da Cruz Júnior, Samuel César

Working Paper

A segurança e defesa cibernética no Brasil e uma revisão das estratégias dos Estados Unidos, Rússia e Índia para o espaço virtual

Texto para Discussão, No. 1850

Provided in Cooperation with:
Institute of Applied Economic Research (ipea), Brasília

Suggested Citation: da Cruz Júnior, Samuel César (2013) : A segurança e defesa cibernética no Brasil e uma revisão das estratégias dos Estados Unidos, Rússia e Índia para o espaço virtual, Texto para Discussão, No. 1850, Instituto de Pesquisa Econômica Aplicada (IPEA), Brasília

This Version is available at:
https://hdl.handle.net/10419/91261

1850
TEXTO PARA DISCUSSÃO

A SEGURANÇA E DEFESA CIBERNÉTICA NO BRASIL E UMA REVISÃO DAS ESTRATÉGIAS DOS ESTADOS UNIDOS, RÚSSIA E ÍNDIA PARA O ESPAÇO VIRTUAL

Samuel César da Cruz Júnior

ipea
Por um Brasil desenvolvido

1850
TEXTO PARA DISCUSSÃO
Brasília, julho de 2013

A SEGURANÇA E DEFESA CIBERNÉTICA NO BRASIL E UMA REVISÃO DAS ESTRATÉGIAS DOS ESTADOS UNIDOS, RÚSSIA E ÍNDIA PARA O ESPAÇO VIRTUAL*

Samuel César da Cruz Júnior**

* O autor agradece a Flavia de Holanda Schmidt e a João Maria de Oliveira pelas valiosas contribuições e sugestões para o aperfeiçoamento deste trabalho.
** Técnico de planejamento e pesquisa da Diretoria de Estudos e Políticas Setoriais de Inovação, Regulação e Infraestrutura (Diset) do Ipea.

Governo Federal

Secretaria de Assuntos Estratégicos da Presidência da República
Ministro interino Marcelo Côrtes Neri

ipea **Instituto de Pesquisa Econômica Aplicada**

Fundação pública vinculada à Secretaria de Assuntos Estratégicos da Presidência da República, o Ipea fornece suporte técnico e institucional às ações governamentais – possibilitando a formulação de inúmeras políticas públicas e programas de desenvolvimento brasileiro – e disponibiliza, para a sociedade, pesquisas e estudos realizados por seus técnicos.

Presidente
Marcelo Côrtes Neri

Diretor de Desenvolvimento Institucional
Luiz Cezar Loureiro de Azeredo

Diretor de Estudos e Relações Econômicas e Políticas Internacionais
Renato Coelho Baumann das Neves

Diretor de Estudos e Políticas do Estado, das Instituições e da Democracia
Daniel Ricardo de Castro Cerqueira

Diretor de Estudos e Políticas Macroeconômicas
Cláudio Hamilton Matos dos Santos

Diretor de Estudos e Políticas Regionais, Urbanas e Ambientais
Rogério Boueri Miranda

Diretora de Estudos e Políticas Setoriais de Inovação, Regulação e Infraestrutura
Fernanda De Negri

Diretor de Estudos e Políticas Sociais
Rafael Guerreiro Osorio

Chefe de Gabinete
Sergei Suarez Dillon Soares

Assessor-chefe de Imprensa e Comunicação
João Cláudio Garcia Rodrigues Lima

Ouvidoria: http://www.ipea.gov.br/ouvidoria
URL: http://www.ipea.gov.br

Texto para Discussão

Publicação cujo objetivo é divulgar resultados de estudos direta ou indiretamente desenvolvidos pelo Ipea, os quais, por sua relevância, levam informações para profissionais especializados e estabelecem um espaço para sugestões.

Texto para discussão / Instituto de Pesquisa Econômica Aplicada.- Brasília : Rio de Janeiro : Ipea , 1990-

ISSN 1415-4765

1.Brasil. 2.Aspectos Econômicos. 3.Aspectos Sociais. I. Instituto de Pesquisa Econômica Aplicada.

CDD 330.908

JEL: O3; O31; O38.

SUMÁRIO

SINOPSE

A computação, eletrônica e a internet proporcionaram o livre e rápido trânsito das informações pelo globo. De certa forma, a sociedade moderna depende de sistemas de controle autônomo. Todavia, esta inovação tecnológica impõe um preço a ser pago: investimento em segurança cibernética referente a pessoas, dados, informações e infraestruturas. Alguns países no mundo já absorveram o tema como uma questão de Estado e institucionalizaram órgãos governamentais e estruturas para cuidar exclusivamente dele. Este texto apresenta alguns pontos relevantes da estratégia internacional para o espaço cibernético dos Estados Unidos, além do posicionamento da Rússia e Índia sobre o tema. Em seguida, apresenta um panorama da situação brasileira, a partir da Estratégia Nacional de Defesa, documento que introduz a responsabilização da defesa do espaço cibernético brasileiro. Mostra o posicionamento, na hierarquia do governo federal, das diversas agências e organizações responsáveis por conduzirem as atividades de inteligência necessárias à segurança do espaço cibernético no Brasil. Por fim, traz um panorama das infraestruturas de tecnologia da informação (TI) ora existentes no Brasil, especialmente na administração pública federal.

Palavras-chave: segurança e defesa cibernética; organização institucional; comparação internacional; Estados Unidos; Rússia; Índia; Brasil.

ABSTRACT[i]

Computing, electronics and internet provides the free and fast flow of information across the globe. In a way, modern society depends on these autonomous control systems. However, this technological innovation requires a price to be paid: investment in cyber security of people, data, information and infrastructure. Some countries have already absorbed the issue as a matter of state and institutionalized government structures to take care exclusively of it. This paper presents some relevant points of the International Strategy for Cyberspace of the United States, besides the positioning of Russia and India on the subject. It then presents an overview of the Brazilian situation, from the the National Defense Strategy, a document that introduces the responsibility of protecting Brazilian cyberspace. It shows the arrangement, in the federal government

---

i. *The versions in English of the abstracts of this series have not been edited by Ipea's publishing department*.
As versões em língua inglesa das sinopses desta coleção não são objeto de revisão pelo Editorial do Ipea.

hierarchy, of the various national agencies and organizations responsible for conducting intelligence activities necessary for the national security of Brazil. Finally, it provides an overview of the IT infrastructure existing in Brazil, especially in the federal public administration.

Keywords: cyber security and defense; institutional arrangement; international comparison; USA; Russia; India; Brazil.

1 INTRODUÇÃO

A sociedade está cada dia mais dependente da internet e dos sistemas de informação e, a despeito disto, as vulnerabilidades de *softwares* e sistemas computacionais permanecem amplamente difusas. Estas vulnerabilidades colocam em risco pessoas, negócios e governos que dependem fortemente da segurança de suas redes (Santos, 2012). O objetivo deste trabalho é apresentar, de forma exploratória, os riscos existentes no espaço cibernético e, ainda, fazer uma comparação entre a estrutura de segurança e defesa cibernética brasileira e de alguns países relevantes no cenário mundial.

Sistemas de informação e comunicação constituem a base do desenvolvimento econômico e social de um país. Pela vertente empresarial, segurança e defesa cibernética são usados para manter o sigilo de informações classificadas do parque industrial nacional, responsável pelas vantagens comparativas ou especializações entre os países. Por sua vez, pelo lado governamental, dizem respeito à proteção, contra ataques ou sabotagens, das infraestruturas críticas de uma nação – por exemplo, do sistema elétrico, das telecomunicações, de transporte, de segurança, do sistema financeiro etc. Em outras palavras, as infraestruturas nacionais dependem de sistemas de segurança e defesa cibernética de modo a garantir, sobretudo, a soberania nacional.

Os eventos relacionados ao ambiente cibernético ocorridos nos últimos anos mostram que há países que já vivem em uma guerra fria cibernética. Dois exemplos recentes confirmam isto. O governo norte-americano reconheceu que houve acessos não autorizados aos arquivos de desenvolvimento dos caças F-35 e F-22 da Força Aérea norte-americana. Cerca de dois anos depois, a China apresentou seus próprios jatos em muitos aspectos semelhantes àqueles invadidos (McCaul, 2012). Outro exemplo recente é a sabotagem, supostamente liderada pelo governo norte-americano, das instalações nucleares do Irã, onde toda a planta de enriquecimento de urânio foi destruída por meio de um vírus de computador (Grego, 2012).

A análise do cenário internacional é relevante, pois é capaz de gerar conhecimento a ser aplicado ao caso nacional. Os dois principais casos a serem estudados seriam Estados Unidos e China. Em virtude da falta de documentos oficiais chineses, optou-se por analisar o caso russo para se ter uma contraparte ao polo norte-americano. A Índia foi a terceira escolha por se constituir um país em desenvolvimento, assim como o Brasil.

O Brasil tem se destacado no cenário mundial por sua ascensão econômica, desenvolvimento social, postura política e organização de grandes eventos.[1] Com isto, tem-se conseguido atrair a atenção não apenas de turistas e investidores, mas também de *hackers*. Atualmente, são registrados cerca de 3 mil incidentes de segurança virtual por mês apenas nas redes da administração pública federal, provenientes de países como Estados Unidos, Brasil, França, Grã-Bretanha, Rússia entre outros (Brasil, 2013a).

O ambiente virtual não tem fronteiras. Assim, uma rede comprometida pode prejudicar outras, sejam elas públicas, privadas, contíguas ou não. Por isto, a colaboração e a constante interação entre os mais diversos atores são essenciais para garantir um elevado nível de proteção cibernética para todos (Mandarino Junior, 2010).

Isoladamente, nem o governo, nem a academia e nem a indústria conseguirão obter sucesso na proteção das próprias redes. São necessárias ações conjuntas entre estes setores. Portanto, constitui-se um indicativo tanto para a academia quanto para a indústria nacional visando suprir uma demanda iminente por sistemas seguros. Prevenir, identificar vulnerabilidades e preparar-se para situações de risco devem ser questões de Estado e não apenas priorização de governo.

A fim de cumprir os objetivos propostos, optou-se por organizar este texto da seguinte forma: na seção dois é apresentada uma revisão da literatura sobre questões relacionadas à defesa cibernética. Em seguida, na seção três, são apresentadas as questões metodológicas adotadas neste estudo. Na quatro, são apresentados os principais pontos das estratégias dos Estados Unidos; e em seguida, na seção cinco, da estratégia russa; e de uma descrição da estratégia do governo indiano, na seção seis. A seção sete, dividida em quatro subseções, traz o caso brasileiro: na subseção 7.1 é apresentada a organização institucional referente à segurança e defesa no Brasil; na 7.2, é feita uma análise desta organização; em seguida, na subseção 7.3, é apresentada a Estratégia Nacional de Defesa; e na subseção 7.4 é apresentado um panorama das infraestruturas de TI no Brasil, especialmente na administração pública federal. As conclusões do trabalho são apresentadas na seção oito. Os apêndices A, B e C apresentam, respectivamente, a tradução de pontos considerados relevantes pelo autor das estratégias dos Estados Unidos, Rússia e Índia.

1. Jogos Pan-Americanos, em 2007; Jogos Mundiais Militares, em 2011; Jornada Mundial da Juventude de 2013; Copa das Confederações, em 2013; Copa do Mundo, em 2014; Jogos Olímpicos, em 2016; e Copa América, em 2019.

2 A DEFESA CIBERNÉTICA

Antes de discorrer sobre aspectos relativos à defesa cibernética cabe apontar alguns conceitos relevantes.

Defesa cibernética diz respeito ao conjunto de ações defensivas, exploratórias e ofensivas, no contexto de um planejamento militar, realizadas no espaço cibernético, com as finalidades de proteger os sistemas de informação, obter dados para a produção de conhecimento de inteligência e causar prejuízos aos sistemas de informação do oponente (Brasil, 2011).

Segurança cibernética refere-se 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 (Brasil, 2011).

De fato, os conceitos de segurança e defesa são complementares. Neste trabalho, o termo segurança será utilizado, pelo cunho governamental, como a proteção de infraestruturas críticas e dos sistemas de informação e comunicação da administração pública federal. Por seu turno, defesa refere-se às ações de proteção do Estado brasileiro frente a ameaças que possam colocar em risco a soberania nacional – função normalmente assumida por militares.

O conceito de segurança faz referência a infraestruturas críticas, as quais são definidas como instalações, serviços, bens e sistemas que, caso sejam interrompidos ou destruídos, provocam sério impacto econômico, político e social à segurança do Estado e da sociedade (Brasil, 2011).

Dessa forma, percebe-se que segurança e defesa cibernética buscam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade dos ativos de informações. Estes ativos são entendidos como o valor tangível e intangível que reflete tanto a importância do ativo de informação para o alcance dos objetivos estratégicos de um órgão ou entidade, quanto o quão cada ativo de informação é imprescindível aos interesses da sociedade e do Estado.

A partir das definições, parte-se para a abordagem do tema.

Por meio de uma rápida análise dos incidentes cibernéticos que vêm ocorrendo pelo mundo, é fácil perceber que, certamente, alguns países já possuem a capacidade de desenvolver armas digitais com alto poder destrutivo, se não já as tiverem desenvolvido. Mas, a exemplo de uma bomba nuclear, não é pelo fato de tê-la desenvolvido que ela virá a ser utilizada.

