UNIVERSIDADE DE BRASÍLIA
Instituto de Ciência Política

DIEGO CAVALCANTE SOUZA DE ATHAYDE

POLÍTICAS PÚBLICAS PARA SEGURANÇA E DEFESA NACIONAL: GARANTIA E EXPLORAÇÃO DO ESPAÇO CIBERNÉTICO BRASILEIRO

Brasília
2016

UNIVERSIDADE DE BRASÍLIA
Instituto de Ciência Política

DIEGO CAVALCANTE SOUZA DE ATHAYDE

Monografia apresentada ao Instituto de Ciência Política da Universidade de Brasília, como requisito parcial para obtenção do Título de Bacharel em Ciência Política.

Orientador: Prof. Dr. Carlos Marcos Batista

Brasília
2016

DIEGO CAVALCANTE SOUZA DE ATHAYDE

POLÍTICAS PÚBLICAS PARA SEGURANÇA E DEFESA NACIONAL: GARANTIA E EXPLORAÇÃO DO ESPAÇO CIBERNÉTICO BRASILEIRO

Monografia apresentada ao Instituto de Ciência Política da Universidade de Brasília, como requisito para obtenção do Título de Bacharel em Ciência Política.

Orientador: Prof. Dr. Carlos Marcos Batista.

Monografia aprovada em 08 de julho de 2016.

Prof. Dr. Carlos Marcos Batista (IPOL-UnB)

Prof. Dr. Terrie Ralph Groth (IPOL-UnB)

Brasília

2016

AGRADECIMENTOS

Diante de todo incentivo e ajuda que recebi para que chegasse a esse trabalho, estou certo que uma página de agradecimento seja pouco diante de tanto que me foi dado.

Em primeiro lugar agradeço a Deus pelo dom da vida e pela graça concedida, pela misericórdia que me contempla em momentos de alegria e adversidade.

Agradeço a minha esposa Talitha pelo amor, dedicação, paciência e suporte em todas as circunstâncias. Ao meu amado filho Guilherme, por toda a alegria que reflete diariamente sobre mim.

Aos meus pais Leimá e Lieti pelo amor, esforço depreendido, ensinamentos e dedicação ao longo da minha vida. Às minhas irmãs Inês e Raquel, por toda a força e incentivo que sempre me deram.

Aos meus cunhados Salem e Régia Karoline, por toda a amizade, suporte e disposição que sempre demonstraram.

Aos queridos tios Antônio Carlos, Junia, Maria Edileusa, Cássia, Haroldo, e Débora, meu sincero obrigado por toda a ajuda e incentivo irrestritos em todos os momentos, sempre dispostos a ajudar com o que fosse necessário.

Ao professor Carlos Batista, não só pela orientação deste trabalho, mas também pelas “puxadas de orelha”, pelo profissionalismo e compreensão quando levávamos o nosso pequeno Guilherme para as aulas de Democracia Digital, meu muitíssimo obrigado.

Ao meu chefe e ex-chefe, nessa ordem, Capitão Bohrer e Tenente Leonardo, pela compreensão e ajuda sempre oportunas no tocante à flexibilidade de horário, o que me permitiu arcar com aulas na UnB. Os senhores tem minha gratidão.

A todos que, mesmo minimamente, torceram pela conclusão deste curso.

O analfabeto do século XXI não será aquele que não consegue ler e escrever, mas aquele que não consegue aprender, desaprender, e reaprender.

Alvin Toffler

RESUMO

A revolução tecnológica possibilitou inúmeros avanços à sociedade moderna, fazendo emergir a chamada “Sociedade da Informação”, a qual se vê prostrada diante da rápida difusão de conhecimento e informações fomentadas pelas TICs. Diante disso, governos e cidadãos passaram a ficar expostos aos perigos e ameaças que circundam o “espaço cibernético”, local onde as interações do mundo interconectado ocorrem. A história recente sinaliza que o ciberespaço pode se tornar um ambiente hostil à segurança de países e cidadãos. Guerras e ataques cujas consequências são sem escalas podem ser iniciados a partir do ambiente virtual, seja fruto de ações de atores isolados ou de grupos governamentais. O fato é que esse cenário traz à tona a necessidade de governos proverem a segurança e defesa de seus espaços cibernéticos, que adquirem as características de verdadeiros Estados-Nações, tendo os ciberviventes como povo, o ciberespaço como território, e a soberania, que reside na capacidade de garantir e explorar esse ambiente virtual. Diante dessas questões, este trabalho monográfico busca analisar as ações do Estado/Governo brasileiro, traduzidas em políticas públicas, com vistas à segurança e defesa do seu espaço cibernético. Para tanto, buscar-se-á identificar os principais atores envolvidos nesses processos, bem como os resultados que permitem identificar medidas efetivas para a proteção do espaço cibernético brasileiro.

