BRASIL INFORMACIONAL: A SEGURANÇA CIBERNÉTICA COMO DESAFIO À SEGURANÇA NACIONAL

Rafael Oliveira de Ávila, Rafael Pinto da Silva

Resumo
O presente trabalho visa à discussão da Segurança Cibernética enquanto um tópico da agenda da segurança internacional e nacional. Para a definição do objeto de estudo é traçado um paralelo entre os conceitos de Segurança da Informação e Segurança Cibernética cuja conclusão é de que estes não devem ser vistos como sinônimos. No plano nacional, da mesma forma que no plano internacional, observa-se um crescente movimento em direção à securitização da informação devido à ocorrência cada vez mais constante de incidentes ligados a crimes e ataques cibernéticos induzindo a tentativas de normatização da temática e a criação de uma agenda global para a temática. Além disso, as ações internas estão concentradas na criação de setores específicos e no mapeamento de oportunidades e desafios. Sendo assim, é identificada e refletida a necessidade de ações mais práticas com o estabelecimento de metas e prazos a fim de prover respostas mais eficazes e rápidas aos desafios e garantir a projeção do Brasil como referência internacional.

Palavras-chave: Informação; Segurança Cibernética; Segurança da Informação; Segurança Internacional.

Abstract
This present article aims at the discussion of Cybersecurity as an item of the agenda of international and national security. For the definition of the subject was drawn a parallel between the concepts of Information Security and Cybersecurity which the conclusion is that that they should not be seen as synonymous. At the national level, as at the international level, there is a growing movement toward the securitization of information due to the frequent occurrence of incidents related to cybercrimes and cyberattacks inducing the creation of norms and the global agenda for the theme. Beyond that, the actions are focused on creating specific organisms and mapping of opportunities and challenges. Therefore, is identified and reflected the need of the establishment of more practical actions with goals and deadlines in order to provide more effective and rapid responses to the challenges and secure the projection of the country as an international benchmark.

Key-words: Information; Cybersecurity; Information Security; International Security.

Introdução

O avanço tecnológico das últimas décadas tem direcionado a sociedade em praticamente todos os seus setores para o que vem se denominando como Sociedade Informacional ou Sociedade da Informação[1]. Esta nova sociedade apresenta como atributos principais a existência de produtos e serviços baseados em tecnologias ligadas à área da computação, das telecomunicações, da robótica e, mais recentemente, da bioinformática e da nanotecnologia. Todas essas, proporcionaram na virada do século XX para o XXI uma gama de transformações sociais, econômicas e políticas que se traduziram em novas formas de acumulação, de produção e de exercício de poder[2] em que a informação[3] e o conhecimento[4] passaram a ser tratados como elementos centrais (CASTELLS,

1 O termo Sociedade da Informação vem sendo largamente utilizado por autores contemporâneos para definir a atual fase da sociedade. Para autores como Jorge Werthein (2000), o conceito de Sociedade da Informação surge para substituir o complexo conceito de Sociedade pós-industrial e como forma de assinalar a emergência de um novo paradigma técnico-econômico potencializado pelo uso intenso das tecnologias da informação e comunicação nas atividades cotidianas e pela ênfase na flexibilidade como idéia central das transformações sociais. Para Castells (1999), a Sociedade Informacional apresenta as seguintes características marcantes: a alta penetrabilidade dos efeitos das novas tecnologias, a informação como recurso produtivo primário, o predomínio da lógica de rede nas diferentes organizações sociais, a crescente convergência das tecnologias e a flexibilidade dos mais diversos processos sociais.

2 Para Braman (2006) as noções centrais que são utilizadas para analisar a questão do poder geralmente foram tratadas de modo simples, no entanto, atualmente, elas tendem a ser mais complexas, pois as transformações sociais derivadas do processo de informatização, bem como de outros fatores, geraram problemas adicionais no estudo do poder. Tradicionalmente, as análises e explanações sobre as definições do poder estiveram orientadas pelas três diferenciações (legal, tradicional, carismático) inauguradas por Weber que define poder como "a possibilidade de que um homem, ou um grupo de homens, realize sua vontade própria numa ação comunitária, até mesmo contra a resistência de outros que participam da ação" (WEBER, 1982, p.211). Braman (2006), por exemplo, analisa o poder a partir de três perspectivas (o instrumental que molda o comportamento humano pela manipulação do mundo material via força física; o estrutural que molda o comportamento humano pela manipulação do mundo social, pelas regras e pela criação de instituições; e o simbólico que molda a partir da manipulação do mundo material, social e simbólico via ideias, palavras e imagens) para apresentar uma quarta forma do poder que, segundo a autora, tem se destacado na sociedade da informação (o poder informacional que molda o comportamento humano pela manipulação das bases informacionais do poder instrumental, simbólico e estrutural). O presente artigo trata do poder a partir do conceito weberiano, tomando as contribuições de Braman (2006) sobre as formas de poder e, sobretudo, sobre o poder informacional para caracterizar as mudanças no exercício do poder na sociedade atual.

3 O termo informação vem sendo amplamente usado nos estudos das mais diversas áreas científicas o que tem dado margem a uma multiplicidade de conceitos que, muitas vezes, vêm sendo empregados de modo errôneo. Braman (2006) promove uma importante discussão a respeito desse fenômeno e, para isso, lista seis diferentes definições para a informação: a) informação como um recurso: quando é tratada como algo que uma entidade – uma pessoa, uma organização ou uma comunidade – deve possuir para o seu funcionamento, ou seja, quando é um input (insumo) para qualquer processo produtivo, de tomada de decisão ou qualquer processo burocrático; b) informação como commodity: quando se trata de algo que se pode comprar ou vender; c) informação como percepção do padrão: quando é tratada como dado padronizado; d) informação como um agente: que, diferentemente das demais definições, não considera a informação como algo usado por outras entidades e possibilita pensar a informação como algo que possui agência, ou seja, pode por si própria fazer as coisas acontecerem; d) informação como um recipiente de possibilidades: trata a informação como possibilidades que se aplicam a uma gama de processos sociais e em todos os níveis da estrutura social; e) informação como uma força constitutiva na sociedade: para Braman (2006), esta é a mais importante definição da informação na perspectiva da tomada de decisão política, pois permite que a informação se aplique a um conjunto de fenômenos e processos sociais e lhe sendo concedido um enorme poder na construção social da realidade humana. Esta dimensão da informação é partilhada também por Soderberg quem infere que a informação "não aparece mais como um produto final acabado, mas como um processo contínuo de trabalho" (apud. MACIEL; ALBAGLI, 2011, p.17). Para a discussão que se segue, é tomada como referência a definição de informação como recurso.

4 Como salientam Álvares e Batista (2007), desde a antiguidade buscam-se definições de conhecimento das quais se destacam os esforços de Sócrates (470-399 a.C.) em indagar o que pode ser conhecido e se é ou não possível um conhecimento absoluto, os trabalhos de Nicolau Cusa (1401-1464) no século XV sobre até onde pode chegar o conhecimento humano, o estudo do conhecimento como um elemento fundamental para tornar o trabalho gratificante em "A Utopia" de Thomas Morus (1478-1535), os questionamentos de John Locke (1632-1704) sobre a origem do conhecimento, a Teoria do Conhecimento de Emanuel Kant (1724-1804) e as reflexões

1999) e importantes para qualquer processo de tomada de decisão dentro de uma organização (BRAMAN, 2006).

