêm sendo tratados no âmbito do Conselho de Defesa Nacional (CDN) e da Câmara de Relações Exteriores e Defesa Nacional (Creden), do Conselho de Governo, por intermédio do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), que exerce as funções de Secretaria-Executiva do citado Conselho e de Presidência daquela Câmara.

Os entendimentos dos termos acima citados normalmente referem-se a:

- Segurança da Informação e das Comunicações:

  Proteção das informações estratégicas nacionais (que transitam por documentos, redes de comunicações, redes computacionais, entre outros);

- Segurança das Infraestruturas Críticas:

  Proteção das instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provocará sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da Sociedade.

- Segurança Cibernética:

  Proteção e garantia de utilização das redes estratégicas de comunicações e computadores.

As competências do CDN estão previstas no artigo 91 da Constituição Federal de 1988 e a regulamentação de sua organização e de seu funcionamento está contida na Lei nº 8.153, de 11 de abril de 1991.

As competências, organização e normas de funcionamento do Conselho de Governo e da Creden estão contidas na Lei nº 10.683, de 28 de maio de 2003, e no Decreto nº 4.801, de 6 de agosto de 2003.

O artigo 6º da Lei nº 10.683/2003 estabelece outras atribuições ao GSI/PR relacionadas aos assuntos anteriormente citados, como, por exemplo, a coordenação das atividades de inteligência federal e de segurança da informação, bem como a coordenação das ações no sentido de prevenir ocorrência e articular o gerenciamento de crises, em caso de greve e iminente ameaça à estabilidade institucional e, ainda, de realizar o assessoramento pessoal ao presidente da República em assuntos militares e de segurança.

Outro dispositivo importante que trata do assunto em pauta é o Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal (APF) e confere à Secretaria-Executiva do CDN, assessorada pelo Comitê Gestor de Segurança da Informação, criado pelo próprio Decreto, e apoiada pela Agência Brasileira de Inteligência (Abin), por intermédio de seu Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações (Cepesc), diversas atribuições para implementação de medidas relativas ao tema.

Da análise dos dispositivos legais citados e, ainda, do Decreto nº 6.391, de 11 de agosto de 2009, que revogando o Decreto nº 5.772, de 8 de maio de 2006, aprova a Estrutura Regimental do GSI/PR, verifica-se que o Gabinete centraliza a coordenação da grande maioria das medidas relativas à Segurança Cibernética e suas áreas conexas de Segurança da Informação e das Comunicações e Segurança das Infraestruturas Críticas.

Na estrutura do GSI/PR destacam-se as seguintes frações, com atribuições relativas ao tema:

- o Departamento de Segurança da Informação e das Comunicações (DSIC);
- a Agência Brasileira de Inteligência (Abin);
- a Secretaria de Acompanhamento e Estudos Institucionais (Saei); e
- a Secretaria de Coordenação e Acompanhamento de Assuntos Militares (Scaam).

Além do já citado Comitê Gestor de Segurança da Informação, outros organismos importantes funcionam sob coordenação do GSI/PR, a saber:

- Grupos de Trabalho de Segurança das Infraestruturas Críticas, nas áreas de energia, telecomunicações, transportes, suprimento de água e finanças;
- Grupo de Trabalho de Segurança das Infraestruturas Críticas da Informação;
- Grupo Técnico de Segurança Cibernética; e
- Grupo Técnico de Criptografia.

Cumpre ressaltar, ainda, a existência da Rede Nacional de Segurança da Informação e Criptografia (Renasic), que funciona coordenada pela Assessoria de Ciência e Tecnologia do GSI/PR, e que se constitui numa rede virtual de troca de informações sobre o tema, na qual participam pesquisadores, profissionais de entidades públicas e privadas, do meio acadêmico, e outros interessados nessas atividades. A Renasic tem gerado sinergia na discussão de problemas e soluções práticas de Tecnologia da Informação e Comunicações (TIC) e de Segurança da Informação e Comunicações (SIC).

Importantes fontes de consulta sobre os assuntos tratados até aqui são encontradas em documentos produzidos pelo DSIC/GSI, como, por exemplo, o *Livro Verde – Segurança Cibernética no Brasil* (MANDARINO JUNIOR; CANONGIA 2010), o *Guia de referência para a Segurança das Infraestruturas Críticas da Informação* (MANDARINO JUNIOR; CANONGIA; GONÇALVES JUNIOR, 2010), a *Compilação da legislação vigente sobre Segurança da Informação e Comunicações* (VIEIRA, 2008) e o volume 1 da *Gestão da Segurança da Informação e Comunicações* (FERNANDES, 2010). Também constitui importante fonte de consulta o livro recentemente editado pelo diretor do DSIC, Raphael Mandarino Junior, sob o título *Segurança e defesa do espaço cibernético brasileiro* (2010).

Outros órgãos importantes relacionados ao setor estão localizados, principalmente, nas estruturas da Casa Civil da Presidência da República, do Ministério da Defesa, em especial nas Forças Armadas, e do Ministério da Justiça, em especial na Polícia Federal.

Defesa Cibernética

O Ministério da Defesa e as Forças Armadas, como membros da Administração Pública Federal (APF), já participam ativamente do esforço nacional nas áreas de Segurança da Informação e Comunicações, Segurança Cibernética e Segurança das Infraestruturas Críticas.

Entretanto, é muito importante a ampliação dessas atividades e das estruturas a elas dedicadas, para atender ao amplo espectro das operações características de Defesa Cibernética, as quais devem abranger:

- no nível estratégico: as ações cibernéticas necessárias à atuação das Forças Armadas em situações de crise ou conflito armado e, até mesmo, em caráter episódico, em situação de paz ou normalidade institucional, ao receber mandado para isso; e

- no nível operacional: as ações cibernéticas, defensivas e ofensivas, relativas ao preparo (capacitação, adestramento ou treinamento) e ao emprego em operações militares, de qualquer natureza e intensidade, que caracterizam o ambiente de Guerra Cibernética.

Em outras palavras, é necessário que as Forças Armadas disponham de equipamentos e sistemas militares que utilizem modernos recursos de TIC, possibilitando o seu emprego eficaz no cumprimento de suas atribuições previstas no artigo 142 da Constituição Federal e regulamentadas, quanto à sua organização, preparo e emprego, pela Lei Complementar nº 97, de 9 de junho de 1999, e suas atualizações.

> Art. 142. As Forças Armadas, constituídas pela Marinha, Exército e Aeronáutica, são instituições nacionais permanentes e regulares, organizadas com base na hierarquia e na disciplina, sob autoridade suprema do presidente da República, e *destinam-se à defesa da Pátria, à garantia dos poderes constitucionais e, por iniciativa de qualquer destes, da lei e da ordem* (grifo nosso).
>
> §1° Lei complementar estabelecerá as normas gerais a serem adotadas na organização, no preparo e no emprego das Forças Armadas [....] (BRASIL. Constituição da República Federativa do Brasil de 1988).

Ao mesmo tempo, é necessário que as Forças Armadas disponham de recursos tecnológicos adequados para a proteção de seus sistemas de comando e controle, de armas e de vigilância, além de uma sólida estrutura de capacitação e adestramento operacionais, bem como de capacitação técnica para que seus recursos humanos possam atuar, com eficiência, em todo o espectro de ações cibernéticas características do emprego de efetivos militares em situações diversas, quer seja na paz, na crise ou nos ambientes de conflito armado ou guerra.

A END formula diretrizes para o preparo e o emprego das Forças Armadas em atendimento às suas Hipóteses de Emprego (HE), estabelecendo ações que devem ser observadas desde o tempo de paz.

Como já explanado, a END estabelece que três setores estratégicos – o espacial, o cibernético e o nuclear – são essenciais para a Defesa Nacional.

Visando dar provimento ao estabelecido na END para esses setores estratégicos, o Ministério da Defesa emitiu, em 9 de novembro de 2009, a Diretriz Ministerial nº 014, definindo responsabilidades sobre a coordenação e a liderança na condução das ações referentes aos setores nuclear, cibernético e espacial, respectivamente, à Marinha, ao Exército e à Aeronáutica.

Na referida diretriz ficou estabelecido que os trabalhos fossem desenvolvidos em duas fases:

- na primeira, seriam definidos os objetivos de cada setor e a abrangência do tema; e
- na segunda, seriam definidas as ações estratégicas e elaboradas as propostas de estruturas, com o máximo aproveitamento e adequação das já existentes.

No que se refere ao Setor Cibernético, o Exército concluiu a 1ª fase ainda em dezembro de 2009, com base nos estudos e propostas de um Grupo de Trabalho (GT) interforças. Os trabalhos daquele grupo prosseguiram e o Exército concluiu a 2ª fase em março de 2010.

O Ministério da Defesa aprovou as propostas do Exército em outubro de 2010, as quais estabelecem nove objetivos estratégicos a serem alcançados para o Setor Cibernético, juntamente com as ações estratégicas previstas para cada um deles.

Os objetivos estratégicos aprovados incluem ações voltadas, especialmente, para atividades de Segurança da Informação e Comunicações, Segurança Cibernética e Segurança das Infraestruturas Críticas, tanto no âmbito do Ministério da Defesa e das Forças Armadas quanto na participação colaborativa, no nível nacional, com as demais instituições envolvidas, em interação com estas, principalmente com o GSI/PR.

Na área de Defesa Cibernética, cumpre destacar duas ações estratégicas referentes ao Objetivo Estratégico nº 1, que estabelece a criação de uma estrutura de Defesa Cibernética subordinada ao Estado-Maior Conjunto das Forças Armadas para inserir o tema nos planejamentos militares conjuntos e a criação do Comando de Defesa Cibernética das Forças Armadas para dar execução aos objetivos estratégicos estabelecidos para o setor e suas ações estratégicas correspondentes.

Portanto, na área de Defesa Cibernética, já estão estabelecidos os parâmetro básicos para a expansão, o aprimoramento e a consolidação do setor, em atendimento ao estabelecido na END e às demandas para alcançar uma estrutura sistêmica eficaz, no âmbito nacional.

A Força Terrestre, como força líder na condução do processo no âmbito da Defesa, antecipou ações no seu campo interno e emitiu, em junho de 2010, a Diretriz para Implantação do Setor Cibernético no Exército e já em agosto do mesmo ano foram emitidas portarias criando o Centro de Defesa Cibernética do Exército (CDCiber) e ativando o seu Núcleo (NuCDCiber), que já se encontra operativo, inicialmente para dar provimento aos oito projetos previstos naquela Diretriz.

Os referidos projetos destinam-se a atender às necessidades prioritárias para o Exército, já com foco na sua atuação de força líder no âmbito da Defesa, e objetiva, em linhas gerais, à (ao):

- expansão e aprimoramento da estrutura de segurança cibernética já existente;
- expansão e aprimoramento da estrutura de capacitação, adestramento e emprego operacional já existente, para atender, também, às necessidades do Setor Cibernético, incluindo, ainda, os assuntos relacionados ao tema nos currículos dos estabelecimentos de ensino da Força;
- estabelecimento de uma estrutura de apoio tecnológico e de pesquisa cibernética;

- estabelecimento de uma estrutura de gestão de pessoal e de arcabouço documental (doutrina, em particular);

- estabelecimento de uma estrutura para atendimento das necessidades de inteligência voltadas para o setor; e

- formatação da estrutura e das missões do Centro de Defesa Cibernética do Exército, a partir do seu Núcleo já ativado.

Cumpre destacar que na área de Defesa Cibernética é de elevada importância a atuação integrada das estruturas operacional, de inteligência e de ciência e tecnologia.

Nessa área, tanto quanto na área de Segurança Cibernética, também é relevante a participação de profissionais, militares e civis, das mais diversas áreas de interesse, bem como a elevada cooperação entre entidades públicas e privadas abrangidas pelo setor, inclusive do meio acadêmico, tanto no âmbito nacional quanto no âmbito das parcerias ajustadas com outros países.

Propostas gerais para a implantação do Sistema Nacional de Segurança e Defesa Cibernética

Como se pode observar do que foi apresentado neste trabalho, o Brasil já possui uma estrutura básica atuante nas áreas de Segurança Cibernética (e suas conexas Segurança da Informação e das Comunicações e Segurança das Infraestruturas Críticas) e de Defesa Cibernética.

Na área de Segurança Cibernética e suas conexas, a estrutura atual confere vantagem fundamental ao concentrar a coordenação das ações principais num órgão da estrutura da Presidência da República, no caso o GSI/PR.

O trabalho do GSI/PR nesse setor é facilitado pela sua estrutura organizacional que permite congregar esforços das principais áreas de interesse, reunindo frações voltadas aos campos técnicos da atividade, à inteligência, à prevenção e gerenciamento de crises e ao campo militar.

Outro fator relevante é a responsabilidade atribuída ao GSI/PR de executar as atividades necessárias ao exercício das competências do CDN e da Creden, organismos que detêm prerrogativas essenciais voltadas ao Setor Cibernético nos campos das decisões estratégicas (CDN) e da formulação das políticas públicas e diretrizes, bem como da articulação de ações que envolvam mais de um Ministério (Creden).

Portanto, é essencial que se mantenham todas essas atribuições vinculadas a um órgão da estrutura da Presidência da República, no caso atual o GSI/PR.

Isso se aplica, também, às atividades de Defesa Cibernética, que embora sejam mais diretamente ligadas ao Ministério da Defesa e às Forças Armadas, necessitam da vinculação ao CDN, para as decisões estratégicas, e à Creden, principalmente para a articulação de ações com outros órgãos públicos e privados de interesse.

Propõe-se aqui o fortalecimento das estruturas já existentes e a adoção de mecanismos que proporcionem a sua atuação sistêmica, como a formulação das políticas e diretrizes públicas correspondentes e da emissão de dispositivos legais que amparem e regulamentem a atuação articulada dos órgãos participantes do sistema. Pode-se buscar subsídios na instituição do Sistema Brasileiro de Inteligência (Sisbin) e nos estudos e propostas para a sua reformulação, elaborados pelo Grupo de Trabalho interministerial organizado com essa finalidade.

Quanto à Defesa Cibernética, já há estabelecidos objetivos estratégicos e ações estratégicas correspondentes, conforme explanado anteriormente. Trata-se agora de buscar implementá-los. Igual processo poderia ser buscado no que se refere à Segurança Cibernética e suas conexas.

Outro ponto importante a destacar é a imperiosa necessidade de o Sistema contemplar a participação e a interação permanentes com a atividade de inteligência.

Neste particular, é importante a expansão das atividades de Inteligência do Sinal para abranger, também, as necessidades cibernéticas, como está ocorrendo em outros países. As Forças Armadas brasileiras já têm estrutura e experiência de atuação nesse ambiente. A partir da expansão e fortalecimento de suas atividades, poder-se-ia pensar em criar uma organização que atendesse às necessidades do Estado brasileiro.

O mais importante, porém, no processo de organização de um Sistema Nacional de Segurança e Defesa Cibernética, é o estabelecimento de um ambiente colaborativo permanente.

Todas as instâncias do Estado envolvidas nesse processo devem buscar a interação fácil entre elas e com as outras entidades de interesse, inclusive dos meios acadêmico e empresarial.

Também é de capital importância a expansão dos programas de capacitação e conscientização hoje existentes na esfera pública federal, bem como estabelecer outros de caráter educativo para atingir outros segmentos prioritários da sociedade.

Conclusão

Se, por um lado, os avanços obtidos na área de Tecnologia da Informação e das Comunicações facilitam nossas vidas e trazem benefícios importantes para a humanidade como um todo, por outro, trazem, também, efeitos colaterais nocivos com os quais temos que aprender a lidar.

A ameaça cibernética é patente e real. Ela se revela na rotina das pessoas e instituições, quer nos ambientes individual, coletivo ou profissional, e se estampa no noticiário da mídia praticamente todos os dias.

No ambiente estratégico do Estado, o combate a essa ameaça deve fazer parte de suas prioridades, a fim de prevenir danos à sociedade e ao próprio Estado, os quais podem assumir proporções consideráveis.

No Brasil, apesar de ser relativamente recente a preocupação com o tema, as ações têm-se intensificado nos últimos anos.

No campo da Segurança Cibernética, as ações ganharam maior impulso a partir da criação do DSIC no GSI/PR, em 2006, e no campo da Defesa Cibernética, ênfase maior passou a ser observada a partir da edição da END, em 2008.

De qualquer modo, o momento atual é propício para acelerar medidas, a fim de se organizar um eficiente Sistema Nacional de Segurança e Defesa Cibernética.

Nesse sentido, as propostas que foram apresentadas no presente trabalho buscaram indicar como parâmetros prioritários:

- a expansão e o aprimoramento da estrutura existente de Segurança Cibernética e suas conexas, Segurança da Informação e Comunicações e Segurança das Infraestruturas Críticas, mantendo-se o princípio de coordenação no órgão da Presidência da República que detém a atribuição de prover o funcionamento do CDN e da Creden, no caso o GSI/PR;

- a consecução dos objetivos estratégicos, com suas ações estratégicas correspondentes, estabelecidos pelo Ministério da Defesa, a fim de contemplar uma estrutura eficiente de Defesa Cibernética no seu âmbito e no das Forças Armadas, intensificando a interação das ações no âmbito nacional;

- o estabelecimento de objetivos estratégicos e ações estratégicas correspondentes, a serem alcançados, também, no âmbito da Segurança Cibernética nacional e suas conexas Segurança da Informação e das Comunicações e Segurança das Infraestruturas Críticas;

- o fortalecimento do espírito cooperativo entre as instituições do setor público e dessas com a academia e o setor privado, a fim de obter maior efetividade no combate à ameaça cibernética;

- a expansão dos programas de capacitação e conscientização existentes atualmente na esfera federal e o estabelecimento de outros de caráter educativo, para atingir outras parcelas consideradas prioritárias da sociedade; e

- o estabelecimento de um Grupo de Trabalho interministerial de alto nível, no âmbito da Creden, a fim de estudar e propor a organização de um Sistema Nacional de Segurança e Defesa Cibernética, com base na expansão, adequação e aprimoramento das estruturas existentes.

Referências bibliográficas

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constitui%C3%A7ao.htm>. Acesso em: 16 dez. 2010.

———. Decreto nº 6.703, de 18 de dezembro de 2008. Aprova a Estratégia Nacional de Defesa, e dá outras providências. Disponível em:< http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Decreto/D6703.htm>. Acesso em: 16 dez. 2010.

CLARKE, Richard; KNAKE, Robert. *Cyber war*. New York, USA: CCCO, 2010. 290p.

FERNANDES, Jorge Henrique Cabral (Org.). *Gestão da segurança da informação e comunicações*. Brasília: Faculdade de Ciência da Informação/UnB, 2010. v. 1. Disponível em: <http://dsic.planalto.gov.br>. Acesso em: 16 dez. 2010.

MANDARINO JUNIOR, Raphael; CANONGIA, Cláudia. *Livro Verde – Seurança Cibernética no Brasil*. Brasília: GSI/PR, 2010. 63p. Disponível em: <http://dsic.planalto.gov.br>. Acesso em: 16 dez. 2010.

MANDARINO JUNIOR, Raphael; CANONGIA, Cláudia; GONÇALVES JUNIOR, Admilson. *Guia de referência para a Segurança das Infraestruturas Críticas da Informação.* v. 1. Brasília: GSI/PR, 2010. 151p. Disponível em: <http://dsic.planalto.gov.br>. Acesso em: 16 dez. 2010.

MANDARINO JUNIOR, Raphael. *Segurança e defesa do espaço cibernético brasileiro*. Recife: CUBZAC, 2010. 182p.

VIEIRA, Tatiana Malta. *Compilação da legislação vigente sobre Segurança da Informação e Comunicações.* Brasília: GSI/PR, 2008. Disponível em: <http://dsic.planalto.gov.br>. Acesso em: 16 dez. 2010.

A SEGURANÇA E AS AMEAÇAS CIBERNÉTICAS: UMA VISÃO HOLÍSTICA

*Otávio Carlos Cunha da Silva**

Introdução

O *espaço cibernético*, a *segurança cibernética* e outras expressões relacionadas são amplamente usadas como se o seu significado fosse claro e fora de qualquer debate. A realidade, porém, é que esses termos mascaram uma série de pressupostos ainda não testados e perguntas sem resposta, apresentando uma séria dificuldade para os decisores políticos e os responsáveis pela segurança nacional.

A segurança cibernética (segurança a partir do espaço cibernético) é amplamente considerada como um problema urgente e de alto nível, que não pode ser ignorado. Mas a natureza exata desse problema ainda não está bem definida. Essa combinação de intuição e de incerteza (misturada com pessimismo) pode subverter a análise, incentivando uma mudança na direção da pior avaliação e uma tendência a focar a política (e despesas) quase exclusivamente em eventos de alto impacto e de baixa probabilidade.

Desde a introdução do circuito integrado na década de 1950, a economia mundial tem crescido cada vez mais dependente de uma infraestrutura de informações digitais. Atualmente, é difícil imaginar uma grande empresa ou organização que não dependa de Tecnologia da Informação e Comunicações (TIC). Indústrias que variam desde ferrovias até venda ao atacado, todas dependem de sistemas de TIC para

* O autor é Coordenador-Geral do Centro de Pesquisa e Desenvolvimento para Segurança das Comunicações (Cepesc), da Agência Brasileira de Informações (Abin). É graduado em Engenharia Elétrica pela Universidade de Brasília (UnB), Administração de Empresas e Economia, ambos pelo Ceub e possui pós-graduação em Gestão do Desenvolvimento Científico Tecnológico e Gestão de Segurança da Informação, ambos pela UnB e Pós graduação em Comércio Internacional pela AEUDF. Na sua carreira, trabalhou como Engenheiro Eletrônico na General Eletric, Engenheiro Eletrônico na Siemens S.A. Já no Cepesc/Abin foi Pesquisador na Divisão de Projetos, Coordenador-Geral de Suporte Técnico, Coordenador-Geral de Segurança da Informação e Diretor do Centro de Pesquisa e Desenvolvimento para Segurança Comunicações.

manter comunicações de negócios essenciais com clientes e fornecedores. No setor financeiro, negócios no valor de centenas de bilhões de dólares são transacionados diariamente por meio de redes de dados globais, públicos e privados. No setor público, as instituições se utilizam de sistemas cibernéticos para o fornecimento de serviços essenciais à sociedade nas mais diversas áreas, tais como: saúde, educação, bem-estar social etc. A dependência da sociedade com relação a redes e sistemas de TIC parece apenas aprofundar o advento da "computação em nuvem", o que significará que a tecnologia digital irá "penetrar cada recanto da economia e da sociedade".[1]

Não é, portanto, nenhum exagero dizer que a economia global agora é dependente de um conhecimento complexo e habilitado em banda larga cibernética. Com a dependência vêm a exposição e a vulnerabilidade, além de um conjunto extenso de oportunidades a serem exploradas pelos inescrupulosos.