Palavras-chave: políticas públicas, sociedade da informação, estratégia, defesa cibernética, segurança cibernética.

ABSTRACT

The technological revolution has enabled numerous advances to modern society, triggering the so-called "information society", which can be seen in front of the rapid spread of prostrate knowledge and information driven by ICTs. Given this, Governments and citizens began to be exposed to the dangers and threats that surround the "cyberspace", where the world's interconnected interactions occur. Recent history signals that cyberspace can become an environment hostile to the security of countries and citizens. Wars and attacks whose consequences are without stopovers can be started from the cyberspace, whether the result of actions of isolated actors or Government groups. The fact is that this scenario brings up the need for Governments to provide the security and defence of its cyber spaces, who acquire the characteristics of true nation-States, having the cyberlivings as people, cyberspace as territory and sovereignty, which resides in the ability to guarantee and explore this virtual environment. Given these issues, this monographic work seeks to analyze the actions of the State/Government, translated into public policies, with a view to the security and defense of his cyberspace. To this end, shall seek to identify the main actors involved in these processes, as well as the results identifying effective measures for the protection of cyberspace.

Keywords: public policy, information society, strategies, cyber defense, cybersecurity.

LISTA DE FIGURAS

LISTA DE TABELAS

ABREVIATURAS E SIGLAS

APF	ADMINISTRAÇÃO PÚBLICA FEDERAL
CDCIBER	CENTRO DE DEFESA CIBERNÉTICA
CDN	CONSELHO DE DEFESA NACIONAL
CF	CONSTIRUIÇÃO FEDERAL
CIC	CIÊNCIAS DA INFORMAÇÃO E COMUNICAÇÃO
COMDCIBER	COMANDO DE DEFESA CIBERNÉTICA
CT&I	CIÊNCIA, TECNOLOGIA E INOVAÇÃO
CTEEP	COMPANHIA DE TRANSMISSÃO DE ENERGIA ELÉTRICA PAULISTA
CTIR GOV	CENTRO DE TRATAMENTO E RESPOSTA A INCIDENTES
DDOS	DISTRIBUTED DENIAL OF SERVICE
DEF CIBER	DEFESA CIBERNÉTICA
DHS	DEPARTMENT OF HOMLELAND SECURITY
DOS	DENIAL OF SERVICE
DOU	DIÁRIO OFICIAL DA UNIÃO
DOUT MIL D CIBER	DOUTRINA MILITAR DE DEFESA CIBERNÉTICA
DSIC	DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO
EB	EXÉRCITO BRASILEIRO
E-GOV	ELETRONIC GOVERNMMENT
ENADCIBER	ESCOLA NACIONAL DE DEFESA CIBERNÉTICA
END	ESTRATÉGIA NACIONAL DE DEFESA
ESD	ESTRATÉGIA SETORIAL DE DEFESA
SEG CIBER APF	ESTRATÉGIA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO E SEGURANÇA CIBERNÉTICA DA ADMINISTRAÇÃO PÚBLICA FEDERAL
FFAA	FORÇAS ARMADAS
GAB CMT EX	GABINETE DO COMANDANTE DO EXÉRCITO
GSI-PR	GABINETE DE SEGURANÇA INSTIRUCIONAL DA PRESIDÊNCIA DA REPÚBLICA

GT SEG CIBER	GRUPO DE TRABALHO PARA SEGURANÇA CIBERNÉTICA
IC	INFRAESTRUTURA CRÍTICA
ICI	INFRAESTRUTURA CRÍTICA DA INFORMAÇÃO
ITU	INTERNATIONAL TELECOMMUNICATION UNION
LOA	LEI DE ORÇAMENTOS ANUAIS
MD	MINISTÉRIO DA DEFESA
NSA	NATIONAL SECURITY AGENCY
OCED	ORGANIZATION FOR ECONOMIC CO-OPERATION DEVELOPMENT
PCD	POLÍTICA CIBERNÉTICA DE DEFESA
PND	POLÍTICA NACIONAL DE DEFESA
PORT	PORTARIA
PR	PRESIDÊNCIA DA REPÚBLICA
PSD	POLÍTICA SETORIAL DE DEFESA
SCADA	SUPERVISORY CONTROL AND DATA ACQUISITION
SEG CIBER	SEGURANÇA CIBERNÉTICA
SEG ICI	SEGURANÇA DAS INFRAESTRUTURAS CRÍTICAS DA INFORMAÇÃO
SIC	SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO
SICI	SEGURANÇA DAS INFRAESTRUTURAS CRÍTICAS DA INFORMAÇÃO
SIMOC	SIMULADOR DE OPERAÇÕES DE GUERRA CIBERNÉTICA
SIN	SISTEMA INTERLIGADO DE ENERGIA
SMDC	SISTEMA MILITAR DE DEFESA CIBERNÉTICA
TICS	TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO
USAF	UNITED STATES AIR FORCE
VANT	VEÍCULO AÉRIO NÃO TRIPULADO

