Política Nacional de Segurança Cibernética: uma necessidade para o Brasil

Alexandre Hosang
CAEPE
ESG

1 Introdução

O Brasil vem se destacando no âmbito das nações mundiais em função do seu desenvolvimento nas últimas décadas, fato este que vem despertando a atenção internacional, particularmente por poder ocupar posição de destaque e gerar conflito de interesses.

O Espaço Cibernético pode ser entendido como sendo o território não físico criado por meios computacionais, onde pessoas físicas e jurídicas, isoladamente ou em grupo, integrantes de empresas, órgãos públicos ou governos, podem se comunicar, realizar pesquisas e trafegar dados de maneira geral, valendo-se de Tecnologias da Informação e Comunicação (TIC) como suporte para seu funcionamento.

Neste contexto, surge a Segurança Cibernética, que, Segundo Mandarino (2010)[1], "... deve ser entendida como a arte de garantir a existência do espaço cibernético brasileiro pela adoção de ações que assegurem disponibilidade, integridade, confidencialidade e autenticidade das informações de interesse do Estado brasileiro."

As ameaças existentes no Espaço Cibernético mundial indicam para a necessidade do estabelecimento de uma Política Nacional de Segurança Cibernética no Brasil, com ênfase nos aspectos de Segurança e Defesa, destacando parâmetros mínimos a serem considerados na elaboração dessa Política, de onde poderão advir propostas de ações.

2 Desenvolvimento

As ameaças reais ou potenciais que existem nos sistemas computacionais de informação e comunicações podem ser entendidas como sendo a causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

[1] Mandarino Junior, Raphael. Segurança e defesa do espaço cibernético brasileiro, Cubzac Editora, Recife, 2010.

A Política de Defesa Nacional (2005, não paginado), destaca conceitos relevantes para este trabalho.

> **Segurança** é 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;
> **Defesa** Nacional é o conjunto de medidas e ações do Estado, com ênfase na expressão militar, para a defesa do território, da soberania e dos interesses nacionais contra ameaças preponderantemente externas, potenciais ou manifestas.

Existem outras definições para estes termos, fato este que pode gerar algum tipo de discrepância no estabelecimento de políticas públicas, relacionadas ao tema Segurança Cibernética. Alguns exemplos disso são apresentados a seguir.

Segundo o Manual da Escola Superior de Guerra, Fundamentos da Escola Superior de Guerra (2009, p. 59), “Segurança é a sensação de garantia necessária e indispensável a uma sociedade e a cada um de seus integrantes, contra ameaças de qualquer natureza.”

Conforme o Glossário das Forças Armadas MD 35-G-01 (2007, p. 75), “Defesa é o ato ou conjunto de atos realizados para obter, resguardar ou recompor a condição reconhecida como de segurança, ou ainda, reação contra qualquer ataque ou agressão real ou iminente.”

2.1 SITUAÇÃO MUNDIAL

O espaço cibernético é uma área na qual, apesar de se ter a compreensão da necessidade de segurança, não existem medidas implementadas de maneira sistemática e articulada que possam garantir a confiabilidade e a preservação dos sistemas empregados.

De maneira incipiente, as Nações vêm se preparando para evitar ou minimizar ataques cibernéticos às redes e sistemas de informação de governo, bem como de todos os demais segmentos da sociedade.

A Sociedade da Informação, apresenta as seguintes características:

- quantidade significativa de sistemas e redes de informação, notoriamente interconectados e interdependentes;

- significativos avanços tecnológicos nos sistemas de informação e comunicação;

- elevado número de acesso à Internet e às redes sociais;

- convergência tecnológica;

- ambientes complexos, com múltiplos sistemas e atores, que apresentam diversidade de interesses.

Como consequência destas características, surgem as seguintes situações:

- aumento significativo de ameaças e de vulnerabilidades à segurança cibernética;

- acelerada dinâmica de mudanças de ambinte em função das inovações surgidas frequentemente.

