AUDIÊNCIA PÚBLICA NO SENADO FEDERAL EM 06 DE DEZEMBRO DE 2013

TEMA: SEGURANÇA CIBERNÉTICA E SOBERANIA NACIONAL

1. INTRODUÇÃO

A vertiginosa evolução tecnológica experimentada pela sociedade nos últimos vinte anos permitiu o ingresso das Tecnologias da Informação e Comunicações em todos os domínios da atividade humana, proporcionado grandes benefícios à humanidade, facilitando o trânsito de informações, a interação e a aproximação entre indivíduos, grupos sociais, políticos e econômicos e entre nações.

Por outro lado, entretanto, temos testemunhado o uso crescente de tais tecnologias como novo instrumento de dominação entre nações, onde o espaço cibernético é utilizado para se manter o "status quo" ou se alcançar maior influência na relação de poder entre as mesmas. Desse modo, surgem verdadeiros "artefatos cibernéticos", alguns desenvolvidos com propósitos nitidamente militares, a exemplo do vírus **Stuxnet,** ao qual tenho me referido em algumas palestras, como a primeira "bomba cibernética", em analogia ao artefato nuclear lançado pelos norte-americanos em Hiroshima em 1945.

Nos dias atuais, os ataques cibernéticos constituem ameaças significativas à estabilidade e à segurança da sociedade e à soberania dos Estados. Sejam eles classificados como "hacktivismo", crime cibernético, espionagem, terrorismo ou ato de guerra perpetrado no espaço cibernético, a diferença, em relação às ameaças cinéticas, é o seu baixo custo, estando acessíveis a grupos de hackers, criminosos, terroristas ou de organizações e países sem grandes recursos tecnológicos ou financeiros. Assim, a adaptação e modernização das instituições e estruturas de estados para enfrentá-los devem ser abordadas com grande responsabilidade e visão estratégica.

2. A ESTRATÉGIA NACIONAL DE DEFESA (END)

O espaço cibernético tornou-se essencial para a Defesa e Segurança Nacionais.

A END, formulada inicialmente no final de 2008, estabeleceu diretrizes para o preparo e o emprego das Forças Armadas, e definiu três setores estratégicos essenciais para a Defesa Nacional – o espacial, o cibernético e o nuclear. Enfatiza que todas as instâncias do Estado devem contribuir para o incremento do nível de Segurança Nacional, com particular ênfase nas medidas para a segurança das infraestruturas críticas nacionais e para o aperfeiçoamento dos dispositivos e procedimentos de segurança que reduzam as vulnerabilidades dos sistemas críticos contra ataques cibernéticos.

Atualmente, o Centro de Defesa Cibernética (CDCiber), criado oficialmente pelo decreto 7809, de 20 de setembro de 2012, coordena e integra, de forma matricial, os trabalhos de diversas instituições governamentais, empresariais e acadêmicas, conforme prescrito na END.

Em 12 de setembro de 2013, a Câmara de Deputados aprovou o projeto de Decreto Legislativo 818/13, que contém os textos da Política Nacional de Defesa, da Estratégia Nacional de Defesa e do Livro Branco de Defesa Nacional.

A atualização da END estabelece, entre outras medidas, ações no sentido de:

-fortalecer o Centro de Defesa Cibernética com capacidade de evoluir para o Comando de Defesa Cibernética das Forças Armadas; de Aprimorar a Segurança da Informação e Comunicações (SIC), particularmente, no tocante à cerificação digital no contexto da Infraestrutura de Chaves-Públicas da Defesa (ICP-Defesa), integrando as ICP das três Forças;

-fomentar a pesquisa científica voltada para o Setor Cibernético, envolvendo a comunidade acadêmica nacional e internacional.

-desenvolver sistemas computacionais de defesa baseados em computação de alto desempenho para emprego no setor cibernético e com possibilidade de uso dual;

-desenvolver a capacitação, o preparo e o emprego dos poderes cibernéticos operacional e estratégico, em prol das operações militares conjuntas e da proteção das infraestruturas estratégicas;

-incrementar medidas de apoio tecnológico por meio de laboratórios específicos voltados para as ações cibernéticas; e

- estruturar a produção de conhecimento oriundo da fonte cibernética, essencial para a segurança e defesa cibernética proativa.

Além disso, destaco, no Livro Branco de Defesa Nacional, as seguintes premissas sobre o setor cibernético:

-a implantação do Setor Cibernético tem como propósito conferir confidencialidade, disponibilidade, integridade e autenticidade dos dados que trafegam em suas redes. Esse projeto representa um esforço de longo prazo, que influenciará positivamente as áreas de ciência e tecnologia e operacional.