SUMÁRIO

1 INTRODUÇÃO

O mundo interconectado é repleto de possibilidades e armadilhas. A era da informação emerge como um baluarte do conhecimento, da troca e da interação, concedendo benesses jamais conhecidas pela humanidade. Nos dias atuais, cada cidadão pode expandir da condição de receptor para a de transmissor de informações, isto graças ao advento tecnológico que criou o ambiente onde pessoas, governos, grupos e movimentos diversos podem interagir simultaneamente. A esse ambiente entende-se o ciberespaço, ambiente virtual onde o mundo globalizado se organiza e funciona.

Este trabalho tem por finalidade trazer à tona o debate sobre segurança e defesa nacional sob a ótica da revolução tecnológica que permitiu o advento da sociedade da informação. Para tanto, está dividido em cinco partes, sendo a primeira uma ambientação ao tema proposto. Nessa seção são elucidados temas afeitos aos estudos de segurança e defesa cibernética, os quais são imprescindíveis para a compreensão da proposta em tela, como a ideia de sociedade da informação, infraestruturas críticas, as conceituações de segurança e defesa cibernética pela perspectiva de países e organismos internacionais, bem como uma análise das possibilidades de uso do ambiente virtual para a desestabilização do mundo real.

A segunda parte trata dos elementos de pesquisa que integram o trabalho, apresentando sua justificativa, objetivos e metodologia. Na terceira parte é abordado o referencial teórico que traça intersecções entre as disciplinas da ciência da informação e comunicação com as áreas temáticas da ciência política. Para tanto, são utilizadas as teorias de políticas públicas pioneiras, formulada por estudiosos clássicos do século XX como Harold Laswell, Herbert Simon, Charles Edward Lindblom e David Easton, os quais continuam sendo o norte teórico de pesquisadores contemporâneos.

Subsequentemente ao marco teórico do trabalho, a quarta parte se debruça sobre a agenda política adotada pelo Brasil para pensar, formular e implementar medidas para a proteção do seu ciberespaço. Para isso são levadas em consideração duas dimensões distintas, mas complementares, a saber, a

segurança e a defesa cibernética. Para elucidar as medidas para a segurança cibernética são abordadas as realizações da Casa Militar da Presidência da República, na figura do GSI-PR. Quanto à defesa cibernética, os atores identificados como protagonistas são o Ministério da Defesa e o Exército Brasileiro. Ao longo dessas duas subseções são tratadas as suas providências para o alcance das políticas e estratégias traçadas para manter o espaço cibernético brasileiro sob segurança.

Por fim serão apresentadas algumas considerações acerca do processo que se criou com vistas à garantia e exploração do ciberespaço brasileiro.

2 AMBIENTAÇÃO AO TEMA

2.1 A Sociedade da informação

O processo de globalização das sociedades diminuiu distâncias e fronteiras, estreitando laços entre as pessoas, organizações, nações e Estados. Um fator de suma importância nesse contexto é a extensão do acesso à informação que se desencadeou paralelamente à evolução tecnológica, principalmente na área de comunicação e informação. Situações do cotidiano que se apresentam vitais aos cidadãos estão completamente ancoradas no acesso e na difusão de informações em alta velocidade, como transações bancárias, as inovações da comunicação social - como *blogs*, tabloides em rede, mídias de promoção e marketing virtual -, sistemas de mensagens instantâneas e páginas pessoais de interação. Assumindo grau de importância macro social, estão os sistemas utilizados por países para o funcionamento de suas bases organizacionais e de serviços básicos da população, como as redes de transmissão e controle de abastecimento elétrico, de fornecimento de água, e as redes lógicas de gestão dos setores financeiros públicos e privados, redes de gestão de transportes, de radiodifusão, bases de dados para controle de renda e tributação contribuintes, entre outros. Levando em conta a dependência que se criou desses sistemas informatizados, é de fácil aceitação quando se afirma que o advento das tecnologias de informação e comunicação fez emergir a chamada “Sociedade da Informação”.