Percebe-se uma interdependência cada vez mais estreita entre aquilo que é material e aquilo que é imaterial[5], dito de outra maneira, observa-se uma interdependência cada vez maior entre serviços e indústria na qual "a informação e o conhecimento incorporados nas produções materiais são cada vez mais importantes" (HERSCOVICI, 2007, p.214). Dessa forma, fala-se em criação de novos espaços (espaço cibernético[6]), em comércio eletrônico, informação biomédica, votação eletrônica, governo eletrônico, redes sociais virtuais, entre outros, que refletem e exemplificam o processo de informatização por qual passa o mundo.

No campo da Segurança Internacional, termos como ataques, crimes e guerra cibernéticos desafiam especialistas tanto do ponto de vista conceitual, como do ponto de vista prático, pois necessitam prover respostas para eventos que não fazem parte de sua agenda principal[7].

Com isso, os conceitos de Segurança Cibernética e de Segurança da Informação[8] passam a se juntar a outros conceitos mais consolidados como o de Sociedade, Economia e Capitalismo Informacional na tentativa de descrever o contexto atual. A Segurança Cibernética passa a ser considerada uma função estratégica dos Estados e como um instrumento cuja importância é cada vez mais evidente

---

de Francis Bacon (1561-1626) e René Descartes (1596-1650) sobre conhecimento e método científico. Contemporaneamente, o termo conhecimento, assim como o termo informação, faz parte da linguagem artificial de várias ciências (XAVIER; COSTA, 1980) e seu entendimento encontra-se compartimentalizado. Para o presente trabalho recorre-se a Ciência da Informação e toma-se como referência o conceito que trata o conhecimento como sendo, simultaneamente, efeito e causa da informação de forma em que "informação é o conhecimento fragmentado para sua melhor assimilação e disseminação, principalmente em meio eletrônico; e conhecimento é todo o saber existente nos seres e na natureza que é explicitado através de sua fragmentação em informação" (SIRIHAL; LOURENÇO, 2007, p.12).

5 Autores como Boutang (2011) entendem essa interação entre o material e o imaterial como uma das características do capitalismo cognitivo, ou seja, "um novo sistema em que a acumulação está vinculada ao conhecimento e a criatividade, e também às formas de investimento imaterial" (p.89). Nesse sistema, "a extração do lucro a partir do conhecimento e da inovação torna-se a questão central da acumulação, tendo papel fundamental no lucro" (p.89). Para exemplificar, o autor recorre à questão dos direitos de propriedade, às alianças, à apropriação das novas tecnologias, à crescente miniaturização (nanotecnologia), entre outros.

6 De acordo com Pierre Levy, o espaço cibernético "é o novo meio de comunicação que surge da interconexão mundial dos computadores. O termo especifica não apenas a infraestrutura material da comunicação digital, mas também o universo oceânico de informações que ela abriga, assim como os seres humanos que navegam e alimentam esse universo" (LEVY, 1999, p.17).

7 O termo agenda se refere ao conjunto de temas, assuntos, questões debatidos entre os atores que fazem parte das relações internacionais. A área de segurança internacional tem sua agenda própria que varia ao longo do tempo e segundo o interesse dos atores principais. Esta agenda de segurança engloba tradicionalmente discussões acerca dos conflitos bélicos, armamentos e poder. Muitos dizem que é uma agenda restrita e limitada. Por isto, autores como Buzan, Waver e Jaap (1998) propõem a ampliação da agenda de segurança internacional a partir da década de 1990 considerando novos temas como, por exemplo, a segurança econômica e ambiental ao mesmo tempo em que continuam a considerar a segurança militar como tema central, "se estabeleceu a distinção entre assuntos de segurança de alta intensidade, e assuntos de segurança de baixa intensidade. Com os assuntos de segurança de alta intensidade, ou hard security, se usa o aparelho militar para enfrentar estas ameaças. Com os assuntos de segurança de baixa intensidade, ou soft security, se usam meios alternativos para conter as ameaças" (MESSARI, 2004, p.133). Dessa forma, na medida em que eventos de ordem cibernética se tornam cada vez mais freqüentes, os especialistas da segurança internacional atentam cada vez mais para o tema, dando-lhe relevância ainda que não corresponda a um dos assuntos de hard security.

8 Os conceitos de Segurança Cibernética e de Segurança da Informação não devem ser entendidos como sinônimos. Na realidade, como é apresentando no Livro Verde de Segurança Cibernética brasileiro (PRESIDÊNCIA DA REPÚBLICA, 2010), mecanismos e ações de Segurança da Informação podem ser desenvolvidos com vistas a fortalecer e implementar elementos capazes de prover a Segurança Cibernética. Uma diferenciação mais aprofundada desses dois termos é um dos pontos-chave da primeira parte do presente artigo.

para a manutenção das infraestruturas críticas de um país (PRESIDÊNCIA DA REPÚBLICA, 2010). Nesse sentido, do ponto de vista das relações internacionais, nota-se um movimento em direção ao desenvolvimento e implementação de políticas nacionais de segurança cibernéticas com fortes sinalizações em termos de legislação nacional, de cooperação internacional e de normalização de metodologias. No âmbito das Nações Unidas, por exemplo, *o Group of Governmental Experts* (GGE) *on Developments in the Field of Information and Telecommunications in the Context of International Security* tem discutido cerca de 40 temas concernentes à Segurança Cibernética para que se possa formular recomendações aos países membro como já é feito pela Organização para a Cooperação e o Desenvolvimento Econômico e pela União Internacional das Telecomunicações. Já no campo do Direito Internacional, a Convenção de Budapeste[9] criada em 2001 na Hungria pelo Conselho da Europa representa um importante avanço, pois definiu e tipificou os principais crimes cometidos na Internet.

O presente artigo discute e propõe a inserção da Segurança Cibernética como um importante tema que deve figurar nas agendas de segurança internacional e da segurança brasileira. Para tanto, está dividido em duas partes. A primeira delas trata da questão conceitual da Segurança Cibernética buscando traçar um paralelo com o conceito de Segurança da Informação. Além, faz inferências sobre as contribuições de Buzan (*et al*. 1998) uma vez que este promove uma linha de raciocínio mais abrangente dos estudos da Segurança Internacional, permitindo que temas como meio ambiente e a economia, por exemplo, possam sofrer processos de securitização[10]. A segunda parte é dedicada à discussão atual de como a Segurança Cibernética vem sendo tratada no Brasil. Nesse sentido, as contribuições de Canongia e Raphael Mandarino (2010), bem como, a análise do Livro Verde da Segurança Cibernética, principal documento de análise situacional elaborado pelo governo brasileiro, são importantes de modo a resgatar a trajetória da Segurança Cibernética no país e para discutir as potencialidades, desafios, oportunidades, e mesmo a perspectiva nacional, que parece indicar em direção à construção de uma Política e das estratégias nacionais de Segurança Cibernética.

9 Também conhecida como Convenção sobre o Cibercrime, entrou em vigor em 2004 após ratificação de cinco países e, atualmente, conta mais de vinte países signatários. A Convenção, em seu preâmbulo, prioriza "uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da cooperação internacional" e reconhece "a necessidade de uma cooperação entre os Estados e a indústria privada" (CONVENÇÃO DE BUDAPESTE, 2001 *apud.* SOUZA; PEREIRA, 2009, p.5). O Brasil não é signatário da Convenção e como bem lembrou o ex-Secretário-Geral do Ministério das Relações Exteriores, Samuel Pinheiro Guimarães, o país não pode aderir à Convenção e sim deve ser convidado pelo Comitê de Ministros do Conselho da Europa como prescreve o Artigo 37º do documento (SOUZA; PEREIRA, 2009).