O ambiente cibernético não existe por si só: sua dinâmica de funcionamento depende de conjunturas e interesses não virtuais. Além disso, o ineditismo de uma arma cibernética é fundamental para a sua eficácia, e utilizá-la de maneira inadequada, ou precocemente, pode significar perda de tempo, ativo, recurso e vantagem comparativa.

Atualmente, apesar de não existir um cenário de guerra declarada entre grandes potências mundiais, os frequentes ataques provocam um clima de desconfiança generalizada.

Há ainda o temor de que a modernização tecnológica, especialmente das infraestruturas críticas, possa ser uma porta de entrada para ataques ou sabotagem de possíveis inimigos (Clarke e Knake, 2011).

A guerra fria cibernética vivida hoje apresenta uma diferença básica do período em que vigorou a guerra fria tradicional. Naquela época, havia um efeito "demonstração" de tecnologias militares que não se vê mais – pelo menos não abertamente como era feito. Praticamente todos os ataques cibernéticos ocorridos até então são apócrifos.

É difícil atribuir a responsabilidade de um ataque a um ou outro país. O ambiente virtual, quando utilizado de maneira inteligente, favorece o anonimato na medida em que os comandos de ataque podem ser distribuídos por servidores espalhados pelo mundo antes de chegar a seu alvo. Frequentemente, redes de países sem acordo diplomático são utilizadas para dificultar uma eventual sequência investigativa. Por esta razão, a maioria dos ataques ocorridos até hoje ainda não foram oficialmente atribuídos a algum país, uma vez que ninguém assume sua autoria (Kramer, Starr e Wentz, 2009). Não obstante a dificuldade de identificação dos autores das atividades maliciosas, é possível especular quem esteja por trás delas.

O processo de rastreamento e identificação de autores no espaço cibernético não é fácil de ser feito, mas também não é impossível. Por exemplo, Estados Unidos e Rússia já se posicionaram no sentido de que qualquer ameaça identificada, seja em qualquer ambiente, poderá ser objeto de retaliação utilizando-se forças militares cinéticas, e não apenas cibernéticas.

Os principais acusados de ataques são os Estados Unidos e a China, fato que apenas remonta, também nessa dimensão, o cenário de força e disputa não virtual. Isto porque estes países estão sempre entre os acusados ou acusadores por roubo de informações, invasões de redes ou ataques de cunho político ou intelectual.

Outros países como Estônia, Irã, Geórgia e Israel, que já se envolveram em conflitos cibernéticos de repercussão internacional, podem ser considerados coadjuvantes, pois, ou foram vítimas, ou, quando atacantes, suas ações estiveram apoiadas nas principais potências.

Independentemente da identificação, os fatos mostram que a tendência é que ataques continuarão a ocorrer com frequência e sofisticação ainda maiores (Bauer e Van Eeten, 2009).

Muito se diz que guerras cibernéticas são assimétricas por possibilitar que um país, considerado pobre, consiga atacar e causar prejuízo a outro, considerado rico, utilizando armas cibernéticas. Todavia, ataques cibernéticos, especialmente a infraestruturas críticas, podem resultar em retaliação com forças militares, como já dito. Ou seja, um país que assume o risco de ser pego operacionalizando atividades maliciosas na rede deve ser capaz de arcar com as eventuais consequências de seus atos.

Além disso, armas de guerra cibernética são armas de aplicação específica, que exploram vulnerabilidades singulares de sistemas customizados. Assim sendo, o custo de desenvolvimento será relativamente elevado pela especialização do *software*, equipe necessária de profissionais altamente capacitados, compra de vulnerabilidades[2] etc. Ademais, as armas cibernéticas também caracterizam-se pela alta volatilidade, pois, uma vez descobertas, são colocadas em desuso muito rapidamente com a substituição de equipamentos ou eliminação das vulnerabilidades.

2. É possível comprar, no mercado negro, vulnerabilidades jamais exploradas (*0-day*) dos mais variados sistemas. Todavia, o custo associado a elas normalmente passa dos milhares, em alguns casos milhões, de dólares.

Esse foi o caso do *Stuxnet*, um vírus espalhado por diversos computadores do mundo, mas que operou apenas nas usinas nucleares do Irã. Conforme noticiário internacional, as linhas de código do vírus apresentam registro de vários teclados do mundo, ou seja, ele pode ter sido desenvolvido em colaboração entre países, ou então isso foi feito apenas para cobrir rastros, não havendo ainda certeza sobre o que de fato ocorreu. Os programadores tiveram acesso a quatro vulnerabilidades "dia zero" do sistema de controle e aquisição de dados (em inglês, *supervisory control and data acquisition* – SCADA), ou seja, quatro vulnerabilidades jamais exploradas de um sistema utilizado praticamente no mundo todo. O mais provável é que essa informação tenha vazado por alguém do fabricante do sistema (Falliere, Murchu e Chien, 2011). O vírus conseguiu alterar a velocidade dos rotores das usinas nucleares e ao mesmo tempo enganava o sistema supervisor para que não detectasse qualquer anormalidade. Com isto, sem ser notado, superaquecia as plantas de produção até sua destruição. Quando se identificou que havia algo errado, os prejuízos estavam estabelecidos e o cenário era irreversível (Falliere, Murchu e Chien, 2011).

A partir da identificação das falhas, o fabricante do sistema se comprometeu a corrigi-las e atualizar o *software* de todas as plantas que utilizam o controlador pelo mundo. Hoje, todo o código fonte do *Stuxnet* está disponível na internet, e a preocupação é como ele poderá ser alterado de maneira a ser reutilizado. Existem indícios de que dois outros vírus são frutos dele, o *Duqu* e o *Flame*, ambos com foco no roubo de informações (Ferran, 2012).

De forma geral, a proteção no espaço cibernético está intrinsicamente ligada aos mecanismos de ataque existentes. Ataque e defesa (ou segurança) são, na prática, duas faces da mesma moeda. Isto porque o sucesso do atacante depende basicamente das vulnerabilidades encontradas na defesa do sistema-alvo. Assim, para se planejar um sistema de defesa adequado, é preciso estar atualizado com os mecanismos e meios de ataques existentes.

A interação e a cooperação com outros atores é claramente uma via necessária, mas não suficiente, para conseguir avançar nas tecnologias de segurança e defesa cibernética. Somente por meio da troca de informações e compartilhamento de boas práticas é possível aumentar as possibilidades de identificação de falhas ou brechas que podem ser exploradas (ataque) ou sanadas (defesa/segurança). Nesse cenário, todos passam a ter importância operacional: sociedade civil, governo, meio acadêmico e setor empresarial.

Outro aspecto a ser destacado é que proteção cibernética refere-se muito mais à capacitação de pessoas do que a investimentos em equipamentos. Portanto, o foco de uma política nacional de segurança da informação deve ser no treinamento de pessoal e formação de especialistas (Takemura, Osajima e Kawano, 2009).

Haja vista que o tema, proteção cibernética, envolve aspectos da soberania nacional, recomenda-se que tenha lugar, atenção e interesse entre os mais altos níveis político-estratégicos de governo. Somente assim o próprio poder público terá condições mínimas e recursos para conduzir as ações necessárias à proteção cibernética nacional e, com isso, garantir que toda a sociedade possa usufruir dos benefícios que a internet e os sistemas computacionais podem oferecer.

3 ASPECTOS METODOLÓGICOS

Os Estados Unidos e a China, atualmente, são os principais atores mundiais no ambiente cibernético. Eles estão entre os mais apontados pela imprensa especializada[3] como responsáveis por ataques a diversos países, especialmente entre eles mesmos.

A fim de analisar a organização institucional de alguns países, buscou-se fundamentar este trabalho em documentos oficiais divulgados pelo governo de cada um deles. A partir de então, deparou-se com a grande dificuldade para se encontrar documentos oficiais reportando a organicidade ou mesmo posicionamento do governo chinês. Por isso, o panorama chinês não é apresentado neste trabalho. De todo modo, sabe-se que por lá opera um regime muito restritivo de acesso às informações aos cidadãos, bem como fortes limitantes à interconexão das redes nacionais com o restante do mundo (Santos, 2012b).

Optou-se, então, por eleger três países que pudessem servir de comparação com o caso brasileiro. Foram selecionados Estados Unidos, Rússia e Índia. Os Estados Unidos foram escolhidos por ser o país de maior liderança no espaço cibernético. A Rússia, por ser, possivelmente, o segundo maior competidor por tecnologias cibernéticas frente aos Estados Unidos. A Índia, por sua vez, foi escolhida por constituir-se em um país em desenvolvimento e cuja realidade política internacional se assemelha ao caso brasileiro.

3. Até hoje, nenhum país assumiu oficialmente a autoria de qualquer ataque já registrado.

Em 16 de maio de 2011, o coordenador de segurança cibernética do presidente Barack Obama, Howard A. Schmidt, anunciou o lançamento da Estratégia Internacional Norte-Americana para o Espaço Cibernético[4] (United States, 2011). Este documento é um marco para o ambiente cibernético mundial, pois, além de ser o primeiro nesse sentido, torna pública a posição estratégica e operacional do maior ator mundial no ambiente virtual.

A partir do posicionamento dos Estados Unidos, outros países começaram a criar ambientes de discussão para formularem seus próprios planos estratégicos. O *site* do Ministério da Defesa russo apresenta um documento intitulado *Visões conceituais sobre as atividades das Forças Armadas da Federação da Rússia no espaço de informação*[5] (Rússia, 2011). Este documento foi elaborado em 2011 e publicado no início de 2012.

Como o documento é disponibilizado apenas na língua russa, foi utilizada a ferramenta *Google Translator,* com ajustes de concordância e coerência, como ferramenta de tradução. Na tradução, nota-se que a expressão "espaço das informações" é utilizada diversas vezes como o equivalente a espaço cibernético. Optou-se por manter a expressão como traduzida: espaço das informações. Quase a metade do documento é dedicada a definições de termos relacionados ao tema e, em seguida, volta-se a trazer princípios e regras de conduta a serem seguidas pela Federação Russa. A análise aqui apresentada tem foco na segunda metade do documento.

Sobre a Índia, em março de 2011, o Ministério das Comunicações e Tecnologias da Informação disponibilizou uma prévia sobre as discussões a cerca do espaço cibernético, cujo título é *Projeto de discussão sobre política nacional de segurança cibernética*[6] (Índia, 2011). O documento traz um panorama das diretrizes e princípios a serem seguidos pela nação indiana.

4. Em inglês, International Strategy for Cyberspace.

5. Em russo, Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве. Tradução do Google Translator, com adaptações.

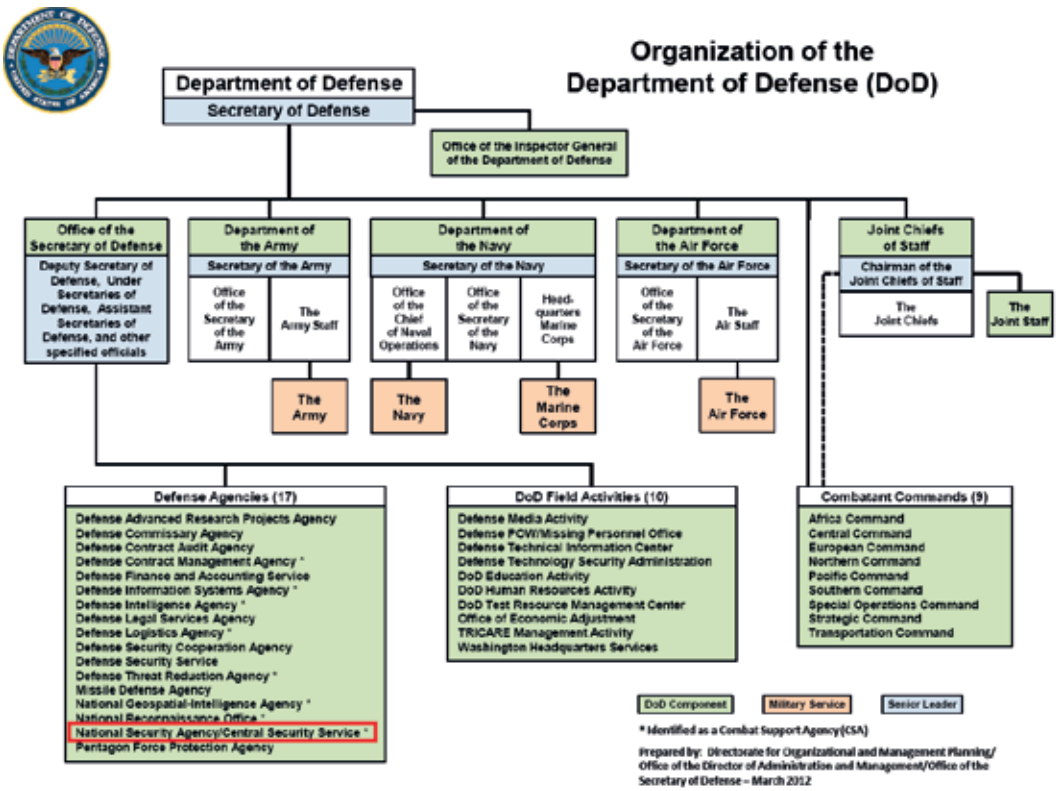
6. Em inglês, *Discussion draft on national cyber security policy*.