O termo surge por ocasião da reconstrução do pós-guerra, ganhando propulsão com a acelerada industrialização que se desencadeou. Uma característica crucial desse processo foi o estreitamento da relação entre o homem e a tecnologia que surgia em seu ambiente geopolítico (OLIVEIRA; BAZI, 2007, p.7). Segundo DANTAS (1998):

> “a Sociedade da Informação caracteriza uma etapa alcançada pelo desenvolvimento capitalista contemporâneo, no qual as atividades humanas determinantes para a vida econômica e social organizam-se em torno da produção, processamento e disseminação da informação através das tecnologias eletrônicas.”

A dependência do acesso irrestrito à informação pode ser vinculada à teoria apresentada por Alvin e Heidi Toffler[1] (1980), que idealizaram o surgimento de um novo modelo de civilização devido ao terceiro grande movimento de alteração dos modos de vida da humanidade. Para os autores, o primeiro movimento que alterou o modo de vida do homem se deu quando a civilização passou a dominar os meios e técnicas agrícolas. O segundo movimento começou quando a atividade agrícola deixou de ser o meio de produção predominante, passando a civilização ao estágio industrial, dominando técnicas e maquinário a vapor. O terceiro movimento é o tecnológico, aqui, ratificado pelo advento da internet dentro do escopo da revolução do uso e difusão das tecnologias da informação (TOFFLER, 1980).

A internet ajudou a difundir o uso e aprimoramento das tecnologias de informação e comunicação (TICs), que abrangem usuários de diferentes características e motivações, desde os que as querem para o fomento da democracia, da governança tecnológica, e da participação cidadã no ambiente eletrônico, até aqueles que se utilizam dos ambientes virtuais motivados por ideologias hostis à segurança de cidadãos e governos.

Alguns fenômenos podem ser destacados como parte integrante da Sociedade da Informação, que envolvem áreas e atores em constante interação, a saber:

a) Elevada convergência tecnológica;

b) Aumento significativo de sistemas e redes de informação, bem como da interconexão e interdependência dos mesmos;

c) Aumento crescente e bastante substantivo de acesso à Internet e das redes sociais;

d) Avanços das tecnologias de informação e comunicação (TICs);

e) Aumento das ameaças e das vulnerabilidades de segurança cibernética; e

f) Ambientes complexos, com múltiplos atores, diversidade de interesses, e em constantes e rápidas mudanças (Livro Verde, pp. 14).

---

[1] TOFFLER, Alvin; TOFFLER, Heidi. Guerra e Anti-Guerra. Livros do Brasil, Lisboa, 1994.

Por ambiente complexo, termo abordado no último dos itens acima, podemos compreender o espaço cibernético, o qual pode ser identificado como sendo "composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam e são processadas ou armazenadas (BRASIL-MD, 2010, p. 9)[2]".

Pierre Levy (2010) analisa o espaço cibernético sob uma ótica de mutações culturais, como um lugar de construção da inteligência coletiva e ampla difusão da informação e do conhecimento, conforme declara no I Seminário de Defesa Cibernética do Ministério da Defesa:

> "O que seria o espaço cibernético? O espaço cibernético é um terreno onde está funcionando a humanidade, hoje. (...) é a instauração de uma rede de todas as memórias informatizadas e de todos os computadores. Atualmente, temos cada vez mais conservados, sob forma numérica e registrados na memória do computador, textos, imagens e músicas produzidos por computador. Então, a esfera da comunicação e da informação está se transformando numa esfera informatizada. (...) Com o espaço cibernético temos uma ferramenta de comunicação muito diferente da mídia clássica, porque é nesse espaço que todas as mensagens se tornam interativas, ganham uma plasticidade e têm uma possibilidade de metamorfose imediata. E aí, a partir do momento que se tem o acesso a isso, cada pessoa pode se tornar uma emissora, o que obviamente não é o caso de uma mídia como a imprensa ou a televisão. (...) Do interior do espaço cibernético encontramos uma variedade de ferramentas, de dispositivos, de tecnologias intelectuais. Por exemplo, um aspecto que se desenvolve cada vez mais, nesse momento, é a inteligência artificial. Há também os hipertextos, os multimídia interativos, simulações, mundos virtuais, dispositivos de tele-presença. (...) O importante é que a informação esteja sob a forma de rede e não tanto a mensagem, porque esta já existia numa enciclopédia ou dicionário" [3].