-sob a coordenação do Exército, significativos avanços têm se concretizado na capacitação de pessoal especializado e no desenvolvimento de soluções de elevado nível tecnológico, contemplando a multidisciplinaridade e dualidade das aplicações, induzindo a indústria nacional a produzir sistemas inovadores.

3. SITUAÇÃO ATUAL

As vulnerabilidades existentes no espaço cibernético brasileiro advém de causas diversas. A principal delas é decorrente da **dependência tecnológica** em relação a países com alto grau de desenvolvimento na área da Tecnologia da Informação e Comunicações e dificilmente será superada em curto prazo.

Outra, de natureza mais complexa, advém da **falta de consciência** a respeito da necessidade de se proteger informações sensíveis, sejam de natureza institucional ou individual. Desta decorrem todas as demais, tais como a falta de investimento no setor, a insuficiência de especialistas de segurança da informação e o não cumprimento de normas de proteção já estabelecidas por agências responsáveis pela segurança cibernética do País.

Agrega-se, às vulnerabilidades citadas anteriormente, o **escasso arcabouço legal nacional e internacional**, que motivou o regime de urgência na tramitação do Marco Civil da Internet e tem marcado a posição do nosso País na necessidade de se discutir o estabelecimento de um marco regulatório também no plano internacional, principalmente após o caso Snowden.

A criação do CDCiber tem servido para incrementar o grau de segurança cibernética no âmbito da Defesa, assim como na integração e coordenação de esforços mais amplos com outros setores do Governo e da sociedade, com resultados expressivos, como ficou demonstrado nos Grandes Eventos. O contexto atual no setor mostra, entretanto, que, além da atual ação político-diplomática do Governo junto à ONU, tais esforços devem ser acelerados, por meio de ações concretas e viáveis no curto e médio prazo, não restritas ao âmbito da Defesa.

A coordenação dos trabalhos e a integração de todos os vetores vocacionados para as atividades do setor cibernético deve ocorrer de forma colaborativa entre os setores público, privado, acadêmico e a base industrial brasileira, com foco na eficácia das ações de defesa cibernética.

O Centro de Defesa Cibernética tem atuado de forma colaborativa e em parceria com diversas agências governamentais como o SERPRO, o GSI (DSIC e ABIN), o MRE, a SAE, os Centros de Tratamento de Incidentes de Rede (CTIR.Gov e CTIR.Br), a ANATEL, a ANEEL, a Polícia Federal, entre outras. Dessa forma, realizou, durante a Rio + 20, Copa das Confederações e Jornada Mundial da Juventude, a coordenação e integração das ações de proteção do ambiente cibernético brasileiro, por meio de um Centro de Monitoramento Cibernético integrado por especialistas da Marinha, Exército, Aeronáutica, daqueles órgãos governamentais e empresas nacionais de software, parceiras indispensáveis no sucesso daqueles eventos.

Ainda dentro dessa forma colaborativa de atuação, o CDCiber organizou, em julho e setembro de 2011, 02 (duas) Jornadas de Trabalho em conjunto com a SEPIN/MCTI, onde foram elaborados 04 (quatro) Programas a serem fomentados pelo MCTI: Escola Nacional de Defesa Cibernética, Supercomputação Nacional de Defesa, Desenvolvimento de Soluções para Segurança de Ambientes Computacionais e Sistema Modular de Defesa Cibernética). Mais de 50 instituições, públicas e privadas participaram das duas Jornadas *(MPOG, MRE, GSI, SAE, TCU, Câmara dos Deputados, PF, CPqD, CGI, CEPESC, CERT.br, ANATEL, RNP, UFSM, USP, UnB, UCB, UECE, UFCG, UFMG,UNICAMP, UNIFEI, C.E.S.A.R, LNCC, Concert Technologies, Medav, Microsoft, Atech, Axur, E-Sec, Cloudshield Technologies, Global Development Network, Aker Security Solutions, DECATRON, GAS Tecnologia, Solentech. Módulo Solutions, Dígitro Tecnologia, Cyberty On Service, ID2 Tecnologia, Techbiz Forense Digital, TECHGRAF,* T*ECSOFT, ABCIC, Montreal e outras).*

4. DEPENDÊNCIA TECNOLÓGICA

O Brasil não dispõe de uma indústria de equipamentos eletrônicos e de telecomunicações que possam substituir a grande parte de componentes importados para suas redes internas, tais como equipamentos de comutação, roteadores, centrais de voz, VoIP e outros considerados críticos para assegurar a disponibilidade, confidencialidade, autenticidade e integridade das suas comunicações internas.