A dependência da sociedade em relação a TIC é agravada pela interdependência crescente dos sistemas de informação, tornando difícil saber quais repercussões as falhas em uma parte do sistema terão em outro. Como a dependência nesses sistemas complexos aumenta, também aumenta a vulnerabilidade da sociedade com seu uso indevido e, portanto, cresce a gravidade das consequências de eventuais ataques ou falhas dos sistemas (que podem, em termos práticos, ser indistinguíveis). Como citado anteriormente, a sociedade está cada vez mais dependente – talvez absolutamente – das tecnologias, as quais os próprios adversários podem se utilizar para atacar.

Nessas circunstâncias, não é fácil determinar o que deve ser protegido, contra quem e com que meios. Contudo, o desafio da segurança cibernética é muito mais profundo. Segurança cibernética é muitas vezes descrita, explicada e analisada dentro de um quadro de política tradicional, onde o idioma e os conceitos organizacionais são muitas vezes derivados dos militares: ameaça, agressão, ataque e defesa estão entre os termos mais familiares. Em alguns casos, pode ser apropriado analisar o problema a partir desse ponto de vista e agir em conformidade com ele. Porém, a aplicação do pensamento ortodoxo da segurança e defesa muitas vezes pode resultar em segurança cibernética sendo entendida como algo em que a intrusão vem de fora, que é "feito" por "eles" contra "nós". No entanto, a correlação entre dependência e vulnerabilidade dá uma indicação importante que segurança cibernética é um problema mais desafiador que isso, que talvez não seja propício apenas uma análise linear com base em ação e reação, causa e efeito. Na verdade, segurança cibernética é provavelmente mais bem com-

[1] Retirado da revista *The Economist*, Let it rise: A special report on corporate IT', *The Economist*, 25 October 2008, p. 3. Disponível em <http://www.economist.com/node/12411882> .Acessado em 19 de fevereiro de 2010.

preendida como um problema complexo, que é caracterizado pela incerteza e não-linearidade, que é dinâmica e constantemente em evolução, e no qual pode ser difícil estabelecer relações causais claras e nítidas dividindo linhas entre sujeito e objeto.

A integridade do conhecimento cibernético global complexo é fundamental não só para o funcionamento corrente da economia mundial, mas também para a segurança e o bem-estar de governos, organizações e pessoas: organismos públicos podem ser atacados, interesses comerciais podem ser fraudados e indivíduos podem ser sujeitos a uma série de agressões.

A análise da segurança cibernética de qualquer sistema, deve ser efetivamente realizada pela caracterização das ameaças cibernéticas que possam alterar o seu funcionamento em termos de integridade, autenticidade, disponibilidade e, em alguns casos, confidencialidade. Embora a tarefa seja aparentemente simples, descritiva, pode ser um difícil compromisso, especialmente porque essas grandes categorias de desafios de segurança podem sobrepor-se consideravelmente.

A internet: um ecossistema

A internet é um sistema global das redes altamente complexo que está constantemente evoluindo e sendo alterado. Os vários ambientes que compõem esse ecossistema[2] operam em vários níveis, cada um dos quais realiza uma função de apoio para os outros níveis, e assim ocorre por toda a rede e, por extensão, no próprio ecossistema da internet.[3] Assim como a internet evolui e muda, o número e a complexidade das ameaças em todo o ecossistema da rede também se transformam e se alteram. A

[2] Um ecossistema é um subconjunto de um ambiente sem limites que funciona como uma unidade. Assim como planejamento prévio em um sistema sem limites é intratável, um ecossistema (cibernético) fornece um espaço de solução viável para a resistência (proteção) e resiliência (recuperação). Modelos de ecossistemas desenvolvidos pelos biólogos para compreender a dinâmica complexa dos sistemas na natureza fornecem uma base para percepção da garantia da informação para sistemas em rede. Ecossistemas cibernéticos formam pares com outros ecossistemas cibernéticos em pontos de troca designados e podem funcionar de forma segura dentro da internet. Exemplos atuais desses ecossistemas dentro da internet incluem intranets, redes ISP, redes virtuais privadas e novas formas de sobreposição de redes, tais como redes de distribuição de conteúdo. (JORGENSEN, 2001).

[3] NORTON, William B. *The Evolution of the U.S. Internet Peering Ecosystem*, November 19, 2003.Disponível em: <http://dev.nanog.org/meetings/nanog31/presentations/norton.pdf>. Acesso em: jul. 2010.

transformação da internet de uma rede de pesquisa de elite em um meio de comunicação de massa alterou drasticamente a equação da ameaça cibernética global. O sistema global de TIC pode ser explorado por uma variedade de usuários ilegítimos e ainda pode ser usado como uma ferramenta de agressão em nível de Estado. Essas atividades podem ser organizadas ao longo de um espectro de execução do crime de nível inferior, individual (*hacking*, por exemplo), ou relacionadas ao comportamento dos intervenientes não estatais e grupos (ou seja, os criminosos e terroristas), e, ainda, aos planos orquestrados pelos governos. É importante observar que, embora este espectro de atividades tenha mérito como um dispositivo organizacional, ele é errado analiticamente. Esses diversos usuários da internet não se enquadram em campos distintos e muito menos em uma hierarquia simples de ameaças. Por exemplo, *hacking* pode ter uso muito grave no crime organizado; criminalidade organizada pode ser vinculada ao terrorismo internacional; e terrorismo pode ser usado como uma ferramenta de agressão do Estado. Esse ponto é colocado de maneira impressionante na autobiografia, escrita na prisão, de Abdul Aziz, também conhecido como Imam Samudra – um dos responsáveis por bombardeio terrorista em Bali em 2002, quando 202 pessoas foram mortas –, que incitava, em página na internet, jovens muçulmanos a "*take the holy war into cyberspace by attacking U.S. computers, with the particular aim of committing credit card fraud*", atacando computadores dos EUA, com o objetivo específico de cometer fraude de cartão de crédito, com o propósito de financiar a luta contra os Estados Unidos e seus aliados.[4]

Níveis das ameaças cibernéticas

Segundo Cornish (2010), em estudo realizado por solicitação do Comitê de Assuntos Exteriores do Parlamento Europeu, podem ser as ameaças cibernéticas classificadas, em termos de criminalidade, em quatro níveis: crime de baixo-nível/individual (*hacking*), criminalidade grave e organizada, extremismo político e ideológico e ataques cibernéticos patrocinados pelo Estado. Esses níveis apresentam uma ampla gama de perigos e riscos, muitas vezes interconectados, que os decisores políticos na área de segurança devem enfrentar.

[4] SIPRESS, A. An Indonesian's Prison Memoir Takes Holy War into Cyberspace, *Washington Post*. Disponível em: <http://www.washingtonpost.com/wp-dyn/articles/A62095-2004Dec13.html>. Acesso em: 19 fev. 2010.

A seguir serão apresentados os níveis das ameaças cibernéticas:

Nível 1: crime de baixo nível/individual (*hacking*)

No espectro das ameaças cibernéticas, o ponto de partida é o *script kiddie*, usando ferramentas de *software* concebidas e fornecidas por terceiros para interferir em redes de computadores, juntamente com o *hacker*. Em qualquer análise de *hacking* de computador um sentimento de equilíbrio é muitas vezes difícil de manter. Para alguns analistas, *hacking* deveria ser considerada uma faceta mais ou menos discreta da segurança cibernética; mas, para outros, não tem coerência e nenhum sentido equivalente a outras ameaças mais graves. A ameaça do *hacking* é muitas vezes superestimada e até mesmo dramatizada, como se a infraestrutura de redes de TIC global fosse ser destruída pelos esforços incessantes de jovens aborrecidos que procuram algum estímulo.

Nível 2: a criminalidade cibernética organizada

A internet tornou-se um ponto central de atividades pessoais, políticas e comerciais, bem como um meio de vital importância para transações financeiras e intelectuais. Não deve surpreender, portanto, o fato de que o interesse criminoso na internet desenvolveu-se na mesma proporção. O mundo cibernético tornou-se um alvo tentador e lucrativo para a moderna empresa do crime.

A meta de toda essa atividade parece suficientemente clara: muitas dessas ameaças podem ser usadas para ganhos financeiros, realizando ações como o roubo de informações confidenciais que podem ser vendidas *on-line*. Essas receitas, em seguida, podem ser usadas para pagar os programadores para continuar criando novas ameaças.[5]

Quanto aos empreendimentos da criminalidade organizada no espaço cibernético, eles podem continuar mais ou menos conforme as definições tradicionais e os entendimentos da criminalidade, ou ela pode adaptar-se às circunstâncias alteradas, evoluindo para algo novo e distinto. Em outras palavras,

[5] SYMANTEC CORPORATION. *Global Internet Security Threat Report*: Trends for July-December 2007 (v. XIII, p. 45-46, April 2008). Disponível em: <http://eval.symantec.com/mktginfo/enterprise/white_papers/bwhitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf>. Acesso em: 01 mar 2010.

uma ameaça cibernética pode ser manifestada pela criminalidade organizada de duas maneiras: por um lado, uma organização criminosa pode fazer uso do espaço cibernético para continuar as suas atividades criminosas, enquanto, por outro lado, um novo gênero de crime organizado pode evoluir, o que é exclusivo do espaço cibernético. Choo e Smith (2008) estabelecem uma distinção entre "tradicionais grupos criminosos organizados" e "grupos de criminosos cibernéticos organizados".[6] Política de segurança cibernética que ignore esta distinção e que pressuponha que a criminalidade cibernética seja uma ameaça unitária, monolítica, irá quase certamente falhar quanto ao foco necessário para o planejamento eficaz.

Grupos criminosos graves, tais como as *triads* asiáticas (organizações criminosas primariamente estabelecidas em Hong Kong e ativas em Taiwan e na China Continental), a Yakuza japonesa e organizações do Leste Europeu talvez explorem o espaço cibernético para uma variedade de efeitos bastante previsíveis, incluindo lavagem de dinheiro, tráfico de drogas, extorsão, roubo de informações de cartão de crédito, fraude de ATM, pirataria de *software*, espionagem industrial, falsificação de documentação e assim por diante.[7] Esse fenômeno tem sido descrito como "a migração do crime organizado do mundo real para o crime organizado do mundo no espaço cibernético".[8]

Entretanto, organizações de crimes cibernéticos irão colocar muito menos ênfase na força física e serão menos interessadas em desenvolver uma associação exclusiva e extremamente leal. Como sugerem Choo e Smith, os membros de uma organização de crimes cibernéticos podem apenas encontrarem-se *on-line*.[9] A organização de crimes cibernéticos normalmente será mais pragmática; movida menos pela fidelidade da gangue que pela necessidade de reunir as competências tecnológicas necessárias no momento certo: no mundo cibernético, sugere Brenner (2002), "força física é insignificante […] força está no *software*, não no número de indivíduos."[10]

[6] CHOO, K. R., e SMITH, R. G. Criminal exploitation of Online Systems by Organized Crime Groups. *Asian Criminologyv*. 3, n. 1, p. 39-40, junho de 2008.

[7] Ibid, p. 40.

[8] BRENNER, S. W. Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships. *North Carolina Journal of Law & Technology*. v.4, Issue 1, p. 24, Fall 2002.

[9] CHOO, K. R., e SMITH, R. G. Criminal Exploitation of Online Systems by Organized Crime Groups, *Asian Criminology* (v. 3, n. 1, p. 39-40, June 2008).

[10] Ibid., p. 27.

Efetivamente, pode haver pouca necessidade de uma organização complexa (muito menos hierárquica) no espaço cibernético. Brenner argumenta que uma estrutura organizacional elaborada não deve ser necessária para os criminosos operarem em um mundo virtual que pode ser construído mais ou menos como os desejos do usuário. O espaço cibernético é mutável; o que o criminoso cibernético necessita é agilidade e capacidade de resposta, em vez de estrutura. Se a criminalidade cibernética requer alguma forma de organização, ela precisa ser não mais do que uma "máfia do momento", que irá desaparecer quando não há mais necessidade de grupos.[11] A criminalidade cibernética usará tecnologia sofisticada e também terá cobertura internacional. A queda do Fórum *Darkmarket* ocasionou detenções no Reino Unido, Alemanha, Turquia e os Estados Unidos depois de seguidos anos de trabalho de investigação.

Grupos de criminosos cibernéticos tendem a adotar uma estrutura não hierárquica em rede. Mais e mais modelos ocasionais de organização estão melhorando sua capacidade de se adaptar rapidamente às circunstâncias em mudança. Geometria variável deste tipo poderia igualmente ser um apelo aos grupos extremistas baseados na criminalidade por uma razão ou outra. Grupos extremistas valorizam uma estrutura que é baseada na eficácia, na criação de riqueza, mas que não requer uma infraestrutura pesada e rastreável.

Nível 3: ideológico e extremismo político

Pelo fato de a internet estar se tornando "o mais importante local de reunião para *jihadis* de todo o mundo, para se comunicar, discutir e partilhar as suas opiniões".[12] O chamado "terrorismo cibernético" começa com *hacking* e baixo nível de criminalidade. Younis Tsouli, descrito como "um dos *ciber-jihadistas* mais famosos do mundo",[13] usa habilidades de *hackers* para invadir e subverter as redes de computadores a fim de distribuir arquivos de vídeo de ataques terroristas e usar o produto da fraude de cartão

[11] Ibid., p. 37-46.

[12] STERNESEN, A. The Internet: a virtual training camp? *Terrorism and political violence* (v. 20, p. 228, 2008)

[13] CORERA, G. The world's most wanted cyber-jihadist, BBC News, 2007. Disponível em: <http://news.bbc.co.uk/go/pr/fr/-/2/hi/americas/7191248.stm>. Acesso em: 01 mar 2010.

de crédito comum para configurar sítios de *jihadi*.[14] Por esses meios, Tsouli tornou-se "o administrador de um dos mais importantes sítios extremistas que facilitou contatos entre milhares de indivíduos".[15]

Após sua detenção e prisão subsequente, atividades de Tsouli foram descritas por um oficial de contra-terrorismo sênior como "a primeira conspiração virtual para assassinar que vimos", bem como uma revelação importante quanto à forma como os extremistas tornaram-se competentes para desempenhar a condução de um planejamento de nível operacional na internet.[16]

A popularidade da internet entre extremistas ideológicos e políticos pode ser explicada de diversas formas, *i.e.*, seu objetivo inicial: ser uma rede que pudesse oferecer rotas redundantes de comunicação de dados entre organizações militares em caso de um ataque nuclear; uma rede com baixo custo de acesso, tendo em vista a questão da guerra fria que predominava à época do estabelecimento da Arpanet (posteriormente denominada Internet). Não é de se surpreender, portanto, que os extremistas são atraídos para um sistema que oferece resistência em construção e anonimato virtual. Eles também podem ser atraídos para um sistema que é de custo quase gratuito, e no qual os investimentos necessários para desenvolver e manter a infraestrutura de comunicações globais já foram feitos – ironicamente por seus inimigos.

A internet é um terreno comum e anárquico que os extremistas podem explorar de maneiras extraordinariamente interessantes, assim como a sociedade o faz, para fins de comunicação e compartilhamento de informações.[17] É também especialmente adequada para utilização por organizações que são deliberadamente opacas na sua estrutura e intenção.

Em termos funcionais, a internet oferece uma série de serviços úteis para os extremistas. Em primeiro lugar, é um meio para comunicações em vários níveis: em claro, criptografados e estegnografados.[18]

---

[14] Retirado de A world wide web of terror, The Economist, 14 July 2007. Disponível em < http://www.economist.com/node/9472498?story_id=9472498 > Acesso em: 01 mar 2010.

[15] CORERA, G. The world's most wanted cyber-jihadist, BBC News, 2007.Disponível em: <http://news.bbc.co.uk/go/pr/fr/-/2/hi/americas/7191248.stm>. Acesso em: 01 mar 2010.

[16] Ibid.

[17] STENERSEN, A. The Internet: a virtual training camp?'. *Terrorism and Political Violence* (v. 20, p.215, 2008).

[18] Diferente da criptografia, a estenografia ("escrita oculta") é uma forma de comunicação encoberta na qual a mensagem em si (e não apenas o significado) é escondida.

Ordens executivas podem ser transmitidas por esses meios, operações podem ser planejadas, e pode-se ainda organizar campanhas para levantamento de fundos. Por meio da utilização de fóruns de discussão, *bulletin boards*, grupos de mídia, postagens em *blogs* e *web*, a internet pode permitir também treinamento e técnicas – e até mesmo ideias – para serem discutidas de forma interativa. Táticas e procedimentos podem ser melhoradas através de um processo de avaliação *on-line* rápida; e doutrinas e ideologias podem ser objeto de crítica.

Existe acordo geralmente mais sobre a importância da internet para a doutrinação, a contratação e a radicalização dos extremistas. Recrutamento tornou-se um recurso importante do extremismo cibernético, de tal forma que um "Fórum de Internet de jihadi al-Qaeda" chegou a carregar um manual de 51 páginas intitulado "A arte de recrutamento", que pretende mostrar como indivíduos podem ser atraídos e, finalmente, estabelecer uma célula ativa *jihadi*.[19] Porém,com tantos recursos disponíveis na internet, recrutamento e radicalização já não são simplesmente uma questão organizacional, mas também, e cada vez mais, uma questão de "auto-incentivo" ou "auto-recrutamento e auto-radicalização".[20]

Depois de radicalizados e treinados por meio da internet, extremistas podem descobrir que a rede continua a ser útil como arma. A ilustração mais clara dessa tendência são os extremistas para quem a internet passou a ser um "espaço de batalha" em seu próprio direito; um território no qual uma *jihad* virtual pode ser combatida. Esses indivíduos podem contribuir por comentar, reproduzir e distribuir os pensamentos de líderes terroristas, coletando e distribuindo informações de fontes abertas úteis para o planejamento operacional e tomando parte em medidas mais ativas, como *hacking* e ataques de negação de serviço (DOS). Claramente, se a infosfera é na verdade um "espaço não governado", é onde os rebeldes estão determinados a lutar e vencer a batalha de ideias.

[19] BAKIER, A. H. Jihadis publish online recruitment manual, Terrorism Focus , v. 5 n. 34, THE JAMESTOWN FOUNDATION, 24 September 2008. Disponível em: <http://jamestown.org/single?no_cache=1&tx_ttnews%5D=5179>. Acesso em:1 mar. 2010.

[20] DRENNAN, S. e BLACK, A. Jihad online: The changing role of the internet, *Jane's Intelligence Review*, August 2007.

Nível 4: agressão cibernética patrocinada pelo Estado

A dimensão interestatal da utilização incorreta do mundo cibernético pode começar em um nível relativamente baixo de tecnologia. Seria um erro assumir, no entanto, que o significado de tais ataques é proporcionalmente baixo. Cita-se o caso de abril de 2008, por exemplo, de relatórios de difusão de um ataque contra oito sítios da internet operados pela Radio Free Europa/Radio Liberty (RFE/RL). Na tentativa orquestrada para saturar os sítios de destino, algo em torno de 50 mil falsos *hits* foram registados a cada segundo. Isso era praticamente a mais sofisticada forma de operação cibernética. No entanto, a origem do ataque foi alegada sem nenhuma exceção "Do ditador de mais longo mandato na Europa, Aleksander Lukashenko da Bielorrússia", declaradamente com o objetivo de limitar a cobertura midiática dos protestos da oposição contra seu regime.[21]

É provável que a guerra cibernética seja um recurso cada vez mais importante no conflito entre Estados-nação nos próximos anos. Na verdade, perdas e ganhos no espaço cibernético podem ser tão decisivos que o caráter da guerra poderia alterar fundamentalmente, assim como a física e os parâmetros territoriais do conflito dão lugar para o virtual e o digital.

Questões críticas

As questões anteriormente descritas demandam um estudo aprofundado e devem ser consideradas estratégicas por qualquer Nação que venha a pleitear um posicionamento entre os principais atores globais que estão, a cada dia que passa, mais dependentes de sistemas de informação interconectados, por intermédio de redes de comunicação, a outros sistemas nacionais ou estrangeiros, utilizando-se da internet como espinha dorsal para viabilização do alto nível de conectividade necessário para negócios, quer na esfera privada e/ou pública.

Antes de qualquer resposta às questões formuladas, mesmo se a vítima de um ataque cibernético não planeja lançar outro ataque em resposta, é importante caracterizar o ataque recebido, para efeitos de

[21] HUGHES, R. A treaty for cyberspace. International Affairs 86: 2, 2010. Blackwell Publishing Ltd. Disponível em: <http://www.cyberdialogue.ca/wp-contents/ Rex-Hughes-A-Treay-for-Cyberspace>. Acesso em: 01 mar. 2011.

forense computacional e aplicação da lei. Para tal, alguns itens são tidos como fundamentais para a caracterização de um ataque e eventual resposta, qualquer que seja ela – até mesmo o silêncio pode ser encarado como uma resposta. Dentre essas questões críticas destacamos: a atribuição, a intenção e a dissuasão cibernética.

Atribuição

A atribuição é o esforço para identificar o responsável por um ataque cibernético. A técnica de atribuição é a capacidade de associar um ataque a um responsável por meio de meios técnicos, com base nas informações disponibilizadas pelo fato do ataque cibernético em si.

A triste realidade é que essa técnica é muito difícil de ser realizada (diz-se muitas vezes que "*bits* não vestem uniformes") e pode ser quase impossível de ser efetivada quando um usuário inconscientemente comprometido ou inocente está envolvido.

A atribuição de um ataque não deve ser confundida com estabelecimento ou identificação de um caminho de acesso para a origem do ataque. A diferença entre atribuição e ter um caminho de acesso é significativa, porque na ausência de um caminho de acesso, neutralização de um ataque cibernético não é possível, embora a retaliação para ele possa ser. O inverso também é verdadeiro: na ausência da atribuição, retaliação ou represálias não são possíveis, apesar de ser possível a neutralização de um ataque cibernético.