Esse ambiente virtual contém, também, as características mencionadas por Manuel Castells (2010) no volume I da série "A Era da Informação: Economia, Sociedade e Cultura", quando afirma que:

> "o registro histórico das revoluções tecnológicas (...) mostra que todas são caracterizadas por sua penetrabilidade, ou seja, por sua penetração em

---

[2] BRASIL. Ministério da Defesa. Exército Brasileiro. Estado-Maior do Exército. Minuta de Nota de Coordenação Doutrinária relativa ao I Seminário de Defesa Cibernética do Ministério da Defesa. Brasília, 2010. p.9. Disponível em: http://www.sescsp.org.br/sesc/conferencias/subindex.cfm?Referencia=168&ID=35&ParamEnd=9

[3] http://www.sescsp.org.br/sesc/conferencias/subindex.cfm?Referencia=168&ID=35&ParamEnd=9

> todos os domínios da atividade humana, não como fonte exógena de impacto, mas como o tecido em que essa atividade é exercida" (CASTELLS, 2010).

Justamente a penetrabilidade exercida nas rotinas corporativas e pessoais que fazem do espaço cibernético ambiente merecedor de maior atenção no que tange às garantias e segurança, pois não possui suas fronteiras claramente definidas, possibilitando disputas assimétricas entre cidadãos, corporações e Estados dentro do mesmo teatro de operações.

Raphael Mandarinno Júnior (2010) menciona três características que se tornam latentes na medida em que a sociedade da informação se estabelece em um determinado país, as quais são elementos importantes na formação de um Estado, e atribuem ao espaço cibernético as mesmas características de um Estado-nação do mundo real, a saber, povo + território + soberania. O povo nada mais é do que os usuários das ferramentas da sociedade da informação, ou seja, os internautas ou ciberviventes. O território do ciberespaço pode ser definido pelo próprio espaço cibernético que se criou, ou seja, o ambiente virtual onde os povos convergem e interagem dinamicamente. Por fim, a soberania desse "lugar" é retratada pela capacidade de atuar, modificar e decidir dentro do ambiente cibernético (MANDARINNO, 2010, p.22).

2.2 Infraestruturas Críticas e Infraestruturas Críticas da Informação

No seio da Sociedade da Informação, além dos próprios usuários, outras instâncias dependentes das redes lógicas de transmissão e armazenamento de informações merecem ter seus sistemas de segurança fortalecidos. São as chamadas "Infraestruturas Críticas - IC". A Portaria n° 45 do Gabinete de Segurança Institucional da Presidência da República Federativa do Brasil define como IC as "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" (Port Nr 45 GSI-PR, 2009).

No Estado brasileiro, algumas das IC existentes se traduzem nos setores de energia, abastecimento, defesa, transporte, telecomunicações, finanças, receita

federal, setor industrial, agências de informação, entre outras. Com o passar do tempo, na estrutura desses setores passou a existir uma dependência horizontal, onde o espaço e redes cibernéticas unem essas infraestruturas (BAGHERY, 2007; GUIA SICI, 2010). Dentro dessas instâncias que permitem o funcionamento do Estado e setores privados, surgem as "Infraestruturas Críticas da Informação – ICI", aqui compreendidas pela definição aceita pelo Conselho de Defesa Nacional brasileiro em 2009, que definiu ser o "subconjunto de ativos de informação que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade" (BRASIL-CDN, 2009, não paginado). Para compreender a definição em sua plenitude, o mesmo Conselho define por ativo de informação todos os "meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso".

O entendimento brasileiro de IC e ICI é ratificado no âmbito internacional quando observado o trabalho publicado no Centro de Estudos para a Segurança de Zurich (2008/2009), que compreende as ICI como:

> "(…) part of the global or national information infrastructure that is essentially necessary for the continuity of a country's crictical infrastructure services. The Critical Information Infrastructure, to a large degree, consists of, but is not fully congruent with, the information and telecommunications sector, and includes components such as telecommunications, computers / softwares, the internet, satellites, fiber-optics, etc. The term is also used for the totality of interconnected computers and networks and their critical information flows. (MANDARINNO, 2010, p.39)"

No ano de 2008, a OCED[4] (Organization for Economic Co-operation Development) emitiu uma série de recomendações a seus membros, inclusive o Brasil, salientando a importância de se prover a segurança de suas infraestruturas

[4] ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD) - Guidelines for the Security of Information Systems and Networks: Towards a culture of security. (Adopted as a Recommendation of the OECD Council at its 1037th Session on 25 July 2002). Paris: OECD. 2002. 28p. e, ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD) COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATION POLICY (ICCP Committee) – OECD Recommendation of the Council on the Protection of Critical Information Infrastructure. (Adopted as a Recommendation of the OECD Council at its 1172th Session on 30 April 2008). Seoul/Korea. June. 2008.