10 Messari (2004), apoiado ao pensamento de Clausewitz e de Buzan e seus companheiros, desenha três esferas sociais: a esfera privada, a esfera pública, e a esfera de segurança. Uma questão sofre processo de politização quando migra da esfera privada para a esfera pública, do mesmo modo em que passa por um processo de securitização quando migra da esfera pública para a esfera de segurança (MESSARI, 2004). O casamento, por exemplo, é um assunto que faz parte da vida privada do indivíduo no ocidente, mas na Índia, por exemplo, é um assunto de ordem pública, portanto, é considerado um objeto político. Já as questões militares, em muitos países, são questões securitizadas por serem vistas como questões críticas para a sobrevivência nacional. Cumpre dizer ainda que, segundo Messari (2004), os assuntos podem ser desecuritizados e despolitizados, sendo que a despolitização de um assunto pode significar o seu retorno para a esfera privada, ou a sua migração para esfera da segurança. "Em suma, a politização é a passagem da esfera privada à esfera pública, a despolitização é a passagem da esfera pública à esfera privada, a securitização é a passagem da esfera pública à esfera de segurança e a desecuritização é a volta de um assunto da esfera de segurança à esfera pública" (MESSARI, 2004, p.134).

1. A informação e a agenda de Segurança Internacional: definindo a Segurança Cibernética

Atualmente, o discurso sobre a existência de significativas inovações produtivas, sociais, políticas e organizacionais em curso e o de que a informação é um elemento central desses processos têm sido cada vez mais reconhecidos (MACIEL; ALBAGLI, 2011). Por esta perspectiva, a informação parece não carregar "em si a simples função de informar uma inovação, ou qualquer outro assunto, mas tem a potencialidade latente de produzir conhecimento" (XAVIER; COSTA, 2010, p.80). Com isso, ela passa ser vista do ponto de vista estratégico por tomadores de decisão, sobretudo do setor privado, que buscam "a definição de modernos sistemas de informação que utilizem, adequadamente, todos os recursos disponíveis da informática para acesso e divulgação da informação dentro das empresas" (LEITÃO, 1993, p.120). Porém, esse tipo de preocupação parece também transitar pelo setor público quando se leva em consideração os crescentes empreendimentos governamentais em direção a informatização dos processos burocráticos tais como a implantação de sistemas de governo eletrônico[11] (*e-government*[12], *m-government*[13] *e t-government*[14]), o voto eletrônico e a digitalização dos processos de divulgação da informação pública em muitos países, ou seja, o aumento da penetrabilidade das novas tecnologias e de seus efeitos (CASTELLS, 1999). Na esfera social, a disponibilização de um amplo conjunto de serviços através da Internet, como o *Internet Banking*[15] e o comércio eletrônico, por exemplo, e a flexibilização dos processos sociais também podem ser fatores que corroboram para que a informação seja vista como um elemento social central, legitimando, assim, o termo informacional para a descrição da sociedade contemporânea (CASTELLS, 1999).

Quando se leva em conta o campo da Segurança Internacional, o surgimento da informação como um insumo estratégico (LEITÃO, 1993) coincide com o repensar do conceito de segurança enquanto área de estudo das Relações Internacionais e o fervilhar de profundas mudanças no campo das Teorias das Relações Internacionais.

O debate acadêmico inaugurado no final da década de 1980 colocou em posições adversas os teóricos que defendiam a expansão do conceito de Segurança Internacional e aqueles que defendiam a sua essência militar e estratégica. Enquanto os primeiros se esforçavam para evidenciar que a distinção entre estudos estratégicos e estudos de segurança estava na centralidade da segurança militar dada pelos estudos estratégicos e no emprego do conceito de segurança em outros setores, tal qual o

11 Em "Governo Eletrônico no Brasil: Aspectos Institucionais e Reflexos na Governança", Paulo Henrique Medeiros (2004) define governo eletrônico a partir das definições dadas por vários autores e instituições. Para o Banco Mundial, por exemplo, o governo eletrônico "refere-se ao uso, por agências governamentais, de tecnologias de informação (como redes de longa distância, Internet e computação móvel) capazes de transformar as relações com cidadãos, empresas e outras unidades do governo" (MEDEIROS, 2004, p.30), enquanto as Nações Unidas definem como a "utilização da Internet e da web para ofertar informações e serviços governamentais aos cidadãos" (MEDEIROS, 2004, p.30).

12 Governo eletrônico via Internet.

13 Governo eletrônico via telefonia móvel.

14 Governo eletrônico via televisão.

15 Também conhecido como Homebanking, Netbanking ou Banco on-line "permite aos clientes bancários executar um amplo conjunto de transações financeiras através de meios eletrônicos" (TEO; TAN; SHAO apud. TAVARES, 2008, p.41).

econômico, o societal e o ambiental, como era proporcionado pelos estudos de segurança; os últimos posicionavam a segurança como um conceito exclusivamente militar e o correlacionavam apenas com as ameaças que põem em risco a sobrevivência do Estado (MESSARI, 2004).

Esses movimentos no campo da Segurança Internacional refletem em muito as mudanças que ocorriam no campo das Teorias das Relações Internacionais em que se questionava o paradigma até então predominante do realismo ao mesmo tempo em que se abria espaço para um diálogo mais intenso entre as abordagens racionalistas, liberais e construtivistas.

O objetivo dos teóricos que defendiam a expansão do conceito de Segurança Internacional, como Buzan (*et al.* 1998), era "tornar mais complexo o conceito de segurança, pulverizando-lo assim entre diferentes setores" (MESSARI, 2004, p. 133). A principal contribuição de Buzan (*et al.* 1998), nesse sentido, foram as distinções analíticas entre cinco setores nos quais podem ocorrer processos de securitização: o militar, o político, o econômico, o societal e o ambiental[16] de modo que a segurança militar continuasse central, mas não a única a ser levada em consideração. "Em suma, era necessário evitar a mobilização de todas as potencialidades nacionais para tratar certas ameaças, mas ao mesmo tempo, era necessário tratar estas questões como ameaças à segurança" (MESSARI, 2004, p. 133).

Neste sentido, Buzan e seus companheiros (*et al.,*1998) visam incorporar outras ameaças que não somente às tradicionais. Para eles, muitos outros objetos (clima, identidade, economia, cultura, por exemplo) podem ser passíveis de serem politizados e/ou securitizados, de modo que os esforços nacionais em segurança passam a ser ampliados. É preciso notar que aos setores propostos por Buzan (*et al*., 1998) podem ser acrescentados outros, bem como novos objetos.

Nesta lógica, podemos propor que mesmo a informação, ou algumas categorias de informação e conhecimento podem ser passíveis de serem politizadas e/ou securitizadas. Indo mais adiante, é possível pensar o informacional como um novo setor dentro da proposta teórica de Buzan (*et al.,* 1998). O informacional poderia se tornar um sexto setor no qual também pode ocorrer processos de securitização[17]. No entanto, o primeiro passo para uma constatação dessa natureza coincide com o propósito da presente discussão e consiste no entendimento de como a informação vem sendo incorporada pelos estudos de segurança, o que pode ser verificado a partir de análises do conceito de Segurança da Informação e do conceito de Segurança Cibernética.