Intenção

No domínio do tradicional conflito militar, é geralmente presumido que os governos nacionais controlam as armas de guerra – fragatas, aviões de ataque, tanques e assim por diante. Assim, se qualquer uma dessas armas é usada, há uma presunção de que ações envolvendo-as tenham sido sancionadas pelo governo controlador, e inferências, muitas vezes, podem ser feitas no que diz respeito à intenção do governo que deflagra essas ações. Contudo, quando outras armas não são controladas exclusivamente pelos governos, inferir a intenção da ação é muito mais problemático. Tal fato é especialmente notório se não é possível estabelecer comunicação com a parte controladora – como pode vir a ser o caso de um ataque cibernético. Atribuição de um ataque cibernético ajuda, mas se a parte identificada

como responsável não é um governo nacional ou outra parte com intenções declaradas na direção do governo, será praticamente impossível determinar a intenção com alta confiabilidade.

Determinações de intenções e atribuição da fonte são muitas vezes complicadas, e inadequadamente tendenciosas, por falta de informação. Em última análise, tais decisões são feitas por seres humanos, que procuram integrar todas as informações disponíveis para processar um acórdão. Essa integração pode ser automatizada, mas são pessoas que programam as regras de integração.

Dissuasão Cibernética

O objetivo da dissuasão é desincentivar o início ou a efetivação de uma ação mais hostil.

A dissuasão cibernética tem de ser passível de repetição,porque nenhum ato viável de retaliação cibernética é suscetível de eliminar o Estado transgressor, conduzir à queda ou derrubada do governo, ou, até mesmo, desarmar o Estado. Assim, um Estado poderia atacar, sofrer retaliação e atacar outro dia. A dissuasão cibernética também é simétrica porque tem lugar entre os pares.

Considerações finais

O espaço cibernético pode ser descrito (embora não calculado) como a soma das inúmeras interações entre inúmeros usuários globais da infraestrutura de TIC. Para conseguir absoluta e perfeita segurança no espaço cibernético seria necessário identificar e isolar todos os usuários malignos e impedir seus componentes e interações. Entretanto, fazê-lo – mesmo que fosse possível –, seria contradizer a essência do espaço cibernético como uma tecnologia global de todos; uma "república" das comunicações e de intercâmbio de informação em nível mundial. De acordo com Vinton Cerf, conhecido como o pai da internet, "se cada jurisdição no mundo insistir em alguma forma de filtragem para seu território geográfico específico, a *web* vai parar de funcionar".[22]

[22] Retirado de Geography and the Net: putting it in its place, *The Economist*, 9 August, 2001.

A segurança cibernética constitui-se em assunto complexo e profundo. Sua análise deve ser executada sob ponto de vista holístico, levando-se em consideração a multiplicidade de áreas do conhecimento que se fazem necessárias para o tratamento adequado dessa questão, ou seja, permitir que os integrantes desse espaço cibernético tenham a garantia de que seus ativos informacionais estejam garantidos em termos de disponibilidade, integridade, autenticidade e, quando necessário, a confidencialidade; que não sejam repudiados e que a infraestrutura crítica seja resiliente o suficiente para continuar operando mesmo sob ataques hostis.

Assim como o espaço cibernético evolui, espera-se que as ameaças e os desafios que emanam dele também evoluam.

A dependência da área de TIC acarreta exposição e vulnerabilidades e um conjunto cada vez maior de oportunidades para exploração por parte dos inescrupulosos, como no "mundo real".

A segurança cibernética deve ser um esforço coletivo e não pode ser vista apenas como responsabilidade de um único ator, o governo. Todos os atores devem participar nesse esforço de manutenção de estabilidade, tendo em vista as inúmeras interações entre todos os sistemas de informação existentes. Logo, se a questão não for analisada, debatida, pesquisada e tratada de maneira conjunta, isto é, todos os atores envolvidos fazendo cada um a sua parte no processo de assegurar a informação, muito será despendido e pouco resultado será obtido.

A segurança cibernética é muito mais do que apenas uma questão de segurança nacional ou defesa militar, ela é uma questão integrada e, para tal, necessita de um esforço integrado dos setores civil e militar, mantendo-se as suas competências individualizadas, mas que sob um ponto de vista estratégico seja aplicado de acordo com a gravidade do assunto em pauta.

Enfim, acreditamos ser fundamental o estabelecimento de um projeto de parceria público-privada na qual as questões relacionadas às ameaças cibernéticas, bem como as ações necessárias para a garantia da segurança do espaço cibernético, sejam tratadas de maneira integrada pelos atores anteriormente mencionados.

Referências

BAKER, Stewart; IVANOV, George; WATERMAN, Shaun. *In the Crossfire*: Critical Infrastructure in the Age of Cyber War. Santa Clara, CA: McAfee, 2010. Disponível em: <http://resources.mcafee.com/content/NACIPReport>. Acesso em: 10 mai. 2010.

BRENNER, S.W. Organized Cybercrime? How cyberspace may affect the structure of criminal relationships. North Carolina Journal of Law and Technology, v. 4 n. 1, 2002.

CARR, Jeffrey. *Inside Cyber Warfare*. Sebastopol, CA: O'Reilly Media, 2009.

CORNISH, Paul. *Cyber Security and Politically, Socially And Religiously Motivated Cyber Attacks*. Directorate-General for External Policies of the Union, Feb. 2009. Disponível em: <http://www.chathamhouse.org.uk/publications/papers/view/-/id/702/>. Acesso em: 1 mar. 2010.

CORNISH, Paul; HUGHES, Rex; LIVINGSTONE David, *Cyberspace and the National*

Security of the United Kingdom: Threats and Responses. United Kingdom: Chatham House, Mar. 2009. Disponível em: <http://www.chathamhouse.org.uk/publications/papers/view/-/id/726/>. Acesso em: 1 mar. 2010.

GOODMAN, Seymour; PORTNOY, Michael, *Global Initiatives to Secure Cyberspace: An Emerging Landscape*. New York, NY: Springer Science, 2009.

EUROPEAN UNION COMMITTEE, HOUSE OF LORD, PARLIAMENT OF THE UNITED KINGDOM. Protecting Europe against cyber-scale cyber-attacks. Parliament of the United Kingdom, March 2010. Disponível em: <http://www.publications.parliament.uk/pa/ld200910/ldselect/ldeucom/68/6802.htm>. Acesso em: 10 mai. 2010.

JORGENSEN, J. *Cyber ecology*: looking for insights into information assurance.Washington, DC: DARPA-Information Survivability Conference and Exposition (DISCEX II), p. 287-296, 2001.

LIBICKI, Martin C. *Cyberdeterrence and Cyber War*. Santa Monica, CA. RAND Corporation, 2009. Disponível em: <http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf>. Acesso em: 1 mar. 2010.

MAZZAFRO, Joseph. *Addressing cyber security through public-private partnership:* an analysis of existing models. Arlington, VA: Intelligence and National Security Alliance, 2009. Disponível em: <http://www.insaonline.org/index.php?id=746>. Acesso em: 1 mar. 2010.

YAMASAKI, T.; USHIO T. An application of a computational ecology model to a routing method in computer networks. *IEEE Transactions on Systems, Man, and Cybernetics-Part B: Cybernetics*,v. 32, n. 1, Feb. 2002.

ESTRATÉGIA DE PROTEÇÃO DA INFRAESTRUTURA CRÍTICA DE INFORMAÇÃO E DEFESA CIBERNÉTICA NACIONAL

*Sérgio Luís Ribeiro**

Resumo

Assim como ocorre em outros países, é papel do Estado proteger suas infraestruturas críticas e, consequentemente, o espaço cibernético e a infraestrutura crítica de informação que a suportam, a fim de criar condições para o desenvolvimento sustentável do país.

A proteção da infraestrutura crítica de informação faz parte da política de Estado, a fim de abranger, além da definição de estratégias, papéis e responsabilidades, um método de entender, analisar e avaliá-las em termos de elementos críticos, ameaças, vulnerabilidades, riscos e controles que visam à prevenção de incidentes que causam impactos não somente à própria infraestrutura, mas também a outros setores, com uma reação em cadeia que pode afetar toda a sociedade.

Uma infraestrutura crítica é formada por diversos elementos, que precisam ser conhecidos, a fim de serem priorizados em uma eventual estratégia de proteção. Essa proteção pode e deve ser dimensionada de acordo com os diferentes cenários e simulações, o que facilitaria o entendimento e otimizaria os recursos existentes.

* O autor é pesquisador em Segurança da Informação da Fundação Centro de Pesquisa e Desenvolvimento (CPqD). Tem graduação em Matemática e pós-graduação em Análise de Sistemas, ambos os cursos pela Pontifícia Universidade Católica de Campinas. Possui, também, MBA Executivo Internacional, pela Fundação Getúlio Vargas. É autor de varias publicações e tem quatro patentes e duas certificações em seu nome. Na sua carreira, trabalhou como engenheiro de Redes, pela Equant (Global One Comunicações Ltda.), e como analista de Suporte em Redes e Telecomunicações, de Suporte e em Segurança de sistemas, pela Robert Bosh Ltda.

Para o país, é importante uma visão holística da situação atual da infraestrutura crítica de informação, na qual seria possível monitorar e acompanhar não só a disponibilidade dos serviços destinados à população, mas também os riscos iminentes do momento. Para tanto, faz-se necessária a definição de uma estratégia e de um sistema de proteção das infraestruturas críticas incluindo a infraestrutura crítica de informação.

Palavras-chave: Infraestrutura crítica de informação. Defesa cibernética. Sistema de proteção de infraestrutura crítica. Sistema de defesa cibernética. Estratégia de proteção da infraestrutura crítica nacional.

Introdução

Cada vez mais, o tema de proteção da infraestrutura crítica de informação – e, consequentemente, a defesa cibernética – tem se tornado um assunto de grande relevância para todos os países e vem recebendo atenção crescente, a ponto de alguns destes terem criado órgãos governamentais com funções específicas para tratar do assunto.

Embora as estratégias adotadas pelos países sejam distintas, o objetivo final é sempre o mesmo: proteger a infraestrutura crítica de informação e seus elementos-chave contra ameaças relacionadas a atividades terroristas e/ou espionagem, desastres naturais e situações de emergência. Isso pode ser alcançado com a estruturação de políticas, órgãos competentes, técnicas e mecanismos que envolvem, por exemplo, metodologias de proteção de infraestrutura crítica e sistemas cuja aplicação possibilite antecipar, identificar e analisar riscos a fim de reduzi-los e ter a capacidade de controlar as consequências de incidentes (tratamento de crise) em situações adversas.

Contextualização

O número crescente de incidentes provocados pela falta de segurança no mundo real ou virtual tem sido uma das grandes preocupações das nações e empresas, que estão sujeitas a riscos de intensidade cada vez maiores. Porém, é notório que planos de proteção estão sendo constantemente intensificados e aplicados, com o sucesso absoluto ainda não sendo alcançado, principalmente em razão do surgimento de novas ameaças emergentes.

Somente como efeito de ilustração, podem-se citar alguns exemplos de incidentes que possuem relação direta ou indireta com a infraestrutura crítica de informação ou defesa cibernética:

- Atentados terroristas de 2001 contra as Torres Gêmeas, nos Estados Unidos da América (National Institute of Standards and Technology, 2010);
- Ataques cibernéticos na Estônia em 2007 (também referenciado como "WWI" - *Web War I*) (SCHNEIER, 2007);
- Vazamento de informações sobre o caça F-35 (DEFENSENews, 2009);
- Ataques cibernéticos a empresas de tecnologia em 2009 (BULEY e GEENBER, 2010);
- Stuxnet: Paralisação das centrífugas no Irã (WASHINGTON POST, 2010);
- WikiLeaks revela informações confidencias de governos (WIKILEAKS, 2010) (ABCNews, 2010);
- Eventos da natureza: Furacão Katrina (NOAA, 2005);
- Alagamentos no Estado de Santa Catarina (SANTA CATARINA, 2008).

É perceptível que, em tempos de guerra ou de crise, ataques cibernéticos podem ser usados como forma de intimidação, ou, ainda, no caso mais ameno, simplesmente com o objetivo de desestabilizar um governo no desgaste da imagem perante a população.

Tais riscos e ataques não afetam somente governos ou empresas, mas a nação como um todo. Ataques cibernéticos, seja na infraestrutura crítica da informação ou ainda em empresas, afetam diretamente os serviços oferecidos aos cidadãos, incluindo também fortes consequências nos aspectos sociais, políticos e econômicos do país.

Além disso, a disseminação das redes de informação, a integração entre diferentes infraestruturas e a interdependência cada vez maior resultam em algumas consequências que não podem ser negligenciadas. Uma delas é que as vulnerabilidades em infraestruturas críticas tendem a crescer, o que tem tornado os problemas cada vez mais complexos. Outra consequência é que uma interrupção pode se propagar de uma rede para outra, ocasionando o efeito cascata de problemas, tornando indisponível um ou mais serviços.

Da mesma forma, um fator que não pode ser esquecido é que ataques cibernéticos podem ser realizados de forma anônima a uma distância segura, ou seja, são difíceis de serem detectados e responsabilizados (NEUMANN, 1995).

Situação atual

Desde fevereiro de 2008, o Brasil vem adotando a seguinte definição para infraestruturas críticas: "são as instalações, serviços e bens que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança nacional" (BRASIL, 2008).

Ainda de acordo com o art. 3º da mesma Portaria, as áreas prioritárias são: telecomunicações, energia, transportes, água e finanças, sem prejuízo de outras que porventura vierem a ser definidas (id ibid).

O Brasil atualmente conta com diversos órgãos de governos com atribuições na área de Segurança da Informação e defesa cibernética, porém, o tema relacionado à proteção de infraestrutura crítica ainda é pouco explorado pelos centros de pesquisa e universidades.

O assunto proteção de infraestrutura crítica é objeto de estudo pela Fundação CPqD desde 2004, e desde então vários resultados foram obtidos, com destaque para o desenvolvimento de um conjunto de

metodologias (ver Figura 1) e de ferramentas de *software* com o intuito de Proteção da Infraestrutura Crítica de Telecomunicações, em parceria com a Anatel e com recursos do Fundo para o Desenvolvimento Tecnológico das Telecomunicações (Funttel). Esses trabalhos propiciaram também depósitos de pedidos de patentes e publicação de artigos em congressos nacionais e internacionais.

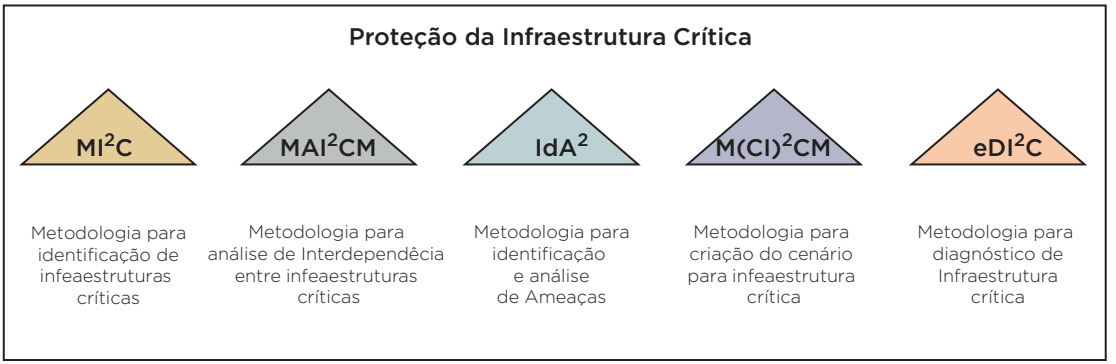

Figura 1 – Conjunto de metodologias para proteção da infraestrutura crítica
Fonte: Elaboração do autor.

No Brasil, além das demandas que são identificadas no dia a dia com relação ao tema, os grandes eventos esportivos como a Copa do Mundo de 2014 e os Jogos Olímpicos de 2016, são também considerados "importadores" de novas ameaças para o país. Isto demanda uma atenção especial, exigindo assim um árduo trabalho que envolve não somente o governo, mas também a iniciativa privada e a sociedade como um todo.

Sendo assim, os desafios vão além de identificar e tratar os riscos, e incluem agir de forma integrada e coordenada, trabalhando nos principais pilares da segurança da informação – prevenção, detecção e resposta a ataques cibernéticos – atividades estas que devem ser suportadas por metodologias formais, sistemas de apoio e pessoal capacitado.

Proposta

O principal conceito de proteção da infraestrutura crítica de informação está diretamente relacionado com a capacidade que o país tem de atuar com a prevenção, detecção e resposta aos graves incidentes que envolvem a infraestrutura crítica de informação de uma nação ou região.

Muitos países vêm investindo em planos estratégicos para mitigar, gerir e executar as ações necessárias para retomar a normalidade após uma situação de emergência provocada por catástrofe natural (como terremoto, furacão e inundação) ou ainda intencional (terrorismo e ataque cibernético, por exemplo).

Porém, graças às peculiaridades de cada país, esses planos e estratégias não são necessariamente aplicáveis a outros. O grande desafio para o Brasil consiste, assim, em formular e executar uma estratégia nacional de proteção da infraestrutura crítica de informação sintonizada com outras iniciativas mundiais, levando em consideração todas as suas características próprias.

Assim, uma estratégia de proteção da infraestrutura crítica de informação e defesa cibernética deve permitir ao governo criar organismos e estratégias para agir de forma preventiva e também para minimizar o impacto provocado pelos eventos e sinistros, incluindo os consequentes transtornos na demora do restabelecimento dos serviços para uma população atingida. Além disso, o sistema deve prover informações e indicadores capazes de gerar subsídios para a formulação e constante evolução de estratégias, leis, normas e regulamentos.

Desta forma, propõe-se direcionar os trabalhos de acordo com as necessidades do país, em ação sinérgica que deve envolver o governo, as universidades e centros de pesquisa, a iniciativa privada (que na sua grande maioria são os proprietários da infraestrutura crítica de informação), além da própria sociedade, num esforço conjunto voltado para a segurança e a defesa cibernética do Brasil.

Modelo de quatro pilares

O primeiro passo para a criação de um órgão de referência em Segurança e Defesa Cibernética eficaz e eficiente é definir suas prioridades e responsabilidades (International Communication Union-D, 2010), tarefa essa primordial para o sucesso da estratégia a ser traçada e seguida pelo país.

Estudos demonstram que um programa efetivo e eficiente deve compreender e tratar tal como sugerido pelo Modelo de Quatro Pilares (ver Figura 2) no qual estão destacadas as quatro tarefas essenciais de proteção da infraestrutura crítica de informação: prevenção, detecção, resposta e gestão de crises.

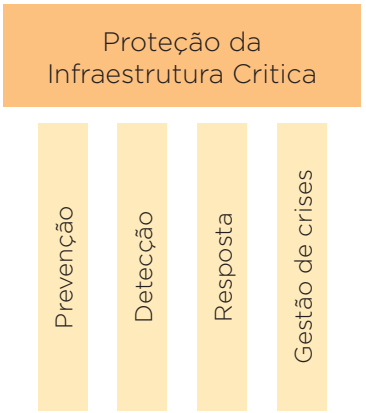

Figura 2 – Modelo de quatro pilares
Fonte: Elaboração do autor.

Prevenção

A prevenção é um componente indispensável de proteção da infraestrutura crítica de informação, tendo como objetivo reduzir o número de brechas de segurança da informação. No entanto, uma vez que as ameaças às infraestruturas críticas são múltiplas, interdependentes e complexas, é irreal esperar que incidentes possam ser totalmente evitados. Um objetivo mais pragmático é garantir que as infraestruturas críticas sejam menos vulneráveis a perturbações, que eventuais falhas sejam de curta duração e limitadas em escopo e que os serviços sejam facilmente restabelecidos após interrupções. A principal

função da prevenção consiste em assegurar que as empresas que operam e gerem a infraestrutura crítica de informação estejam preparadas para lidar com incidentes.

De uma forma ou de outra, todos os pilares de proteção da infraestrutura crítica de informação devem conter elementos de prevenção. Nessa proposta, a prevenção é definida em sentido estrito, consistindo de atividades que procuram aprimorar a prontidão das instituições para enfrentar incidentes de segurança. Isso envolve a divulgação de recomendações e orientações sobre melhores práticas, informações sobre ameaças específicas e a realização de treinamentos e exercícios. Vale notar que a prevenção não pode ser abordada em um nível puramente técnico: perigos potenciais têm de ser avaliados constantemente com auxílio de análises e avaliações de risco.

Detecção

Com o intuito de promover a segurança e evitar tecnologias particularmente vulneráveis, é fundamental que as novas ameaças emergentes sejam identificadas e as novas vulnerabilidades sejam descobertas o mais rapidamente possível. Com esse objetivo, o órgão responsável pela proteção de infraestrutura crítica da informação deve participar de uma ampla rede nacional e internacional, permitindo o compartilhamento de informações técnicas e não técnicas. A cooperação internacional é indispensável, pois os riscos não estão limitados às fronteiras geográficas de um único país.

Em estreita colaboração com os peritos técnicos dos CERTs (Computer Emergency Response Teams), o órgão deve identificar novas formas de ataques o mais rapidamente possível. Além disso, outras análises da situação geral, não técnicas, são necessárias – como, por exemplo, sobre o surgimento de organizações criminosas. Assim, o órgão de proteção da infraestrutura crítica de informação deve ter acesso restrito a informações relevantes prestadas pelos serviços de inteligência.

No entanto, a rede de contatos dos CERTs e dos serviços de inteligência se torna limitada sem a estreita colaboração dos operadores da infraestrutura crítica de informação. Afinal, esses operadores são aqueles que são afetados em primeiro lugar por um novo ataque; caso não reportem o incidente, a detecção e o alerta precoce tornam-se impossíveis. O compartilhamento de informações, assim, ocorre apenas em condições de estrita confiança. Por essa razão, a credibilidade e a confiança depositada pelos operadores no órgão de proteção da infraestrutura crítica de informação são essenciais para que este receba informações sobre incidentes em tempo hábil.

Resposta

A resposta inclui a identificação e a correção das causas de um incidente. Inicialmente, o órgão de proteção da infraestrutura crítica de informação deve fornecer suporte técnico e apoio à instituição afetada. No entanto, o ideal é que o órgão não cuide diretamente da resposta a incidentes dessas organizações e nem ofereça soluções completas, mas sim que preste aconselhamento e orientação sobre a forma de tratar um incidente, auxiliando na estruturação necessária em todos os componentes das infraestruturas crítica e coordenando todas as atividades.