Além disso, existe a dependência em relação às operadoras não nacionais de grande parte da nossa infraestrutura de telecomunicações. Nesse contexto, vale mencionar o fato de que a lei norte-americana conhecida como CALEA (*Communications Assistence for Enforcement Act*) obriga os fabricantes americanos a tornar possível a coleta de dados de interesse para a segurança daquela superpotência. As recentes revelações do Sr Edward Snowden fazem-nos inferir que tal lei tem sido cumprida à risca.

Existe, portanto, a necessidade de uma estratégia de amplo alcance no sentido de buscar o desenvolvimento autóctone para a produção de componentes críticos no setor, por meio da intensificação da pesquisa tecnológica e inovação, ação esta já iniciada pelo Ministério da Ciência, Tecnologia e Inovação (MCTI), por meio de uma série de programas, a exemplo do INOVA AERODEFESA.

O Brasil ainda não dispõe de um órgão nacional, com estrutura tecnológica capacitada, para certificar e homologar produtos utilizados pelas empresas de tecnologia da informação e comunicações em seu território. Em recente audiência pública na Câmara dos Deputados, levantei a questão sobre a necessidade de se atribuir tal tarefa a uma agência governamental já existente ou, se necessário, criar-se uma nova estrutura com tal atribuição, do que seria uma Agência Nacional de Segurança Cibernética.

5. UM MODELO PARA O PAÍS

No âmbito do MD, o modelo de desenvolvimento baseado no tripé governo, instituições acadêmicas e indústria nacional tem alcançado resultados promissores. Em menos de 2 anos de implantação do setor de defesa cibernética, já existem produtos tais como o próprio CDCiber, o simulador de defesa cibernética, o primeiro antivírus brasileiro e ferramentas de gestão de risco e de inteligência que se mostraram muito eficazes na proteção dos ativos de informação relacionados aos últimos Grandes Eventos (Rio+20, Copa das Confederações e Jornada Mundial da Juventude).

Mais do que simples produtos, a forma cooperativa e integradora de atuação entre as diversas agências envolvidas naqueles eventos, sob a coordenação do MD, pode servir como modelo para o País na busca da segurança e defesa cibernéticas mais abrangentes.

Paralelamente, a ofensiva político-diplomática do Brasil junto à Organização das Nações Unidas no sentido de se discutir um ordenamento no espaço cibernético, parece ter

sido a postura mais adequada e possível na presente conjuntura. Nações de peso no cenário mundial começam a demonstrar apoio à proposta brasileira, a exemplo da Alemanha. No entanto, não sejamos ingênuos, como nação, a ponto de acreditar que tal ofensiva será suficiente na defesa dos interesses nacionais. O Brasil deve fazer um esforço no sentido de dotar sua Defesa de condições mínimas para dissuadir ações que ameacem seu patrimônio e buscar independência tecnológica, se não total, pois que tal objetivo é cada vez mais inviável num mundo de economia globalizada, pelo menos que garanta a segurança de seus ativos de toda ordem, em especial no ambiente cibernético, ajudando a preservar sua soberania no concerto das nações.

Muito obrigado.

Complemento

1) SITUAÇÃO ORÇAMENTÁRIA

O programa de implantação da defesa cibernética tem se desenvolvido, de forma limitada, tendo em vista a inexistência de ação orçamentária própria para o MD. Até o momento, as Forças empregam seus próprios recursos. No âmbito do Exército Brasileiro (EB), a quem cabe a coordenação e integração da Defesa Cibernética, foi elaborado um programa para ser concluído em 4 anos, com uma média de R$ 100 milhões por ano. Para o primeiro ano, 2012, havia uma previsão de R$ 81 milhões, tendo sido alocados R$ 61,6 milhões, dos quais 99,88% foram empenhados. No presente exercício, 2013, dos R$ 110 milhões planejados inicialmente, foram alocados somente R$ 90 milhões. Para 2014 e 2015, há uma previsão de R$ 70 e R$ 81,7 milhões, respectivamente. Dessa forma, em relação ao planejamento inicial de R$ 399,6 milhões, há um déficit de R$ 90,1 milhões, atualmente. Tais valores dizem respeito somente ao orçamento do Exército Brasileiro.