4 ESTRATÉGIA CIBERESPACIAL NORTE-AMERICANA

Os Estados Unidos têm como principal órgão responsável pela condução da política nacional de segurança da informação a National Security Agency (NSA). A NSA é a agência responsável por todas as questões afetas à segurança cibernética do governo norte-americano. A NSA integra a estrutura do Departamento de Defesa (em inglês, Department of Defence – DoD), equivalente ao Ministério da Defesa brasileiro.

A NSA, há sessenta anos, é a agência responsável pela segurança das comunicações e tecnologias da informação dos órgãos federais do governo norte-americano. Ela chegou a financiar a própria criação da internet na década de 1960 (Tanenbaum, 2011). Além disso, ela é a responsável por dar apoio ao DoD, à Comunidade de Inteligência (U.S. Intelligence Community), às agências de governo e aos parceiros na indústria com produtos e serviços relacionados ao espaço cibernético (United States, 2013). Na figura 1, é apresentado o arranjo institucional da defesa norte-americano.

FIGURA 1
Estrutura organizacional do Departamento de Defesa norte-americano



Fonte: United States (2012a).

Os Estados Unidos contam, ainda, com dezesseis agências e escritórios responsáveis por conduzirem as principais atividades de inteligência necessárias para garantir a segurança nacional. Estes dezesseis organismos atuam tanto independentemente como em conjunto, agregados no que chamam de Comunidade de Inteligência Norte-Americana, ou U.S. Intelligence Community (The Technolytics Institute, 2012). São eles:

1) Central Intelligence Agency (CIA)
2) Air Force Intelligence, Surveillance & Reconnaissance Agency (AFISRA)
3) Army Military Intelligence (MI)
4) Defense Intelligence Agency (DIA)
5) Marine Corps Intelligence Activity (MCIA)
6) National Geospatial-Intelligence Agency (NGA)
7) National Reconnaissance Office (NRO)
8) National Security Agency (NSA)
9) Office of Naval Intelligence (ONI)
10) DOE Office of Intelligence and Counter Intelligence (OICI)
11) DHS Office of Intelligence and Analysis (I&A)
12) Coast Guard Investigative Service (CGIS)
13) Federal Bureau of Investigation (FBI)
14) Drug Enforcement Administration (DEA)
15) State Department Bureau of Intelligence and Research (INR)
16) Treasury Office of Terrorism and Financial Intelligence (TFI)

O esforço coletivo dessas organizações é direcionado para adquirirem informações nas mais diversas áreas – por exemplo, militar, política, terrorismo internacional, *hacktivismo*[7] etc. Os órgãos citados já são tradicionais e muitos deles existem há décadas. Entretanto, apenas em junho de 2009 foi criado o U.S. Cyber Command (USCyberComm), órgão responsável pela coordenação das ações de prevenção e defesa cibernética norte-americanas.

7. Junção de *hack* e *activismo*: promoção ou divulgação de ideais políticos, ideologias, luta pela liberdade de expressão ou informação ética.

O USCyberComm é uma subunidade das Forças Armadas subordinada ao Comando Estratégico norte-americano. Desta forma, o USCyberComm foi criado para ter acesso e cooperação tanto das forças militares como de outros órgãos integrantes da comunidade de inteligência.

O comandante do USCyberComm também exerce a função de diretor da Agência de Segurança Nacional (NSA) e chefe do Serviço Central de Segurança (em inglês, Central Security Service – CSS). Com isto, uma só pessoa é responsável tanto pela segurança quanto pela defesa naquele país. Na prática, muitas ações de defesa confundem-se com segurança e, por isso, as políticas de ambas devem estar muito bem alinhadas.

A partir disso, é possível notar que o espaço cibernético norte-americano, apesar de possuir várias frentes de colaboração, possui apenas um responsável pela segurança e defesa cibernética nacional.

O USCyberComm pode ser considerado apenas uma peça de todo o sistema de proteção, criado basicamente para a gerência das atividades. E mesmo antes de sua criação, ações no ambiente cibernético já eram uma realidade dentro da NSA.

No início de 2011, os Estados Unidos anunciaram o lançamento da sua Estratégia Internacional para o Espaço Cibernético (United States, 2011). O documento inicia destacando a importância do tema para o desenvolvimento da humanidade e condiciona os benefícios das tecnologias da informação e comunicação a um ambiente confiável e seguro. Valoriza, ainda, aspectos relacionados à promoção da liberdade de expressão e associação, privacidade e o livre fluxo de informações.

A estratégia é apresentada como um convite a todos os interessados, sejam países, sociedade civil, setor privado ou usuários, a se juntarem e colaborarem a fim de colocar em prática a proposta governamental então apresentada. Reforça a importância de parcerias, capacitação humana, abertura comercial, respeito à propriedade e a promoção dos direitos universais.

Todavia, afora todas as vantagens oferecidas, o documento assegura o direito de defesa que poderá ou não seguir as vias diplomáticas. Assim, assumem que poderão ser tomadas medidas de retaliação utilizando forças militares. Ou seja, apenas deixa claro

que o ambiente cibernético não se restringe ao virtual, e que ações cibernéticas poderão tomar proporções como qualquer outra ofensiva militar inimiga.

Em âmbito nacional, o documento afirma que os Estados Unidos irão garantir a segurança e a estabilidade das redes internas. Com isto, pode-se inferir que medidas coercitivas poderão ser tomadas contra o setor privado de modo a garantir a proteção das redes.

Iniciativas de monitoramento e controle de tráfego de dados entre cidadãos já estão em andamento. Por exemplo, com o intuito de reprimir a pirataria de conteúdo digital, o governo está com um programa de identificação de endereços IPs[8] suspeitos de compartilharem conteúdo indevidamente. Assim que identificados, os suspeitos persistentes na violação ao direito de propriedade recebem seis avisos para se justificarem ou cessar o ilícito; caso contrário, sua velocidade de conexão pode ser rigorosamente reduzida (US Internet, 2013).

Por último, destaca-se que o texto deixa claro que segurança e defesa cibernética dependem muito mais da capacitação de pessoas, ou capacidade intelectual, que de produtos e equipamentos. Com isto, é observada uma supervalorização nos esforços para capacitação humana e difusão de informações.

5 ESTRATÉGIA CIBERESPACIAL RUSSA

Ao que parece ser uma resposta ao documento norte-americano, a Rússia disponibilizou no *site* do seu Ministério da Defesa um documento intitulado *Visões conceituais sobre as atividades das Forças Armadas da Federação da Rússia no espaço da informação* (Rússia, 2011).

O documento traz, além da parte introdutória e conceitual, basicamente, as mesmas garantias fundamentais mencionadas no documento norte-americano. Uma nítida diferença é que o documento russo apresenta metas e princípios menos generalistas e mais voltados à realidade da nação russa. Diferentemente dos Estados Unidos, não se colocam como os líderes mundiais do desenvolvimento da internet. Com isso, valorizam acordos, por exemplo, com nações parceiras e/ou contíguas que compartilham a mesma política de governo.

8. O endereço IP é uma identificação de um dispositivo em uma rede. Cada computador na possui um IP (*internet protocol* ou protocolo de internet) único, que é o meio pelo qual as máquinas se comunicam na internet.

Valoriza o respeito ao Estado de direito e os princípios da legalidade. Reconhece a complexidade do novo paradigma e as várias dimensões envolvidas em torno do tema. Reconhece que, apenas por meio de interação e cooperação com outros países, é possível evoluir, na velocidade necessária, no campo dos sistemas de proteção.

O documento não menciona ações ofensivas russas no espaço das informações. Pelo contrário, evidencia a busca pela erradicação de fatores que possam gerar conflitos, mas, caso eles ocorram, aponta que soluções diplomáticas devem ser tomadas, com base no direito internacional. Todavia, destaca a possibilidade de utilização de forças cinéticas em um eventual conflito cibernético com fulcro no princípio do direito da autodefesa para repelir a agressão tanto contra o Estado russo quanto contra seus aliados.

O documento não trata da estrutura organizacional por trás da segurança e defesa cibernética. Por meio de pesquisas na internet também não foi possível encontrar algum documento que clarificasse a questão.

Para mais detalhes sobre o documento, ver os apêndices com a tradução dos pontos considerados relevantes pelo autor deste texto.

6 ESTRATÉGIA CIBERESPACIAL INDIANA

Outro país que também pretende se colocar como um ator no espaço cibernético é a Índia. Sendo um dos membros do BRICS, seu posicionamento torna-se relevante para o Brasil.

O país ainda não possui uma estratégia oficial, mas no *site* do Departamento de Eletrônica e Tecnologias da Informação, ligado ao Ministério das Comunicações e Tecnologias da Informação indiano, é possível ter acesso aos documentos preliminares com princípios para o setor (Índia, 2011).

O documento começa apresentando as agências interessadas ou relacionadas ao tema:

1) National Information Board (NIB)
2) National Crisis Management Committee (NCMC)
3) National Security Council Secretariat (NSCS)

4) Ministry of Home Affairs
5) Ministry of Defence
6) Department of Information Technology (DIT)
7) Department of Telecommunications (DoT)
8) National Cyber Response Centre - Indian Computer Emergency
9) Response Team (CERT-In)
10) National Information Infrastructure Protection Centre (NIIPC)
11) National Disaster Management of Authority (NDMA)
12) Standardisation, Testing and Quality Certification (STQC) Directorate
13) Sectoral CERTs

Pelo texto, infere-se não haver um órgão exclusivamente responsável pela condução das ações relacionadas à segurança e defesa cibernética. A princípio, o tema é abordado, pelos órgãos, à medida que couber a cada um e, por meio da cooperação geral, é possível conduzir as ações de proteção.

Salienta a necessidade de integração entre os setores público e privado, bem como a interação com outros países, por considerar que de outra forma não é possível alcançar níveis aceitáveis de segurança cibernética.

O documento reconhece que as soluções em segurança cibernética devem estar à frente de tecnologias tradicionais como *antivírus* e *firewalls*. Deve haver correlação de informações efetivas a partir de múltiplas fontes e monitoramento em tempo real de ativos que precisam ser protegidos e, ao mesmo tempo, garantir que recursos e capacitação adequada estejam prontos para lidar com situações de risco. Assim como os outros países, reconhece a clara necessidade de foco nas pessoas e nos processos, aliados às melhores soluções de tecnologia disponíveis. De outra forma, a política se torna ineficaz.

Por fim, um aspeto fundamental e inovador destacado pelo texto é que questões de segurança devem ser integradas já na fase de projeto conceitual de sistemas, quando este vier a ser desenvolvido e implantado, ajustadas às infraestruturas críticas, e não tratadas como problemas tardios a serem resolvidos.

7 O BRASIL

7.1 Organização institucional brasileira

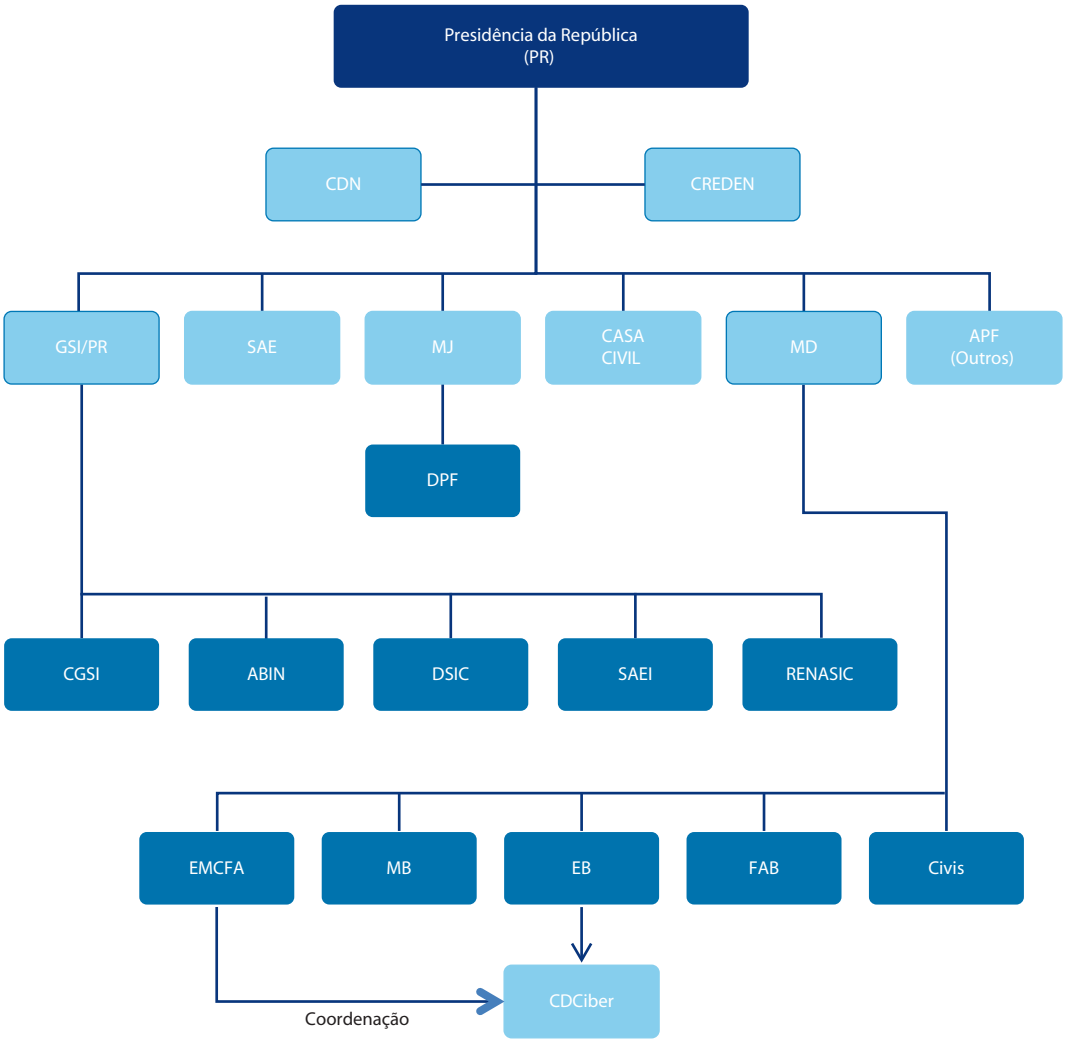
A sistematização de instituições e a distribuição de competências entre os organismos para o desenvolvimento de segurança e defesa cibernética é bem recente no Brasil. Algumas instituições que existem há décadas ainda precisam ser adaptadas à nova temática e realidade social. Segurança e defesa cibernética são tratadas no Brasil por diversos organismos. Incluem-se instituições públicas, desde o nível estratégico, de governo, até os operacionais, além da atuação de entidades não governamentais representando o setor privado.