Um dos principais requisitos a ser satisfeito por esse órgão é operar um serviço de notificação de incidentes de segurança em regime ininterrupto (24x7). Atacantes preferem executar seus ataques a infraestruturas de informação fora do expediente normal, esperando encontrar menor reação (isto é, menor número de contramedidas imediatas). É fato que os danos causados por um ataque dependem do tempo decorrido até a resposta, razão pela qual o tratamento do incidente deve começar o mais rapidamente possível. O apoio prestado pelo órgão de proteção de infraestruturas críticas de informação se torna mais útil caso esteja sempre disponível.

No entanto, tal como a prevenção e detecção, a resposta a incidentes não deve se limitar a medidas técnicas. Em particular, a repressão aos atacantes pela via legal é uma parte vital da resposta. A aplicação da lei pode não ser capaz de ajudar diretamente as vítimas de um ataque, mas pode ajudar a proteger outras vítimas potenciais, aumentando o risco de captura, e julgamento dos atacantes, dissuadindo assim ações semelhantes no futuro. Dado que muitos ataques são levados a cabo por atores internacionais, as instituições afetadas muitas vezes não sabem como acionar as autoridades policiais responsáveis em outros países, tarefa que deve ser conduzida pelo órgão de proteção da infraestrutura crítica de informação.

Além disso, uma resposta adequada deve incluir a análise dos incidentes. Em cooperação com a vítima, o órgão de proteção da infraestrutura crítica de informação deverá elaborar um relatório final sobre o incidente, a fim de compartilhar as informações com outras instituições. O setor privado tende a concentrar-se principalmente sobre as lições aprendidas para melhorar seus sistemas internos, cabendo ao governo adotar uma abordagem mais ampla. Os ensinamentos adquiridos devem ser trocados com todos os participantes para melhorar o planejamento para situações de crise. Empresas e setores do governo que não foram afetados pelo ataque podem rever seus planos de emergência e tomar medidas para evitar erros.

Gestão de crises

A gestão de crises deve ser parte integrante de uma estratégia de proteção da infraestrutura crítica de informação desde sua concepção. A minimização dos efeitos de quaisquer rupturas na sociedade e no Estado é uma das missões essenciais dos governos. Por esse motivo, o órgão responsável pela proteção da infraestrutura crítica de informação deve ser incorporado na estrutura nacional de gestão de crises, posicionado de modo que tenha acesso direto aos tomadores de decisão, uma vez que uma de suas funções primordiais é alertar as pessoas e as organizações responsáveis. Em caso de uma crise nacional, o órgão deve ser capaz de oferecer assessoria direta para o governo.

No âmbito governamental, o órgão de proteção da infraestrutura crítica de informação deve agir como o centro de competência para todas as questões relacionadas com segurança e defesa cibernética. Como isso diz respeito a diversas agências, a unidade deve atuar de forma colaborativa com diversos parceiros do governo. Como consequência, procedimentos de gestão de crises devem ser ensaiados regularmente. Um plano de gestão de crise bem concebido é inútil se não funcionar em situações de emergência quando realmente é necessário e colocado à prova. O órgão de proteção da infraestrutura crítica de informação deve realizar, assim, exercícios frequentes com outras organizações governamentais e com operadores das infraestruturas críticas, não se limitando somente a infraestrutura crítica de informação, de forma que todos os participantes fiquem familiarizados com suas responsabilidades, deveres e os riscos em tempos de crise.

Estratégia de proteção da infraestrutura crítica de informação

Com o desenvolvimento formal de uma estratégia de proteção, métodos e sistemas e a consequente aplicação no contexto da análise, é possível fazer que a infraestrutura crítica de informação funcione adequadamente, com a minimização da interferência de problemas naturais, ambientais, erros humanos e operacionais ou, ainda, de ataques maliciosos.

A organização e a formalização possibilitadas pelos métodos permitem que diferentes aspectos de um mesmo problema sejam tratados, evitando assim a falsa sensação de segurança, que é bastante

comum. Além disso, a aplicação faz que erros no projeto e na implementação possam ser evitados, eliminados, conhecidos ou tolerados.

Outro objetivo deve considerar o desenvolvimento de ferramenta e sistema de gerenciamento de segurança cibernética para identificar, prevenir, tratar e responder de forma adequada aos incidentes de segurança (intencionais ou não) dentro da infraestrutura crítica de informação. Esse trabalho deve também considerar questões como privacidade, legislação e regulamentos, e tem a necessidade de ser executado em estreita cooperação com todos os atores, governo, iniciativa privada e sociedade.

Nesse contexto, ficam claras a necessidade e a importância de se formular uma estratégia nacional para proteção da infraestrutura crítica de informação e defesa cibernética, a qual defina os objetivos a serem perseguidos, as políticas a serem implementadas, os órgãos de governo a serem engajados e as atribuições e responsabilidades de seus executores.

Objetivos

Os principais objetivos de uma estratégia de proteção da infraestrutura crítica de informação são:

- Garantir que a infraestrutura crítica de informação funcione adequadamente a despeito da ocorrência de incidentes como fenômenos naturais, erros humanos ou ataques maliciosos.
- Evitar a ocorrência de incidentes que possam afetar a operação da infraestrutura crítica de informação.
- Sobrevindo tais incidentes, minimizar seu impacto na infraestrutura crítica de informação e em outras infraestruturas críticas.

Ações

Com foco nos objetivos mencionados, propõem-se as seguintes ações:

- Identificar a infraestrutura crítica de informação
    - Identificar os elementos (chave) que compõem a parte crítica da infraestrutura de informação.

- Priorizar os elementos da infraestrutura crítica de informação
  - Atribuir prioridade aos elementos mais críticos identificados, a fim de permitir uma alocação mais eficiente dos recursos disponíveis.

- Definir informações necessárias à supervisão
  - Definir e estabelecer indicadores e métricas para supervisão e controle da infraestrutura crítica de informação.

- Identificar e avaliar e riscos
  - Identificar ameaças.
  - Identificar vulnerabilidades.
  - Estimar impactos.
  - Implementar controles.
  - Monitorar controles.
  - Comunicar eventos.

- Prevenir a ocorrência de incidentes
  - Tomar ações pró-ativas que reduzam a ocorrência de incidentes que afetem a infraestrutura crítica de informação ou outras infraestruturas críticas.

- Definir normas e padrões aplicáveis
  - Estabelecer as normas e padrões a serem seguidos na definição de políticas, implantação de controles, realização de auditorias, homologação ou certificação de sistemas e produtos etc.

- Homologar ou certificar sistemas e produtos
  - Garantir que os sistemas e produtos utilizados obedeçam a padrões de segurança mínimos.

- Identificar instrumentos legais necessários (existentes ou não)
  - Analisar e inventariar leis, decretos, portarias etc. necessários para o tratamento jurídico de incidentes (para atribuição de responsabilidades, criminalização de condutas etc.).

- Detectar a ocorrência de incidentes e prover respostas adequadas
  - Identificar, registrar e avaliar incidentes.
  - Informar, avisar e alertar.
  - Responder adequadamente a incidentes.

- Recuperar ambiente operacional.
- Identificar instrumentos legais necessários.
- Definir normas e padrões aplicáveis.

Fatores críticos

Para que a estratégia seja bem-sucedida, é necessário observar ao menos os seguintes fatores críticos:

- Coordenação nacional
  - A importância para a nação das diversas infraestruturas críticas demanda a formulação de uma estratégia nacional de proteção da infraestrutura crítica de informação integrada.

- Mobilização de outros setores
  - Os órgãos de governo responsáveis pelas infraestruturas críticas devem criar e executar estratégias de proteção específicas e, considerando a interdependência entre as diversas infraestruturas críticas, devem atuar de forma coordenada entre si, trocando ferramentas, informações e experiências. A utilização de recursos de fundos setoriais pode contornar dificuldades burocráticas e agilizar o início do processo.

- Cooperação público-privada
  - Dada sua complexidade, a proteção da infraestrutura crítica de informação requer que órgãos de governo, empresas do setor privado e organizações do terceiro setor trabalhem de forma coordenada, harmônica e cooperativa.

- Formação de competências
  - A proteção da infraestrutura crítica de informação demanda profissionais altamente especializados de diversas áreas, fator que deve ser contemplado com a inclusão do tema proteção de infraestruturas críticas em programas de graduação já existentes e com a criação de programas de pós-graduação sobre o assunto, fomentando atividades de P&D e contribuindo para o estabelecimento de uma comunidade acadêmica nacional interessada em proteção de infraestruturas críticas.

- Cooperação internacional
    - A interconexão entre a infraestrutura crítica de informação de diferentes países faz que nenhum país possa proteger sua própria infraestrutura de forma isolada, tornando imperativa a cooperação internacional para permitir o intercâmbio de experiências e a troca de informações, em situações de crise ou não.

- Conscientização da sociedade
    - A proteção da infraestrutura crítica de informação não é tarefa apenas de governos e empresas, mas também da sociedade como um todo. A informatização crescente faz que o cidadão não seja apenas espectador (que pode apenas sofrer as consequências de um eventual incidente), mas sim protagonista, já que suas ações podem contribuir involuntariamente para afetar (positiva ou negativamente) o funcionamento das infraestruturas críticas.

Sistema de segurança e defesa cibernética

É de extrema importância que os sistemas a serem desenvolvidos possuam, ao menos, as características citadas anteriormente, além de uma futura capacidade de monitoramento, de criação de cenários e de simulação que consequentemente fornecem insumos suficientes para a segurança e a proteção do espaço cibernético. Essas funcionalidades previstas no sistema possibilitarão também a geração de subsídios para criação de leis, políticas e normas, além do gerenciamento técnico de todos os aspectos envolvidos com a prevenção, monitoramento e resposta a incidentes (que devem ser realizadas pelos diferentes atores envolvidos) e também da internalização de novos conhecimentos e competências por meio do desenvolvimento de núcleos de excelência e transferência de conhecimentos nas áreas abordadas. Assim, seria factível a capacitação dos centros de P&D, universidades nacionais, bem como do Estado, trazendo, desta forma, melhores condições para o desenvolvimento do país em áreas essenciais para a sociedade e para o próprio governo.

Conforme pode ser observado na Figura 3, esse sistema de segurança e defesa cibernética possibilitará o mapeamento e análise em tempo real da infraestrutura crítica de informação, permitindo a visualização e o gerenciamento dos elementos críticos, de acordo com os níveis de risco e criticidade envolvidos. As funcionalidades de cenários e simulação são essenciais em eventos de grande porte, como a Copa do Mundo de 2014, por exemplo, para que possam ser planejados com a visão dos elementos funda-

mentais para o seu sucesso, o que possibilita prevenção, detecção e resposta de eventos nos diferentes serviços públicos e privados que estabelecem a infraestrutura crítica de informação e são essenciais para a realização com sucesso do evento.

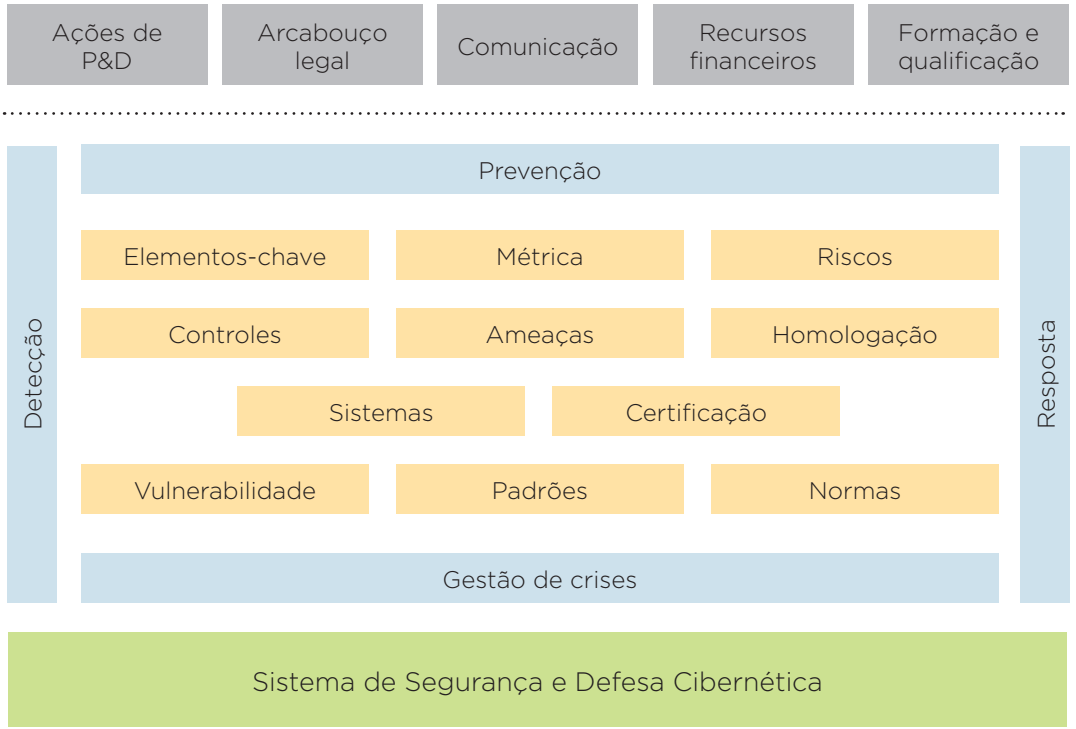

Figura 3 – Sistema de segurança e defesa cibernética
Fonte: Elaboração do autor.

O sistema fornece também insumos e subsídios suficientemente fortes para que o planejamento de marcos regulatórios seja realizado, favorecido pela visão holística da interdependência existente entre diferentes infraestruturas críticas.

Assim, é de suma importância a elaboração de uma estratégia e de um sistema que apóiem e direcionem decisões para a proteção da infraestrutura crítica de informação e da defesa cibernética nacional.

Conclusão

Não deve ser motivo de surpresa que vários países – acompanhados por organizações internacionais como International Communication Union-D (ITU), Organização para Cooperação e Desenvolvimento Econômico (OCDE), Grupo dos Oito etc. – já tenham tomado iniciativas com relação à proteção de suas infraestruturas críticas de informação, que são essenciais para a operação de outras infraestruturas críticas (energia, transporte, água etc). Além disso, o tema é universalmente reconhecido como um componente essencial da política de segurança nacional.

Com essa visão, esses países definiram necessidades de curto prazo apoiados em planos de longo prazo, criando órgãos de governo específicos para tratar do tema, definindo estratégias e implantando sistemas de proteção sofisticados e abrangentes. Tais programas buscam contemplar diferentes aspectos da proteção da infraestrutura crítica de informação, tratando desde a redução de vulnerabilidades até a luta contra a criminalidade cibernética até a defesa contra o ciberterrorismo.

É fácil constatar que a dependência de cidadãos, empresas e governos em relação aos serviços oferecidos por tais infraestruturas críticas é tanto maior quanto mais expressivo for o desenvolvimento econômico do país em questão.

A percepção dessa crescente dependência, intensificada pelo aumento da ameaça de atos terroristas, contribuiu decisivamente para que tais iniciativas fossem desencadeadas em curto espaço de tempo.

Esse mesmo desenvolvimento econômico tem resultado, entretanto, na necessidade de vultosos recursos financeiros e tecnológicos para proteger eficientemente tais infraestruturas críticas, bem como a infraestrutura crítica de informação subjacente.

É praticamente considerada um consenso a necessidade da cooperação internacional para a proteção da infraestrutura crítica de informação nacional. Essa atitude é também incentivada pelo fato de o cibercrime e o ciberterrorismo ignorarem as fronteiras geográficas. Outro ponto a destacar é a necessidade da cooperação público-privada, já que partes significativas da infraestrutura crítica de informação são de propriedade de empresas privadas, que são as responsáveis pela operação e gerenciamento.

A proteção da infraestrutura crítica de informação não é somente tarefa para especialistas, mas também diz respeito ao cidadão comum, pois um computador doméstico pode ser utilizado como plataforma de ataques de negação de serviço, por exemplo, caso medidas adequadas de proteção não sejam tomadas. O cidadão também é e deve ser considerado parte integrante da infraestrutura crítica, pois pode ser pessoalmente prejudicado ao usar um serviço como internet *banking* pela presença de um vírus ou por uma mensagem eletrônica de *phishing*. Uma manifestação clara desse entendimento é o relatório "OECD *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*" (OECD, 2010), que busca conscientizar governos, empresas e cidadãos sobre a importância da segurança da informação e, assim, colaborar para a criação de uma cultura a esse respeito.

Num país de dimensões continentais como o Brasil, a infraestrutura crítica de informação possui caráter estratégico diferenciado, pois desempenha papel essencial tanto para a segurança e a soberania nacionais como para a integração cultural e o desenvolvimento econômico. Por essa razão, deve ser um objetivo estratégico e permanente proteger a infraestrutura crítica de informação, a fim de assegurar a continuidade de operação dos serviços considerados essenciais.

A proteção da infraestrutura crítica de informação é uma tarefa difícil, não somente pela complexidade dos sistemas, redes, pessoas e ativos da infraestrutura crítica de informação que fornecem os serviços essenciais em nossas vidas diárias, mas também por causa da grande interdependência com relação a outras infraestruturas críticas (energia, finanças, águas, transporte, comunicações entre outras).

Assim, devem ser conduzidos, no escopo de um direcionamento estratégico que contemple a criação de um centro especializado de referência, o desenvolvimento de metodologias e sistemas, a definição de métricas e indicadores e a cooperação entre os setores público e privado, além da comunidade internacional. Esses elementos devem ser baseados em um arcabouço legal e um marco regulatório consistentes com essas finalidades.

Referências

ABCNews. *WikiLeaks Releases Confidential Diplomat Cables*, 2010. Disponível em: <http://abcnews.go.com/Politics/wikileaks-releases-classified-diplomat-cables-us-state-department/story?id=12260376>. Acesso em: 1 nov. 2010.

DEFENSENews. *Hackers Crack Pentagon F-35*. Data: report, 2009. Disponível em: <2009.http://www.defensenews.com/story.php?i=4048737>. Acesso: 30 nov. 2010.

SANTA CATARINA (Estado). *Defesa Civil*, 2008. Disponível em: <www.defesacivil.sc.gov.br>. Acesso em: 30 nov. 2010.

BRASIL. Portaria n. 2, de 8 de fevereiro de 2008, art. 2 e 3. *Diário Oficial da União*, n. 27. Gabinete de Segurança Institucional, Brasília, DF, 11 fev. 2008. Seção 1, Ano CXLV.

BULEY, Taylor; GEENBER, Andy. *Google China Hackers' Unexpected Backdoor*, 2010. Disponível em: <http://www.forbes.com/2010/01/14/google-china-mcafee-technology-cio-network-hackers.html>. Acesso em: 30 nov. 2010.

International Communication Union-D. *Generic National Framework For Critical Information Infrastructure Protection,* 2010. Disponível em: <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf>. Acesso em: 2 dez. 2010.

LEWIS, T. G. *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*. Hoboken, John Wiley & Sons, Inc., 2006. 474 p.

NEUMANN, Peter G. *Computer-Related Risks,* Addison-Wesley, 1995. 384p.

NATIONAL Institute of Standards and Technology. *NIST and the World Trade Center*, 2001. Disponível em:<http://wtc.nist.gov/>. Acesso em: 1 dez. 2010.

NOAA. *Hurricane Katrina - Most destructive hurricane ever to strike the U.S.*, 2005. Disponível em: <http://www.katrina.noaa.gov>. Acessado em: 1 dez. 2010.

RIBEIRO, Sérgio Luís; FRANCO, João Henrique de Augustinis; SUIAMA, Danilo Yoshio. *Contextualização e estratégia para a proteção de infra-estrutura crítica*, fev. 2008. Projeto Funttel "Proteção de Infra-estrutura Crítica de Telecomunicações (PICT)". PD.30.11.67A.0058A-RT.01.AC. Campinas: CPqD, 2008. 56 p. (Relatório técnico; cliente: Anatel).

ORGANISATION for Economic Co-operation and Development. *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*. 2002. http://www.oecd.org. Acesso em: 6 dez. 2010.

SCHNEIER, Bruce. *"Cyberwar" in Estonia,* 2007. Disponível em: <http://www.schneier.com/blog/archives/2007/08/cyberwar_in_est.html>. Acesso em: 30 nov. 2010.

WASHINGTON POST. *Ahmadinejad: Iran's nuclear program hit by sabotage*. Disponível em: <http://www.washingtonpost.com/wp-dyn/content/article/2010/11/29/AR2010112903468.html>. Aceso em: 30 nov. 2010.

WIKILEAKS. Disponível em: <http://wikileaks.ch/mirrors.html>. Acesso em: 2 dez. 2010.

USO DE REDES SOCIOTÉCNICAS PARA A SEGURANÇA CIBERNÉTICA NACIONAL

*José Eduardo Malta de Sá Brandão**

Resumo

Este artigo apresenta algumas propostas de estratégia para a formação de redes sociotécnicas em segurança cibernética, com o objetivo de enfrentar os desafios para a definição de políticas e a criação e implantação de um Sistema de Segurança e Defesa Cibernética Nacional. Para isso, foi realizado um estudo sobre a situação da pesquisa em segurança da informação e de sistemas computacionais no Brasil, mapeando os principais grupos de pesquisa e suas linhas de atuação. Tal estudo deve servir de base para a identificação e o desenvolvimento de competências no setor, para a formação das redes.

Palavras-chave: segurança cibernética, defesa cibernética, segurança da informação, rede sociotécnica.

* Possui doutorado em Engenharia Elétrica pela Universidade Federal de Santa Catarina (2007), mestrado em Ciência da Computação pela Universidade Federal da Paraíba (1996) e bacharelado em Estatística pela Universidade de Brasília (1990). Atualmente é pesquisador do Instituto de Pesquisa Econômica Aplicada (Ipea) na área de informática, no Distrito Federal. Tem experiência acadêmica em cursos de graduação e pós-graduação e extensa experiência profissional na área de Ciência da Computação, atuando principalmente nos seguintes temas: gerenciamento de redes, sistemas distribuídos e segurança. O foco atual de suas pesquisas científicas está na segurança de sistemas computacionais.