A conjuntura atual mostra que tais recursos não são suficientes, considerando-se que os mesmos estão restritos ao âmbito do EB e que, embora tendo dotação na Lei Orçamentária Anual (LOA), seus recursos foram contingenciados, e não consideram as novas demandas evidenciadas contra os interesses nacionais, amplamente discutidas após o "caso Snowden".

Nesse contexto, o Grupo de Trabalho de Defesa Cibernética propõe a adoção de algumas medidas emergenciais e de médio prazo no sentido de acelerar o processo de fortalecimento da segurança e defesa cibernética do País, os quais montam da ordem de R$ 400.000.000,00.

2) AÇÕES EMERGENCIAIS

- Capacitar, em maior escala, os recursos humanos, por meio do Instituto de Defesa Cibernética (IDCiber), embrião da futura Escola Nacional de Defesa Cibernética;

- Disseminar o uso de tecnologias já desenvolvidas por empresas e institutos de pesquisa nacionais, tais como: antivírus DEFESA/BR, simulador de Guerra Cibernética, ferramentas de gestão de risco e inteligência, Criptogov, Segov e outras;

- Implantar solução criptográfica nacional e interoperável, valendo-se de capacidades já adquiridas, no âmbito da APF;

- Aprovar a Doutrina Militar de Defesa Cibernética;

- Implantar o Programa de Desenvolvimento Conjunto de Defesa Cibernética;

- Criar o programa temático "Defesa Cibernética" no Plano Plurianual;

- Priorizar a aplicação dos recursos do INOVA AERODEFESA no setor cibernético;

- Criar o Comando de Defesa Cibernética (aos moldes do COMDABRA), inicialmente, ativar seu Núcleo no Centro de Defesa Cibernética;

- Incluir as aquisições para o setor cibernético como de interesse vital para a Defesa na Lei N° 12.598, de 22 de março de 2012, priorizando a indústria nacional;

- Inserir os projetos/programas do setor cibernético gerenciados pela Defesa no Programa de Aceleração do Crescimento (PAC);

- Garantir a transferência e permanência do pessoal especializado que atua no Sistema de Defesa Cibernética;

- Criar cargos DAS para atender as necessidades do setor cibernético;

- Definir os recursos do setor cibernético como de descentralização obrigatória;

- Definir, com a mais alta prioridade, a criação e complementação de claros de pessoal do setor cibernético em todos os níveis do MD e demais órgãos da APF; e

- Determinar a adoção ampla e aderente às normas previstas para a infraestrutura de chaves públicas brasileira (ICP-Brasil).

3) AÇÕES DE MÉDIO PRAZO

- Criar a Escola Nacional de Defesa Cibernética, vinculada à Defesa;

- Acelerar a aprovação do Marco Civil da Internet;

- Implantar laboratórios de certificação de processos e soluções (*hardware e software*) de tecnologia da informação e comunicações, vinculado ao MD;

- Elaborar um Programa Nacional de Segurança Cibernética;

- Confeccionar a Política de Segurança Cibernética;

- Desenvolver os programas do MD/MCTI (Escola Nacional de Defesa Cibernética, Supercomputação Nacional de Defesa, Desenvolvimento de Soluções para Segurança de Ambientes Computacionais e Sistema Modular de Defesa Cibernética) formulados em 2011;

- Mapear os ativos das principais infraestruturas críticas do País;

- Contribuir com propostas para a elaboração de arcabouço jurídico internacional sobre o espaço cibernético na ONU, tendo como escopo os princípios basilares do Marco Civil da Internet;

- Contribuir com a estruturação das Instituições de Segurança para fazerem cumprir a Lei N° 12.735 e 12.737, de 30 de novembro de 2012;

- Aperfeiçoar e difundir a legislação referente à Segurança da Informação e Comunicações;

- Construir o Comando de Defesa Cibernética com estrutura organizacional matricial e sinérgica, tendo como vetores principais os órgãos da APF;

- Implantar o Programa Nacional de Segurança Cibernética com foco na capacitação dos recursos humanos; na confecção e atualização do arcabouço doutrinário; no desenvolvimento nacional da ciência, tecnologia e inovação; no aperfeiçoamento da inteligência e na preparação e no emprego operacional. O Programa deverá ter a participação de vários Ministérios na sua gerência e estar sob coordenação e integração do Comando de Defesa Cibernética; e

- Estabelecer parcerias para o desenvolvimento de ações conjuntas no espaço cibernético com os países integrantes da UNASUL e do BRICS.