críticas de informação, medidas estas que, no entendimento da OCED, representam indicativos essenciais à segurança do espaço cibernético (OCED, 2008). As recomendações são as seguintes:

i. Definir a política e as normas específicas (Seg Ciber e Seg ICI), com objetivos claros, no âmbito do mais alto nível de governo;
ii. Atuar como o órgão central de governo com competência (responsabilidade e autoridade) para prover as melhores condições de implantação da política de segurança cibernética e seus objetivos;
iii. Promover tanto a cultura de, quanto a educação em, segurança cibernética;
iv. Promover mútua cooperação entre os stakeholders – setor privado, agência(s), terceiro setor, governo – visando à efetiva implantação da política nacional de segurança cibernética;
v. Atuar com transparência assegurando delegação de competência, ou seja, governança estabelecida, facilitando e fortalecendo a cooperação, em especial entre governo e setor privado;
vi. Rever sistematicamente a política, normas e respectivo(s) marco(s) legal(is), com especial atenção às ameaças e vulnerabilidades das infraestruturas críticas da informação de cada país, buscando minimizar riscos e desenvolver novos instrumentos e/ou mecanismos de segurança da informação e comunicações;
vii. Desenvolver e exercer macro-coordenação da política e estratégia nacional de segurança cibernética, envolvendo cúpula de governo e setor privado;
viii. Promover e exercer a macro-coordenação do monitoramento e da avaliação de risco, baseados na análise das vulnerabilidades e ameaças das infraestruturas críticas da informação, visando proteger a economia e a sociedade contra altos impactos;
ix. Promover e exercer a macro-coordenação do processo nacional de gestão de risco, orientando desde aspectos da organização, ferramenta(s), até mecanismos de monitoramento, para a implementação de uma estratégia nacional de gestão de risco que compreenda:
x. Estrutura organizacional apropriada que promova melhores práticas de segurança, e que incluam prevenção, proteção, resposta e recuperação de ameaças naturais e maliciosas; e,
xi. Sistema de medidas que permita avaliar continuamente o processo, o que inclui itens de controle, níveis de maturidade, exercícios e testes apropriados;
xii. Promover e exercer a macro-coordenação da capacidade de resposta à incidentes em redes computacionais, como as das equipes que atuam em CERTs/CSIRTs, incluindo mecanismos de forte cooperação e comunicação entre tais equipes;
xiii. Estreitar as relações com o setor privado:
xiv. Estabelecendo parcerias público-privadas e acordos de cooperação, com foco na gestão de risco, tratamento de incidentes e recuperação de sistemas e redes de informação e comunicações, e na gestão da continuidade de negócios;

xv. Estimulando o intercâmbio regular de informação, por meio do estabelecimento de acordos com cláusulas específicas para o caso de conhecimentos sensíveis ou informações classificadas;
xvi. Estimular e apoiar a aceleração da inovação da segurança cibernética por meio da pesquisa e do desenvolvimento;
xvii. Promover a cooperação bilateral e multilateralmente, em nível regional e global, visando trocas de experiências e fortalecimento das estratégias de segurança cibernética. (Fonte: OCED, 2008).

Diante das recomendações da OCED, o Brasil adotou diversas iniciativas no sentido de alcançá-las paralelamente às medidas pensadas pelo governo, as quais serão tratadas em momento oportuno neste trabalho.

2.3 Segurança e defesa cibernética: definições

Visando compreender em que consiste a Segurança Cibernética, este trabalho tratará três perspectivas conceituais para elucidar o tema, que configuram os conceitos defendidos pelos seguintes atores internacionais: União Europeia – EU; *Department of Homeland Security* (DHS) do Governo dos Estados Unidos da América; e Governo da República Federativa do Brasil.

A visão da *International Telecommunication Union* - ITU[5], organização que engloba governos europeus e setores privados no que tange à telecomunicação global, representa bem o conceito de segurança cibernética aceito pela União Europeia, quando entende que:

> "Segurança cibernética é basicamente sobre como fornecer proteção contra acesso não autorizado, manipulação e destruição de recursos críticos e ativos. Esses recursos e ativos, assim como as questões relacionadas, variam e dependem do nível de desenvolvimento dos países. Eles também dependem do que consideram ser um recurso crítico, os esforços estão dispostos e aptos a fazer e a sua avaliação dos riscos que estão dispostos a aceitar como resultado de medidas de segurança cibernética inadequado (ITU, 2007)".[6]

[5] http://www.itu.int, acessado em 25 de abril de 2016.
[6] ITU Global Cybersecurity Agenda (GCA): Framework for International Cooperation in Cybersecurity. ITU, 2007. p. 10. apud Canongia, Claudia, março 2009.