É preciso notar, todavia, que a informação perpassa todos os setores propostos por Buzan (*et al*., 1998). De fato, ambos os processos, politização e securitização, são permeados por informações

16 A ideia de Buzan (et al. 1998) é que a segurança incorporaria cinco grandes setores. Dois deles já seriam os setores tradicionais do campo – político e militar, os demais seriam novos setores. O setor militar, neste caso, diz respeito aos dois níveis de interação da ofensiva armada e das capacidades defensivas dos Estados e as percepções dos Estados sobre as intenções dos demais; o político diz respeito à estabilidade organizacional dos Estados, os sistemas de governo e as ideologias que lhes garantem a legitimidade; o econômico ao acesso aos recursos financeiros e aos mercados necessários para sustentar níveis aceitáveis de bem estar e de poder estatal; o societal à sustentabilidade, dentro de condições aceitáveis para a evolução, de padrões lingüísticos, culturais, religiosos, de costumes e de identidade nacional e, enfim, o ambiental que diz respeito à manutenção da biosfera local e planetária como sistema essencial no qual todas as outras gerações humanas dependem (BUZAN, et al. 1998).

17 A questão da criação do setor informacional, na qual se define o objeto, evidencia os atores de referência, elementos de ameaça, por exemplo, é objeto de pesquisa de um trabalho ainda em construção promovido pelos autores do presente artigo.

e conhecimentos específicos que interferem em suas dinâmicas [informação seria percebida como elemento horizontal na dinâmica da segurança, pois se insere em todos os demais setores]. Para além disso, o que se propõe aqui é que a informação e o conhecimento de forma geral podem ser objetos politizáveis e securitizáveis, como é o aquecimento global, por exemplo, dentro do setor ambiental. Determinadas informações podem ser, em nosso entendimento, securitizáveis. Com isto, a informação e o conhecimento são estudadas em uma perspectiva verticalizada e como objeto referente de um setor próprio.

A disseminação de informação ao mesmo tempo em que promove a geração de conhecimento (COSTA; XAVIER, 2010), "expõe ainda mais a fragilidade e os riscos a que estão expostos os usuários, os sistemas que utilizam e os dados armazenados e tratados por tais sistemas" (MARCIANO; LIMA-MARQUES, 2006, p.92). Deste modo, passam a ser corriqueiros incidentes tais como as fraudes digitais, os furtos de senhas, os ataques a sítios da Internet promovidos por *hackers*, além do aumento do número de vulnerabilidades, ou seja, falhas de mecanismos computacionais em *softwares* ou em *hardwares* (MARCIANO; LIMA-MARQUES, 2006). Esses fenômenos ativam uma preocupação sobre a vulnerabilidade de usuários e das informações em redes, abrindo espaço para a construção do que tem se denominado como Segurança da Informação. Para além disso, existe a preocupação específica com as denominadas guerras cibernética e eletrônica, com os ataques a sistemas de defesa, com as quebras de códigos e com o vazamento de informações que são consideradas estratégicas para as nações.

A literatura tem explicitado com eficiência conceitos de Segurança da Informação centrados em suas funções, mas não logra o mesmo quanto à descrição do que de fato ela é, ou seja, abundam as análises funcionais, mas são escassas as análises descritivas da segurança da informação, pois, geralmente, relacionam-se atividades por ela realizadas, mas não dão significado ao que ela efetivamente é (MARCIANO; LIMA-MARQUES, 2006; LORENS, 2007).

A ausência de um conceito único tem levado estudiosos de diferentes campos científicos a sugerirem definições para o termo as quais, na maioria das vezes, possuem uma ótica setorial, privilegiando apenas um dos setores da Segurança da Informação: os sistemas de informação[18], seus usuários[19] ou a sociedade que tem sua estrutura modificada por esses sistemas (MARCIANO; LIMA-MARQUES, 2006).

O conceito apresentado por João Luiz Marciano e Mamede Lima Marques é um dos poucos que conseguem abordar estas três dimensões e busca o equilíbrio entre as visões subjetiva e objetiva da Segurança da Informação ao mesmo tempo em que traz para o nível cognitivo dos usuários da informação a concepção do fenômeno da segurança (LORENS, 2007). Para eles,

18 Para João Luiz Marciano e Mamede Lima-Marques "um sistema de informações é (...) a somatória do sistema social no qual ele se apresenta, compreendendo os usuários e suas interações entre si e com o próprio sistema, e do complexo tecnológico sobre o qual estas interações se sustentam" (MARCIANO; LIMA-MARQUES, 2004, p. 95).

19 O usuário de um sistema de informação "é o indivíduo para o qual se concretiza o fenômeno do conhecimento mediante as informações providas por aquele sistema" (MARCIANO; LIMA-MARQUES, 2004, p. 95).

> Segurança da Informação é um fenômeno social no qual os usuários (aí incluídos os gestores) dos sistemas de informação têm razoável conhecimento acerca do uso destes sistemas, incluindo os ônus decorrentes expressos por meio de regras, bem como sobre os papéis que devem desempenhar no exercício deste uso (MARCIANO; MARQUES, 2004, p. 95).

Repetindo o dilema do conceito de Segurança da Informação, o conceito de Segurança Cibernética tampouco se apresenta de maneira exata e objetiva, pois como salienta Xihgan LI (2006), Segurança Cibernética é um conceito relativo já que existem várias maneiras de se responder a pergunta: "O que é Segurança Cibernética?". Segundo este autor o conceito de Segurança Cibernética é comparativo, pois se por um lado, ele inclui a comparação entre segurança e técnicas de ataque, por outro, inclui a comparação entre técnicas de segurança e medições (LI, 2006, p.13).

Observa-se que as definições de Segurança Cibernética têm surgido no âmbito de agências e organismos governamentais, em organizações internacionais e em corporações privadas de modo desuniforme. A União Internacional das Telecomunicações, na tentativa aparente de reverter esse impasse, apresenta uma arquitetura conceitual que redireciona a definição de Segurança Cibernética para a realidade de cada país. Segundo a organização, Segurança Cibernética "significa basicamente prover proteção contra acesso, manipulação, e destruição não autorizada de recursos críticos e bens" (CANONGIA; MANDARINO, 2009, p.26). Desse modo, o conceito de Segurança Cibernética está em acordo com o nível de desenvolvimento dos países e com que aquilo que cada país considera como sendo recurso crítico e ações de proteção cibernética.

Diante dessas considerações, o conceito de Segurança Cibernética proposto por Raphael Mandarino parece ser, fora o uso do termo arte, o mais próximo do adequado[20]: "segurança cibernética é entendida como a arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação[21] e suas infraestruturas críticas[22]" (MANDARINO *apud*. CANONGIA; MANDARINO, 2009, p.26).

No entanto, a inexatidão e a profusão dos conceitos de Segurança da Informação e de Segurança Cibernética somado com a possibilidade de relativização desse último tem aberto margem para a fusão dos dois conceitos o que é um equívoco. Entende-se a Segurança Cibernética como a forma pela qual se prover proteção no Espaço Cibernético aos ativos de informação e aos recursos críticos, já a Segurança da Informação pode ser entendida como o meio pelo qual isso ocorre já que está definida como a forma de proteção da informação em que os usuários dos sistemas de informação

20 Consideramos inapropriado o uso do vocábulo arte para a designação de algo que pode ser conhecido e aprendido visto o entendimento da técnica ou do estudo sistemático da mesma e que não depende de talento ou da providência divina para seu exercício, como parece carregar a noção de arte. O mesmo vale para política, que não é a arte de governar, ou para a guerra, que não é a arte de utilizar os exércitos em campanhas.