Exemplo recente de ciberguerra, talvez o mais importante dos últimos tempos, foi o Stuxnet, que foi um vírus que controlou parcialmente uma usina de enriquecimento de urânio iraniana, causando estragos a algumas de suas centrífugas.

O Stuxnet foi um worm[2] projetado para atacar o sistema industrial SCADA[3], desenvolvido pela Siemens, mais especificamente o sistema de controle das centrífugas de enriquecimento de urânio do Irã, em 2010, fazendo-as girar mais rapidamente do que o normal e causando rachaduras em seu interior, sem que os funcionários percebessem o ocorrido. Como a usina não tem acesso à Internet, estima-se que o vírus tenha sido infiltrado por algum dispositivo com saída USB, como pendrives. Para computadores com sistemas operacionais comuns como o Windows ou Mac OS X, o Stuxnet não causa danos, sendo fácil removê-lo.

Considerando que os desafios da segurança cibernética são muitos, é de fundamental importância desenvolver um conjunto de ações colaborativas entre governo, setor privado, academia e sociedade em geral, de forma a melhor entender a situação e fazer frente aos aspectos vulneráveis que a perpassam.

2.2 SITUAÇÃO DO BRASIL

Como desafio do século XXI, a Segurança Cibernética vem se destacando como função estratégica de Estado, sendo essencial à manutenção do

---

[2] Um **worm** (verme, em português), em computação, é um programa auto-replicante, semelhante a um vírus. Enquanto um vírus infecta um programa e necessita deste programa hospedeiro para se propagar, o Worm é um programa completo e não precisa de outro para se propagar. Um worm pode ser projetado para tomar ações maliciosas após infestar um sistema, além de se auto-replicar, pode deletar arquivos em um sistema ou enviar documentos por email.

[3] **Sistemas de Controle de Supervisão e Aquisição de Dados**: ou abreviadamente SCADA (proveniente do seu nome em inglês Supervisory Control and Data Aquisition) são sistemas que utilizam software para monitorar e supervisionar as variáveis e os dispositivos de sistemas de controle conectados através de drivers específicos. Estes sistemas podem assumir topologia mono-posto, cliente-servidor ou múltiplos servidores-clientes

funcionamento das infraestruturas críticas do país, tais como Energia, Telecomunicações, Transporte, Defesa, Finanças.

O Brasil, inegavelmente, na última década, tornou-se um 'player' importante no cenário mundial. Certamente o seu conhecimento sensível, produzido em diferentes áreas dos campos científico e tecnológico, pode se tornar objeto de cobiça por parte de outros países. Pode-se afirmar que o país para se desenvolver não pode abdicar da segurança do seu espaço cibernético, sendo que a proteção deste relaciona-se, diretamente, com a própria soberania nacional.

De maneira geral, o Espaço Cibernético brasileiro apresenta as seguintes características:

- dos três parâmetros da informação – armazenagem, processamento e trânsito –, os dois primeiros são em grande parte hospedados fora do país e, quanto ao terceiro, a banda não pode ser externalizada;

- a infraestrutura é dominada em sua essência por empresas multinacionais estrangeiras;

- existem talentos em todas as áreas, mas em número insuficiente perante o tamanho do espaço brasileiro, sendo que muitos estão fora do país; e

- normalmente os profissionais da área são formados em dois compartimentos que não se comunicam de forma eficaz, quais sejam: o da Academia e o ambiente muito especializado do autodidatismo e/ou das certificações; esse último foi criado basicamente pelas empresas para a geração de recursos humanos especializados em seus produtos.

A Política de Defesa Nacional (2005, não paginado) destaca.