O *Department of Homeland Security* – DHS do Governo dos Estados Unidos da América compreende que:

> "Segurança cibernética inclui a prevenção de danos para uso não autorizado de ativos de informação ou exploração dos sistemas electrónicos de informação e comunicação, bem como as informações neles contidas, para garantir a confidencialidade, integridade e disponibilidade. Segurança cibernética também inclui restauração de sistemas eletrônicos de informação e comunicação no caso de um desastre natural ou ataque terrorista"[7] (ITU, 2007)".

O Estado Brasileiro adotou a definição desenvolvida pelo ex-Diretor de Segurança da Informação e Comunicação do Gabinete de Segurança Institucional da Presidência da República (DSIC-GSI/PR), Raphael Mandarinno Júnior, que esboçou em sua monografia de especialização em Gestão da Segurança da Informação Comunicação, realizado em 2009 junto ao Departamento de Ciência da Informação e Comunicação (CIC) da Universidade de Brasília, o seguinte conceito: “a arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas" (LIVRO VERDE, 2010, p. 19). O conceito ora formulado foi apresentado ao Grupo de Trabalho para Segurança Cibernética do Ministério da Defesa, sendo referendado e aceito, culminando na Portaria n° 045 do GT Seg Ciber, de 08 de setembro de 2009, cuja publicação no Diário Oficial da União n° 172 se deu em 09 de setembro de 2009.

As três definições convergem no tocante à garantia dos ativos, proteção contra acessos não autorizados, e à manutenção das Infraestruturas Críticas de países que possuam em seu interior as condicionantes que possam incluí-los na chamada Sociedade da Informação. O conceito difundido na Europa salienta, ainda, que o grau de segurança cibernética depende do estado do desenvolvimento tecnológico dos países, que implementarão medidas proporcionais ao seu arcabouço de desenvolvimento tecnológico. O conceito aceito pelos EUA visa à capacidade de restauração dos sistemas de informação em casos de desastres

---

[7] National Infrastructure Protection Plan: Partnering to enhance protection and resiliency, DHS, 2009. p.12. apud Canongia, Claudia, março2009.

naturais ou atentados terroristas, possibilidades sempre em riste no âmbito político daquele país. O conceito brasileiro contempla de maneira mais abrangente a capacidade de dar continuidade à sociedade da informação existente em um país.

Adentrando no que se compreende como Defesa Cibernética, é mister que primeiramente seja conhecido o conceito de "defesa". De acordo com o Glossário das Forças Armadas[8], defesa é definida como "o ato ou conjunto de atos realizados para obter, resguardar ou recompor a condição reconhecida como de segurança", ou ainda, a "reação contra qualquer ataque ou agressão real ou iminente" (MD35-G-01;2007).

A partir dessa interpretação, é compreensível que a defesa caminhe paralelamente à segurança, sendo esta sua razão de ser. A defesa mira o estado de segurança, dessa forma, o manifesto da defesa de um Estado, em qualquer área que seja, presume atos pensados em planejamento futuro, atos responsivos, e atos de recondicionamento.

Adotando definição elaborada pelo Comando Militar brasileiro, a Defesa Cibernética consiste no:

> "(...) uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de Comando e Controle do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC2) do oponente e defender os próprios STIC2. Abrange, essencialmente, as Ações Cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação à TIC." (Dout Mil Def Ciber, 2014, p. 18)

Evoluindo a partir do conceito convencional de defesa, neste momento é pensado o campo de batalha virtual, ou cibernético, onde as ações ofensivas e defensivas se desencadearão. Novamente é mencionada a necessidade de

[8] BRASIL. Ministério da Defesa. Glossário das Forças Armadas – MD35-G-01.

proteção a sistemas de informação, esses na qualidade de componentes de Infraestruturas Críticas. Fica evidente a necessidade de atividades de inteligência concomitantemente às ações de defesa cibernética, dado ser objeto da inteligência militar a lide com ativos de informação, sendo a própria ideia de "inteligência", quando aplicada ao âmbito militar, oriunda das seções e departamentos de informação e contrainformação, não importando o meio pelo qual ela é difundida.