21 A Portaria 45 do Conselho de Defesa Nacional, ativos de informação são "meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso" (PORTARIA 45 SE-CDN, 2009).

22 Em acordo com a Portaria 45 Gabinete de Segurança da Institucional da Presidência da República, no Brasil, infraestruturas críticas "são instalações, serviços, bens e sistemas que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade" (PORTARIA 45 GSI, 2009).

têm razoável conhecimento acerca das regras de uso destes sistemas.

Uma vez definido o objeto de estudo cumpre questionar o motivo pelo qual este esteja em voga na última década dentro da agenda de segurança internacional. A resposta para tal questionamento tem sido apontada por especialistas e cientistas de áreas multidisciplinares como resultado do alto número de ataques cibernéticos registrados em todo o mundo contra sistemas de informação governamentais (CANONGIA; MANDARINO, 2009).

Para Zolnerkevic (2011), por exemplo, o fator crucial para que a Segurança Cibernética passasse a ser um tema amplamente discutido, sobretudo pela imprensa internacional, talvez, tenha sido a intensa divulgação na Internet de mensagens confidenciais, principalmente, de embaixadas norte-americanas pela organização transnacional não-governamental *Wikileaks*. O *Wikileaks* ficou conhecido por revelar informações da diplomacia estatal e, com isso, conduziu ao questionamento sobre o fundamento do aspecto público dessa instituição.

Mas antes disso, alguns incidentes no Espaço Cibernético já poderiam ser entendidos como preocupantes para a manutenção da harmonia no sistema internacional. *Hackers* chineses, em 2007, foram acusados de promover ataques cibernéticos aos Estados Unidos e Alemanha. Segundo as acusações os criminosos cibernéticos penetraram nas redes de informação de órgãos políticos e de defesa nacional[23]. Em 2009, a Estônia, acusou o governo russo de orquestrar ataques cibernéticos em 2007, como forma de retaliação à remoção de um memorial de guerra soviético. Os ataques deixaram fora de operação os *sites* do parlamento da Estônia durante três semanas (CANONGIA; MANDARINO, 2009).

Em 2009, os Estados Unidos registraram ataques ao site do Departamento de Defesa durante quatro dias consecutivos que teriam o objetivo de saturar o acesso e a conexão da Internet até que o acesso fosse interrompido (SILVA, 2009 *apud.* CANONGIA; MANDARINO, 2009). No mesmo ano, o governo da Coreia do Sul também registrou ação similar e em ambos os casos os dados dos setores de inteligência dos dois países localizaram fontes dos ataques em 16 países (SILVA, 2009 *apud.* CANONGIA; MANDARINO, 2009).

Em 2010, ocorreram fatos emblemáticos como a ordem de ataque do governo chinês ao *site* da Google, *site* de buscas na internet que abandonou a China em janeiro de 2010 sob alegação de que estaria sofrendo ataque cibernético cujas confirmações vieram quase um ano depois por meio de documentos vindos da embaixada norte-americana na China e divulgados pelo *Wikileaks*[24]. No mesmo ano, o Irã identificou um ataque cibernético aos reatores de sua usina nuclear causados por vírus, levando especialistas e autoridades iranianas a descrever o episódio como o primeiro míssil cibernético teleguiado. Posteriormente, foi descoberto que a origem do vírus detectado no Irã possui relação com resultados de operações conjuntas entre Israel e os Estados Unidos o que corrobora

23 The Guardian (08/01/07): "*China denies hacking the Pentagon*". Disponível em: http://www.guardian.co.uk/world/2007/sep/04/china.usa Acessado em: 24 Jun. 2011.

24 BBC Brasil (05/12/10): "Autoridades da China ordenaram ataque ao Google, diz documento" Disponível em: http://www.bbc.co.uk/portuguese/noticias/2010/12/101205_china_google_wikileaks_rw.shtml Acessado em: 24 Jun. 2011.

com as acusações do Irã de que os ataques partiram dos Estados Unidos pelo fato do governo norte-americano se sentir ameaçado frente ao suposto desenvolvimento de armas nucleares pelo governo iraniano que justifica seu programa de enriquecimento de urânio como sendo para fins pacíficos[25].

No quadro mais recente de ataques cibernéticos, fazem parte da lista a Coreia do Sul, o Fundo Monetário Internacional (FMI) e o Brasil. A Coreia do Sul acusa a Coreia do Norte por um ataque que paralisou um de seus maiores bancos em abril de 2011. A promotoria pública de Seul classificou o episódio como sendo um ato de terrorismo cibernético provocado pelo mesmo programa utilizado em ataques anteriores conduzidos por *hackers* que, supostamente, estariam a serviço da Coreia do Norte[26]. Em junho de 2011, o FMI registrou um ataque cibernético que, segundo a instituição, teve o objetivo de roubar informações sensíveis e privilegiadas[27]. Já no Brasil, a segunda semana de junho de 2011 entrou para a história da trajetória nacional da Segurança Cibernética como a semana em que o governo foi alvo do maior ataque cibernético até então registrado no país[28]. Um grupo de *hackers* conseguiu atacar os *sites* da Presidência da República, do Portal Brasil, da Receita Federal, da Petrobras, do Ministério do Esporte, do Instituto Brasileiro de Geografia e Estatística e do Ministério da Cultura fazendo-os apresentar dificuldades de navegação, ficar fora de operação ou desfigurados mediante um número alto de acessos simultâneos produzidos por robôs[29].

O relatório anual "No Fogo Cruzado: As Infraestruturas Essenciais na Era da Guerra Cibernética" produzido pelo Centro de Estudos Estratégicos e Internacionais em 2010 apontou que de um total de 600 diretores de segurança da informação de 14 países, 59% acreditam que os autores de ataques cibernéticos podem ser governos estrangeiros e, nesse sentido, os Estado Unidos com 36% e a China com 33% são apontados como as maiores ameaças[30].

Outro indicador de que a Segurança Cibernética vem atraindo a atenção no âmbito da Segurança Internacional são as constantes recomendações em matéria de segurança da informação anunciadas por organizações internacionais tais como as Nações Unidas, a União Internacional de Telecomunicações (UIT), a Organização para a Cooperação e o Desenvolvimento Econômico (OCDE) e de outras instituições já vítimas de ataques cibernéticos como é o caso do FMI. A OCDE, em 2009, lançou diretrizes sobre o cenário da sociedade informacional a nível mundial e dentre elas ressaltou o "aumento das ameaças e das vulnerabilidades, apontando para a urgência de ações na direção da criação, manutenção e fortalecimento da cultura de segurança" (CANONGIA; MANDARINO, 2009,

25 Reuters (25/04/2011): "Irã diz ter detectado segundo ataque cibernético ao país". Disponível em: http://br.reuters.com/article/idBRSPE73O00Z20110425 Acessado em: 24 Jun. 2011.

26 BBC Brasil (03/05/2011): "Coreia do Sul acusa Norte por ataque de hackers contra banco". Disponível em: http://www.bbc.co.uk/portuguese/noticias/2011/05/110503_coreias_banco_ataque_cc.shtml Acessado em: 24 Jun. 2011.

27 Reuters (12/06/2011): "Ataque cibernético ao FMI buscava informações" privilegiadashttp://br.reuters.com/article/businessNews/idBRSPE75B05L20110612 .Acessado em: 24 Jun. 2011.