> Os avanços da tecnologia da informação, a utilização de satélites, o sensoriamento eletrônico e inúmeros outros aperfeiçoamentos tecnológicos trouxeram maior eficiência aos sistemas administrativos e militares, sobretudo nos países que dedicam maiores recursos financeiros à Defesa. Em conseqüência, criaram-se vulnerabilidades que poderão ser exploradas, com o objetivo de inviabilizar o uso dos nossos sistemas ou facilitar a interferência à distância.

Ainda neste mesmo documento, existe como diretriz: “aperfeiçoar os dispositivos e procedimentos de segurança que reduzam a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra ataques cibernéticos e, se for o caso, permitam seu pronto restabelecimento.”

Como decorrência, a Estratégia Nacional de Defesa (END) (2008, p. 5) prevê o fortalecimento de três setores de importância estratégica: o espacial, o cibernético e o nuclear.

> 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 se faça também a partir do espaço.

Considerando ainda o que está previsto na END, o Exército tem a responsabilidade de ser o coordenador das ações de Defesa Cibernética, no âmbito das Forças Armadas. Como consequência, o Exército Brasileiro está criando o Centro de Defesa Cibernética, vem se articulando nesta área e, institucionalmente, consolidando sua posição.

Conforme destaca o Livro Verde – Segurança Cibernética no Brasil (2010, p. 13). “Chama a atenção que o chamado espaço cibernético, não tem suas fronteiras ainda claramente definidas, impacta o dia a dia de todos os dirigentes governamentais, de empreendimentos privados e dos próprios cidadãos.”

Observa-se, portanto, que existe a noção da importância de se tomar ações que favoreçam e permitam estabelecer a segurança no espaço cibernético, embora não se tenha a exata dimensão do que isso possa representar, bem como quais as medidas que efetivamente podem e devem ser adotadas para se atingir este objetivo.

Por outro lado, percebe-se, de maneira geral, que as pessoas confiam nos sistemas de pagamento online e web banking em virtude do fato de que estes tipos de ferramentas vêm sendo usados por mais usuários a cada ano que passa. É certo que este uso, frequentemente, é feito de maneira moderada, pois se tem notícia de atividades de estelionato e coleta de informações pessoais.

Atualmente o Brasil conta com diversos órgãos de governos com atribuições na área de Segurança de Informação e defesa cibernética, porém, apesar de constar nas agendas desses órgãos, o tema ainda pode ser considerado incipiente e muito pouco explorado, pois são identificadas poucas ações e incentivos, principalmente quando se trata do campo acadêmico.

A atual situação permite dizer que não se tem uma estrutura brasileira consistente que possa fazer frente a um possível cenário de ameaças reais ou de conflito no espaço cibernético, pois a situação ainda é de definição de

responsabilidades desde o mais alto nível de governo até as esferas governamentais mais simples, o que dificulta, em muito, qualquer ação geral de maneira integrada.

Neste contexto, uma Política Nacional de Segurança Cibernética poderia facilitar o enfrentamento deste desafio que é de todos, é premente, e requer agilidade na formação de senso comum a fim de que o país cresça, em segurança, se apropriando dos benefícios da Internet, rede global em mudança contínua, minimizando impactos negativos decorrentes de eventuais desastres ou de forma maliciosa.

2.2.1 Iniciativas brasileiras

O Estado brasileiro, ao longo do tempo, tem demonstrado relativa preocupação com a segurança de nosso Espaço Cibernético e, ainda que se possa afirmar que não se esteja completamente protegido, várias ações foram realizadas para tal fim, destacando-se a criação de órgãos e a implementação de iniciativas.