Em relação ao setor público federal, a competência está descentralizada entre diversas entidades. Cada uma possui uma abordagem específica, conforme a missão da instituição, de modo que todas possam contribuir com a proteção do espaço cibernético no território nacional. A cooperação, o trabalho em conjunto e a disseminação ordenada de informações tornam-se essenciais em um mundo conectado e em constante evolução.

De forma resumida, as ações operacionais em segurança cibernética do governo federal são conduzidas pelo Departamento de Segurança da Informação e Comunicações (DSIC) do Gabinete de Segurança Institucional (GSI) da Presidência da República (PR). E a defesa, pelo Centro de Defesa Cibernética (CDCiber), que compõe a estrutura do Exército Brasileiro (EB), vinculado ao Ministério da Defesa (MD). Todavia, existe todo um sistema hierárquico de tomada de decisão estratégica a partir da Presidência da República até que chegue ao nível operacional, conforme apresentado na figura 2 adiante.

Segurança e defesa cibernética são tratadas, quando necessário, pelo Conselho de Defesa Nacional (CDN). O Art. 91 da Constituição Federal de 1988 define que trata-se de órgão de consulta do presidente da República nos assuntos relacionados à soberania nacional e à defesa do Estado democrático. Constitui um órgão de Estado e tem sua secretaria-executiva exercida pelo ministro-chefe do Gabinete de Segurança Institucional da Presidência da República (GSI/PR).

FIGURA 2
Sistema institucional de segurança e defesa cibernética brasileiras



Fonte: Brasil (2011, p. 211).

A Câmara de Relações Exteriores e Defesa Nacional (Creden) é um órgão de governo para assessoramento do presidente da República nos assuntos pertinentes às relações exteriores e defesa nacional. Sua presidência cabe ao ministro-chefe do GSI/PR e, entre outras de suas atribuições, encontra-se a segurança da informação.

A Casa Civil da Presidência da República também tem papel relevante por meio da garantia da execução de políticas, certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da Infraestrutura de Chaves Públicas Brasileiras (ICP/Brasil). Esta atribuição é de competência do Instituto Nacional de Tecnologia da Informação (ITI), autarquia federal vinculada à Casa Civil que tem o objetivo manter o ICP/Brasil.

Dentro da Presidência da República, o Gabinete de Segurança Institucional cumpre o papel de coordenador, no âmbito da administração pública federal (APF), de assuntos estratégicos que afetam a *segurança* da sociedade e do Estado, quais sejam: segurança das infraestruturas críticas nacionais; segurança da informação e comunicação; e segurança cibernética.

O GSI/PR é desconcentrado, estrategicamente, em cinco outros órgãos, listados a seguir.

1) Comitê Gestor de Segurança da Informação (CGSI) – 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 no Decreto nº 3.505, de 13 de junho de 2000, que instituiu a Política de Segurança da Informação nos órgãos e entidades da APF.
2) Secretaria de Acompanhamento e Estudos Institucionais (SAEI) – entre suas competências, encontram-se: acompanhar temas com potencial de gerar crises para o Estado, para a sociedade e para o governo; articular órgãos e instituições para prevenir a ocorrência de crises; coordenar o acionamento do Gabinete de Crises em caso de grave e iminente ameaça à estabilidade institucional; e coordenar a realização de estudos sobre assuntos relacionados à segurança institucional;
3) Agência Brasileira de Inteligência (Abin) – apesar do nome, não se classifica como agência no ordenamento jurídico brasileiro, mas, sim, como órgão central do Sistema Brasileiro de Inteligência (Sisbin). Tem por missão coordenar as ações do Sistema Brasileiro de Inteligência, produzir e salvaguardar conhecimentos sensíveis, atuando em duas frentes: inteligência e contrainteligência. Esta última, entendida como adoção de medidas que protejam os assuntos sigilosos relevantes para o Estado e a sociedade e que neutralizem ações de inteligência executadas em benefício de interesses estrangeiros. A Abin conta, ainda, 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.

4) Departamento de Segurança da Informação e Comunicações (DSIC) – o DSIC tem como atribuições planejar, implantar e coordenar políticas de segurança da informação e comunicações na APF; regulamentar a segurança de informações e comunicações para toda a APF; capacitar os servidores públicos federais, bem como os terceirizados, sobre segurança da informação e comunicações (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).

5) Rede Nacional de Segurança da Informação e Criptografia (RENASIC) – funciona coordenada pela Assessoria de Ciência e Tecnologia do GSI/PR e se constitui em uma 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 nestas atividades. Conforme o *site* da RENASIC, a rede tem gerado sinergia na discussão de problemas e soluções práticas de Tecnologia da Informação e Comunicações (TIC) e de SIC.

Se, por um lado, coube ao Gabinete de Segurança Institucional a gerência superior dos assuntos afetos à segurança, por outro, o Ministério da Defesa, por meio do Exército Brasileiro, assumiu as ações de defesa cibernética.

O Ministério da Defesa apresentou, em 2008, a Estratégia Nacional de Defesa (END),[9] com o objetivo de elaborar um plano de defesa focado em ações estratégicas de médio e longo prazo para modernizar a estrutura nacional de defesa. A END, aprovada pelo Decreto nº 6.703, de 18 de dezembro de 2008, definiu três setores estratégicos para defesa nacional: nuclear, cibernético e espacial. Delegou à Marinha do Brasil a gerência do programa nuclear; à Força Aérea, o programa espacial; e ao Exército Brasileiro, a liderança da defesa cibernética em território nacional.

O mencionado dispositivo legal também estabeleceu que as capacitações cibernéticas devem incluir, como parte prioritária, as tecnologias de comunicações entre todos os contingentes das Forças Armadas, de modo a assegurar sua capacidade de atuar em rede. Aponta, ainda, que todas as instâncias do Estado devem contribuir para o incremento do nível de segurança nacional, com particular ênfase nas infraestruturas

9. Há uma nova versão da END em tramitação no Congresso Nacional. Os arquivos enviados pelo Ministério da Defesa estão disponíveis em: <http://goo.gl/KzUYk>.

críticas. Devem aperfeiçoar os dispositivos e procedimentos de segurança que reduzem as vulnerabilidades dos sistemas relacionados à defesa nacional contra ataques cibernéticos e, se for o caso, que permitam seu pronto restabelecimento.

Assim, como resultado da delegação recebida a partir da END, o Exército Brasileiro, por meio da Portaria nº 666, de 4 de agosto de 2010, criou o Centro de Defesa Cibernética (CDCiber). Todavia, para que o Exército consiga oficializar a criação de um novo órgão, é preciso mudar sua estrutura regimental, e isso só é feito por meio da chancela presidencial. Em 2010, foi feita uma proposta de criação do Centro de Defesa Cibernética e, atualmente, a proposta está no Ministério do Planejamento, Orçamento e Gestão (MP), que estuda as implicações orçamentárias e de planejamento integrado do governo. Do MP, vai para a Casa Civil, para a sanção presidencial. A despeito disto, o CDCiber já está em operação desde 2011.

Em sua estrutura, para o apoio tecnológico, o Exército conta com o Centro de Desenvolvimento de Sistemas (CDS). Quando se decide pela elaboração de um determinado projeto no âmbito interno, por exemplo, é no CDS que os engenheiros militares vão desenvolver as linhas códigos de acordo com os padrões, requisitos técnicos e operacionais do sistema. Na parte de pesquisa, o Exército conta com o Instituto Militar de Engenharia (IME), com cursos de graduação, mestrado e doutorado. Não obstante a existência destes órgãos ligados ao Exército Brasileiro, atualmente o CDCiber está buscando solidificar parcerias com demais centros acadêmicos e de pesquisa, além de manifestar apreço por projetos elaborados em conjunto com o setor privado (Santos, 2012a).

Entre os objetivos do CDCiber estão a criação de um simulador de guerra cibernética, a elaboração de antivírus nacional, o desenvolvimento de um sistema de criptografia e a capacitação de militares para situações críticas. Estes objetivos vêm sendo atingidos com o apoio da iniciativa privada nacional, com alguns sistemas já em operação.

O Centro de Defesa Cibernética ainda não possui infraestrutura física própria e, até 2012, contava com a atuação direta de cerca de trinta militares. Teve um orçamento próprio aprovado para o quadriênio 2012-2015 de R$ 400 milhões a serem liberados em quatro partes iguais a cada ano. Além das funções previstas na portaria de sua criação, o CDCiber ainda atuou como gerente de segurança e defesa na Rio+20.

Por ocasião, aumentou seu orçamento de 2012 em 20% devido ao novo desafio. Pretende atuar como gerente operacional da proteção dos sistemas computacionais na Copa das Confederações, em 2013, nas Olimpíadas, em 2016, na Visita do Papa ao Brasil, em 2013, e na Copa do Mundo, em 2014.

Os órgãos até então mencionados não constituem a totalidade dos organismos públicos atuando no tema. Representam apenas uma lista dos principais atores governamentais. Sem dúvida, há dezenas de outros que dão suporte à política de proteção cibernética nacional, a exemplo da Polícia Federal (PF), Ministério da Justiça (MJ), Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança (CERT), Serviço Federal de Processamento de Dados (Serpro), centros de pesquisa e universitários, além dos profissionais de TIC nos órgãos públicos.

Além do setor público, ainda existem as organizações privadas que atuam proporcionando segurança na rede, proteção de dados, sistemas de criptografia, antivírus etc. Este setor é um braço forte e mais eficiente em termos operacionais e produtivos em relação ao setor público. Percebendo isso, o Exército Brasileiro tem se utilizado da capacidade da indústria nacional para desenvolver ferramentas estratégicas para o programa de segurança nacional. Contudo, a quantidade de empresas nacionais ainda é muito reduzida frente aos desafios do futuro. Atualmente, há cerca de 35 empresas de desenvolvimento e/ou fornecimento de soluções robustas em segurança ou defesa cibernética localizadas no país.[10] O setor público jamais conseguirá atingir níveis desejados de segurança ou defesa sem parcerias com o setor privado e vice-versa.

7.2 Análise institucional brasileira

O espaço cibernético é, por sua natureza, um ambiente de compartilhamento. Assim, é notório que o sucesso de um sistema de proteção cibernética depende, precipuamente, da colaboração de diversos atores.

No Brasil, fez-se a opção por segregar a direção das ações de segurança da informação e defesa cibernética em dois órgãos distintos e independentes entre si, respectivamente: GSI/PR e CDCiber/EB/MD.

10. Informações verbais, obtidas por meio de entrevista direta com alguns empresários atuantes no setor. As entrevistas ocorreram em 2011 e 2012 durante eventos de segurança da informação promovidos pela iniciativa privada (Rio de Janeiro) e durante eventos promovidos pelos militares brasileiros (Rio de Janeiro e Brasília).

Essa configuração tende a fragilizar o programa de proteção cibernética nacional na medida em que passa a depender da afinidade, integração e colaboração dos dirigentes de tais instituições. É natural que cada entidade tenha as suas prioridades, pois cada uma terá que prestar contas de seu trabalho de formas e a autoridades distintas. Assim, o nível de colaboração passa a ser relativizado conforme a conveniência do momento.

Além disso, essa dicefalia favorece tanto a sobreposição de tarefas quanto lacunas por indefinição de responsabilidades. Por exemplo, a partir da criação do CDCiber, o GSI/PR passou a dividir tarefas operacionais com ele de modo a compatibilizar as funções de cada um. Se estivessem em uma mesma estrutura hierárquica, isto favoreceria uma melhor distribuição de tarefas – além de ganharem força, visto que cada um possui uma estrutura relativamente pequena, com cerca de cinquenta pessoas.

Atualmente, o GSI/PR se apoia nas recomendações e decisões do TCU para conseguir fazer valer suas iniciativas. No Acórdão nº 1.233/2012, o TCU estabelece que, caso as normas estabelecidas pelo GSI/PR não sejam cumpridas, os órgãos sujeitos a tais regulamentos estarão em desconformidade com o ordenamento jurídico, sendo, assim, sujeitos à sanção:

> 9.8. Recomendar, com fulcro na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Gabinete de Segurança Institucional da Presidência da república (GSI/PR) que:
>
> (...)
>
> 9.8.2. em atenção a Lei 10.168/2003, art. 6º, IV, oriente os órgãos e entidades sob sua jurisdição que a implantação dos controles gerais de segurança da informação positivados nas *normas do GSI/PR não é faculdade, mas obrigação da alta administração, e sua não implantação sem justificativa é passível da sanção prevista na Lei 8.443/1992*, art. 58, II (subitem 0) (Brasil, 2012a, grifo nosso).