Introdução

O termo *infraestrutura* referia-se originalmente às redes físicas que suportavam o funcionamento das cidades e incluíam estradas, água, esgoto, cabos de energia e linhas de telecomunicações. O conceito atual de infraestruturas críticas ultrapassa a noção física, envolvendo estruturas para interconexões e funções que permitem que a sociedade possa sobreviver e prosperar, incluindo a informação.

As infraestruturas críticas da informação são vitais para os Estados. A incapacidade ou a destruição de tais ativos, sistemas ou redes teria um impacto debilitante na segurança nacional, na economia nacional, na saúde e na segurança pública ou em qualquer combinação desses elementos (MILLER; LACHOW, 2008).

Os ativos de informação estão todo o tempo sob a ameaça de violação de sua integridade, disponibilidade e confidencialidade. Essas ameaças podem vir na forma de desastres naturais, acidentes normais ou ataques deliberados (ibid.).

Devido à carência de recursos humanos capacitados, o Estado sozinho não conseguirá assegurar a segurança das infraestruturas críticas de informação. Por isso, este artigo propõe algumas alternativas estratégicas, que envolvem: a busca pela multidisciplinaridade; o incentivo à formação de redes sociotécnicas com objetivos específicos; o fomento à pesquisa temática; e a formação acadêmica e profissional.

A seção seguinte deste documento visa contextualizar os temas tratados no texto. A Seção 3 apresenta uma análise da situação da pesquisa cibernética no Brasil. Na quarta seção, são apresentadas propostas para a criação e a manutenção das redes sociotécnicas em segurança cibernética. A quinta seção propõe algumas estratégias para a segurança cibernética envolvendo as redes. Finalmente, na última seção, são apresentadas as conclusões do documento.

Contextualização

Conceitos iniciais

Neste artigo, adotamos os conceitos de Infraestruturas Críticas da Informação e de Ativos de Informação definidos pelo Grupo de Trabalho de Segurança das Infraestruturas Críticas da Informação (GT-SICI), instituído pela Portaria nº 34 CDN/SE, de 5/8/2009, no âmbito do Comitê Gestor de Segurança da Informação (CGSI).

As Infraestruturas Críticas da Informação são "o subconjunto de ativos de informação que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade".

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

São consideradas prioritárias as áreas definidas nos incisos de I a V do art. 3º da Portaria nº 2, do Gabinete de Segurança Institucional da Presidência da República, de 8 de fevereiro de 2008: energia, transporte, água, telecomunicações e finanças.

A expressão *segurança cibernética*, no contexto deste documento, envolve as áreas de segurança das infraestruturas críticas de informação.

Estratégias tradicionais de segurança

Segundo Miller e Lachow (2008), as estratégias de segurança das infraestruturas críticas envolvem: prevenção e proteção; resiliência; e dissuasão. A prevenção e a proteção incluem todas as ações que envolvem tanto para prevenir a ocorrência de um incidente, quanto para minimizar o seu impacto. A história demonstra que falhas de infraestrutura são inevitáveis. Por isso, os sistemas críticos devem incorporar o conceito de resiliência, pelo qual um sistema deve continuar operando sob pressão ou condições adversas. Apesar de a dissuasão ser considerada uma medida de prevenção, ela deve incorporar a capacidade de retaliação a fim de coagir os adversários contra ataques aos ativos do Estado.

Os métodos de segurança citados não são novidade. Porém, os processos, os mecanismos e as técnicas utilizados para implementá-los devem evoluir constantemente, acompanhando as ameaças potenciais. Essa evolução torna imprescindível o investimento constante em pesquisa e capacitação de recursos humanos.

Redes sociotécnicas

Segundo Law (1992), a ciência não é diferente de outras instituições. Assim o que é verdadeiro para a ciência também é para outras instituições. Dessa forma, as construções científicas também podem ser adotadas por outros elementos sociais, como o Estado.

A teoria das redes sociotécnicas sugere que a evolução simultânea da sociedade, dos artefatos tecnológicos e do conhecimento da natureza deve ser estudada a partir de três conceitos: tradução, ator-mundo e rede (LATOUR, 1994, 2000; CALLON, 1986).

Para Law (1992), as *redes* sociotécnicas são formadas por elementos humanos e inumanos. Assim, no escopo da segurança cibernética, elas podem ser compostas por pessoas, instituições, equipamentos, *softwares* e pelo próprio conhecimento.

O conceito de *tradução* permite entender como as relações são estabelecidas, como se expandem e como são mantidas. Essa se realiza quando, em determinada situação, um ator consegue produzir uma nova interpretação dos seus interesses e divulgá-la para outros, convencendo-os de sua visão, isto é, consegue construir uma versão e impô-la à sociedade. Assim, traduzir (ou trasladar) significa deslocar objetivos, interesses, dispositivos e seres humanos. Implica a invenção de um elo antes inexistente e que de alguma forma modifica os elementos imbricados. As cadeias de tradução referem-se ao trabalho pelo qual os atores modificam, deslocam e trasladam os seus vários e contraditórios interesses.

O *ator-mundo*, ou ator iniciador, é aquele que inicia a construção de uma rede. Ele busca ligar-se a entidades heterogêneas, especificando a sua identidade, seu espaço dentro da rede, o tipo de laço que os une, o seu tamanho e a história de que eles vão fazer parte (LATOUR, 2000). O ator-mundo é

então quem faz as associações e as ligações de um objeto técnico ou de um conhecimento científico aos demais componentes da rede.

Ainda com relação à *rede*, Latour (2000) afirma que o número de atores envolvidos na construção dos fatos científicos não se limita aos cientistas que estão em laboratório, a quantidade de atores que participam da rede é bem maior. Os trabalhos dos cientistas em laboratório parecem alcançar sucesso, quando outros atores prepararam o terreno. Por isso, para se compreender a construção da rede, é necessário acompanhar um número muito maior de atores do que aqueles que estão fazendo ciência em laboratório.

A aplicação e o estudo das redes sociotécnicas na área de segurança cibernética permitiriam ao Estado incentivar a formação dessas redes estratégicas e assumir o papel de ator-mundo delas.

O acompanhamento das redes sociotécnicas pelo Estado implica conhecer não somente os artefatos gerados, mas, segundo Latour (2000), "como fatos e artefatos são modificados pelos atores, não sendo apenas transmitido de um ator a outro, mas também coletivamente composto pelos atores".

Recursos humanos e gestão

Segundo Kalil e Irons (2007), o apoio do governo às pesquisas na universidade ajuda a criar e a ampliar a força de trabalho com competências especializadas. A criação dessa força de trabalho pode ser fundamental para o desenvolvimento de políticas específicas.

Após detectar que não seria capaz de recrutar pessoas com as habilidades necessárias em segurança cibernética, o governo norte-americano buscou aumentar o número de alunos de graduação e pós-graduação com experiência no setor. Um dos mecanismos encontrados para o fomento da pesquisa e a capacitação no setor foi a criação de um programa governamental específico, o Federal Cyber Service: Scholarship for Service (SFS)[1], que distribui "bolsas de serviço" para estudantes de graduação e pós-graduação na área de segurança da informação e segurança computacional.

[1] Mais informações em: <https://www.sfs.opm.gov/>.

No Brasil, o Gabinete de Segurança Institucional da Presidência da República, por meio do Departamento de Segurança da Informação e Comunicações, vem promovendo o curso de formação de gestores de segurança (FERNANDES, 2010). Foram capacitados 35 alunos no curso 2007-2008, e cerca de 180 estão realizando o curso no momento. Essa quantidade de gestores ainda é ínfima diante da demanda do próprio governo, que possui aproximadamente 6 mil entidades públicas e 320 redes de governo[2].

Levando-se em conta somente a legislação, seria necessária em cada entidade pública a presença de um gestor. Em um cenário simples, cada entidade precisaria ainda de, pelo menos, dois analistas de segurança para auxiliar no planejamento e na execução das atividades mínimas, que envolvem a política de segurança, a gestão de riscos, a continuidade do negócio, o tratamento e a resposta a incidentes. Portanto, há no momento uma demanda de 6 mil gestores e de 12 mil técnicos em segurança cibernética. Isso significa capacitar cerca de 2% de toda a força de trabalho dos 927 mil servidores públicos federais.

Mantendo a velocidade atual de formação de 180 gestores a cada dois anos, levaríamos quase 70 anos para formar somente este perfil profissional para atender apenas à demanda atual.

Para completar a situação, não há carreira específica de analistas em segurança cibernética, incentivos financeiros aos gestores em SIC nos órgãos públicos nem orçamento específico para a segurança cibernética nos órgãos de governo (MANDARINO JUNIOR; CANOGIA, 2010).

Fomento à pesquisa e ao desenvolvimento

O Brasil possui programas genéricos de distribuição de bolsas de pesquisa promovidos pela Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (Capes), vinculada ao Ministério da Educação, e pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), vinculado ao Ministério da Ciência e Tecnologia.

[2] Informações contidas na palestra proferida por Eduardo Wallier Vianna, no 16º seminário RNP de capacitação e inovação – SCI. Disponível em: <http://www.rnp.br/capacitacao/sci/2010/programa.php?apresentacao=576>.

Os programas de fomento específicos são promovidos pela Financiadora de Estudos e Projetos (Finep)[3], no âmbito do governo federal. Essa empresa pública, vinculada ao Ministério da Ciência e Tecnologia, atua na cadeia da inovação com foco em ações estratégicas, estruturantes e de impacto para o desenvolvimento sustentável do Brasil.

As empresas e as instituições públicas e privadas de ensino e pesquisa podem utilizar os recursos públicos para o desenvolvimento de pesquisa científica ou tecnológica ou de inovação. Os financiamentos são concedidos por meio de concorrências públicas divulgadas em editais dos fundos setoriais.

Entre os fundos setoriais da instituição está o CT-Info, que estimula as empresas nacionais a desenvolver e produzir bens e serviços de informática e de automação, investindo em atividades de pesquisa científicas e tecnológicas.

Outro fundo de financiamento importante é o Funtel, que está sob a gestão do Ministério das Comunicações. O objetivo do fundo é estimular o processo de inovação tecnológica, incentivar a capacitação de recursos humanos, fomentar a geração de empregos e promover o acesso de pequenas e médias empresas a recursos de capital, para ampliar a competitividade da indústria brasileira de telecomunicações.

Outros fundos também atuam diretamente no fomento das infraestruturas críticas definidas na Portaria nº 34 do CDN/SE e de outras áreas consideradas estratégicas: os fundos de transporte CT-Aero, CT-Aqua e CT-Transportes, para os setores aeronáutico, aquaviário e de logística, respectivamente; o CT-Energ e o CT-Petro, para as área de energia, petróleo e gás natural; e o CT-Hidro, para a área de recursos hídricos.

Além dos fundos setoriais, foram definidas, em 2004, as ações transversais, que são programas estratégicos do Ministério da Ciência e Tecnologia (MCT), que têm ênfase na Política Industrial, Tecnológica e de Comércio Exterior (Pitce) do governo federal e utilizam recursos de diversos fundos setoriais simultaneamente.

[3] Mais informações em: <http://www.finep.gov.br>.

Pelo menos duas experiências de políticas públicas de fomento com enfoques específicos são referência na formação de redes sociotécnicas: o Programa Nacional de Educação na Reforma Agrária (Pronera) e a TV digital brasileira.

No caso do Pronera, o Estado fomenta a formação básica e a capacitação técnica nos assentamentos da reforma agrária (FREITAS, 2008). As universidades, as escolas municipais, as instituições de extensão rural, as organizações não governamentais e os movimentos sociais formam redes sociotécnicas.

Para a discussão e a criação do Sistema Brasileiro de TV Digital (SBTVD), a Finep direcionou, com sucesso, investimentos na pesquisa e no desenvolvimento de processos, tecnologias e produtos para um segmento específico (ROCHA, 2007).

Rede Nacional de Segurança da Informação e Criptografia

Por meio da Portaria nº 31, de 6 de outubro de 2008, o Gabinete de Segurança Institucional da Presidência da República instituiu a Rede Nacional de Segurança da Informação e Criptografia (Renasic)[4].

O principal objetivo da Renasic é elevar a competência brasileira em SIC, buscando a integração entre as pesquisas que ocorrem nas universidades, nos institutos de pesquisa, nos órgãos governamentais e nas empresas.

Essa é uma primeira experiência na formação de uma rede sociotécnica com enfoque em segurança cibernética. Apesar de ter sido criada há mais de dois anos, com duração prevista de quatro anos, são poucos os produtos gerados. A falta de recursos é o principal entrave.

O acompanhamento dessa rede pode servir de aprendizado para a formação de outras redes.

[4] Mais informações em: <https://wiki.planalto.gov.br/comsic/bin/view/ComSic/RENASIC>.

Um perfil da pesquisa em segurança cibernética no Brasil

Um dos passos iniciais para o desenvolvimento do setor é conhecer melhor a situação da pesquisa e do desenvolvimento tecnológico da segurança cibernética no Brasil. Esse conhecimento permite identificar e acionar potenciais atores sociais para a formação de redes sociotécnicas em segurança cibernética.

Para obter um panorama inicial da situação da pesquisa em segurança cibernética no Brasil, foi elaborado um questionário com 11 perguntas que buscavam identificar os principais pesquisadores, a sua formação acadêmica, o tipo de pesquisa e a atuação dos pesquisadores, os grupos, as linhas e as instituições de pesquisa.

O questionário foi aplicado pela internet, de forma *on-line*, no período de 23 de novembro a 31 de dezembro de 2010. Sua divulgação ocorreu por meio das listas de discussão mantidas pela Sociedade Brasileira de Computação (SBC), para um grupo selecionado de 70 pesquisadores que atuam, ou atuaram nos últimos anos, em segurança da informação e de sistemas computacionais no Brasil. Também foi solicitada a divulgação do questionário a outros grupos que atuam no setor.

Essa pesquisa preliminar obteve 109 respostas e reflete parcialmente a situação atual da pesquisa em segurança cibernética no Brasil, cujos resultados serão apresentados e analisados a seguir.

Perfil dos pesquisadores

A pesquisa permitiu que os entrevistados classificassem sua atuação profissional em uma ou mais áreas: líder de grupo de pesquisa, pesquisador, profissional, professor, estudante, empresário e interessado no assunto.

Do grupo pesquisado, 62,4% são líderes de grupos de pesquisa ou se consideram pesquisadores em segurança da informação ou de sistemas computacionais. Entre esses, 51,4% são líderes de grupos de pesquisa, correspondendo a 32,1% do total pesquisado. A grande quantidade de líderes de pesquisa pode ser um indício de que os grupos de pesquisa no País ainda são muito pequenos.

Daqueles que não se consideram pesquisadores, 12,8% atuam como professores, 13,8% são estudantes, 2,8% são empresários e 8,3% se dizem profissionais, conforme ilustra a Figura 1.

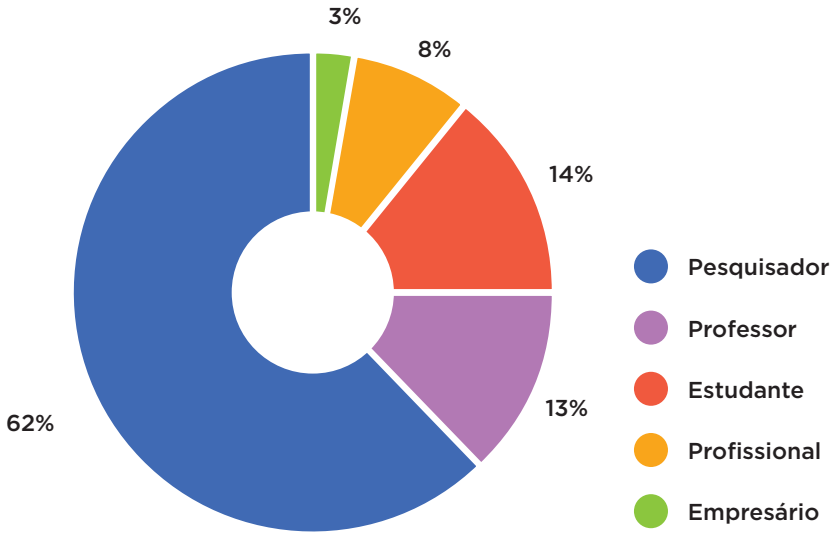

Figura 1 - Distribuição por área de atuação profissional
Fonte: Elaboração do autor.

Locais de pesquisa

Os pesquisadores que responderam ao questionário indicaram o estado federativo em que atuam no País ou se atuam no exterior. Desses, 4,6% estão atuando no exterior, enquanto os demais 95,4% estão distribuídos em 16 estados da Federação, conforme ilustra a Figura 2.

Os pesquisadores que atuam no exterior trabalham principalmente em instituições de ensino ou de pesquisa no Uruguai, no Canadá, na Grã-Bretanha, em Israel, no Peru e em Portugal.

Além dos estados que aparecem na Figura 2, também foram identificados pesquisadores em outros quatro estados: Amazonas, Pernambuco, Rio Gande do Norte e Sergipe, porém não responderam ao questionário.

A atuação em segurança cibernética não é distribuída uniformemente no País. A maior concentração de pesquisadores está no Estado de São Paulo, que tem quase um quarto do total, seguido pelo Paraná, pelo Rio Grande do Sul e por Santa Catarina. A Região Sul concentra mais de 40% dos pesquisadores, superando a Região Sudeste. No Centro-Oeste, o Distrito Federal também se destacou, com 9% do total.

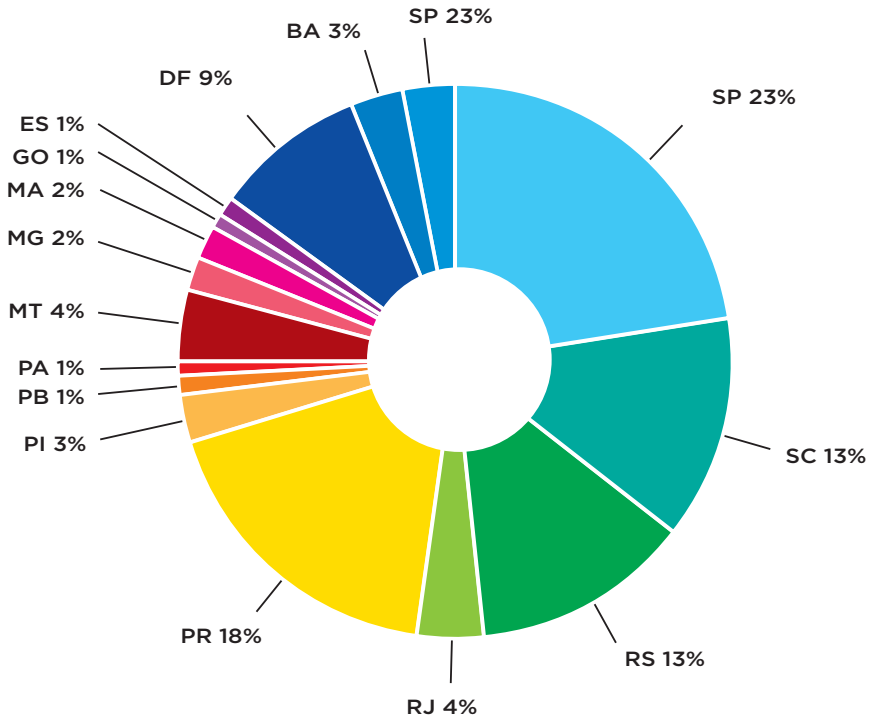

Figura 2 - Locais de atuação dos pesquisadores
Fonte: Elaboração do autor.

Os pesquisadores atuam em 66 instituições distintas, do Brasil e do exterior. A maioria dos pesquisadores, 73%, atua em instituições públicas de ensino ou de pesquisa, 23% estão em instituições privadas no Brasil e 4% atuam no exterior, conforme a distribuição na Figura 3.

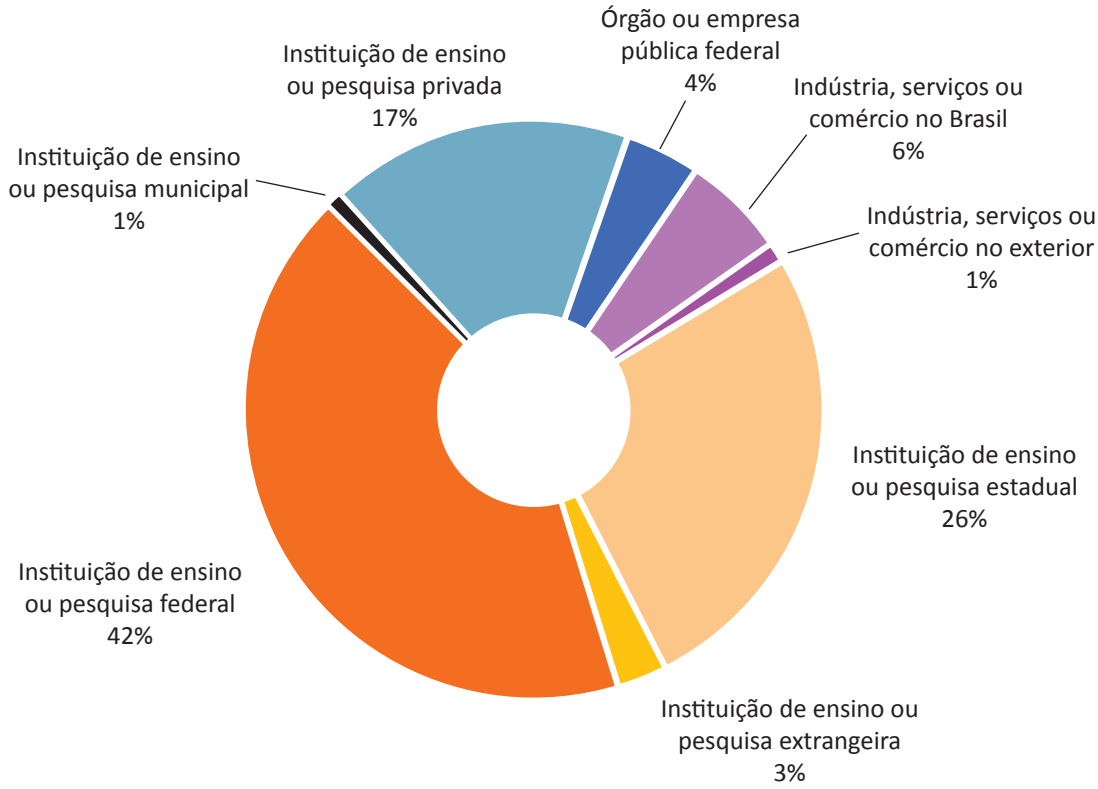

Figura 3 - Distribuição da atuação nas instituições
Fonte: Elaboração do autor.