Nesta direção, destacam-se as principais ações implementadas:

- criação do Comitê Gestor da Internet – CGI, com a participação dos diversos segmentos da sociedade; cabe salientar que segurança não é a preocupação central do CGI;

- a publicação do decreto 3505/2000, que estabeleceu a Política de Segurança da Informação (PSI), a ser implantada pelo GSIPR; no entanto, não houve a definição dos meios a serem utilizados nessa implementação, sendo que, no momento, esta já se encontra defasada perante as mudanças da última década;

- criação do Departamento de Segurança da Informação e Comunicação (DSIC) no Gabinete de Segurança Institucional da Presidência da República (GSIPR), em 2006, com o objetivo de coordenar as ações normativas e operacionais no âmbito da Administração Pública Federal (APF), previstas na PSI;

- criação da Comunidade de Segurança da Informação e Criptografia (ComSic) e da Rede Nacional de Segurança da Informação e Criptografia (Renasic) no GSI, em 2008, para cuidar dos aspectos de fomento de Ciência e Tecnologia (C&T) em todos as áreas da Segurança Cibernética, também previstos na PSI; essa iniciativa transcende à APF e foi estabelecida em articulação com o Ministério da Ciência e Tecnologia (MCT); e

- a publicação da Estratégia Nacional de Defesa, que estipula a Segurança Cibernética como sendo uma de suas prioridades.

Destacam-se, ainda, a criação da CESeg – Comissão Especial em Segurança da Informação e de Sistemas Computacionais, que é uma das Comissões Especiais da Sociedade Brasileira de Computação (SBC), a implantação da Infraestrutura de Chaves Públicas, a atualização e criação de normatização sobre o tema, capacitação de recursos humanos, desenvolvimento de produtos criptográficos, e criação de Grupos Técnicos para tratar da segurança de Infraestruturas Críticas.

Além disso, ocorrem iniciativas tais como a especialização de agentes da Polícia Federal para tratar de crimes cibernéticos, o fortalecimento dos sistemas financeiros, que são alvos mais frequentes desses tipos de crime, e as ações de empresas de grande porte, que possam ser consideradas alvos de ataques cibernéticos.

Apesar dessas iniciativas isoladas do Estado Brasileiro, particularmente por intermédio do GSIPR e de empresas de grande porte para atender demandas próprias, a população em geral está ciente da existência das ameaças do espaço cibernético, mas não de suas possibilidades e de como fazer frente a tais ameaças. Pode-se considerar que a criação do DSIC foi o primeiro passo para oficializar a preocupação com o assunto.

Observa-se que há esforços de múltiplos atores que atuam diretamente e/ou perpassam o tema, sem, contudo, haver arcabouço único com enfoques político e estratégico para a concretização de ações efetivas de integração e otimização de tais esforços, deixando o País com brechas de segurança a serem mapeadas e superadas.

Verifica-se a necessidade de uma ação coordenada do Estado Brasileiro para garantir o funcionamento das infraestruturas críticas da nação, em caso de ameaça ou ataque cibernético.

2.2.2 Crimes Cibernéticos

Outro aspecto importante a ser considerado neste estudo se relaciona aos crimes cibernéticos, particularmente devido aos efeitos danosos que podem advir do mau uso dos sistemas de informação e comunicação por pessoas mal intencionadas.

Neste sentido, já ocorreram diversas iniciativas no Congresso Nacional para tratar desse tema, no entanto, até o presente momento, não existe consenso para o estabelecimento da legislação pertinente e, consequentemente, verifica-se a ausência de legislação específica que tipifique os crimes cibernéticos.

Apesar dos esforços de alguns setores da Administração Pública, ainda há brechas na legislação brasileira, não havendo leis para alguns tipos de ações que já são consideradas crime em outros países. Além disso, não há uma política clara embasando uma ação contra outro país que tenha afetado de alguma forma infraestrutura crítica nacional por meios cibernéticos e muitas questões ainda estão merecendo algum tipo de tratamento, sendo que esse avanço está sendo mais lento do que a situação exige.

2.2.3 Relações com outros países

Destaca-se que o Brasil não é signatário da Convenção de Budapeste[4] que data da década de 1990, a qual não atende às exigências atuais de crimes cibernéticos, dado os avanços tecnológicos ocorridos e tampouco é suficiente em termos da cooperação internacional.