Já o CDCiber não tem função regulamentar. Suas iniciativas possuem pouca reverberação fora do ambiente militar, ou mesmo do Exército, porquanto são fundamentadas nas diretrizes estabelecidas na END.

Ao delegar a liderança das ações de defesa cibernética ao Exército Brasileiro, a END também criou uma multiplicidade de lideranças dentro do próprio Ministério da Defesa. Isto porque defesa cibernética deve ter representação nas três Forças, o que de

fato já ocorre atualmente. Cada unidade das Forças Armadas possui seu próprio núcleo de proteção cibernética, cuidando daquilo que lhe cabe. Isto pode fragilizar a defesa cibernética como um todo. Acredita-se que tal fato pode ser evitado caso o comando das ações cibernéticas se constitua em uma unidade autônoma, com representação das três Forças, subordinado apenas ao Ministério da Defesa.

Essa atribuição de liderança de defesa cibernética ao Exército Brasileiro é contraproducente. O programa nuclear, atribuído pela END à Marinha do Brasil, deve ser conduzido por ela uma vez que é a maior beneficiada direta do sucesso do programa (submarino nuclear), além de já vir acumulando experiência na área há décadas. O mesmo ocorre com o Programa Espacial que, mesmo que toda a sociedade se beneficie, é razoável que a Força Aérea seja a responsável por sua condução, dada a própria natureza das pesquisas envolvidas. Por sua vez, a defesa cibernética não se limita a uma área de atuação. Sua difusão em todos os sistemas das Forças Armadas exige ações coordenadas e um nível decisório mais elevado dentro da estrutura institucional brasileira.

Esta é, em parte, a estrutura adotada pelo governo norte-americano. O USCyberComm (equivalente ao CDCiber no Brasil) está dentro da NSA, responsável pela segurança e defesa cibernética governamental. A NSA, por sua vez, faz parte do DoD (equivalente ao Ministério da Defesa no Brasil), mas fora das Forças Armadas. Ou seja, nessa estrutura, o USCyberComm tem ascendência sobre todas as Forças Armadas norte-americanas.

7.3 Estratégia cibernética brasileira

O Brasil ainda não possui um documento que estabeleça as diretrizes próprias de uma estratégia nacional para a defesa cibernética. Ou seja, ainda não há um plano integrado de metas, objetivos e responsáveis para a melhoria da segurança e defesa cibernética a médio e longo prazo.

Não obstante, a Estratégia Nacional de Defesa (Brasil, 2008) trouxe algumas diretrizes referentes à defesa nacional, de forma mais geral, tais como:

- desenvolver, lastreado na capacidade de monitorar/controlar, a capacidade de responder prontamente a qualquer ameaça ou agressão: a mobilidade estratégica;
- fortalecer três setores de importância estratégica: o espacial, o cibernético e o nuclear;

- unificar as operações das três Forças, muito além dos limites impostos pelos protocolos de exercícios conjuntos;
- desenvolver, para atender aos requisitos de monitoramento/controle, mobilidade e presença, o repertório de práticas e de capacitações operacionais dos combatentes;
- rever, a partir de uma política de otimização do emprego de recursos humanos, a composição dos efetivos das três Forças, de modo a dimensioná-las para atender adequadamente ao disposto na Estratégia Nacional de Defesa;
- estruturar o potencial estratégico em torno de capacidades;
- preparar efetivos para o cumprimento de missões de garantia da lei e da ordem, nos termos da Constituição Federal;
- estimular a integração da América do Sul; e
- capacitar a indústria nacional de material de defesa para que conquiste autonomia em tecnologias indispensáveis à defesa.

Para a defesa cibernética, a Estratégia Nacional de Defesa aponta 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. (...) 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 (Brasil, 2008, p. 33 e p. 66).

O Brasil mantém uma postura internacional de promoção da paz e utilização das Forças para proteger ou repelir ameaças estrangeiras. Todavia, não se sabe, *a priori*, quais seriam as medidas a serem tomadas caso o Brasil se torne vítima de ataques cibernéticos identificáveis. Para cada grupo de ameaças – *hackers*, ativistas, grupos internacionais, países estrangeiros etc. –, acredita-se que o país irá definir a forma como proceder.

Por meio dos relatos oferecidos pelo general de divisão José Carlos dos Santos, Chefe do CDCiber, o Exército tem buscado manter contato com outros países a fim de estabelecer acordos de parcerias de modo a trocar informações e experiências, especialmente com países mais desenvolvidos na área que o Brasil. Vários são os convites

recebidos pelo Brasil para participar de eventos internacionais sobre o espaço cibernético. Países como Estados Unidos, Inglaterra e Argentina já se mostraram interessados no programa brasileiro para o espaço cibernético. Além disso, vários são os convites de parcerias tecnológicas, para troca de experiências, feitos por outros países e empresas internacionais (Santos, 2012b).

7.4 Infraestrutura de TI no Brasil

Ataques de natureza exploratória, por busca de informações ou obtenção de lucro indevido, já são uma realidade não apenas no Brasil, mas também no restante do mundo. Conforme informações do GSI/PR, as redes da administração pública federal atualmente recebem cerca de 3 mil ataques virtuais por mês (Brasil, 2013a). Organismos nacionais e internacionais de vigilância de rede analisam que o Brasil tem uma das infraestruturas de rede mais vulneráveis e desprotegidas do mundo (Hoepers, 2011; Symantec Corp., 2011; Falliere, Murchu e Chien, 2011).

Levantamento feito por Falliere, Murchu e Chien (2011) aponta que as grandes *botnets*[11] encontradas no Brasil contribuíram para sua primeira colocação, dentro da América Latina, no quesito computadores infectados por *bots*, zumbis e hospedeiros de *phishing*. Na América Latina, o Brasil ocupa a primeira colocação em todos os critérios de vulnerabilidade avaliados no estudo.

Outros organismos de pesquisa também analisam o cenário mundial de atividades maliciosas e, em nenhum deles, o Brasil se encontra em situação confortável.

Alguns organismos internacionais realizam um monitoramento contínuo das redes ao redor do mundo para verificar o nível de vulnerabilidade delas. Por exemplo, de acordo com Composit Blocking List (CBL),[12] o Brasil é classificado como o décimo país com maior quantidade de endereços IP comprometidos. De acordo com a Barracuda Networks,[13] o Brasil ocupa a segunda colocação em envio de *spam* pelo mundo,

11. *Botnets* ou redes de *bots* é o apelido para *robot* (robô). Eles recebem este nome por executarem uma variedade de tarefas automatizadas em nome de seus mestres (os criminosos cibernéticos), que normalmente se encontram em um local remoto, conectados via internet.
12. Disponível em: <http://cbl.abuseat.org/country.html>. Acesso em: 8 mar. 2013.
13. Disponível em: <http://www.barracudacentral.org/data/spam>. Acesso em: 8 mar. 2013.

contribuindo com 6,77% de toda a atividade mundial. Como resultado desta fragilidade, a Federação Brasileira de Bancos (Febraban) divulgou que a rede bancária brasileira teve um prejuízo de cerca de R$ 1,5 bilhão em 2011 com fraude eletrônica (CIAB, 2012) – fruto de um sistema altamente dependente das TICs e ao mesmo tempo muito vulnerável, seja em tecnologia ou por despreparo dos usuários.

Em relação à administração pública federal (APF), por onde circulam diariamente as informações mais sensíveis do país, a situação não é diferente. Em 2007, 2010 e 2012, o Tribunal de Contas da União (TCU) realizou amplo levantamento acerca da governança de tecnologia da informação no âmbito da APF, abrangendo, respectivamente, 255, 315 e 350 órgãos. Os resultados apresentados pelos relatórios indicam situação crítica desde 2007.

Com uma situação geral ruim já em 2007, mesmo com recomendações feitas pelo tribunal, foi constatado que nenhum dos indicadores relativos à segurança da informação – que envolve confidencialidade, integridade e disponibilidade da informação – apresentou avanço substancial. Isto significa que, um ano e meio depois dos alertas formulados pelo Acórdão nº 1.603/2008 – Plenário/TCU –, a administração pública permanecia exposta aos mesmos riscos, sem ter agido para reduzi-los. A seguir, alguns trechos podem ser transcritos:

> Ainda assim, o panorama da governança de TI, não obstante alguns progressos, permanece desolador. (...) um ano e meio depois dos alertas formulados pelo acórdão 1.603/2008 – Plenário, a administração pública permanece exposta aos mesmos riscos, não tem agido para reduzi-los, não consegue estimar suas consequências e continua a desconhecer a não proteger suas informações críticas adequadamente (TCU, 2010).

Em 2010, os resultados apontaram que, no que diz respeito à política de recursos humanos, em 20% das instituições, os gestores de TI não são escolhidos pela alta administração com base na competência. Trinta e cinco por cento das instituições da APF não preenchem pelo menos 75% das funções gerenciais de TI com pessoal do quadro próprio, e 75% não mantêm política de desenvolvimento de gestores de TI, o que compromete o desenvolvimento da área no longo prazo.

O TCU levantou, ainda, que, em 2010, apenas 5% das unidades encontravam-se no estágio aprimorado de governança de TI, com:

> (...) evidências do elevado compromisso da alta administração com a direção da instituição em todos os níveis, por meio de planejamento consistente e sistemático, fixação clara de objetivos e metas, monitoração e execução de auditorias" e ainda "o quadro de pessoal recebe qualificação sistemática e os processos de trabalho são formais e mensurados (TCU, 2010).

Já em 2012, o TCU constatou melhorias mais significativas em relação a 2010, mas ainda não suficientes.

> O levantamento de governança de TI 2012 revelou, de forma geral, melhoria da situação em relação ao levantamento de 2010. Contudo, ainda há instituições na faixa inicial de governança de TI, o que está distante do aceitável, tendo como referência os modelos de boas práticas de governança de TI e a legislação e a jurisprudência vigentes. (...) Quanto à gestão de segurança da informação, chamou bastante atenção a redução da quantidade de instituições que realizam análise de risco, insumo básico para outras ações de gestão de TI, como a continuidade do negócio. (...) Considerando apenas as instituições participantes dos levantamentos de 2010 e 2012, foi possível verificar, com razoável segurança estatística, que houve melhoria de 7,4 pontos percentuais na média geral do índice de governança de TI – iGovTI (TCU, 2012b).

Em acréscimo a todo o cenário na APF, destaca-se, ainda, que o estudo foi feito exclusivamente por meio do preenchimento de questionários pelas unidades consultadas, sem qualquer coleta de evidências comprobatórias pela equipe de levantamento. Com isto, existe a possibilidade de um viés nos resultados, pois é natural que as respostas dos interessados procurem destacar aspectos favoráveis de suas condutas. Isto significa que a situação real pode ser pior.

Conforme dito no início deste texto, segurança e defesa estão intimamente relacionadas e, por vezes, dependem uma da outra. Logo, falhas nos sistemas de tecnologia de informação dedicados à segurança, especialmente no âmbito da APF, impactam diretamente a confiabilidade dos sistemas de defesa cibernética.

8 CONCLUSÃO

O objetivo deste trabalho foi apresentar, de forma exploratória, os riscos existentes no espaço cibernético e, ainda, fazer uma comparação entre a estrutura de segurança e defesa cibernética brasileira e alguns países relevantes no cenário mundial.

Sistemas de informação e comunicação constituem-se a base do desenvolvimento econômico e social de um país. Além disso, todas as infraestruturas críticas nacionais dependem, em alguma medida, de sistemas de segurança e defesa cibernética de modo a garantir, sobretudo, a soberania nacional.

O suposto roubo dos projetos de desenvolvimento dos caças norte-americanos F-35 e F-22 pelos chineses e a destruição das instalações físicas nucleares do Irã por um vírus de computador são apenas exemplos do potencial econômico e social das tecnologias de informação e comunicação.

O Brasil, por adotar uma postura internacional de promoção de paz, não deve se preocupar em produzir armas cibernéticas ou algo do tipo, mas, sim, com a proteção de suas redes. O conhecimento apropriado por anos de pesquisa na extração do petróleo em águas profundas pela Petrobras, montagem de aeronaves pela Embraer, tecnologias agrícolas na fronteira do conhecimento desenvolvidas pela Embrapa, e tantas outras vantagens comparativas nacionais não podem estar abrigadas em um ambiente vulnerável. Além disso, dados governamentais sensíveis e informações sigilosas são diariamente manipulados por dispositivos eletrônicos ou computacionais e, por consequência, suscetíveis a invasões.

A maior parte das redes da administração pública federal apresenta níveis inaceitáveis de segurança, conforme relatórios de avaliação de governança de TI do TCU. Apesar de apresentar melhoras a partir de 2007, o quadro geral da APF ainda se mantém distante dos níveis adequados. Além da vulnerabilidade, dados do GSI/PR mostram que a APF registra cerca de 3 mil incidentes virtuais de segurança por mês. Certamente, deve haver incidentes que não são sequer identificados.