Quanto à formação acadêmica, a Figura 4 apresenta uma distribuição com 65,6% dos pesquisadores com formação de pós-graduação *stricto sensu*. Outros 19,6% dos entrevistados já concluíram cursos de especialização. Essa distribuição indica alta capacitação das pessoas que atuam na área.

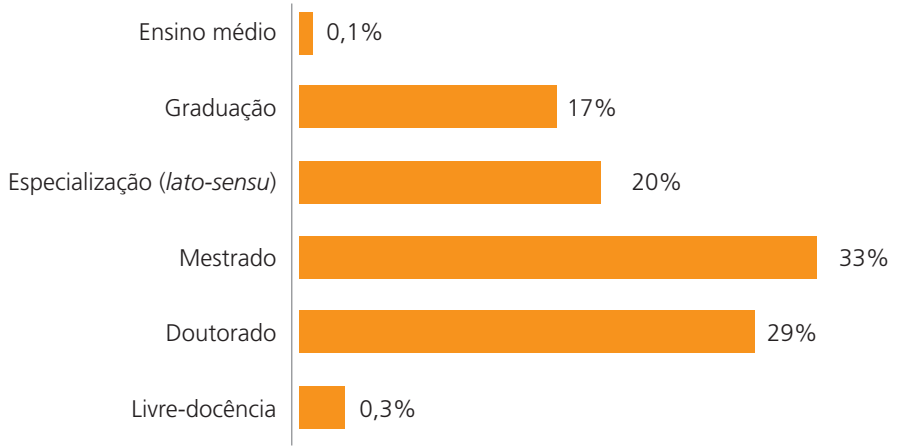

Figura 4 - Distribuição da formação acadêmica dos pesquisadores
Fonte: Elaboração do autor.

Linhas de pesquisa

A relação de linhas de pesquisa foi baseada na classificação adotada pela Comissão Especial em Segurança da Informação e de Sistemas Computacionais da Sociedade Brasileira de Computação[5], para a identificação dos artigos científicos do Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg).[6]

[5] Mais informações em: <http://labcom.inf.ufrgs.br/ceseg/index.php>.
[6] Mais informações em: <http://labcom.inf.ufrgs.br/ceseg/index.php?option=com_content&task=view&id=48&Itemid=81>.

A lista não é uma unanimidade entre os pesquisadores. Porém, é a única classificação atualmente disponível no Brasil. Foram acrescidas ao formulário outras linhas de pesquisa e os pesquisadores indicaram mais 16 opções.

É desejável a criação de uma nova taxonomia que inclua a identificação de grandes áreas e de subdivisões, permitindo melhor identificação de especialistas e das áreas cobertas por eles.

Os entrevistados tiveram liberdade de selecionar quantas linhas de pesquisa desejassem, de acordo com sua preferência. Cada um indicou, em média, seis opções, nem sempre correlacionadas. Alguns entrevistados chegaram a marcar quase todas as opções disponíveis.

A grande quantidade de linhas de pesquisa selecionadas pelos pesquisadores indica que muitos deles podem estar atuando de forma dispersiva, em áreas nem sempre correlatas. A fim de atender à grande demanda de oportunidades e cobrir as lacunas da falta de pessoal capacitado no setor, os poucos pesquisadores acabam atuando em diferentes áreas.

Por outro lado, esse perfil profissional atenderia às necessidades de multidisciplinaridade desejadas no setor de segurança cibernética, desde que comprovada sua capacidade técnica de autuar em diversas áreas simultaneamente.

Observando a Tabela 1, constata-se que a maior concentração ficou na área de segurança em redes, que foi relacionada por 43% dos entrevistados, seguida por vulnerabilidades, ataques e detecção de intrusões.

Tabela 1 - Atuação dos pesquisadores nas linhas de pesquisa

Linhas de pesquisa	% de pesquisadores atuando
Segurança em redes	43%
Vulnerabilidades, ataques e detecção de intrusões	39%
Políticas de segurança	30%
Segurança em sistemas distribuídos	28%
Segurança em serviços *web*	25%
Auditoria e análise em sistemas	24%
Controle de acesso	21%
Segurança em dispositivos móveis, sistemas embarcados e redes sem fio	21%
Teste e avaliação da segurança	21%
Tolerância a falhas	18%
Tecnologias de *firewall*	17%
Algoritmos e técnicas criptográficas	17%
Segurança em grades computacionais e em nuvem	17%
Segurança em sistemas operacionais	17%
Tolerância a intrusões	16%
Metodologias de gestão de riscos	15%
Padronização e normalização em segurança	15%
Criminalística computacional	14%
Guerra e defesa cibernética	14%
Protocolos de segurança	14%
Autenticação e gerência de identidade	13%
Metodologias de desenvolvimento de sistemas seguros	13%
Segurança em aplicações (TV digital, e-banking, etc.)	11%
Segurança em redes virtuais	11%
Pragas virtuais (desenvolvimento, análise e defesa)	10%
Segurança na internet do futuro	10%
Medidas e sistemas de contingência face a desastres	9%
Segurança em redes P2P e redes de sobreposição	9%
Modelos de confiança	8%
Hardware criptográfico, RFID e cartões inteligentes	7%
Anonimato	6%

Linhas de pesquisa	% de pesquisadores atuando
Gerência de chaves	6%
Metodologias de certificação de sistemas e de *softwares* seguros	6%
Sistemas de confiança	6%
Votação eletrônica	6%
Biometria e sistemas biométricos	6%
Segurança em *middleware* (Java RMI, J2EE, CorbaSec, .Net, etc.)	6%
Segurança adaptativa	5%
Ataques e contramedidas de *hardware*	1%
Autenticidade de dados	1%
Computação de alto desempenho e robótica autônoma	1%
Desenvolvimento ágil	1%
Ecossistemas de negócios e serviços	1%
Informática educativa	1%
Integracão de redes heterogêneas	1%
Métodos formais para segurança	1%
Privacidade	1%
Proteção de propriedade intelectual e DRM	1%
Protocolos de autenticacão	1%
Segurança em sistemas embarcados críticos	1%
Sistema de BI	1%
Sistemas de computação móvel	1%
Sistemas de detecção de intrusos	1%
Smart Grid	1%
SmartCards e certificação digital	1%
Veicular Ad-Hoc Network (Vanet)	1%

Fonte: Elaboração do autor.

Tipos de pesquisas realizadas

Os pesquisadores foram questionados quanto aos tipos de pesquisa que realizavam. Os entrevistados tiveram liberdade de selecionar quantos tipos de pesquisa desejassem, de acordo com sua preferência.

Cerca de 44% dos pesquisadores indicaram atuar em somente um tipo de pesquisa, com predominância na pesquisa aplicada (21%), seguida pela pesquisa teórica (13%) e pelo desenvolvimento de novos produtos, processos e tecnologias voltados ao mercado (7%).

Computando-se todas as respostas, verificou-se, conforme a Figura 5, uma predominância da realização de pesquisa acadêmica aplicada, com 70,6%. A realização de pesquisa acadêmica pura ou básica (teórica) obteve 40,4%.

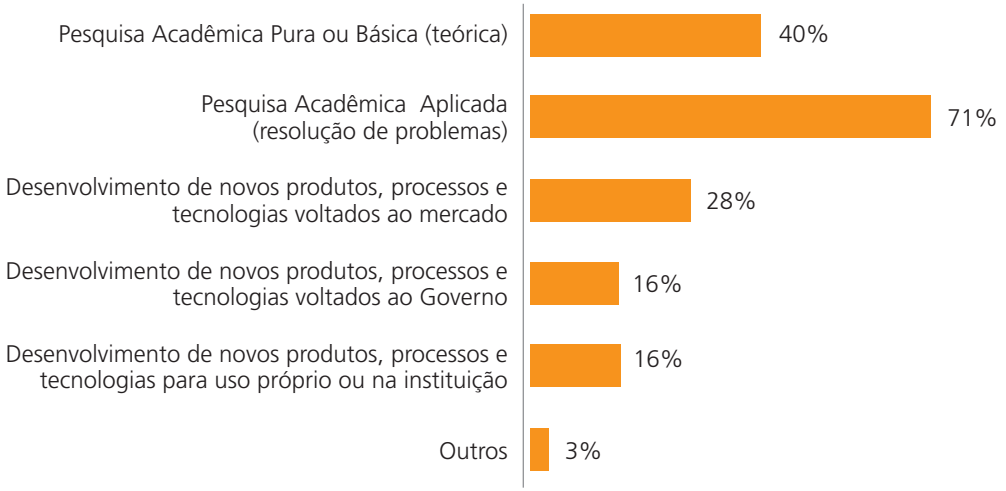

Figura 5 - Tipos de pesquisas conduzidas
Fonte: Elaboração do autor.

Grupos de pesquisa

Os pesquisadores entrevistados fazem parte de 26 grupos de pesquisa no Brasil, distribuídos em 16 instituições. Os pesquisadores também relacionaram sua participação em cinco grupos no exterior, conforme a Tabela 2.

A maioria dos grupos indicados não está registrado formalmente no Diretório de Grupos de Pesquisa[7] mantido pelo CNPq, que deveria conter as informações sobre os grupos de pesquisa em atividade no País.

Grupo de pesquisa	Instituição
CPqD	CPqD
Laboratório de Transferência de Tecnologia	FURB
Instituto Nacional de Ciência e Tecnologia em Sistemas Embarcados Críticos (INCT-SEC)	INCT-SEC
Distributed Systems Research Group	PUC-PR
Laboratório de Direito e Tecnologia	PUC-PR
Senai Santa Catarina	SENAI Santa Catarina
Laboratório de Sistemas Distribuídos	UFBA
Laboratório de Sistemas Distribuídos (LSD)	UFMA
Labsac - Laboratório de Sistemas em Arquiteturas Computacionais	UFMA
Escalabilidade e Eficiência em Sistemas de Computação	UFMG
Núcleo de Redes Sem Fio e Redes Avançadas (NR2)	UFPR
Grupo de Redes de Computadores do Instituto de Informática da Universidade Federal do Rio Grande do Sul.	UFRGS
Distributed Mobile Computing and Network Security	UFSC
Grupo de Pesquisa em Automação e Sistemas (GPAS)	UFSC
Laboratório de Segurança em Computação (Labsec)	UFSC
Grupo de Redes e Gerência	UFSC
GMob - Sistemas de Computação Móvel e Pervasiva	UFSM
Grupo de Linguagens de Programação e Banco de Dados (GLPBD)	UFSM
SEGet - Grupo de pesquisa em Segurança e Gestão da Informação - UFSM	UFSM
Gente - Grupo de Estudos sobre Novas Tecnologias na Educação	UNEMAT

[7] Mais informações em: <http://www.cnpq.br/gpesq/apresentacao.htm>.

Grupo de pesquisa	Instituição
Sistemas Computacionais Avançados	UNESP Bauru
Análise de Algoritmos	Unicamp
LCA	Unicamp
Computação Pervasiva e Alto Desempenho	USP
Laboratório de Segurança de Dados	USP
Laboratório de Arquitetura e Redes de Computadores (Larc)	USP
Garoa Hacker Clube	*Garoa*
iDefense Labs Vulnerability Contribution Program	*iDefense*
Navigators	*Universidade de Lisboa*
Centre for Applied Cryptographic Research (CACR)	*University of Waterloo*
Cloud Security Alliance	*Cloud Security Alliance*

Tabela 2- Grupos de Pesquisa
Fonte: Elaboração do autor.

Estratégias para a formação das redes sociotécnicas

As redes sociotécnicas em segurança cibernética podem ser formadas e mantidas por meio das estratégias definidas a seguir.

O papel do Estado

Propõe-se que o Estado deve assumir o papel de ator-mundo nas redes sociotécnicas em segurança cibernética, incentivando a criação dessas redes e participando ativamente na construção do conhecimento.

A formação das redes, contudo, não se dá sem conflitos. Cabe ao ator-mundo mediar esses conflitos, definindo a temática a ser tratada, traduzindo, analisando, entendendo e respeitando as relações dinâmicas estabelecidas dentro de cada rede.

Criação das redes

As redes sociotécnicas podem ser usadas tanto para as discussões, quanto para a execução das estratégicas de segurança cibernética.

A discussão, a definição clara e a revisão constante das estratégias de segurança cibernética para proteção das infraestruturas críticas fazem parte da construção das redes sociotécnicas em segurança cibernética. A identificação dos atores envolvidos e os temas a serem tratados também devem ser priorizados.

Essas ações permitirão ao Estado acompanhar, analisar e interagir com as redes, porém sem interferir na criatividade e nas soluções apresentadas, mas incentivando a dinâmica das redes focadas nas estratégias nacionais.

Funcionamento das redes

As redes sociais, por meio de ferramentas de colaboração e listas de discussão, vêm prestando enorme auxílio à área de segurança cibernética. Porém, as discussões mantidas nesses fóruns ainda carecem de focos estratégicos.

Em seu documento de desafios, a SBC (2006) argumenta que eventos de *brainstorming* para discutir estratégias são muito raros e propõe a criação de um centro para discussão de pesquisa que incentive tais atividades.

Os encontros e discussões focados em temas específicos tendem a ser mais produtivos, como ocorrem em Dagstuhl[8], na Alemanha, onde os participantes podem ficar imersos por até uma semana para discutir os temas de pesquisa em computação.

As redes sociotécnicas em segurança cibernética podem funcionar tanto de forma virtual quanto presencial, desde que mantidos os temas que unem os atores envolvidos.

[8] Mais informações em: <www.dagstuhl.de>.

Redes dinâmicas

As redes podem ser formadas para auxiliar na resolução de crises e de problemas urgentes. Para isso, é pré-requisito o mapeamento prévio das competências e perfis de pessoas, grupos e instituições que possam ser ativados dinamicamente, quando necessário. Também é preciso o inventário de recursos físicos e tecnológicos que serão usados pelos envolvidos.

O uso de recursos de modelagem e a ativação de processos computacionais dinâmicos podem ser adaptados para a modelagem e a ativação dinâmica das redes. A linguagem BPEL4People (KLOPPMANN et al., 2005), uma extensão da linguagem WS-BPEL (*Web Services Business Processes Execution Language*) (JORDAN; EVDEMON, 2007) para a definição de *web services*, pode ser usada para modelar as redes dinâmicas.

A adoção de ferramentas computacionais para a criação, a ativação e o acompanhamento das atividades das redes sociotécnicas é desejável, mas não deve ser a única opção. Em momentos de crise, por exemplo, nos quais os recursos computacionais podem estar inoperantes, as redes sociotécnicas devem ser montadas e acessadas por qualquer meio de comunicação disponível.

Interação entre redes

Como discutido anteriormente, é necessário promover a multidisciplinaridade na solução dos problemas relacionados à segurança das infraestruturas críticas. As redes sociotécnicas temáticas são uma solução para assuntos específicos. Porém, é preciso identificar os pontos de intersecção entre as redes para que os temas possam ser discutidos de forma mais abrangente e integrada.

Temas que permeiam mais de um assunto devem ser transversais às redes estabelecidas, criando-se redes sobrepostas, que possam contribuir para as questões relacionadas à multidisciplinaridade.

Outro requisito para a formação das redes multidisciplinares é a identificação e o incentivo aos atores que podem ser o ponto de intersecção entre as redes e que terão como missão auxiliar na interação entre os diversos temas que devem ser abordados.

Taxonomia unificada

Conforme verificado durante a pesquisa apresentada na seção "Um perfil da pesquisa em segurança cibernética no Brasil", a identificação dos temas relacionados à segurança cibernética é essencial não só para a pesquisa no setor, mas, também, para a formação e o acompanhamento das redes sociotécnicas.

Uma taxonomia unificada ajudará na identificação de competências e na organização e recuperação do conhecimento gerado pelas redes.

Estratégias em segurança cibernética

Em maio de 2006 a Sociedade Brasileira de Computação produziu um documento listando os principais desafios da computação no Brasil (SBC, 2006). Desde a produção desse documento, pouca coisa mudou no cenário nacional. As propostas apresentadas para superar esses desafios envolvem os seguintes quesitos, que podem ser integralmente transpostos para a área de segurança cibernética e das infraestruturas críticas: multidisciplinariedade; integração com a indústria; transformação da fuga de cérebros em vantagem; e estabelecimento de um centro para discussão de pesquisa.

A seguir são apresentadas algumas propostas que envolvem esses e outros quesitos, visando ao desenvolvimento de ações e de políticas públicas.

As estratégias propostas a seguir devem servir de subsídio para a formação das redes sociotécnicas de segurança cibernética incentivadas pelo Estado.

Incentivo à multidisciplinaridade

A multidisciplinaridade é um quesito identificado também por Mandarino Junior e Canogia (2010), quando reconhecem que há muitos atores de governo envolvidos no desafio político-estratégico da segurança cibernética. Esse quesito também é necessário para identificar e solucionar a questão da

interdependência das infraestruturas críticas identificadas por Canoglia, Gonçalves Júnior e Mandarino Junior (2010).

No quesito multidisciplinaridade, o documento da SBC (2006) prega que se deve "desenvolver modelos de ensino e pesquisa *joint venture* entre áreas, que visem à formação de profissionais e cientistas que possam trabalhar neste novo mundo, com ênfase em multi e interdisciplinaridade". Essa interação não deve ocorrer apenas entre a computação e outros domínios científicos, mas também dentro da computação.

No caso específico das infraestruturas críticas, a multidisciplinaridade envolve, não exaustivamente, conhecimentos dos vários domínios da computação e das diversas áreas de segurança, além de conhecimentos jurídicos e específicos dos setores críticos já citados.

Integração entre governo, universidade e indústria

A necessidade de maior integração das instituições governamentais com a indústria também é tratada como um desafio por Mandarino Junior e Canogia (2010), que verificaram que cerca de 80% dos serviços de rede estão a cargo do setor privado. Também sugerem ajustes na Política de Desenvolvimento Produtivo (PDP) para inserção do setor cibernético e maior integração do setor privado à segurança cibernética do País.

Para a SBC (2006), a pesquisa de boa qualidade reverte-se em benefícios sociais e econômicos e deve ser considerada a aproximação entre a pesquisa e a indústria para efeitos do desenvolvimento tecnológico de qualidade e indicação de novas áreas com o potencial de se transformarem em mercados emergentes.

Apesar de a pesquisa no Brasil propor novas tecnologias de segurança, estas raramente chegam a se tornar produtos que atendam às demandas governamentais ou podem ser adotadas de forma confiável.

A aproximação do governo com a indústria e com os pesquisadores é essencial, para fomentar a transformação das novas tecnologias em produtos específicos que atendam às estratégias de Estado para a segurança cibernética.

Formação de recursos humanos

A formação de recursos humanos na área de segurança cibernética no Brasil ainda é muito lenta, problema esse compartilhado com outras nações. O governo norte-americano saiu à frente na busca de soluções, incentivando financeiramente seus cidadãos a buscar formação em segurança cibernética.

No Brasil, apesar dos recentes esforços governamentais, as ações de capacitação em segurança cibernética ainda são incipientes e isoladas. A formação em massa de mão de obra é uma necessidade urgente. O incentivo à formação acadêmica de graduação e pós-graduação deve ser considerado para o atendimento urgente e fique, pelo menos, em conformidade com a legislação.

Para se enfrentar o desafio da formação de mão de obra em segurança cibernética no Brasil, as políticas públicas devem focar na capacitação de gestores, de técnicos e de novos pesquisadores.

Devem ser consideradas ações urgentes de curto prazo para a capacitação de servidores públicos em médio e longo prazo, visando à formação de mão de obra especializada para atender às demandas do Estado e da sociedade.

A formação de gestores em SIC por uma única instituição de ensino não conseguirá atender a toda a demanda. Com a experiência obtida nos cursos de formação de gestores, já seria possível estruturar uma ementa mínima e estendê-los às instituições que possuam competência acadêmica para ministrá-los.

O fomento ao ensino no curto, médio e longo prazo pode ser feito por meio de programas de cátedras que incentivem a inclusão de disciplinas focadas na segurança cibernética, a criação de novos cursos de graduação e pós-graduação, a distribuição de bolsas de iniciação científica para alunos de graduação e a criação de cursos técnicos de nível médio.

Aproveitamento de cérebros

Ao longo dos anos, técnicos e pesquisadores brasileiros foram atraídos para o exterior. Como pôde ser observado na seção anterior, cerca de 5% dos pesquisadores estão atuando em instituições de pesquisa ou em entidades privadas no exterior. Esses recursos humanos altamente capacitados poderiam ser incentivados a focar suas pesquisas e atividades nas áreas estratégicas do País.

Conforme identificado pela SBC (2006), "(...) eles podem ser usados como contato para aumentar a cooperação em pesquisa do Brasil com o resto do mundo". Esses pesquisadores podem facilitar a integração com instituições, professores e pesquisadores estrangeiros, além de auxiliar na formação de mão-de-obra brasileira no exterior.

Fomento à pesquisa e ao desenvolvimento

Os programas de fomento já existentes nos fundos setoriais da Finep podem ser usados para incentivar a pesquisa e o desenvolvimento de tecnologias de segurança nos setores críticos específicos.

Como a segurança das infraestruturas críticas envolve diversas áreas interdependentes, seria possível criar no âmbito da Finep uma nova ação transversal específica que promovesse a capacitação de recursos humanos, a disseminação do conhecimento, a pesquisa e o desenvolvimento de novos produtos e metodologias de segurança cibernética, abrangendo os diversos setores envolvidos.

Conclusões

Este artigo apresentou uma proposta de uso das redes sociotécnicas como poderosa ferramenta de auxílio na gestão do conhecimento em segurança cibernética voltado principalmente às infraestruturas críticas.

As redes sociotécnicas permitem ao Estado otimizar o uso dos recursos humanos e materiais existentes e a interação entre as diversas áreas de conhecimento envolvidas na segurança das infraestruturas críticas.

No papel de ator-mundo das redes, o Estado pode incentivar a discussão de soluções para os temas estratégicos e interagir com os diversos atores envolvidos em múltiplas redes temáticas.