Assim, como resultado da Convenção do Crime Cibernético, ocorrida no ano de 2010, em Salvador/BA, foi emitida Declaração, consensada por 158 países sobre tal aspecto, fato este que abriu a oportunidade de criação de grupo para tratar globalmente a matéria – crime cibernético.

Neste contexto surge a Estratégia Internacional dos Estados Unidos da América para Espaço Cibernético, *International Strategy for Cyberspace,* que descreve a visão daquele país para o futuro desse Espaço e define uma agenda de parceria com outras nações e povos com este enfoque. Neste documento, que será abordado a seguir, pode-se observar que estão presentes aspectos relacionados com parceiras a serem realizadas com outros países.

2.3 PARÂMETROS

O entendimento sobre a importância da segurança cibernética caracteriza-se, cada vez mais, como condição essencial para o desenvolvimento dos países,

[4] A Convenção sobre o Cibercrime, também conhecida como Convenção de Budapeste, é um tratado internacional de direito penal e direito processual penal firmado no âmbito do Conselho da Europa para definir de forma harmônica os crimes praticados por meio da Internet e as formas de persecução. Esta convenção trata basicamente de violações de direito autoral, fraudes relacionadas a computador, pornografia infantil e violações de segurança de redes

requerendo para tanto, dentre outras ações, a promoção de diálogos e de intercâmbios de ideias, de iniciativas, de dados e informações, de melhores práticas, para a cooperação sobre o tema, no país e entre países.

Estima-se levar em consideração a definição das necessidades de curto prazo, apoiadas em planos de longo prazo, criando órgãos de governo específicos para tratar do tema, estabelecendo estratégias e implantando sistemas de proteção sofisticados e abrangentes. Tais programas devem contemplar diferentes aspectos de uma Política Nacional de Segurança Cibernética (PNSC), compreendendo desde a redução de vulnerabilidades e a luta contra a criminalidade cibernética até a defesa contra o ciberterrorismo.

Conforme as diretrizes estabelecidas no Livro Verde – Segurança Cibernética no Brasil (2010, p.43).

> A Política Nacional de Segurança Cibernética deverá ter, como uma de suas premissas, a sua construção a partir de visão multidisciplinar, interinstitucional, em que múltiplas competências se complementam na solução de problemas e na identificação de oportunidades.

Vale destacar algumas recomendações da Organização para Cooperação e Desenvolvimento Econômico (OECD12) aos países membros sobre segurança das infraestruturas críticas de informação, as quais são entendidas, em geral, como indicativos das competências essenciais de segurança cibernética, particularmente relacionados ao estabelecimento de políticas, conforme apresentado no Livro Verde – Segurança Cibernética no Brasil (2010, p.26 e 27).

> - definir a política e as normas específicas, com objetivos claros, no âmbito do mais alto nível de governo;
> - atuar como o órgão central de governo com competência (responsabilidade e autoridade) para prover as melhores condições de implantação da política de segurança cibernética e seus objetivos;
> - promover tanto a cultura de, quanto a educação em, segurança cibernética;
> - promover mútua cooperação entre os stakeholders – setor privado, agência(s), terceiro setor, governo – visando à efetiva implantação da política nacional de segurança cibernética;
> ...
> - rever sistematicamente a política, normas e respectivo(s) marco(s) legal(is), com especial atenção às ameaças e vulnerabilidades das infraestruturas críticas da informação de cada país, buscando minimizar riscos e desenvolver novos instrumentos e/ou mecanismos de segurança da informação e comunicações; e
> - desenvolver e exercer macro-coordenação da política e estratégia nacional de segurança cibernética, envolvendo cúpula de governo e setor privado.