Por meio da comparação internacional, foi possível identificar diferenças estruturais, principalmente entre Brasil e Estados Unidos, destacadas no quadro 1 adiante.

QUADRO 1
Comparativo das principais diferenças encontradas entre Brasil, Estados Unidos, Rússia e Índia

	Estados Unidos	Rússia	Índia	Brasil
Arranjo institucional	US Cyber Command cuida da defesa e NSA cuida da segurança, ambos dentro da estrutura do DoD e com o mesmo dirigente.	-	Não há um órgão que assuma as responsabilidades da segurança e defesa. Algumas ações são tomadas no Ministério das Comunicações e Tecnologias da Informação.	Segurança: GSI/PR Defesa: CDCiber/EB/MD São estruturas distintas e com lideranças distintas.
Orçamento de gestão em 2012 para segurança e defesa cibernética	DoD: US$ 2,3 bilhões CyberComm: U$ 119 milhões (United States, 2012b)	-	-	GSI/PR: US$ 7 milhões CDCiber: US$ 45 milhões (Hulse, 2012)

Diretrizes	• Espaço cibernético:
	  • Aberto
	  • Interoperável
	  • Seguro
	  • Confiável
	• Liberdades fundamentais
	• Respeito à propriedade
	• Privacidade
	• Proteção contra o crime
	• Autodefesa
	• Estabilidade de rede
	• Governança multilateral
	• Dever de diligência
		• Respeito ao Estado de direito
		• Prioridade (Rússia)
		• Atenção à complexidade do ambiente virtual
		• Interação internacional
		• Cooperação
		• Inovação
			• Prioridade governamental
			• Vanguarda tecnológica
			• Inteligência cibernética
			• Hierarquia
			• Foco da política em pessoas
			• O tema deve ter força a partir dos níveis estratégicos
				Defesa nacional:
				• Dissuadir hostilidades
				• Agilidade de resposta a ameaças
				• Fortalecer o setor cibernético
				• Flexibilidade operacional
				• Unificar a operação das três Forças
				• Estruturar o potencial estratégico em torno de capacidades
				• Preparar combatentes
				• Integração da América do Sul
				• Capacitar a indústria nacional

Resumo	Propõem-se a liderar o processo regulatório e influenciar o desenvolvimento da internet para o mundo a partir do que julgam ser melhor para todos.	Já reconheceram a importância do setor e, em resposta às iniciativas dos Estados Unidos, estão se estruturando para eventuais conflitos cibernéticos.	Ainda com pouca expressão no espaço cibernético. Está atenta ao que vem acontecendo no mundo e não pretende se distanciar das discussões.	Apesar de algumas ações estarem em andamento, a infraestrutura nacional de TI é ruim. A organização institucional tende a não favorecer ações integradas.

A diferença de investimento em gestão de defesa cibernética entre o Brasil e os Estados Unidos já era esperada. Não apenas pela própria condição econômica de cada país, mas também pela postura internacional e ausência de desafetos declarados.

Já a diferença do arranjo institucional entre os dois países é algo notável. Enquanto, nos Estados Unidos, segurança e defesa cibernética possuem uma liderança única, no Brasil, optou-se por separá-las. O Brasil fez a opção por segregar a direção das ações de segurança da informação e defesa cibernética em dois órgãos distintos e independentes entre si, respectivamente, GSI/PR e CDCiber/EB/MD.

Essa configuração tende a fragilizar o programa tanto de defesa quanto de segurança cibernética, pois, além de isolá-los, ambos passam a depender da afinidade, integração e colaboração dos dirigentes maiores de tais instituições. Cada entidade presta contas de seu trabalho de formas e a autoridades distintas, e isto dificulta ações conjuntas de longo prazo.

Considerando apenas os aspectos de defesa, o mesmo volta a ocorrer. O CDCiber está dentro da estrutura do Exército Brasileiro, mas a área cibernética tem abrangência nas três Forças.

Ao delegar a liderança das ações de defesa cibernética ao Exército Brasileiro, a Estratégia Nacional de Defesa também criou uma multiplicidade de lideranças dentro do próprio Ministério da Defesa. Isto porque as questões cibernéticas devem ter igual relevância nas três Forças e não apenas no Exército. Com isto, apesar de cada Força possuir um núcleo dedicado à defesa cibernética, como já vem ocorrendo, cabe ao núcleo do Exército Brasileiro a liderança do tema dentro das Forças Armadas. Isto fragiliza a defesa cibernética como um todo.

Seria mais lógico se o CDCiber estivesse dentro da estrutura de Estado-Maior Conjunto das Forças Armadas (EMCFA) e não no Comando do Exército. Assim, poder-se-ia contar com militares das três Forças – e por que não também civis – atuando em conjunto, coordenados e integrados.

Diante do exposto, avalia-se que, no Brasil, tanto a segurança quanto a defesa ainda se encontram em estágio embrionário de organização, todavia algumas ações já vêm sendo tomadas.

Por outro lado, nota-se que as maiores economias mundiais, bem como demais países em desenvolvimento, também não estão muito avançados em relação à sistematização e organização dos mecanismos de proteção cibernética. A começar pelos Estados Unidos, que apenas em 2009 criaram, oficialmente, o Comando de Defesa Cibernética.

Por meio de uma análise das estratégias cibernéticas nacionais, nota-se que até mesmo as grandes potências estão em busca de parceiros e aliados para, por meio de troca de experiências, conseguirem avançar na proteção e salvaguarda dos dados.

Acredita-se que esse amplo convite ao estabelecimento de novas parcerias é resultado da percepção de que ações individuais não avançam na velocidade necessária. Certamente, os países mais ricos possuem instrumentos mais sofisticados e orçamento muito superior em relação ao Brasil. Todavia, tecnologias ligadas a sistemas digitais, especialmente quando envolvem elaboração de *software*, inteligência, talento e criatividade dos desenvolvedores, podem superar eventuais vantagens tecnológicas e orçamentárias (Takemura, Osajima e Kawano, 2009). Exemplo disto são as frequentes invasões

a sistemas superprotegidos, como as ocorridas no Pentágono, Sony, RSA Security e MasterCard, por grupos dedicados ao cibercrime.

O Brasil ainda conta com um parque empresarial pequeno, com cerca de quarenta empresas de desenvolvimento e/ou fornecimento de soluções robustas em segurança ou defesa cibernética localizadas no país.

O Estado tem capacidade de ser o propulsor da iniciativa privada rumo ao desenvolvimento de novas soluções em segurança e defesa. Nesse sentido, algumas ações podem ser tomadas, como:

- organizar o regime legal, regulatório e tributário da indústria nacional de material de defesa para que ela tenha condições de abrir mão das necessidades momentâneas do mercado para priorizar os imperativos estratégicos nacionais;
- criar fundos perenes de apoio à pesquisa em defesa cibernética a serem feitas pela iniciativa privada, mas com a possibilidade de integração com o meio acadêmico ou institutos de pesquisa;
- o componente estatal da indústria de material de defesa deve ter por vocação fomentar o que o setor privado não possa projetar e fabricar, a curto e médio prazo, de maneira rentável;
- o Estado precisa ser vitrine dos produtos nacionais para os clientes estrangeiros; isto porque uma empresa que não consegue vender seus produtos no mercado interno dificilmente terá êxito ao tentar vendê-los no mercado internacional; e
- o futuro das capacitações tecnológicas nacionais de defesa depende mais da formação de recursos humanos do que do desenvolvimento de aparato industrial. Daí a primazia da política de formação de especialistas em ciência básica e aplicada.

Ao se fazer uma análise da vulnerabilidade das redes brasileiras, percebe-se que o Brasil ainda tem muito que avançar para conseguir se equiparar aos países ricos. Todavia, para se conseguir esse emparelhamento partindo-se da fase de maturidade da tecnologia, o processo torna-se muito caro e, mesmo assim, com poucas chances de sucesso.

Sabe-se que os recursos são escassos e que as grandes potências mundiais dispõem de orçamento e realizam investimentos muito superiores, se comparados aos países emergentes. O ponto de entrada mais promissor, para países em desenvolvimento como o Brasil, é a fase inicial de desenvolvimento, fase esta pela qual o mundo atravessa. Basta lembrar que os países ricos estão rogando por possibilidade de parcerias.

Essa janela de oportunidade está atualmente aberta ao Brasil. Ela consiste no momento ideal para se investir em capacidade, instrumentos e recursos de modo a otimizar a busca por um ciberespaço aberto, confiável, seguro e interoperável.

Diante do caráter evidentemente exploratório do texto, espera-se que ele sirva de ponto de partida para novas pesquisas e propostas de arranjos institucionais, bem como de subsídio a políticas de incentivo de apoio à indústria de fornecimento de materiais de defesa nacionais.

REFERÊNCIAS

BAUER, J. M.; VAN EETEN, M. J. G. Cybersecurity: stakeholder incentives, externalities, and policy options. **Telecommunications policy**, v. 33, n. 10, p. 706-719, 2009.

BRASIL. **Estratégia nacional de defesa**. Brasília: MD, 18 dez. 2008. Disponível em: <http://www.defesa.gov.br/projetosweb/estrategia/arquivos/estrategia_defesa_nacional_portugues.pdf>.

_____. Secretaria de Assuntos Estratégicos – SAE. Desafios estratégicos para a segurança e defesa cibernética. Brasília: SAE, 2011. Disponível em: <http://www.sae.gov.br/site/wp-content/uploads/Seguranca_Cibernetica_web.pdf>.

_____. Gabinete de Segurança Institucional da Presidência da República – GSI/PR. **Estatísticas de incidentes de rede na APF**: 4º trimestre/2012. Brasil: CTIR/DSIC/GSI/PR, 2013a. Disponível em: <http://www.ctir.gov.br/arquivos/estatisticas/2012/Estatisticas_CTIR_Gov_4o_Trimestre_2012.pdf >.

_____. Ministério do Planejamento, Orçamento e Gestão. **Compras de TI movimentam R$ 5 bi**. Brasília: MP, 8 fev. 2013b. Disponível em: <http://www.planejamento.gov.br/noticia.asp?p=not&cod=9384&cat=94&sec=7>.

CIAB – CONGRESSO INTERNACIONAL DE AUTOMAÇÃO BANCÁRIA. **Fraudes eletrônicas causaram prejuízo de R$ 1,5 bilhão em 2011**. São Paulo, 2 out. 2012. Disponível em: <http://www.ciab.com.br/blog/index.php/fraudes-eletronicas-causaram-prejuizo-de-r-15-bilhao-em-2011/>.

CLARKE, R. A.; KNAKE, R. **Cyber war**: the next threat to national security and what to do about it. [s.l.]: Ecco, 2011.

FALLIERE, N.; MURCHU, L. O.; CHIEN, E. **W32.Stuxnet dossier**. Cupertino: Symantec, Feb. 2011. Disponível em: <http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf>.

FERRAN, Lee. **Bigger Than flame, stronger than Stuxnet**: why "idiot" humans are best Cyber Weapon. ABC News, 1th June 2012. Disponível em: <http://abcnews.go.com/blogs/headlines/2012/06/bigger-than-flame-stronger-than-stuxnet-why-idiot-humans-are-best-cyber-weapon/>. Acesso em: 13 set. 2012.

GREGO, M. **Obama ordenou ataque ao Irã com Stuxnet, diz NYT**. Disponível em: <http://exame.abril.com.br/tecnologia/noticias/obama-ordenou-ataque-ao-ira-com-stuxnet-diz-nyt>. Acesso em: 1º dez. 2012.

HOEPERS, C. **Segurança da internet no Brasil**.[s.l.]: Ipea. Disponível em: <http://www.cert.br/docs/palestras/certbr-ipea2011.pdf>. Acesso em: 9 e 29 ago. 2011.

HULSE, J. Brasil encara desafios da cibersegurança. **DefesaNet**, Porto Alegre, 30 out. 2012. Disponível em: <http://www.defesanet.com.br/cyberwar/noticia/8388/Brasil-encara-desafios-da-ciberseguranca>. Acesso em: 28 fev. 2013.

ÍNDIA. Ministry of Communications and Information Technology. **Discussion draft on national Cyber security policy**. New Delhi, 2011. Disponível em: <http://deity.gov.in/sites/upload_files/dit/files/ncsp_060411.pdf>.

KRAMER, F. D.; STARR, S. H.; WENTZ, L. (Eds.). **Cyberpower and national security**. [s.l.]: Potomac Books, 2009.

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

MCCAUL, M. **House Passes McCaul-Lipinski Cybersecurity Enhancement Act to secure federal networks, critical infrastructure and America's competitive edge**. Disponível em: <http://mccaul.house.gov/press-releases/house-passes-mccaullipinski-cybersecurity-enhancement-act-to-secure-federal-networks-critical-infrastructure-and-americas-competitive-edge/>. Acesso em: 26 fev. 2013.

PEREZ, C. Technological change and opportunities for development as a moving target. **Cepal Review**, n. 75, p. 109-130, Dec. 2001. Disponível em: <http://www.eclac.org/publicaciones/xml/5/20135/lcg2150i_Perez.pdf >.

RÚSSIA. Ministério da Defesa. **Visões conceituais sobre as atividades das Forças Armadas da Federação da Rússia no espaço de informação**. Moscou, 2011. (Tradução do autor). Disponível em: <http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle>. Acesso em: 5 jul. 2012.