28 BBC Brasil (25/06/2011): "Entenda os ataques de hackers contra sites do governo brasileiro. Disponível em: http://www.bbc.co.uk/portuguese/noticias/2011/06/110625_qa_hacker_jc.shtml Acessado em: 28 jun. 2011.

29 BBC Brasil (25/06/2011): "Entenda os ataques de hackers contra sites do governo brasileiro. Disponível em: http://www.bbc.co.uk/portuguese/noticias/2011/06/110625_qa_hacker_jc.shtml Acessado em: 28 jun. 2011.

30 Disponível em BBC Brasil (01/02/2010): "Brasil é um dos países mais vulneráveis a ataques cibernéticos, diz pesquisa. Disponível em: http://www.bbc.co.uk/portuguese/noticias/2010/02/100201_ataque_cibernetico_ vdm.shtml Acessado em: 24 Jun. 2011.

p.24).

A UIT, a sua vez, por meio de seu Secretário Geral Dr. Hamadoun I. Touré, possui uma proposta mais abrangente que trata da criação da Agenda Global de Segurança Cibernética com o propósito de construir uma plataforma para a cooperação internacional baseada no esforço de todas as partes interessadas a fim de aumentar a segurança e a confiança na sociedade informacional. Criada em 2007, a Agenda Global de Segurança Cibernética está constituída por cinco pilares: medidas legais, medidas técnicas e de procedimento, estruturas organizacionais, capacitação e cooperação internacional.

Sendo assim, é possível perceber que mesmo não sendo um tema que compõe a agenda central da Segurança Internacional (não é um assunto de *hard security*), a Segurança Cibernética tem alcançado destaque nesse campo de estudo das Relações Internacionais nos últimos anos devido ao aumento de incidentes do uso inadequado do Espaço Cibernético. Esses incidentes vêm gerando três movimentos importantes: 1) motivam governos em todo mundo que buscam ampliar suas habilidades técnicas e legais em Segurança da Informação a fim de proteger seus indivíduos usuários de sistemas de informação. Este é o caso do Brasil, por exemplo, que será analisado na seção seguinte; 2) mobilizam discussões no âmbito de organizações internacionais, que passam a se dedicar a temática da Segurança Cibernética na tentativa, inclusive, de desenhar uma agenda global específica; e 3) fazem avançar o processo de securitização da informação, isto é, confirmam o surgimento de um movimento pela politização e subsequente securitização da informação, confirmando aquilo que este artigo propõe que é o surgimento de um sexto setor, nos termos da proposta de Buzan (*et al.*, 1998).

2. O Brasil e a o desafio da segurança no Espaço Cibernético

É na década de 1990 que a Segurança Cibernética começa a ganhar importância específica no Brasil, principalmente, no que tange aos aspectos legais e jurídicos que a envolvem. Atualmente, leis têm sido propostas para tratar especificamente de temas relacionados à segurança da informação em formato digital, como o comércio eletrônico, e as leis já existentes mostram-se abrangentes (MARCIANO, 2006).

No plano governamental brasileiro, marcam o início das preocupações com a Segurança Cibernética o Decreto 4.553 da Presidência da República que vigora sobre a classificação das informações em 2002 e antes dele, em 2001, a instituição do ICP-Brasil, ou seja, o PKI (*Public Key Infrastructure*) nacional, um conjunto de técnicas, práticas e procedimentos elaborado para suportar um sistema criptográfico com base em certificados digitais. O ICP-Brasil foi criado por medida provisória e transformou o País no primeiro do mundo a ter legislação específica para as questões de informação digital (ICP-BRASIL, 2011).

No âmbito normativo, marca o quadro de ações mais recentes a publicação da Instrução Normativa do Gabinete de Segurança Institucional da Presidência da República (GISPR) Nº 01/2008,

que disciplina compulsoriamente a Gestão de Segurança da Informação e Comunicações

> na Administração Publica Federal (APF), direta e indireta, a qual define que 'Segurança da Informação e Comunicações (SIC) são ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações', inovando e ampliando, portanto, o escopo tradicionalmente conhecido e adotado na segurança da informação (CANONGIA; MANDARINO, 2009, p.38).

Em sua fase de trabalho inicial, o GSIPR buscou traçar um estudo para entender as estratégias usadas pelos demais países e qual a metodologia empregada para tratar da segurança cibernética. Este estudo chegou à conclusão curiosa de que inexistem modelos formatados e testados para o entendimento de como agir de forma estruturada na prevenção e combate a crimes e ataques cibernéticos. Esta constatação pode ser vista como um dos fatores que levou ao governo introduzir o tema na agenda da Administração Pública Federal a partir da instituição da Portaria Nº45 do Diário Oficial da União e criando o Grupo Técnico de Segurança Cibernética que é composto por representantes dos Ministérios da Justiça, da Defesa, das Relações Exteriores, e dos Comandantes da Marinha, do Exército e da Aeronáutica.

Uma das primeiras ações desse grupo foi a elaboração em 2010 do Livro Verde da Segurança Cibernética no Brasil com o objetivo de

> expressar potenciais diretrizes estratégicas para o estabelecimento da Política Nacional de Segurança Cibernética, articulando visão de curto (2 a 3 anos), médio (5 a 7 anos), e longo (10 a 15 anos) prazo no tema, abrangendo, como ponto de partida, os seguintes vetores: Político-estratégico, Econômico, Social e ambiental, CT&I, Educação, Legal, Cooperação Internacional, e Segurança das Infraestruturas Críticas (PRESIDÊNCIA DA REPÚBLICA, 2010, p.17).

A criação deste documento refletiu o interesse e a preocupação do governo em viabilizar iniciativas que favoreçam o maior engajamento e sincronicidade em torno da Segurança Cibernética e para que estas iniciativas possam se tornar realidades em um curto espaço de tempo, propiciando, assim, a construção da doutrina e da política nacional específica (PRESIDÊNCIA DA REPÚBLICA, 2010). Nesse sentido, o Livro Verde pode ser visto como o instrumento pelo qual o governo apresenta a análise situacional a fim de desenhar propostas e diretrizes na perspectiva de formulação de um marco teórico e legal que seria o Livro Branco da Segurança Cibernética, ou seja, uma Política Nacional de Segurança Cibernética.

Dos sete vetores que o Livro Verde da Segurança Cibernética faz referência a oportunidades e desafios nacionais, três se apresentam interessantes para a presente análise.

Do ponto de vista político-estratégico, o Livro Verde da Segurança Cibernética faz apontamentos que buscam legitimar o discurso do Brasil como um país ativo no que diz respeito ao tratamento do tema na esfera internacional, uma vez que podem ser identificados atores com amplos conhecimentos sobre o tema dentro do governo federal, bem como a expressiva participação do País em diversas redes de contatos e fóruns, nacionais e no exterior, como, por exemplo, o *Group of Governmental Experts* (GGE) *on Developments in the Field of Information*

and Telecommunications in the Context of International Security[31] no âmbito das Nações Unidas, a Convenção do Crime Cibernético[32] em Salvador em 2010, o *Working Party on Information Security and Privacy* - WPISP, e o *Comittee for Information, Computer and Communications* – ICCP, ambos organizados pela OCDE[33].