No âmbito do Governo Federal brasileiro, proposta elaborada pela Secretaria de Assuntos Estratégicos, da Presidência da República, intitulada Brasil 2022 -

Trabalhos Preparatórios (2010, p. 376), destaca na área de Segurança Institucional, especificamente na Meta 3, o seguinte: “estabelecer no País Sistema de Segurança e Defesa Cibernética, envolvendo, também, os sistemas de informação ligados às infraestruturas críticas.” Nesta meta são previstas as seguintes ações:

> - implantar um órgão de referência em segurança de sistemas de informação e comunicação e das infraestruturas críticas da informação;
> - integrar esforços e estabelecer prioridades por intermédio de Comitê Gestor dos Sistemas de Tecnologia da Informação e Comunicação.
> - 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.

Visando facilitar o entendimento sobre o tema, bem como a possível implementação de políticas públicas, visualizou-se dividir os parâmetros nas seguintes classes e níveis:

- Político: podem englobar as diversas políticas públicas e legislativas que abordem o tema. Ou seja, o que fazer.

- Técnico Científico: podem abranger as pesquisas científicas sobre o tema

- Técnico Operacional: podem incluir estudos técnicos e as técnicas elaboradas nos diversos órgãos e instituições que surgirem do emprego prático , tendo como origem profissionais especializados ou não.

- Usuários: de maneira geral são todas as pessoas que fazem uso de tecnologias de informação e comunicação, que podem possuir conhecimentos avançados, intermediários ou básicos.

Com relação aos parâmetros políticos, segundo o Guia de Referência para a Segurança das Infraestruturas Críticas da Informação (2010, p. 20), “são três os fatores considerados na formulação de estratégias para atender os requisitos mínimos necessários à Segurança das Infraestruturas Críticas da Informação: segurança, resiliência e capacitação.”

Segundo o Guia de Referência para a Segurança das Infraestruturas Críticas da Informação (2010, p. 86), aborda-se a resiliência.

> A resiliência possibilita às organizações trabalharem, de forma independente e interdependente, para garantir a continuidade dos seus objetivos de negócio durante a interrupção de eventos, tais como: desastres naturais, acidentes industriais e atos terroristas, e para melhorar as parcerias com os serviços de gestão de emergência que visam assistir as comunidades.

Com a adoção deste conceito, considera-se a proposta de se tratar a resiliência com o foco operacional, considerando os segmentos de gestão da segurança da informação e comunicações, que inclui: gestão de riscos, gestão de operação de tecnologia da informação e comunicações e gestão de continuidade de negócios. Com a evolução, o foco pode ser ampliado para a toda a organização, com a meta de criar uma organização resiliente.

Visando a criação e o fortalecimento da cultura de segurança da informação e comunicações, as organizações podem estabelecer ações direcionadas em três níveis: sensibilização/conscientização, treinamento e educação.

O motivo preponderante para o estabelecimento de uma Política Nacional de Segurança Cibernética (PNSC) é justamente nortear ações a serem desenvolvidas pelo Estado, com o envolvimento de setores estratégicos da academia e da iniciativa privada e da sociedade em geral, visando preservar a liberdade de ação no espaço cibernético brasileiro e garantir a segurança dos ativos estratégicos de informação nacionais.

A PNSC deve definir parâmetros para a atividade de segurança cibernética no País, estabelecendo pressupostos, objetivos, instrumentos e diretrizes para os diversos atores envolvidos na atividade.

Na expressão Política do Poder Nacional, observa-se a necessidade de se criar marco legal que permita regular o tema contra ataques e crimes cibernéticos, tanto internos quanto externos ao país, e que estejam alinhados com eventuais convenções internacionais acordadas.