Com essas redes, também foi proposto um conjunto de ações de políticas públicas específicas para o incentivo e o fomento às atividades de segurança cibernética, envolvendo a criação da cultura de multidisciplinaridade, a formação e o aproveitamento de recursos humanos.

Como parte do processo de formação das redes, foi realizada uma pesquisa visando identificar pesquisadores, suas linhas de pesquisa, a sua formação e atuação e os principais grupos de pesquisa em segurança cibernética.

Referências bibliográficas

CALLON, Michel. The sociology of an actor-network: the case of electric vehicle. In: CALLON, M.; LAW, J.; RIP, A. (Eds.). *Mapping the dynamics of science and technology*. Sociology of science in the real world. London: The Macmillan Press, 1986.

CANONGIA, Cláudia.; GONÇALVES JÚNIOR, Admilson.; MANDARINO JUNIOR, Rafael (Orgs.). *Guia de referência para a segurança das infraestruturas críticas da informação.* Brasília: Gabinete de Segurança Institucional, Departamento de Segurança da Informação e Comunicações, 2010.

FERNANDES, Jorge H. C (Org.). *Gestão da segurança da informação e comunicações*. Brasília: Faculdade de Ciência da Informação/UnB, 2010. v. 1

FREITAS, Helena C. A. In: ARCE, Alberto; BLANCO, Gustavo; HURTADO, Margarita (Orgs.). *Política públicas como objeto social*. Guatemala: Flacso, 2008. v. 1, p. 271-287.

JORDAN, Diane; EVDEMON, John. *Web Services Business Process Execution Language Version 2.0*. OASIS Standard, 2007.

KALIL, Tom; IRONS, John. *A national innovation agenda progressive*: policies for economic growth and opportunity through science and technology. Washington, DC: Center for American Progress, 2007.

KLOPPMANN, Matthias et al. *WS-BPEL Extension for People – BPEL4People*. A Joint White Paper by IBM and SAP, 2005.

LATOUR, Bruno. *Ciência em ação*: como seguir cientistas e engenheiros sociedade afora. São Paulo: Editora Unesp, 2000.

LATOUR, Bruno. *Jamais fomos modernos*: ensaio de antropologia simétrica. Rio de Janeiro: Ed. 34, 1994.

LAW, J. Notes on the theory of the actor network: ordering, strategy and heterogeneity. *Systems Practice,* v. 5, n. 4, p. 379-393, 1992.

MANDARINO JUNIOR, Raphael; CANONGIA, Cláudia. *Livro verde – Segurança cibernética no Brasil.* Brasília: GSI/PR, 2010.

MILLER, Robert A.; LACHOW, Irving. Strategic fragility: infrastructure protection and national security in the Information Age. *Defense Horizons*, Center for Technology and National Security Policy, n. 59, Jan. 2008.

ROCHA, Juliana A. Financiamentos impulsionam tecnologia da TV Digital. *Revista Inovação em Pauta*, Finep, v.1, n.1, 2007.

CONCLUSÃO

CONCLUSÃO

*Otávio Santana do Rêgo Barros **
*e Ulisses de Mesquita Gomes ***

"Não há bons ventos para quem não sabe aonde quer chegar." (Provérbio chinês)

Setor estratégico cibernético

A partir da análise dos artigos elaborados pelos autores, em complemento à Reunião Técnica de Segurança e Defesa Cibernética, os organizadores apresentam, como conclusão, uma proposta para estudo do setor de segurança e defesa cibernética, visando a fundamentar futuras políticas públicas. Ressaltam, ainda, a necessidade de que a Secretaria de Assuntos Estratégicos e o Ministério da Defesa atuem sinergicamente para a concretização de metas de curto prazo que mobilizem o governo e a sociedade para o desafio de proteger o espaço cibernético brasileiro.

* O Coronel Otávio Santana do Rêgo Barros exerce o cargo de Assessor Especial Militar do Ministro de Assuntos Estratégicos da Presidência da República. Na sua carreira militar realizou os cursos da Academia Militar das Agulhas Negras, de Aperfeiçoamento de Oficiais, de Comando e Estado-Maior e o Curso de Altos Estudos de Política e Estratégia da ESG. Desempenhou as seguintes funções: Instrutor da Escola de Sargento das Armas e da Escola de Aperfeiçoamento de Oficiais, integrou a Cooperação Militar Brasileira no Paraguai, Oficial do Gabinete do Comandante do Exército no Centro de Inteligência do Exército e Chefe da Segunda Assessoria do Gabinete do Comandante do Exército. Comandou o 10º Esquadrão de Cavalaria Mecanizado, o 11º Regimento de Cavalaria Mecanizado e o Batalhão de Infantaria de Força de Paz Brasileiro na ONU em Porto Príncipe - HAITI.

** O Tenente Coronel Ulisses de Mesquita Gomes exerce o cargo de Assessor Militar do Ministro de Assuntos Estratégicos da Presidência da República. É bacharel em Direito pela UFMG. Na sua carreira militar realizou os cursos da Academia Militar das Agulhas Negras, de Aperfeiçoamento de Oficiais, de Comando e Estado-Maior e de Preparação de Militares do Exército Brasileiro para Missões de Paz. Desempenhou as seguintes funções: Instrutor do Centro de Preparação de Oficiais da Reserva, Oficial de Planejamento da Missão das Nações Unidas no Haiti e Comandou a Companhia de Comando da Brigada de Infantaria Paraquedista.

Metas de curto prazo (2011 a 2014)

Estão listadas, a seguir, as três metas que devem ser atingidas em curto prazo pelo Governo brasileiro, na visão da Secretaria de Assuntos Estratégicos, com a finalidade de implementar o Setor Estratégico Cibernético no País:

- estabelecer a Política Nacional de Segurança e Defesa Cibernética;
- estabelecer a Estratégia Nacional de Segurança e Defesa Cibernética;[1] e
- estabelecer o Sistema de Segurança e Defesa Cibernética.

Cenário atual

A Estratégia Nacional de Defesa (END) define o setor cibernético, juntamente com os setores nuclear e espacial, como estratégico e essencial para a Defesa Nacional. O que se deseja é que as três Forças, em conjunto, possam atuar em rede, de forma segura, quer para atender às suas especificidades, quer para o emprego em Operações Conjuntas (Op Cj).

Textualmente, a END prevê que:

> As capacitações cibernéticas se destinarão ao mais amplo espectro de usos industriais, educativos e militares. Incluirão como parte prioritária, as tecnologias de comunicação entre todos os contingentes das Forças Armadas de modo a assegurar sua capacidade para atuar em rede. Contemplarão o poder de comunicação entre os contingentes das Forças Armadas e os veículos espaciais. No setor cibernético, será constituída organização encarregada de desenvolver a capacitação cibernética nos campos industrial e militar.

[1] Países como os Estados Unidos da América (EUA), Reino Unido, Japão, Espanha e Austrália, já possuem suas políticas e estratégias nacionais de segurança cibernética (Junior & Canongia, 2010).

> Todas as instâncias do Estado deverão contribuir para o incremento do nível de Segurança Nacional, com particular ênfase sobre as medidas para a segurança das áreas de infraestruturas críticas, incluindo serviços, em especial no que se refere à energia, transporte, água e telecomunicações[2], a cargo dos Ministérios da Defesa, das Minas e Energia, dos Transportes, da Integração Nacional e das Comunicações, e ao trabalho de coordenação, avaliação, monitoramento e redução de riscos, desempenhado pelo Gabinete de Segurança Institucional da Presidência da República.
>
> Nos três setores, as parcerias com outros países e as compras de produtos e serviços no exterior devem ser compatibilizadas com o objetivo de assegurar espectro abrangente de capacitações e de tecnologias sob domínio nacional.
>
> O Ministério da Defesa e as Forças Armadas intensificarão as parcerias estratégicas nas áreas cibernética, espacial e nuclear e o intercâmbio militar com as Forças Armadas das nações amigas, neste caso particularmente com as do entorno estratégico brasileiro e as da Comunidade de Países de Língua Portuguesa e militar (Brasil, 2008).

No Brasil, conforme preconizado no Decreto nº 4.801/2003 e suas atualizações, o Gabinete de Segurança Institucional da Presidência da República (GSI/PR) é responsável pela coordenação das medidas de segurança da informação[3], segurança cibernética e segurança das infraestruturas críticas, a serem tomadas pelos diversos órgãos da Administração Pública Federal (APF).

No âmbito do Ministério da Defesa, atenção especial recai sobre o Exército Brasileiro, responsável por coordenar e integrar as ações atinentes à Defesa Cibernética dentro das Forças Armadas, conforme Diretriz Ministerial nº 0014/2009, de 9 de novembro de 2009.

[2] O GSI/PR introduziu o setor finanças como mais uma área a ser monitorada dentre as infraestruturas críticas.

[3] Segurança da Informação é a proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento (Brasil, 2000).

A formulação de políticas públicas que promovam um robusto sistema de Segurança e Defesa Cibernética para o País requer insumos de todos esses domínios e pode beneficiar-se de iniciativas de cooperação internacional.

É importante conhecer o grau de vulnerabilidade do país com relação aos diversos sistemas e às infraestruturas críticas de informação, bem como conceber um sistema eficaz de medidas preventivas e de respostas contra ataques cibernéticos (Junior & Canongia, 2010).

Destaque-se a importância do estabelecimento de programas de cooperação entre o governo e a sociedade, com apoio da academia, bem como a cooperação com governos e a comunidade internacional, a fim de desenvolver programas de capacitação e a implementar o Sistema de Segurança e Defesa Cibernética Brasileiro (Junior & Canongia, 2010).

Verifica-se na atualidade que a maioria dos países possui uma estrutura similar de Defesa Cibernética. Dentro da visão estratégica desses governos, a Defesa Cibernética está a cargo do Ministério da Defesa, que é responsável pela implantação de um Comando de Defesa Cibernético centralizado. Este coordena como as Forças Armadas devem se equipar, se preparar e empregar seus recursos humanos e materiais para fazerem frente às ameaças que advêm do espaço cibernético (Rêgo Barros & Gomes, Seminário Cyber Warfare, 2011).

Para o Brasil, a estratégia a ser empregada no campo cibernético é a de dispor de um órgão de referência em Segurança e Defesa Cibernética, com recursos humanos dotados de alta competência técnica e parque tecnológico especializado e atualizado (Rêgo Barros & Gomes, Seminário Cyber Warfare, 2011).

Análise do cenário atual

Usando a ferramenta de análise SWOT (*sthrengths, weaknesses, opportunities, threats*) e admitindo como "empresa" o governo federal, os organizadores apresentam a seguir os principais fatores de força, de fraqueza, de ameaça e de oportunidade, tanto no ambiente interno quanto no externo, em relação à implementação do Setor Estratégico Cibernético pelo governo federal.

	POSITIVO	NEGATIVO
INTERNO	A publicação da END	A falta de orçamento específico para a área de Segurança e Defesa Cibernética
	A publicação do PNSIEC	A dificuldade do Governo Federal em coordenar a SIC na APF
	A criação do CTIR.Gov	A ausência de linhas de fomento para desenvolvimento de soluções tecnológicas
	A criação do CDCiber	A ausência de carreira de Estado na área de cibernética
	A Segurança Cibernética incluída nos objetivos da Creden	A falta de integração nos sistemas de proteção das IEC
	A proposta de criação do CDCFA	A necessidade de ajustar o SISBIN para enquadrar o setor cibernético
EXTERNO	O reconhecimento do Brasil como protagonista em vários temas globais	A complexidade nas relações entre Estados
	Os acordos bilaterais de cooperação em segurança da informação com outros países	A falta de clareza sobre a importância da Segurança e Defesa Cibernética para diversos atores
	Excelentes Universidades e Institutos de Pesquisa Nacionais em Segurança da Informação	A inexistência de marco jurídico legal sobre cibernética
	O reconhecimento do Brasil como ator importante no cenário cibernético mundial	A convergência tecnológica facilitando a perpetração de crimes
	As parcerias e as ações colaborativas entre países	O aumento significativo de sistemas de comunicação e de rede e suas interconexões
		A falta de desenvolvimento de uma cultura em Segurança e Defesa Cibernética
		A falta de preocupação do setor privado quanto à Segurança e Defesa Cibernética

Figura 1 - Análise SWOT
Fonte: Elaboração dos autores.

Objetivos a conquistar

Ações políticas

Visando cumprir sua atribuição de promover o planejamento governamental de longo prazo e contribuir para implementação da Estratégia Nacional de Defesa no que tange ao setor cibernético brasileiro, a SAE projeta, no âmbito de sua Assessoria de Defesa, instituir o Comitê Gestor de Atividades de Cibernética e de Tecnologia da Informação (CGCTI).[4]

O comitê será responsável pela elaboração das políticas e estratégias para o setor cibernético e, posteriormente, pelo acompanhamento e atualização desses documentos, em coordenação com os integrantes do comitê e demais usuários da Administração Pública Federal (APF).

O comitê terá como objetivos principais:

- elaborar estudos e prestar subsídios para a preparação de ações dos órgãos da Presidência da República em temas relacionados a atividades de cibernética e de tecnologia da informação; e

- promover a articulação dos órgãos da APF com competência sobre atividades de cibernética e de tecnologia da informação para a discussão e estudo das opções estratégicas do País sobre o tema.

Visualiza-se, ainda, o desencadeamento das seguintes ações:

- conceber um modelo institucional de proteção contra ataques cibernéticos e criar o respectivo marco legal;

- desenvolver programa nacional interdisciplinar de pesquisa em segurança de sistemas de informação, envolvendo recrutamento e capacitação de recursos humanos; e

- estabelecer programas de cooperação entre governo, sociedade civil e comunidade técnica internacional (Junior & Canongia, 2010).

[4] A Exposição de Motivos Interministerial n° 003 - SAE/MP, de 05 de Fevereiro de 2010, enviada à Casa Civil, propõe a criação do CGCTI.

Outra importante ação a ser desencadeada é alterar o Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal, a fim de incluir a Secretaria de Assuntos Estratégicos/PR como integrante do Comitê Gestor de Segurança da Informação (CGSI).

Ações estratégicas e operacionais

Estabelecidos os critérios e as ações por meio do CGCTI, será necessário operacionalizar as seguintes ações:

- criar o Comando de Defesa Cibernética das Forças Armadas (CDCFA), com participação de civis e militares das três Forças Armadas, vinculado ao EMCFA e subordinado ao Exército Brasileiro (Rêgo Barros & Gomes, Seminário Cyber Warfare, 2011);
- assegurar, de forma conjunta, o uso efetivo do espaço cibernético pelas Forças Armadas e impedir ou dificultar a sua utilização contra os interesses da defesa nacional;
- capacitar e gerir recursos humanos necessários à condução das atividades do setor cibernético no âmbito das Forças Armadas;
- colaborar com a produção do conhecimento de inteligência, oriundo da fonte cibernética, de interesse para o Sistema de Inteligência de Defesa (Sinde) e demais órgãos de governo envolvidos na proteção do Estado brasileiro;
- elaborar e manter atualizada a doutrina de emprego das Forças Armadas nas atividades do setor cibernético;
- integrar as estruturas de C&T das três Forças Armadas e as atividades de pesquisa e desenvolvimento para atender às necessidades do setor cibernético; e
- contribuir para a segurança dos ativos de informação da Administração Pública Federal, situados fora do âmbito do Ministério da Defesa, bem como daqueles vinculados às estruturas civis.

Necessidades orçamentárias

Atualmente, quando as possibilidades de estabelecimento de ações na área da segurança e defesa cibernética são analisadas, verifica-se que é prematuro apresentar propostas orçamentárias globais para concretização das metas aludidas anteriormente.

É fato que os atores envolvidos nessa área de segurança e defesa cibernética já estão em movimento, mas cada elemento com foco específico em seus interesses institucionais.

No entanto, a END prevê que, de maneira associada, o Ministério da Defesa, em coordenação com os Ministérios da Fazenda; do Desenvolvimento, Indústria e Comércio Exterior; do Planejamento, Orçamento e Gestão; e da Ciência e Tecnologia com as Forças Armadas deverá:

> Estabelecer ato legal que garanta a alocação, de forma continuada, de recursos financeiros específicos que viabilizem o desenvolvimento integrado e a conclusão de projetos relacionados à Defesa Nacional. (Brasil, 2008)

Necessidades de recursos humanos (RH)

Identificou-se que se deve desenvolver um programa nacional de capacitação em segurança cibernética e de recrutamento, que seja construído a partir da visão interdisciplinar que o tema requer no curto, médio e longo prazos, nos níveis: básico; técnico; de graduação; especialização; mestrado; e doutorado.

Percebe-se, ainda, a imperiosa necessidade de se incluir nos currículos de ensino do País a obrigatoriedade de temas como segurança da informação, segurança cibernética e correlatos.

Por fim, augura-se a possibilidade de formar mais especialistas com conhecimento das tecnologias avançadas na área de cibernética e computação de alto desempenho.

Indústria nacional de produto de defesa

As complexas estruturas tecnológicas que servirão de base para o estabelecimento de uma segura proteção cibernética do País exigem a implementação de programas que desenvolvam a pesquisa e o desenvolvimento, suportados por computadores de alto desempenho. A supercomputação e suas possibilidades são nichos tecnológicos não compartilhados por nações mais poderosas e desenvolvidas.

A Secretaria de Assuntos Estratégicos e o Ministério da Defesa, ao perceberem essa lacuna em nosso esqueleto tecnológico e aproveitando acordo firmado entre o Brasil e a França para cooperação em diversas áreas sensíveis, resolveram promover a instalação de um polo científico na área de supercomputadores.

Por solicitação do governo francês, a parceria em nosso território deverá ser firmada com uma empresa ligada diretamente ao governo brasileiro.

Proposta de modelo institucional

Visão geral do sistema de segurança e defesa cibernética brasileiro

Apresenta-se, a seguir, quadro contendo uma proposta do Sistema de Segurança e Defesa Cibernética Brasileiro nos níveis Político, Estratégico e Operacional, na visão da SAE, o qual representa a estrutura básica necessária para atuar, simultaneamente, nas áreas de segurança e defesa cibernética.

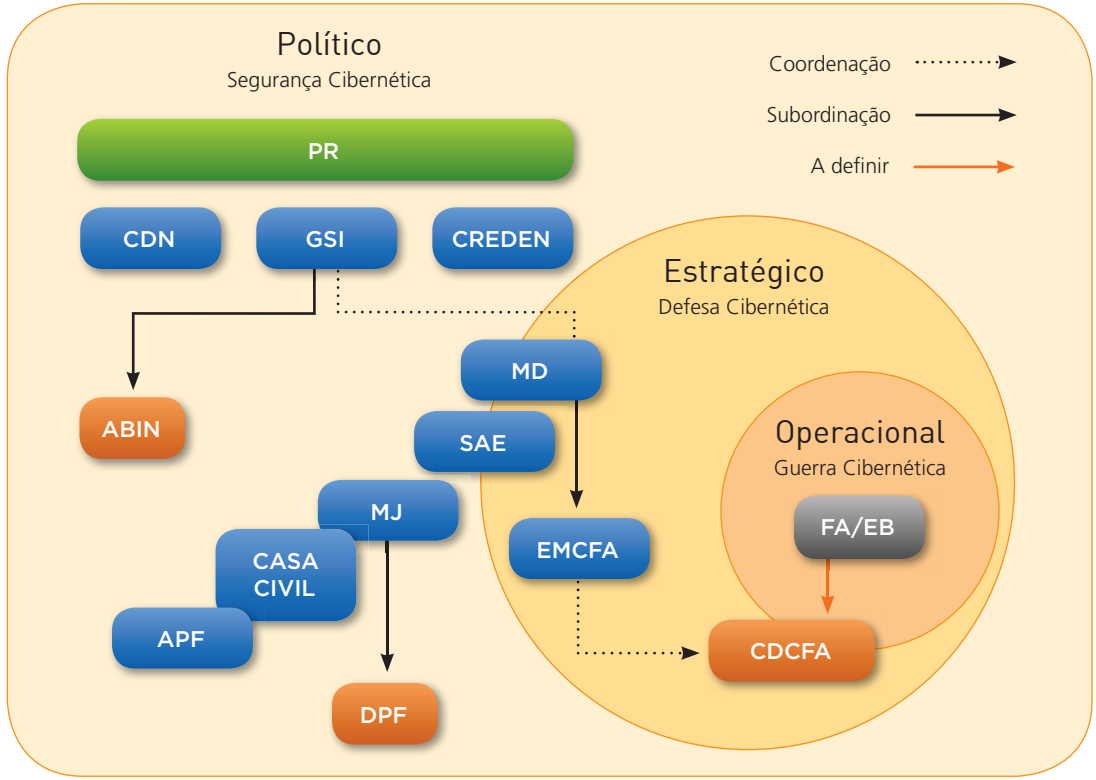

Figura 2 - Sistema de Segurança e Defesa Cibernética Brasileiro
Fonte: Elaboração dos autores.

Observando-se o diagrama, depreende-se que o sistema visualizado terá abrangência nacional e capilaridade desde o mais alto nível político, representado pelo GSI/PR e a APF, passando pelo MD, que realiza a ligação Político-Estratégica, até os mais baixos escalões de comando das Forças Armadas que atuem no nível operacional e tático.

Engajar toda a sociedade na preservação dos interesses nacionais que venham a ser afetados dentro do espaço cibernético é objetivo ambicioso, mas que deve ser perseguido. Sua consecução constitui condição sine qua non para a melhoria da defesa contra ataques cibernéticos dirigidos aos interesses nacionais.

Integrantes do sistema de segurança e defesa cibernética brasileiro

Segurança Cibernética

Conselho de Defesa Nacional (CDN)

O CDN é o órgão de consulta do Presidente da República nos assuntos relacionados à soberania nacional e à defesa do Estado democrático de direito.

Constitui-se em um órgão de Estado, com sua secretaria-executiva sendo exercida pelo ministro-chefe do Gabinete de Segurança Institucional da Presidência da República (GSI/PR). As competências do CDN estão previstas no artigo 91 da CF/88 e a regulamentação de sua organização e de seu funcionamento estão contidas na Lei nº 8.153, de 11 de abril de 1991.

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.

Foi criada pelo Decreto nº 4.801, de 6 de agosto de 2003, e sua presidência cabe ao ministro-chefe do Gabinete de Segurança Institucional da Presidência da República (GSI/PR). Entre suas atribuições, encontram-se a segurança da informação, segurança cibernética e segurança das infraestruturas críticas (Brasil, 2003).