No entanto, são igualmente identificados grandes desafios como a constatação de 2 mil tentativas de invasão maliciosa, por hora, detectadas nas 320 grandes redes do governo; a falta de clareza sobre a importância e real dimensão da problemática; o baixo fluxo e intercâmbio de informação entre as equipes de tratamento de incidentes em sistemas de informação do governo e entre estas e as redes de inteligência de governança; a carência de senso comum e de arcabouço conceitual da segurança cibernética; a extensão da capacidade da Defesa Brasileira para abranger, além do espaço convencional, o espaço cibernético; e as capacidades dissuasórias do país abrangendo o Espaço Cibernético (PRESIDÊNCIA DA REPÚBLICA, 2010).

O segundo vetor que chama a atenção é o de cooperação internacional. Nesse sentido, são desafios para o Brasil a extensão continental; a tendência crescente nas relações internacionais de bipolaridade entre os Estados Unidos e a China, inclusive nas questões do Espaço Cibernético; a ausência de instrumentos internacionais específicos contra crimes cibernéticos; a articulação nacional, ainda incipiente, em termos de definição de ações transnacionais de segurança cibernética; e a demanda por ações conjuntas entre os Estados. Por outro lado, se apresentam como oportunidades a tendência crescente de multipolaridades para o tratamento do tema tendo a Rússia e o Brasil como vanguardistas desse movimento; os acordos bilaterais de cooperação em segurança da informação e comunicação, firmados, por exemplo, com a Espanha, Rússia, França, e em negociação com outros países, tais como Itália, Israel e Luxemburgo; e o reconhecimento internacional do Brasil, como um país ativo em relação ao tema da segurança cibernética (PRESIDÊNCIA DA REPÚBLICA, 2010).

E o terceiro vetor diz respeito à questão da segurança das infraestruturas críticas do país cujos desafios estão na falta de clareza e de identificação das interdependências nas infraestruturas críticas e seus respectivos graus de criticidade e impactos; na ausência de integração das várias políticas setoriais, iniciativas e investimentos de segurança das infraestruturas críticas; nos movimentos tardios de definição de prioridades estratégicas com foco na prevenção; no limitado número de infraestruturas críticas nacionais já priorizadas; nos crescentes riscos de ataques cibernéticos; e no insuficiente número de equipes de resposta e tratamento de incidentes em rede computacionais e de especialistas

31 Nesta instância, o Brasil esteve representado pelo Ministério da Defesa e o GSIPR participa na qualidade de observador. Este é um espaço no qual já foram debatidos, nos últimos anos, cerca de 40 itens, sendo que dentre os itens considerados polêmicos e para futuras recomendações, tem-se o de não proliferação de armas de informação.

32 Esta Convenção ocorreu em 2010, em Salvador e como um de seus resultados foi emitida uma Declaração, consensada por 158 países sobre a ineficácia da Convenção de Budapeste devido aos avanços tecnológicos. A Convenção de Salvador abriu a oportunidade de criação de um grupo para tratar globalmente do assunto.

33 Ambos ocorreram em Paris nos anos de 2009 e 2010 e o Brasil teve a oportunidade de apresentar a proposta de realização de "Estudo comparativo das estratégias nacionais de segurança cibernética" que foi plenamente aceita sendo e orientou a criação de um grupo conformado por países que voluntariamente se comprometeram em avançar com as discussões que trazem esta finalidade.

com competência para desempenhar tais atividades. Já como oportunidades podem ser assinalados a criação do Plano Nacional de Segurança das Infraestruturas Críticas (PNSIEC)[34]; a existência de Grupos Técnicos de Segurança das Infraestruturas Críticas de Energia, Transportes, Comunicações, Água, e Finanças, criados no âmbito da Câmara de Relações Exteriores e Defesa Nacional; e a formação do Grupo de Trabalho de Segurança das Infraestruturas Críticas da Informação no âmbito do Comitê Gestor de Segurança da Informação e Comunicações, do Conselho de Defesa Nacional (PRESIDÊNCIA DA REPÚBLICA, 2010).

Além, cabe mencionar os pontos cruciais do ponto de vista legal e normativo que também são trazidos à discussão pelo Livro Verde. Trata-se da ausência de legislação nacional específica de Segurança Cibernética, em especial contra crimes cibernéticos; da ausência de regulação e mecanismos de certificação de segurança cibernética; e da diversidade de termos e respectivas definições a serem harmonizados em nível nacional e internacional (PRESIDÊNCIA DA REPÚBLICA, 2010).

A principal crítica que pode ser feita ao Livro Verde da Segurança Cibernética bem como à trajetória da temática no Brasil está localizada na ausência de metas claras e objetivas a serem perseguidas para a formulação de uma política e de uma estratégia nacional de Segurança Cibernética. Em termos de descrição e mapeamento situacional da temática no país o Livro Verde é um importante instrumento, cumprindo desta forma o seu objetivo principal. Contudo a falta de um plano que consista de metas, prazos e meios e que faça dialogar oportunidades e os desafios já identificados pode ser um fator capital para o retardamento e morosidade de ações de prevenção e combate aos ataques e crimes cibernéticos no Brasil.

Sendo assim, ainda que a busca pelo protagonismo internacional em matéria de Segurança Cibernética seja interessante para o Brasil do ponto de vista da Segurança Internacional, já que a Segurança no Espaço Cibernético é um dos temas em voga, no presente estágio da discussão interna parece ser fundamental para o Brasil fazer convergir esforços de seus órgãos, setores e recursos especializados para prover respostas a aspectos críticos como é o caso da inexistência de legislação nacional para o tema, a não-integração das várias políticas setoriais, a necessidade de ações transnacionais de segurança cibernética e a falta de investimento para a segurança das infraestruturas críticas.

Para todos esses desafios a cooperação técnica internacional com instituições internacionais e com outros Estados, ao que tudo indica, pode ser uma facilitadora, assim como o sucesso desses empreendimentos deve ter como consequência a projeção do País a um nível superior no cenário internacional.

Conclusão

34 Segundo o Livro Verde da Segurança Cibernética este Plano "prevê o estabelecimento de um processo integrado, por meio da criação de cultura de segurança e proteção, em todas as esferas de poder, de recursos humanos qualificados, equipamentos, instalações, conhecimentos, serviços, rotinas, dados, informações e processos estratégicos, e busca estender o esforço das iniciativas ao setor privado" (2010, p.40).

Levando em consideração tudo aquilo que fora anteriormente discutido e analisado, é possível inferir as considerações finais sob três ângulos. O primeiro deles se refere ao aspecto conceitual. Sobre os conceitos de Segurança da Informação e de Segurança Cibernética pode-se concluir que não correspondem e nem descrevem a mesma coisa, uma vez que a Segurança Cibernética se refere à forma de proteção dos ativos de informação no Espaço Cibernético e a Segurança da Informação é o meio pelo qual esta proteção ocorre.

O segundo ângulo está ligado à Segurança Internacional e a sua relação com a informação enquanto recurso. Nesse sentido, é possível concluir que os incidentes de crimes e ataques cibernéticos no quadro recente do cenário internacional, bem como movimentos como o *Wikileaks* têm promovido o avanço da discussão sobre a normatização internacional de crimes cibernéticos e criação de uma agenda global de Segurança Cibernética o que caracteriza ao mesmo tempo em que corrobora para a securitização da informação, ou seja, o surgimento de um sexto setor, nos termos da proposta de Buzan (*et al.,* 1998).