Na expressão Econômica do Poder Nacional, verifica-se a necessidade de se criar Subfunção específica para as atividades de segurança cibernética na Lei de Diretrizes Orçamentária (LDO), sendo que o montante a ser destinado deve levar em consideração eventual demanda reprimida pela ausência de previsão anterior, com vistas a criar capacidade de resposta da Nação para enfrentar potenciais ameaças cibernéticas, para promover a devida regulação do mercado, por meio da adoção de padrões e especificações técnicas, bem como de modelos de gestão, de acompanhamento, e de auditoria desse tipo de atividade, de se estreitar parcerias e ações colaborativas com o setor privado, estimulando as parcerias públicas privadas e as empresas estratégicas, promovendo o setor cibernético no país e de se apoiar o segmento das micro, pequenas e médias empresas do país, em

especial aquelas atuantes no comércio eletrônico, de forma a promover a cultura da segurança cibernética.

Na expressão Psicossocial do Poder Nacional, observa-se a necessidade de se utilizar as redes sociais da Internet em prol da criação e o fortalecimento da consciência nacional sobre segurança cibernética, de se desenvolver programa de inclusão digital que incorporem a conscientização dos usuários sobre ameaças cibernéticas e segurança cibernética, de se defender os direitos de privacidade do cidadão brasileiro, de se apoiar o desenvolvimento da Internet no Brasil, promovendo política de acessibilidade com segurança do cidadão, de se aplicar políticas de incentivo para a integração do setor privado à segurança cibernética do país.

Na expressão Científico Tecnológica do Poder Nacional, verifica-se a necessidade de se promover o fortalecimento da ciência e as pesquisas básica e aplicada, do desenvolvimento de tecnologias e metodologias, e da inovação em segurança cibernética.

Neste contexto, surge outro aspecto relevante que é a cooperação internacional sobre o tema, no qual se evidencia a necessidade de se promover a cooperação bilateral e multilateralmente, em nível regional e global, visando trocas de experiências e fortalecimento de uma estratégia nacional de segurança cibernética, de se institucionalizar no país uma autoridade nacional de segurança, com a finalidade de se sistematizar o processo de credenciamento de órgãos, entidades, empresas, e pessoas para intercâmbio de informações classificadas, entre governos, de se promover acordos de cooperação técnica de segurança cibernética, de se estabelecer programas de cooperação específicos entre Governo e Sociedade, bem como com outros Governos e a comunidade internacional, de se articular acordos internacionais de modo a potencializar a segurança cibernética do País, sua capacidade de defesa e dissuasão, além do aumento e atualização das suas competências essenciais.

A Criação de uma Agência Brasileira de Segurança da Informação, a qual teria competência e responsabilidade de monitorar o Espaço Cibernético Nacional, colocando controles de tráfego ao longo dos backbones, mesmo sendo estes de propriedade de empresas de telecomunicações internacionais. Atualmente existem agências deste tipo em países tais como: Coréia do Sul e Japão.

Quanto aos parâmetros Técnico Científicos, cabe analisar, sob o enfoque científico, as iniciativas realizadas em órgãos governamentais de todos os níveis, bem como na iniciativa privada, buscando conjugar interesses, equacionar eventuais discrepâncias e articular esforços com a finalidade de tornar mais eficiente os trabalhos realizados.

Quanto aos parâmetros Técnico Operacionais, considera-se que na atualidade as iniciativas de técnicos que buscam soluções práticas para problemas do dia-a-dia são cada vez mais frequentes e permitem, muitas vezes, encontrar soluções inteligentes e simples para problemas complexos. Estas iniciativas devem ser aproveitadas e, para tanto, devem ser analisadas e avaliadas com a finalidade de se verificar a viabilidade de serem aproveitadas por outros setores, tanto da Administração Pública, quanto pela iniciativa privada e pelas universidades. Resumidamente, no campo técnico operacional verifica-se a necessidade de se articular iniciativas e de se aproveitar a capacidade de produção de setores técnicos.

Os serviços prestados por essas áreas são de vital importância para os cidadãos, para as organizações e para o Estado, cuja proteção permanente visa garantir a continuidade da prestação dos serviços mesmo em situações de crise.

Quanto aos parâmetros de usuários, observa-se que os mesmos são os atores essenciais para o bom funcionamento do processo da implementação de qualquer iniciativa na área de segurança, pois se constata que este pode ser tornar a parte mais vulnerável de todo o sistema de informação e comunicação.