SANTOS, G. D. J. C. General detalha implantação do centro de defesa cibernética, novo órgão brasileiro. **Folha de S. Paulo**, 7 maio 2012a. Disponível em: <http://www1.folha.uol.com.br/tec/1085498-general-detalha-implantacao-do-centro-de-defesa-cibernetica-novo-orgao-brasileiro.shtml>. Acesso em: 7 mar. 2013.

_____. O centro de defesa cibernética: uma visão de futuro. *In*: CICLO DE ESTUDOS ESTRATÉGICOS, 11. Rio de Janeiro: ECEME, 24 maio 2012b. Disponível em: <http://www.eceme.ensino.eb.br/ciclodeestudosestrategicos/index.php/CEE/index/schedConfs/archive>.

SYMANTEC CORP. Disponível em: <http://br.norton.com/cybercrime/bots.jsp>. Acesso em: 14 set. 2011

TAKEMURA, T.; OSAJIMA, M.; KAWANO, M. Positive analysis on vulnerability, information security incidents, and the countermeasures of Japanese internet service providers. **International journal of business, economics, finance and management sciences**, v. 1, n. 3, 2009. Disponível em: <http://www2.itc.kansai-u.ac.jp/~a084034/pdf/v1-3-29.pdf>.

TANENBAUM, A. S. **Computer networks**. 5. ed. [s.l.]: Prentice Hall PTR, 2011.

TCU – TRIBUNAL DE CONTAS DA UNIÃO. **Relatório de levantamento**: avaliação da governança de tecnologia da informação na administração pública federal. Brasília, 2010. Disponível em: <http://goo.gl/kGgOY>.

_____. Acórdão nº 1.233/2012 – Plenário. Brasília, 2012a. p. 18.

_____. **Relatório de levantamento**: avaliação da governança de tecnologia da informação na administração pública federal. Brasília, 2012b. Disponível em: <http://goo.gl/K5lZZ>.

THE TECHNOLYTICS INSTITUTE. **Cyber Warfare**: the Cyber commander's Ehanadbook. McMurray: Technolytics, 2012.

UNITED STATES. The White House. **International strategy for cyberspace**: prosperity, security, and openness in a networked world. Washington, May 2011. Disponível em: <http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>.

_____. Directorate for Organizational and Management Planning.

_____. **Organization of the Department of Defence**. Washington, March 2012a. Disponível em: <http://odam.defense.gov/omp/Functions/Organizational_Portfolios/Organization_and_Functions_Guidebook/DoD_Organization_March_2012.pdf>.

_____. Department of Defense. **The federal budget**. Fiscal year 2012. Washington, 2012b. Disponível em: <http://www.whitehouse.gov/omb/factsheet_department_defense>. Acesso em: 27 fev. 2013.

_____. National Security Agency – NSA. **About NSA**. Washington, 2013. Disponível em: <http://www.nsa.gov/about/index.shtml>.

_____. Government Accountability Office – GAO. **Information technology**. Washington, [s.d.]. Disponível em: <http://goo.gl/gfyPR>.

US INTERNET "six strikes" anti-piracy campaign begins. **BBC news**, 26 Feb. 2013. Disponível em: <http://www.bbc.co.uk/news/technology-21591696>.

APÊNDICES

APÊNDICE A

Estratégia norte-americana para o espaço cibernético[14]

A estratégia norte-americana é apresentada como um convite a todos os interessados – sejam países, sociedade civil, setor privado ou usuários – a se juntar e colaborar a fim de colocar em prática a visão governamental então apresentada. Reforça a importância de parcerias, capacitação humana, abertura comercial, respeito à propriedade e a promoção dos direitos universais.

O documento é dividido em quatro tópicos principais: *i*) Construção de uma política para o ciberespaço; *ii*) O futuro do ciberespaço; *iii*) Prioridades políticas; e *iv*) Seguindo em frente.[15]

Construção de uma política para o ciberespaço

Infraestruturas digitais estão se tornando, a cada dia, a coluna dorsal da prosperidade econômica, do desenvolvimento das comunidades científicas, da força militar, da transparência governamental e da sociedade livre. Movimentos sociais e políticos contam com a internet para disponibilizar novas e mais formas de ação e organização.

Para que seja possível a materialização de todos os benefícios que as tecnologias em rede prometem ao mundo, esses sistemas devem funcionar de forma segura e confiável. As pessoas devem confiar no fato de que os dados fluirão até o destino sem interrupções. Assegurar o livre fluxo de informações, a segurança e a privacidade dos dados e a integridade das redes de comunicação é essencial para a prosperidade econômica, segurança e promoção dos direitos universais, tanto para os norte-americanos quanto para o restante do mundo.

O futuro de um ciberespaço aberto, interoperável, seguro e confiável depende de as nações reconhecerem e protegerem aquilo que deve ser permanente, enquanto confrontam aqueles que trabalham para desestabilizar ou enfraquecer nosso mundo, crescentemente interconectado.

14. Excertos relevantes, tradução nossa.
15. Em inglês: "*I. Building cyberspace policy; II. Cyberspace's future; III. Policy priorities; IV. Moving foward*".

Abordagem estratégica

Os Estados Unidos buscarão uma política para o ciberespaço internacional que favoreça inovações que direcionem a economia americana e melhore a vida em todo o planeta. Todo este trabalho estará fundamentado em princípios essenciais não apenas para a política estrangeira norte-americana, mas também para o futuro da própria internet.

- Construindo sucesso: os Estados Unidos estão comprometidos a preservar e aumentar os benefícios das redes digitais para as nossas sociedades e economias.
- Reconhecendo os desafios: os Estados Unidos reconhecem que o crescimento dessas redes traz consigo novos desafios para a segurança econômica e nacional, bem como para a comunidade global.
- Fundamentada em princípios: os Estados Unidos vão enfrentar esses desafios, preservando seus princípios fundamentais. São eles: liberdade fundamental, privacidade e liberdade de fluxo de informações.

O futuro do ciberespaço

Visualiza-se um futuro em que o acesso confiável à internet esteja disponível em qualquer ponto do globo terrestre a um preço que famílias e empresas possam pagar. Computadores se comunicando pelas redes globais e permitindo a comunicação instantânea e confiável entre amigos e colegas. Conteúdo oferecido em linguagem local além de livre trânsito para além das bordas políticas dos países. Novas tecnologias melhorando a agricultura e promovendo saúde pública, compartilhadas com aqueles que mais precisam. A solução de problemas difíceis sendo resolvidos pela colaboração de *experts* e inovadores. Isto é, em parte, o futuro que os Estados Unidos estão plantando e trabalhando para realizar.

Os Estados Unidos e um número crescente de parceiros já lançaram as bases para esse futuro. Não é uma conclusão precipitada, e não se pode construí-lo sozinho. Embora o progresso possa ser lento e intensivo em recursos, a comunidade internacional deve se unir em apoio a este investimento de longo prazo. Isto deve ser feito com a clara compreensão de que esta visão para o ciberespaço serve tanto a interesses nacionais como a objetivos internacionais compartilhados. O sucesso deste plano será medido por meio de mais meio século de tecnologias da informação transformacional como o último.

O futuro a se plantar

O espaço cibernético a se plantar recompensa a inovação e cria possibilidade aos indivíduos. Ele conecta pessoas e fortalece as comunidades. Cria melhores governos e expande a transparência (*accountability*). Garante as liberdades fundamentais e aumenta a privacidade pessoal. Constrói entendimento, esclarece normas de comportamento e aumenta a segurança nacional e internacional. Para sustentar este ambiente, a colaboração internacional é mais do que uma boa prática: é o primeiro princípio.

Objetivo

Os Estados Unidos irão trabalhar internacionalmente para promover uma infraestrutura de informação e comunicação aberta, interoperável, segura e confiável, que comporte o comércio internacional, fortaleça a segurança internacional e promova a liberdade de expressão e inovação. Para atingir este objetivo, pretende-se construir e manter um ambiente em que as normas de comportamento responsáveis guiem as ações de governo, preservar parcerias, e apoiar o Estado de direito no espaço cibernético:

a. aberto e interoperável: um espaço cibernético que capacita;
b. seguro e confiável: um espaço cibernético que perdura; e
c. segurança por meio de normas:
    i) defesa das liberdades fundamentais;
    ii) respeito à propriedade;
    iii) respeito à privacidade;
    iv) proteção contra o crime;
    v) direito de autodefesa;
    vi) interoperabilidade global;
    vii) estabilidade da rede;
    viii) acesso confiável;
    ix) governança multilateral; e
    x) dever de diligência em segurança cibernética.

O papel dos Estados Unidos no futuro do espaço cibernético

A fim de concretizar esse futuro e ajudar a promulgar normas positivas, os Estados Unidos irão combinar diplomacia, defesa e desenvolvimento para aumentar a prosperidade, a segurança e a abertura de modo que todos possam se beneficiar das tecnologias em rede. Estas três abordagens são fundamentais para os esforços em nível internacional. Na segunda metade do século XX, os Estados Unidos ajudaram a forjar uma nova arquitetura internacional de pós-guerra de cooperação econômica e de segurança. No século XXI, irão trabalhar para concretizar esta visão para um ciberespaço pacífico e confiável, utilizando o mesmo espírito de cooperação e de responsabilidade coletiva.

No campo da diplomacia, buscarão fortalecer parcerias. Os Estados Unidos criarão um ambiente favorável para que os mais diversos países possam atuar em cooperação e responsabilidade, sobretudo reconhecendo o valor intrínseco de um ciberespaço aberto, confiável, seguro e interoperável. Buscarão tantos aliados quanto possível para conseguirem implementar a estratégia ora apresentada. Destacam a relevância da ação conjunta entre governo, firmas, provedores de internet, vendedores de *hardware* e *software* até o usuário final. Reconhecem que ações isoladas não se mostram efetivas diante de um mundo conectado. Ou seja, todos possuem papel importante na construção de um ciberespaço com potencial pleno em que todos possam ser beneficiados.

Utilizarão a defesa para dissuadir e impedir ameaças. Os Estados Unidos irão, junto com outras nações, incentivar um comportamento responsável e se oporão àqueles que buscarem prejudicar redes e sistemas; dissuadirão e impedirão atores maliciosos. Reservam-se o direito de defender estes ativos nacionais vitais da forma como julgar necessário e apropriado. Alertam que responderão a atos hostis oriundos do ciberespaço da mesma forma como qualquer outra ameaça identificada, incluindo-se, em última instância, a força militar. Reservam-se o direito de usar todos os meios necessários – diplomacia, informacional, econômico ou militar – de maneira consistente com o direito internacional, de forma a defender a sua nação, parceiros, aliados ou os próprios interesses. Os Estados Unidos buscarão agir de uma maneira que reflita valores sociais e a legitimidade, buscando, sempre que possível, um amplo apoio internacional.

Objetivando a promoção do desenvolvimento, terão foco na promoção da prosperidade e segurança. Os Estados Unidos irão facilitar a capacitação externa em segurança cibernética, bilateralmente e por meio de organizações multilaterais, de modo que cada país

tenha os meios necessários para proteger sua infraestrutura digital. Buscarão fortalecer as redes globais, e ainda buscarão construir parcerias mais estreitas em consenso para a abertura, interoperabilidade, segurança e confiança das redes. Comprometem-se a atuar no fornecimento de conhecimento e capacidade para construir e preservar sistemas digitais novos e pré-existentes. A assistência à capacitação norte-americana deve ser vista como um investimento, um compromisso, e uma importante oportunidade de diálogo e parcerias, ou seja, são ativos para possíveis negociações e acordos.

Prioridades políticas

Para realizar plenamente esse futuro no qual o espaço cibernético beneficiaria a todos, o governo dos Estados Unidos organiza suas atividades em sete áreas de atividades interdependentes. Cada uma exige colaboração dentro do governo, com parceiros internacionais e com o setor privado. Tomando-se como um todo, formam as linhas de ação do plano estratégico norte-americano:

1) Economia: promover padrões internacionais e inovadores, mercados abertos. Manter um ambiente de livre comércio que encoraje as inovações tecnológicas. Proteger a propriedade intelectual, incluindo segredos comerciais, de eventuais roubos. Assegurar padrões técnicos de segurança e interoperabilidade.
2) Proteção de redes dos Estados Unidos: reforçar a segurança, confiabilidade e resiliência. Promover a cooperação no ciberespaço, particularmente na elaboração de normas de conduta para os estados (norte-americanos) sobre segurança cibernética. Reduzir intrusões e interrupção das redes norte-americanas. Garantir robustez em gerenciamento de incidentes, resiliência e capacidade de recuperação das infraestruturas de informações. Melhorar a segurança da cadeia de fornecimento de alta tecnologia, em coordenação com a indústria.
3) Aplicação da lei: expandir colaborações e o Estado de direito. Participar plenamente do desenvolvimento de políticas internacionais contra o cibercrime. Harmonizar leis internacionais de cibercrime por meio da expansão de adesão à Convenção de Budapeste. Ter o foco no combate aos crimes cibernéticos e nas atividades ilegais e não na restrição de acesso à internet. Negar aos terroristas e a outros criminosos a possibilidade de explorarem a internet para o planejamento operacional, financiamento ou a realização de ataques.
4) Militar: preparar para os desafios de segurança do século XXI. Reconhecer e adaptar-se às crescentes necessidades militares em termos de segurança e confiabilidade de rede.