O terceiro e último ângulo diz respeito à trajetória brasileira da Segurança Cibernética que, a sua vez, permite concluir que internamente a Segurança Cibernética e a Segurança da Informação são tratadas como duas coisas distintas e interligadas e que a agenda nacional parece acompanhar a agenda internacional partindo da constatação de que a Segurança Cibernética vem alcançando destaque ainda que não seja um assunto de *hard security*. As confirmações dessa observação estão na criação de órgãos e setores específicos para a temática e do Livro Verde da Segurança Cibernética.

Desta forma, pode-se dizer que o ponto de convergência entre as agendas nacional e internacional de segurança em matéria da Segurança Cibernética está na crescente atenção dada aos incidentes de ataques e de crimes no Espaço Cibernético e em dois importantes aspectos: o papel estratégico que a cooperação técnica entre o Brasil e as instituições internacionais e outros Estados evidencia para que os desafios nacionais possam ser superados e a vontade do Brasil em se projetar no cenário internacional como referência para a temática.

Referências Bibliográficas

ÁLVARES, Lillian; BATISTA, Fábio Ferreira. Ciência da Informação e Gestão do Conhecimento: a convergência a partir da Sociedade da Informação. In: ENANCIB – Encontro Nacional de Pesquisa em Ciência da Informação, 8, 2007, Salvador.

BOUTANG, Yann Moulier. Wikipolítica e economia das abelhas. Informação, poder e política em uma sociedade digital. In: MACIEL, Maria Lucia; ALBAGLI, Sarita (orgs.). Informação, conhecimento e poder: mudança tecnológica e inovação social. Rio de Janeiro: Garamond, 2011, p.67-102.

BRAMAN, Sandra. *Change of State: information, policy and power*. Cambridge: MIT Press, 2006, pp.545.

BRASIL. Portaria n. 45, de 08 de setembro de 2009. Institui, no âmbito da Câmara de Relações Exteriores e Defesa Nacional (CREDEN), o Grupo Técnico de Segurança Cibernética e dá outras providências. Diário Oficial da União, n. 172, 09 set. 2009.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. Institui Grupo Técnico de Segurança Cibernética, no âmbito da Câmara de Relações Exteriores e Defesa Nacional. Portaria nº 45, de 8 de setembro de 2009. Diário Oficial da União, nº 172, Pag. 2, 2009.

BUZAN, Barry; WAEVER Ole; WILDE, Jaap de. *Security: A new Framework for Analysis*. Londres: Lynne Rienner Publishers, 1998.

CANONGIA, Claudia, MANDARINO, Raphael. Segurança cibernética: o desafio da nova Sociedade da Informação. Parceria. Estratégica. Brasília, DF., v.14 n.29, jul-dez 2009, p.21-46.

CASTELLS, Manuel. A era da informação: economia, sociedade e cultura. Volume I: A sociedade em rede. 3ª Ed. São Paulo: Paz e Terra, 1999, pp.617.

HERSCOVICI, Alain. Economia do conhecimento, trabalho "imaterial" e capital intangível: uma contribuição teórica. Revista Redes.com n.4, 2007, p.207-223.

ICP-BRASIL. Disponível em: http://icp-brasil.certisign.com.br/ Acessado em: 26 jun. 2011.

LEITÃO, Dorodame Moura. A informação como insumo estratégico. Ciência da Informação. Brasília, v. 22, n.2, maio/ago. 1993, p.118-123.

LÉVY, Pierre. Cibercultura. Trad. Carlos Irineu da Costa. 1ªEd. São Paulo: Editora 34, 1999, pp.264.

LI, Xingan. *Cybersecurity as a Relative Concept*. Information and Security - An International Journal, Sofia, v.18, p.11-24, 2006.

LORENS, Evandro Mário. Aspectos normativos da segurança da informação: um modelo de cadeia de regulamentação. 2007. 128pp. Dissertação (Mestrado). Programa de Pós-graduação em Ciência da Informação, Faculdade de Economia, Administração, Contabilidade e Ciência da Informação e Documentação, Universidade de Brasília, Brasília, 2007.

MACIEL, Maria Lucia; ALBAGLI, Sarita (orgs.). Informação, conhecimento e poder: mudança tecnológica e inovação social. Rio de Janeiro: Garamond, 2011, pp.332.

MANDARINO, Raphael; CANONGIA, Claudia. Segurança cibernética: o desafio da nova Sociedade da Informação. Brasília: Parceria Estratégica. v.14, n.29 , jul-dez.2009, p. 21-46.

MARCIANO, João Luiz; LIMA-MARQUES, Mamede. O enfoque social da segurança da informação. Brasília: Ciência da Informação, v.35, n.3, set./dez. 2006, p. 89-98.

MARCIANO, João Luiz. Segurança da Informação - uma abordagem social. 2006. 212pp. Tese (Doutorado em Ciência da Informação) - Faculdade de Economia, Administração, Contabilidade e Ciência da Informação e Documentação, Universidade de Brasília, Brasília, 2006.

MEDEIROS, Paulo Henrique Ramos. Governo Eletrônico no Brasil: Aspectos Institucionais e Reflexos na Governança, 2004, p.30.

MESSARI, Nizar. Existe um novo cenário de segurança internacional? In: GOMEZ, José Maria (comp.). *América Latina y el (des)orden global neoliberal.* Rio de Janeiro: Clacso, 2004, p.131-149.

PRESIDÊNCIA DA REPÚBLICA. Presidência da República, Casa Civil, Subchefia para Assuntos Jurídicos: Decreto nº 3.505, de 13 de junho de 2000. Brasília, 2000.

PRESIDÊNCIA DA REPÚBLICA. Gabinete de Segurança Institucional Secretaria Executiva Departamento de Segurança da Informação e Comunicações. Livro Verde da Segurança Cibernética no Brasil. Brasília, DF., 2010, 63pp.

RANGEL, Leandro; ÁVILA, Rafael. A Guerra e o Direito Internacional. Coleção Para Entender. Belo Horizonte: Del Rey, 2009, pp.176.

SIRIHAL, Adriana Bogliolo; LOURENÇO, Cíntia de Azevedo. Informação e conhecimento: aspectos filosóficos e informacionais. Informação & Sociedade: estudos, João Pessoa, v.12, n.1, p.67-92, 2002.

SOUZA, Gills Lopes Macedo; PEREIRA, Dalliana Vilar. A Convenção de Budapeste e as leis brasileiras. In: Seminário Cibercrime e Cooperação Penal Internacional, n.1, 2009, João Pessoa.

TAVARES, Juliana Paiva. Caracterização das Soluções Tecnológicas do *E-Banking* em Portugal. 2008. 167pp. Dissertação (Mestrado). Programa de Pós-graduação em Informática, Departamento de Engenharias, Universidade de Trás-os-Montes e Alto Douro, Vila Real, 2008.

UIT. *The Global Cybersecurity Agenda*, 2010

WEBER, Max. *Economia y sociedad: esbozo de sociologia comprensiva*. Trad. José Medina Echavarria *et al.* 2ªEd. México: Fondo de Cultura Económica, 1984. pp.1237.

WERTHEIN, Jorge. A Sociedade da Informação e seus desafios. Ciência da Informação, Brasília, v.29, n.2, p.71-77, mai/ago. 2000.

XAVIER, Rodolfo Coutinho Moreira; COSTA, Rubenildo Oliveira da. Relações mútuas entre informação e conhecimento: o mesmo conceito?. Ciência da Informação, Brasília, DF, v. 39 n.2, p.75-83, maio/ago., 2010.

ZOLNERKEVIC, Igor. A rede em pé de guerra. Unespciência. São Paulo: UNESP, p.26-28, fev.2011.