Além disso, a capacitação destes usuários pode ser considerada como sendo aspecto essencial para a prevenção de atitudes perigosas para a segurança cibernética.

Neste contexto, há que se avaliar o real nível de capacitação de cada usuário, permitindo avaliar o perfil desse usuário e estudando medidas preventivas que possam favorecer a segurança cibernética. Como ideia geral, pode se dividir os usuários em nível avançado de conhecimento, nível intermediário de conhecimento e em nível básico de conhecimento, sendo que este último pode englobar as pessoas que praticamente não possuem conhecimentos a respeito do tema.

A Estratégia Internacional para o Ciberespaço, *International Strategy for Cyberspace (2011),* dos Estados Unidos da América (EUA), lançada em maio de 2011, pode ser considerada no estabelecimento de parâmetros para uma Política Nacional para o setor no Brasil, levando em conta o avançado nível tecnológico e a

experiência daquele país em atividades relacionadas ao tema, englobando aspectos relacionados que combinam diplomacia, defesa e desenvolvimento.

Portanto, com as mudanças tecnológicas ocorridas recentemente, pode se pensar em agregar incumbência de controle do espaço cibernético para o Ministério das Comunicações e/ou para a Agência Nacional de Telecomunicações (ANATEL). Modificação do MC para Ministério das Comunicações e da Cibernetica com objetivo de ser órgão governamental responsável por articular e coordenar iniciativas.

Finalmente constata-se a demanda de criação de órgão que permita a articulação das atividades a serem desenvolvidas no setor e possibilite a conjugação de esforços com vistas a aumentar o rendimento e evitar o desperdício de recursos.

3. CONCLUSÃO

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

Aspecto relevante é a necessidade de uma efetiva Governança na área de Tecnologia da Informação e Comunicação, considerando a necessidade de efetivo controle do espectro por onde circulam as informações.

É notório, portanto, que muitas ações são necessárias para criar condições preeminentes da Segurança das Infraestruturas Críticas de Informação, principalmente, no que diz respeito ao entendimento das diretrizes para a proteção da sociedade e do Estado.

Conclui-se que existem diversos órgãos da Administração Pública, organizações da iniciativa privada e instituições de Ensino e Pesquisa que vem desenvolvendo iniciativas e ações no intuito de preservar a segurança do espaço cibernético brasileiro. Porém, verifica-se a necessidade de maior integração, além da interação que já ocorre, e a articulação destes organismos e suas respectivas ações com a finalidade de promover a cultura de segurança e a difusão de experiências adquiridas.

REFERÊNCIAS

_____. Presidência da República. **Estratégia Nacional de Defesa.** Decreto N. 6.703, de 18 de dezembro de 2008. Brasília, DF, 2008.

_____. **Política de Defesa Nacional.** Decreto N. 5.484, 30 de junho de 2005. Brasília, DF, 2005.

_____. Presidência da República. Gabinete de Segurança Institucional. **Instrução Normativa GSI Nº 1 – Disciplina a Gestão da Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.** Brasília, 2008.

_____. Presidência da República. Gabinete de Segurança Institucional. Norma Complementar Nº02/IN01/DSIC/GSIPR – **Metodologia de Gestão de Segurança da Informação e Comunicações.** Brasília, 2008.

ESCOLA SUPERIOR DE GUERRA (Brasil). **Fundamentos da Escola Superior de Guerra.** Volume I – Elementos Fundamentais. Rio de Janeiro, 2009. v.1 66 p.

Mandarino Junior, Raphael. **Segurança e defesa do espaço cibernético brasileiro**, Cubzac Editora, Recife, 2010

UNITED STATES OF AMERICA. ***International Strategy for Cyberspace.*** *Seal of the President of United States, Washington, DC, 2011.25 p.*