Construir e reforçar parcerias existentes para enfrentar potenciais ameaças no ciberespaço. Expandir a cooperação com aliados e parceiros de modo a aumentar a segurança coletiva.

5) Governança na internet: promover estruturas eficazes e inclusivas. Priorizar transparência (*accountability*) e inovação na internet. Preservar a segurança e estabilidade das redes globais, incluindo sistema de nomes de domínios (DNS). Promover e aprimorar ambientes de discussão dos problemas de governança da internet.

6) Desenvolvimento internacional: construir capacidade, segurança e prosperidade. Compartilhar o conhecimento, treinamento e outros recursos necessários para os países que buscarem adquirir capacitação técnica em cibersegurança. Desenvolver continuamente e compartilhar regularmente as melhores práticas em cibersegurança. Fortalecer a capacidade dos Estados no combate ao cibercrime. Fortalecer relações com os formuladores de políticas públicas voltadas para melhora da capacitação técnica, oferecendo contato regular e permanente com especialistas e correspondentes do governo norte-americano.

7) Liberdade na internet: defesa aos fundamentos de liberdade e privacidade. Apoiar para que a sociedade civil tenha plataformas seguras e confiáveis para exercer livremente os direitos de liberdade de expressão e associação. Colaborar com a sociedade civil e organizações não governamentais a manter sistemas de proteção e salvaguarda de dados de modo a evitar e impedir invasões e intrusões. Incentivar a cooperação internacional para a efetiva proteção de privacidade de dados comerciais. Garantir a interoperabilidade de ponta a ponta de uma internet acessível a todos.

Seguindo em frente

Os benefícios da tecnologia em rede não devem ser reservados como se fossem privilégio de poucas nações. Contudo, a conectividade não é um fim em si mesmo. Ela deve ser apoiada em um espaço cibernético que seja aberto à inovação, interoperável mundo afora, seguro o suficiente para conquistar a tranquilidade das pessoas e confiável o suficiente para apoiar o seu trabalho delas.

Esta estratégia é um mapa que permite aos departamentos do governo e agências dos Estados Unidos definirem melhor e coordenarem o seu papel na política internacional referente ao ciberespaço. Executar de forma específica o futuro e planejar as implementações a serem seguidas. É um chamado para o setor privado, à sociedade civil e aos usuários finais para reforçarem os esforços por meio da conscientização, parceria e ação.

Mais importante ainda, é um convite para outros Estados e os povos se juntarem aos Estados Unidos na realização desta visão de prosperidade, segurança e abertura neste novo mundo conectado Estes ideais são fundamentais para a preservação do espaço cibernético como conhecido atualmente e, além disso, para a criação, juntos, do futuro a ser construído.

APÊNDICE B

Estratégia russa para o espaço cibernético[1]

O texto apresenta os princípios das Forças Armadas da Federação Russa, aplicados ao espaço cibernético. São eles:

1) Respeito ao Estado de Direito. Conformidade com o princípio da legalidade. Exige que as Forças Armadas da Federação Russa no curso de suas ações no ciberespaço sejam guiadas por normas e princípios da legislação russa vigente, bem como pelas normas e princípios universalmente reconhecidos e pelo direito internacional.
2) Prioridade. Respeito pelo princípio das necessidades prioritárias das Forças Armadas da Federação Russa durante suas atividades no espaço de informações. Prioridade pela intenção de coleta de informações atuais e confiáveis sobre as ameaças, e em segunda instância o desenvolvimento de medidas de proteção. Tudo isto cria condições favoráveis para o controle eficaz de tropas e armas necessárias para preservar o estado moral e psicológico da população russa.
3) Complexidade. O cumprimento do princípio de integralidade exige que as Forças Armadas da Federação da Rússia, no âmbito das suas atividades no espaço das informações, usem todas as forças eficazes disponíveis para enfrentar os desafios que se apresentam. Em geral, as atividades no espaço das informações consistem nas atividades de exploração, camuflagem operacional, guerra eletrônica, comunicações, gerenciamento automatizado, informações de pessoal, bem como proteção dos sistemas de informação contra atividades maliciosas.
4) Interação. Respeito pelo princípio da interação requer que o Ministério da Defesa russo coordene as suas ações no espaço de informações com outros órgãos federais do Poder Executivo.
5) Cooperação. Respeito pelo princípio da cooperação exige a coordenação de esforços com países amigos e organizações internacionais. O principal objetivo da cooperação para o desenvolvimento em nível global é o estabelecimento de um regime jurídico internacional, incluindo as atividades militares dos Estados no espaço das informações global, baseadas nos princípios e normas do direito internacional.
6) Inovação. Respeito pelo princípio da inovação requer das Forças Armadas da Federação Russa que, para a preparação e execução de tarefas, sejam utilizadas

1. Excertos relevantes, tradução nossa.

tecnologias avançadas, ferramentas e técnicas, bem como seja agregada uma equipe de segurança da informação altamente qualificada. Portanto, para projetar e fabricar ferramentas e tecnologias, os centros de inovação mais avançados da Federação Russa devem estar envolvidos em pesquisa e potencial de produção. O desenvolvimento em si é realizado dentro dos programas estaduais e departamentais e de investigação. Especialistas serão formados em instituições educacionais de ensino superior do Ministério da Defesa da Federação Russa, ou em outras instituições de ensino da Federação Russa.

Em seguida são apresentada três regras de conduta das Forças Armadas da Federação Russa: dissuadir, prevenir e resolver conflitos armados no espaço de informações. No que tange à prevenção e dissuasão, os pontos adiante são destacados.

1) Desenvolver um sistema que garanta a segurança das Forças Armadas da Federação Russa, destinado a conter e resolver conflitos armados no espaço de informações.
2) Manter a força e os meios para garantir a segurança em constante prontidão para repelir as ameaças à natureza político-militar do espaço de informações.
3) Cooperar de forma prioritária com os países do Tratado de Segurança Coletiva, da Comunidade de Estados Independentes e da Organização de Cooperação de Xangai, para expandir o círculo de parceiros e desenvolver a cooperação com eles com base no interesse comum no reforço da segurança internacional, em conformidade com as disposições da Carta da ONU e outras normas de direito internacional.
4) Buscar concluir um tratado da ONU para garantia da segurança da informação internacional, ampliar a aplicação das normas normalmente reconhecidas e princípios do direito internacional sobre o espaço de informações.
5) Tomar todas as medidas possíveis para a detecção precoce de potenciais conflitos militares no espaço de informações, bem como expor os promovedores dos conflitos, instigadores e cúmplices.
6) Identificar os fatores que favoreçam o aumento da ocorrência de conflitos e estabelecer controle sobre eles, de modo a evitar situações de emergência.
7) Tomar medidas urgentes para combater a evolução (ou exacerbação de conservação) de conflito e sua transição para um estado que aumente significativamente o custo de resolução.
8) Tomar medidas para evitar a propagação de conflito em áreas vizinhas ao território russo, que possuem acordos internacionais, e a dissolução de diferenças que irão exigir esforço e custo adicional.

9) Tomar medidas para neutralizar os fatores que derem origem a um conflito com a finalidade de promover a interação direta entre os lados conflitantes na direção de uma cooperação construtiva.

10) A formação necessária da opinião pública envolve a orientação adequada e mobilização, a fim de criar um espaço de informações global e um ambiente mitigante da possibilidade de conflitos.

Já com relação à resolução de conflitos, a Federação Russa considera legítimo o uso das Forças Armadas e outras tropas para repelir a agressão contra ela e (ou) de seus aliados. Lidar com o Conselho de Segurança e outras instituições de segurança coletiva, bem como proteger os seus cidadãos, mesmo que fora da Federação Russa, em conformidade com os princípios normalmente reconhecidos, normas do direito internacional e os tratados internacionais da Federação da Rússia.

As Forças Armadas da Federação Russa são guiadas pelas regras a seguir para resolver conflitos armados no espaço de informação.

1) Utilizar, em primeiro lugar, meios de negociação, conciliação, apelos ao Conselho de Segurança da ONU, a outras organizações ou acordos regionais ou outros meios pacíficos.

2) No caso da existência de tensões, buscar evitar conflitos extremos, formas destrutivas de guerra e especialmente aquelas que podem levar à desestabilização da situação internacional e o surgimento de uma crise.

3) Durante conflitos, manter os meios de comunicação nacionais e estrangeiros em operação, para a livre informação pública, elevar sua eficácia e influência sobre o desenvolvimento e a consolidação dos resultados alcançados para resolver o conflito de contradições.

APÊNDICE C

Estratégia indiana para o espaço cibernético[1]

O documento começa apresentando as agências interessadas ou relacionadas ao tema, a saber:

- National Information Board (NIB)
- National Crisis Management Committee (NCMC)
- National Security Council Secretariat (NSCS)
- Ministry of Home Affairs
- Ministry of Defence
- Department of Information Technology (DIT)
- Department of Telecommunications (DoT)
- National Cyber Response Centre - Indian Computer Emergency
- Response Team (CERT-In)
- National Information Infrastructure Protection Centre (NIIPC)
- National Disaster Management of Authority (NDMA)
- Standardisation, Testing and Quality Certification (STQC) Directorate
- Sectoral CERTs

Adiante são apresentadas as considerações fundamentais para a segurança cibernética.

1) A segurança do ciberespaço não é uma questão opcional, mas sim uma necessidade imperativa, pois impacta na segurança nacional, segurança pública e bem-estar econômico.
2) As soluções em cibersegurança devem estar à frente de tecnologias tradicionais como antivírus e *firewalls*. Devem ser dinâmicas por natureza e necessariamente capazes de detectar, prevenir e impedir ataques.
3) A inteligência em cibersegurança pode ser considerada uma componente da segurança do ciberespaço a fim de antecipar ataques, adotar medidas de defesa adequadas e contra atacar quando sujeito a tentativas de invasão.

1. Excertos relevantes, tradução nossa.

4) Correlação de informações efetivas a partir de múltiplas fontes e monitoramento em tempo real de ativos que precisam ser protegidos e ao mesmo tempo garantir que recursos e capacitação adequada estejam prontos para lidar com situações de risco.

5) Necessidade de uma postura adequada de segurança e adotar contramedidas baseadas na hierarquia de prioridade e compreensão de interdependências, em vez de tentar se defender de todas as tentativas de intrusão e ataque.

6) Política de segurança depende fundamentalmente de pessoas, processos e tecnologia. Assim sendo, há uma clara necessidade de foco nas pessoas e nos processos, enquanto tentam utilizar as melhores soluções de tecnologia disponíveis. De outra forma, a política se torna ineficaz.

7) Utilização de recursos humanos adequadamente treinados e qualificados, em conjunto com incentivos adequados para a obtenção de resultados efetivos no campo de mais alta especialização da cibersegurança.

Questões de segurança devem ser integradas já na fase de projeto conceitual de sistemas – quando virá a ser desenvolvido, implantado e ajustado às infraestruturas críticas – e não serem tratadas como problemas tardios a serem resolvidos.

O documento salienta que segurança cibernética está entre os maiores desafios do século XXI. Os efeitos das ameaças representam riscos significativos para a segurança pública e para a estabilidade de uma comunidade global conectada, como um todo. Os motivos para os ataques são os mais variados, indo desde simples demonstração de capacidade técnica à roubo de dinheiro ou informações, ou mesmo uma extensão dos conflitos entre Estados. Destaca que nenhuma nação, isoladamente, conseguirá superar este desafio. Dessa forma, valoriza a importância de parcerias entre nações aliadas, sociedade civil e o setor privado.

Ipea – Instituto de Pesquisa Econômica Aplicada

EDITORIAL

Coordenação
Cláudio Passos de Oliveira

Supervisão
Everson da Silva Moura
Reginaldo da Silva Domingos

Revisão
Andressa Vieira Bueno
Clícia Silveira Rodrigues
Idalina Barbara de Castro
Laeticia Jensen Eble
Leonardo Moreira de Souza
Luciana Dias
Marcelo Araujo de Sales Aguiar
Marco Aurélio Dias Pires
Olavo Mesquita de Carvalho
Regina Marta de Aguiar

Editoração
Aline Rodrigues Lima
Bernar José Vieira
Daniella Silva Nogueira
Danilo Leite de Macedo Tavares
Jeovah Herculano Szervinsk Junior
Leonardo Hideki Higa
Cristiano Ferreira Araujo (estagiário)
Diego André Souza Santos (estagiário)

Capa
Luís Cláudio Cardoso da Silva

Projeto Gráfico
Renato Rodrigues Bueno

Livraria do Ipea

SBS – Quadra 1 - Bloco J - Ed. BNDES, Térreo.
70076-900 – Brasília – DF
Fone: (61) 3315-5336

Correio eletrônico: livraria@ipea.gov.br

Composto em adobe garamond pro 12/16 (texto)
Frutiger 67 bold condensed (títulos, gráficos e tabelas)
Impresso em offset 90g/m^2
Cartão supremo 250g/m^2 (capa)
Brasília-DF

Missão do Ipea
Produzir, articular e disseminar conhecimento para aperfeiçoar as políticas públicas e contribuir para o planejamento do desenvolvimento brasileiro.

ISSN 1415-4765

ipea Instituto de Pesquisa Econômica Aplicada

SECRETARIA DE ASSUNTOS ESTRATÉGICOS DA PRESIDÊNCIA DA REPÚBLICA

GOVERNO FEDERAL
BRASIL
PAÍS RICO É PAÍS SEM POBREZA