Comitê Gestor de Segurança da Informação (CGSI)

O Decreto nº 3.505, de 13 de junho de 2000, instituiu a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal (APF) e criou o Comitê Gestor de Segurança da Informação. Este tem a atribuição de assessorar a secretaria-executiva do Conselho de Defesa Nacional na consecução das diretrizes da Política de Segurança da Informação, bem como na avaliação e análise de assuntos relativos aos objetivos estabelecidos naquele Decreto.

Gabinete de Segurança Institucional da Presidência da República (GSI/PR)

O GSI/PR é o órgão da Presidência da República encarregado da coordenação, no âmbito da APF, de alguns assuntos estratégicos que afetam a segurança da sociedade e do Estado, quais sejam: Segurança Cibernética, Segurança da Informação e das Comunicações (SIC) e Segurança das Infraestruturas Críticas Nacionais.

No tocante às infraestruturas críticas nacionais, foram selecionadas cinco áreas prioritárias, a saber: energia, telecomunicações, transportes, água e finanças. Avalia-se a inclusão do setor informação, visto que permeia todas as áreas anteriores, pois as infraestruturas críticas dependem cada vez mais de redes de informação para a sua gerência e controle (Carvalho, 2010).

Para o cumprimento da atribuição de coordenar as atividades de Segurança da Informação, o GSI/PR conta, em sua estrutura organizacional, com os seguintes órgãos subordinados:

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.

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.

Departamento de Segurança da Informação e Comunicações (DSIC)

O DSIC tem como atribuição articular as atividades de Segurança da Informação e Comunicações (SIC) na APF nos seguintes aspectos:

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

Secretaria de Acompanhamento e Estudos Institucionais (SAEI)

Dentre as missões atribuídas à SAEI, que podem se enquadrar no campo da segurança cibernética, destacam-se:

- realizar estudos estratégicos, especialmente sobre temas relacionados com a segurança institucional;
- apoiar o ministro de Estado no exercício das atividades da secretaria-executiva do Conselho de Defesa Nacional e da presidência da Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo; e
- apoiar o secretário-executivo nas atividades de coordenação do Comitê da Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo.

Demais grupos coordenados pelo GSI/PR relacionados com a área:

- Grupos de Trabalho de Segurança das Infraestruturas Críticas, nas áreas de energia, telecomunicações, transportes, suprimento de água e finanças;
- Grupo de Trabalho de Segurança das Infraestruturas Críticas da Informação;
- Grupo Técnico de Segurança Cibernética; e
- Grupo Técnico de Criptografia.

Rede Nacional de Segurança da Informação e Criptografia (Renasic)

A Rede Nacional de Segurança da Informação e Criptografia (Renasic) funciona coordenada pela Assessoria de Ciência e Tecnologia do GSI/PR e se constitui numa rede virtual de troca de informações sobre o tema, na qual participam pesquisadores, profissionais de entidades públicas e privadas, do meio acadêmico, e outros interessados nessas atividades. A Renasic tem gerado sinergia na discussão de problemas e soluções práticas de Tecnologia da Informação e Comunicações (TIC) e de Segurança da Informação e Comunicações (SIC).

Casa Civil da Presidência da República

Dentre as atribuições da Casa Civil da Presidência da República, merece destaque, por seu inequívoco enlace com o Setor Cibernético, a relacionada com a execução das políticas de certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da Infraestrutura de Chaves Públicas Brasileiras (ICP-Brasil).

Ministério da Justiça

O Ministério da Justiça, por meio do Departamento de Polícia Federal (DPF), é responsável pelas ações de repressão a crimes praticados no espaço cibernético.

Secretaria de Assuntos Estratégicos

A SAE possui a atribuição de realizar estudos e pesquisas destinados a promover o planejamento de longo prazo governamental e contribuir para a implementação da Estratégia Nacional de Defesa.

Em razão dessas missões, realiza encontros para discutir, no âmbito da APF e academia, a orientação do tema Segurança e Defesa Cibernética.

O último encontro realizado com essa característica discutiu as bases para o estabelecimento de um Sistema de Segurança e Defesa Cibernética Brasileiro que venha a envolver também os sistemas de informação ligados às infraestruturas críticas.

Defesa Cibernética

Ministério da Defesa

O Ministério da Defesa e as Forças Armadas, como membros da Administração Pública Federal (APF), já participam ativamente, no nível político, do esforço nacional nas áreas de Segurança da Informação e Comunicações, Segurança Cibernética e Segurança das Infraestruturas Críticas.

Entretanto, é muito importante a ampliação dessas atividades e das estruturas a elas dedicadas, para atender ao amplo espectro das operações características de Defesa Cibernética, as quais devem abranger:

- no nível estratégico: as ações cibernéticas necessárias à atuação das Forças Armadas em situações de crise ou conflito armado e, até mesmo, em caráter episódico, em situação de paz ou normalidade institucional, ao receber mandado para isso; e

- no nível operacional: as ações cibernéticas, defensivas e ofensivas, relativas ao preparo (capacitação, adestramento ou treinamento) e ao emprego em operações militares, de qualquer natureza e intensidade, que caracterizam o ambiente de guerra cibernética.

Em outras palavras, é necessário que as Forças Armadas disponham de equipamentos e sistemas militares que utilizem modernos recursos de TIC, possibilitando o seu emprego eficaz no cumprimento de suas atribuições previstas no artigo 142 da Constituição Federal e regulamentadas, quanto à sua organização, preparo e emprego, pela Lei complementar nº 97, de 9 de junho de 1999 e suas atualizações.

Estado-Maior Conjunto das Forças Armadas (EMCFA)

Compete ao Estado-Maior Conjunto das Forças Armadas elaborar o planejamento do emprego conjunto das Forças Armadas e assessorar o Ministro de Estado da Defesa na condução dos exercícios conjuntos e quanto à atuação de forças brasileiras em operações de paz, além de outras atribuições que lhe forem estabelecidas pelo Ministro de Estado da Defesa (Brasil, 2010).

Comando de Defesa Cibernética das Forças Armadas (CDCFA)

Vinculado ao Estado-Maior Conjunto das Forças Armadas visualiza-se a criação do Comando de Defesa Cibernética das Forças Armadas. Este será composto por civis e militares das três Forças Armadas, o qual realizará o planejamento, o emprego, a coordenação e a orientação técnica e normativa das atividades do sistema brasileiro de defesa cibernética, 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 Ministério da Defesa 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 segurança e defesa cibernética.

Centro de Defesa Cibernética do Exército Brasileiro (CDCiber)

O Exército Brasileiro, como Força coordenadora e integradora na condução do processo de estabelecimento das estruturas de Defesa Cibernética no âmbito da Defesa, antecipou ações no seu campo interno e emitiu, em junho de 2010, a Diretriz para Implantação do Setor Cibernético no Exército, e já em agosto do mesmo ano foram assinadas as portarias criando o Centro de Defesa Cibernética do Exército (CDCiber) e ativando o seu Núcleo (Nu CDCiber), que já se encontra operativo, sendo a referência no âmbito das Forças Armadas.

Modelo institucional do sistema de segurança e defesa cibernética brasileiro

Considerando os aspectos abordados até este ponto, apresenta-se a seguir um organograma contendo uma proposta do modelo institucional do Sistema de Segurança e Defesa Cibernética Brasileiro a ser adotado no País. Tal proposta representa a estrutura básica necessária para atuar, simultaneamente, nas áreas de segurança e defesa cibernética.

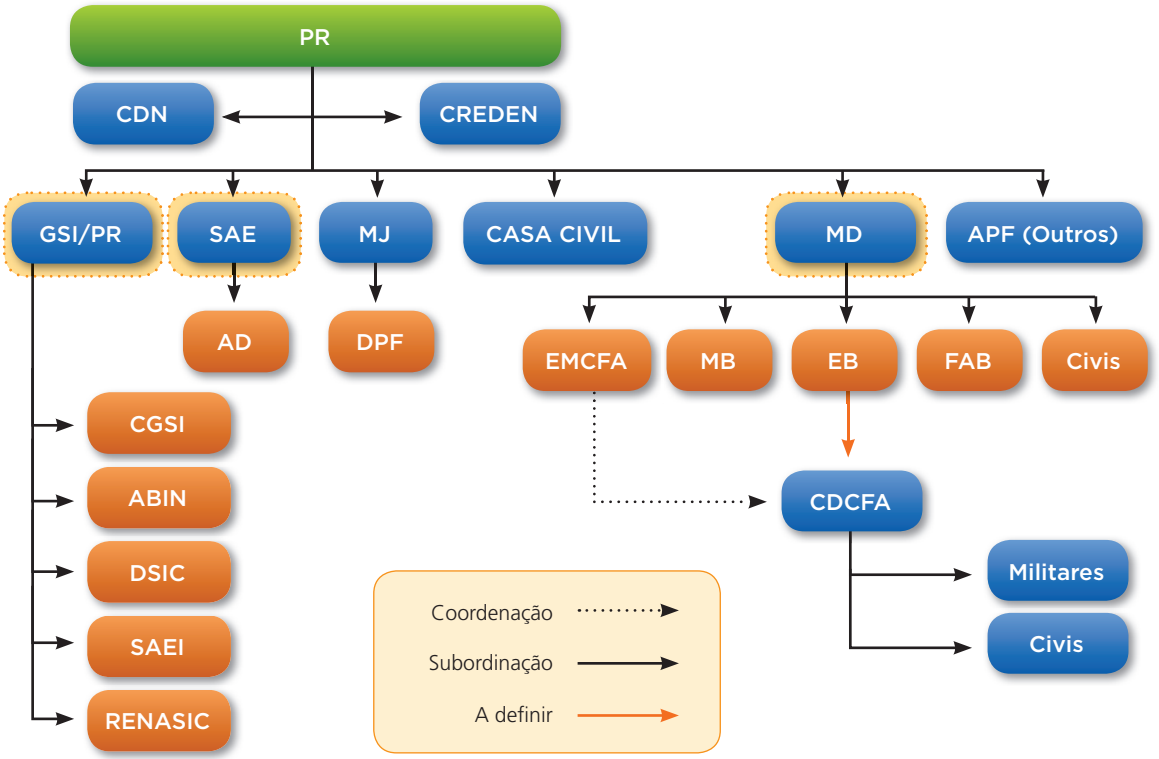

Figura 3 - Modelo Institucional do Sistema de Segurança e Defesa Cibernética Brasileiro
Fonte: Elaboração dos autores.

No organograma apresentado, estão destacados os órgãos que poderão assumir a responsabilidade, como órgão central, por normatizar, supervisionar, coordenar e controlar as atividades cibernéticas brasileiras, desde o campo da segurança cibernética até o campo da defesa cibernética.

O GSI encontra-se envolvido na elaboração de propostas que normatizem a atividade cibernética na APF, por meio do DSIC. Esta estrutura, por estar ligada diretamente a um órgão de assessoramento da Presidência da República, poderá, se elevado o seu "status" na cadeia decisória, assumir a função de órgão gestor central do sistema.

A SAE, órgão cuja missão é propor políticas públicas de longo prazo no campo estratégico, possui no seu DNA a carga genética de coordenar as atividades que envolvam vários ministérios, o que facilitará a integração das decisões a serem tomadas e que normatizem o sistema brasileiro de segurança e defesa cibernético. No entanto, carece de um reforço em recursos humanos para abarcar todas as tarefas imaginadas para o órgão central.

O MD, por estar envolvido na materialização dos objetivos previstos para os setores estratégicos, de acordo com a END, encontra-se maduro para solucionar os desafios relacionados à defesa cibernética. No entanto, poderá sofrer resistência ao assumir o papel de órgão central do sistema, em razão da sociedade brasileira não estar conscientizada da importância que o tema defesa desempenha para o futuro do país.

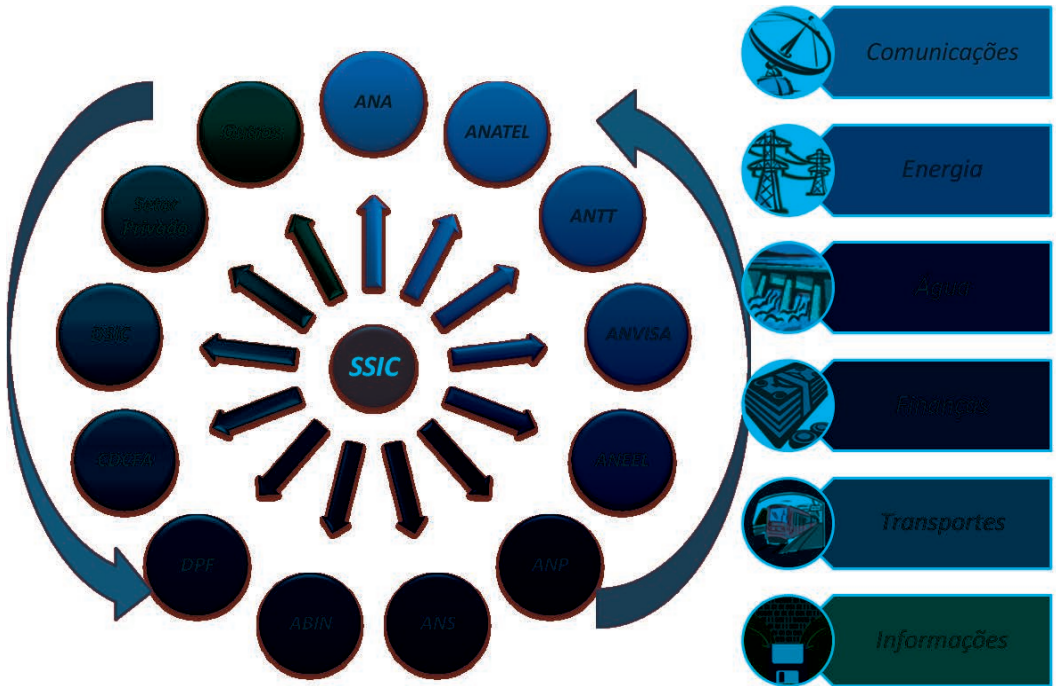

Figura 4 - Modelo Institucional do Sistema de Segurança e Defesa Cibernética Brasileiro – Outra Abordagem - 1

Fonte: Elaboração dos Autores

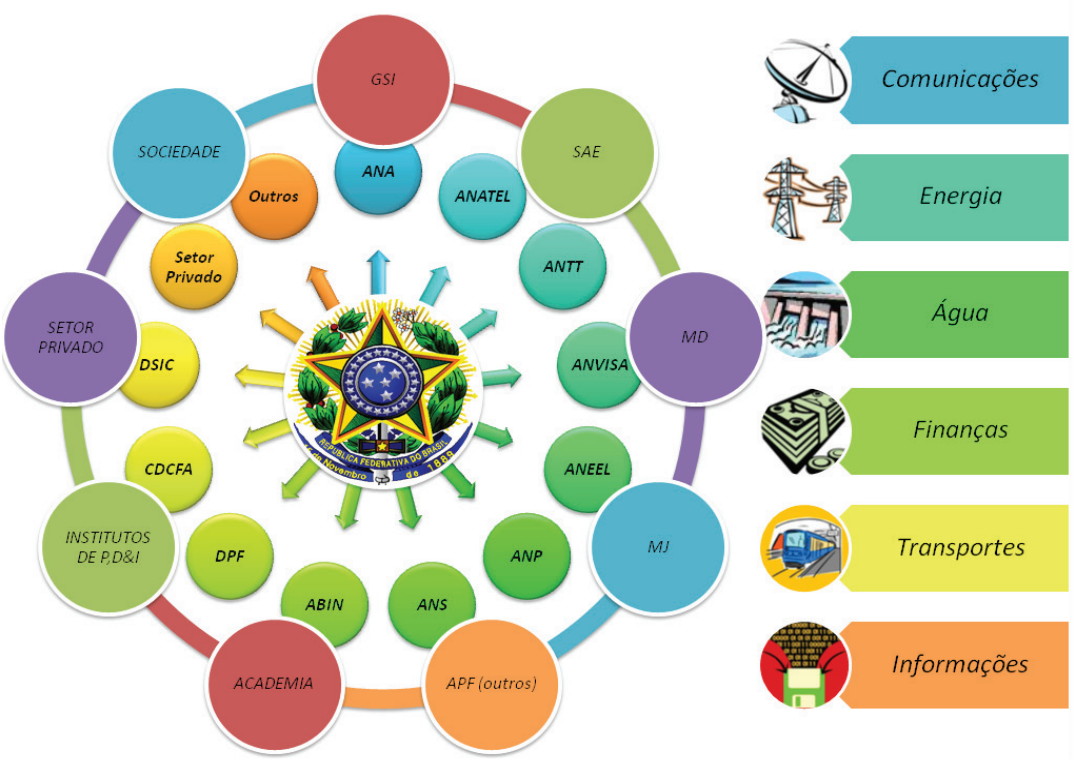

Figura 5 - Modelo Institucional do Sistema de Segurança e Defesa Cibernética Brasileiro – Outra Abordagem - 2

Fonte: Elaboração dos Autores

Nas figuras 4 e 5, sugere-se uma nova proposta do modelo institucional, na qual o órgão central se ligaria de forma matricial a todos os atores que lidam com a segurança das infraestruturas críticas do País e que comporiam o Sistema de Segurança e Defesa Cibernética Brasileiro. O mesmo poderia se chamar de Secretaria de Segurança da Informação e Comunicação (SSIC).

Seu chefe teria *status* de Ministro de Estado[5] e estaria vinculado diretamente à Presidência da República, como hoje se verifica com a Secretaria de Assuntos Estratégicos, Secretaria de Comunicação Social, Secretaria de Direitos Humanos, Secretaria de Relações Institucionais e outras.

[5] Um conselheiro *ad hoc* para assuntos relacionados à segurança e defesa cibernética.

A Secretaria de Segurança da Informação e Comunicações (SSIC) teria por missão principal: normatizar; supervisionar; coordenar; e controlar o Sistema Brasileiro de Segurança e Defesa Cibernética.

A ligação direta da SSIC com a Presidência da República, o que significaria FORÇA, e a capilaridade com outros órgãos, o que significaria COMPARTILHAMENTO, permitiria a essa Secretaria unir esforços para vencer os obstáculos que se apresentam na quinta dimensão do combate.

Sua estrutura base contaria com representantes de todos os órgãos participantes do conselho consultivo, atuando em caráter episódico, que teriam a liberdade de ligar-se diretamente com aqueles a quem representassem, visando a identificar as ameaças, fraquezas, oportunidades e forças da constante análise do ambiente cibernético brasileiro e internacional.

Para a condução dos trabalhos da SSIC, seria constituído um gabinete permanente com atribuições específicas de tratar da relatoria das reuniões, produção da documentação e elaboração das normas a serem elevadas à Presidência da República.

As agências e quaisquer outros órgãos governamentais e não governamentais com responsabilidades na área de segurança e defesa cibernética, dentro de suas especificidades, continuariam atuando com a independência necessária até que todo o sistema estivesse integrado.

Os grupos técnicos[6] constituídos para tratarem da segurança das infraestruturas críticas seriam, inicialmente, os principais clientes da SSIC, para, a partir desse suporte, aumentarem a segurança de suas operações e, por consequência, da sociedade brasileira.

[6] O assunto Segurança das Infraestruturas Críticas foi incluído no Artigo 1º do Decreto 4.801, de 6 de agosto de 2003 (decreto que cria a Câmara de Relações Exteriores e Defesa Nacional - Creden), como proposta desta Câmara, por intermédio da Resolução nº 2, de 24 de outubro de 2007, sendo modificado pelo Presidente da República pelo Decreto nº 7.009, de 12 de novembro de 2009.

Referências bibliográficas

BRASIL. Constituição da República Federativa do Brasil. out. 1998. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constitui%C3%A7ao.htm>. Acesso em 6 abr. 2011.

BRASIL. Decreto nº 3.505, de 13 de julho de 2000.. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/D3505.htm>. Acesso em: 1 de jun. 2011.

BRASIL. Decreto nº 4.801, de 6 de agosto de 2003. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto/2003/d74801.htm>. Acesso em: 1 jun. 2011. BRASIL.. Decreto nº 4.801. de 6 de agosto de 2003. Disponível: <http://www.planlato.gov.br/ccivil/decreto/2003/d4801.htm>. Acesso em: 1 jun. 2011.

BRASIL. (18 de Dezembro de 2008). Estratégia Nacional de Defesa. Acesso em 1 de Junho de 2011 Disponível: <http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Decreto/D6703.htm>.

BRASIL. Ministério da Defesa. Diretriz Ministerial nº 014/2009. Brasília,2009.

BRASIL. Lei Complementar 136, de 25 de agosto de 2010. Disponível: <https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp136.htm>. Acesso em: 30 mai. 2011.

CARVALHO, P. S. O Setor Cibernéticos nas Forças Armadas. In: REUNIÃO TÉCNICA DE SEGURANÇA E DEFESA CIBERNÉTICA. Brasília, 2010.

JÚNIOR, R. M. Reflexões sobre Segurança e Defesa Cibernética. In: REUNIÃO TÉCNICA SEGURANÇA E DEFESA CIBERNÉTICA. Brasília, 2010a.

JÚNIOR, R. M. Um estudo sobre a segurança e a defesa do espaço cibernético brasileiro. In: REUNIÃO TÉCNICA DE SEGURANÇA E DEFESA CIBERNÉTICA. Brasíia, 2010b.

JÚNIOR, R. M., CANONGIA, C. Livro Verde: Segurança Cibernética no Brasil. Brasília, 2010.

OLIVEIRA, J. R. Sistema de Segurança e Defesa Nacional: abordagem com foco nas atividades relacionadas à Defesa Nacional. In: REUNIÃO TÉCNICA SOBRE SEGURANÇA E DEFESA CIBERNÉTICA. Brasília, 2010.

RÊGO BARROS, O. S., GOMES, U. M. Seminário Cyber Warfare. Londres, 2011.

Esta obra foi impressa pela Imprensa Nacional
SIG, Quadra 6, Lote 800
70610-460, Brasília - DF, em agosto de 2011
Tiragem: 2.000 Exemplares

SECRETARIA DE ASSUNTOS ESTRATÉGICOS
PRESIDÊNCIA DA REPÚBLICA

ISBN 978-85-85142-32-2