2.4 O cyberspace como campo de batalha

Após elucidar os conceitos de sociedade da informação, espaço cibernético, Infraestruturas Críticas e Infraestruturas Críticas da Informação, assim como os conceitos de Segurança e Defesa Cibernética, convêm identificar casos reais de ameaças e ataques cibernéticos, no intuito de melhor compreender a necessidade de países pensarem estratégias para a segurança e defesa de seus *cyberspaces*. Para tanto, serão abordados exemplos tratados por Richard A. Clark e Rob Knake (2010) no livro *Guerra Cibernética: a próxima ameaça à segurança e o que fazer a respeito*[9]*.* A obra serviu de referencial teórico para a formulação da estratégia do governo dos Estados Unidos para o seu *cyberspace*, aliando-se a outros especialistas e militares que pensavam a temática enquanto política de Estado (CLARK; KNAKE, 2010)[10].

Em 06 de setembro de 2007, no lado leste do território sírio, havia um prédio até então livre de suspeitas. Porém, segundo pronunciamento do governo de Israel e imagens internas do local apresentadas pela *National Security Agency* - NSA, ali existia a construção de um reator nuclear financiado pelo governo norte-coreano. No dado dia, caças F-15 *Eagle* e F16 *Falcon* israelenses entraram no espaço aéreo sírio e iniciaram um ataque à edificação onde o reator era construído, bombardeando o local, causando a destruição de anos de trabalho secreto. O presidente sírio, Bashar al-Assad, em pronunciamento, declarou que o local se tratava de um prédio vazio, sem nenhuma importância estratégica ou militar para o

[9] CLARK, Richard A; KNAKE, Rob. Cyber War: the next threat to national security and what to do about it. Harper Collins, 2010.
[10] O livro utilizado foi adquirido via plataforma Kindle, logo, quando a referência trata informa a página, na verdade refere-se à posição onde a ideia se encontra no e-book.

país. A Coréia do Norte, curiosa e oportunamente, se disse indignada com a invasão do espaço aéreo sírio (CLARK; KNAKE, 2010, p.261-272).

Sobre o fatídico dia, algo pairava sem explicação: de que maneira caças israelenses entraram no espaço aéreo sírio e proferiram ataques a alvos e, em seguida, retraíram sem serem percebidos pelos modernos sistemas de defesa antiaéreos sírios? Anos antes o governo da Síria havia investido milhões de dólares na negociação com Moscou para obtenção do moderno sistema de defesa antiaérea russo, e cobraram explicações de seus fornecedores. O governo russo prometeu enviar especialistas à Damasco para somar esforços e concluírem qual o motivo da não observação do ataque aéreo. Após análises a amarga constatação foi que Israel havia dominado as redes de dados e os sistemas de defesa antiaérea da Síria, implantando em seus radares imagens de um dia qualquer, sem atividade no espaço aéreo, ocultando, dessa forma, o ataque que se desencadeava (CLARK; KNAKE; 2010, p.314).

Para explicar os ataques proferidos por Israel, três hipóteses consideradas plausíveis foram levantadas pelos especialistas. A primeira sugere que o governo israelense tenha utilizado um Veículo Aéreo Não Tripulado (VANT) para dissimular os dados que permitem os radares antiaéreos captar intrusos no espaço aéreo. Esses radares lançam feixes de ondas de rádio que alcançam os objetos em movimento, que por sua vez, refletem as ondas de volta para os sensores em terra, possibilitando precisarem a localização, altitude, velocidade e tamanho da aeronave em movimento. Ao lançar um VANT no espaço aéreo sírio, Israel refletiria os dados de retorno para outra direção, o que faria o sistema de defesa deixar de receber dados de movimentação aérea. A segunda hipótese é que agentes israelenses tenham implantado *backdoors*[11] ou *trojan horses*[12] em determinadas linhas de

[11] "Backdoors" são programas que instalam um ambiente de serviço em um computador, tornando-o acessível à distância, permitindo o controle remoto da máquina sem que o usuário saiba. Assim, o computador poderá ser totalmente controlado de longe - por outra pessoa, em outra máquina - possibilitando ao invasor qualquer atitude: ver arquivos, ler emails, ver todas as senhas, apagar arquivos, dar boot na máquina, conectar via rede a outros computadores aos quais tenha acesso, executar programas em seu computador, tais como jogos, logar todas as teclas digitadas da máquina para um arquivo (comprometendo acessos a sites seguros - cartão de crédito, homebanking etc) e formatar seu disco.

[12] O “Cavalo de Tróia” (ou "Trojan Horse") embute um código que possibilita que um estranho acesse o computador infectado e envie dados dele para outras máquinas, sem que o proprietário saiba.

código do software que comanda o sistema de defesa aérea sírio. Esses artefatos, quando inseridos nas linhas de código, fariam o sistema de defesa responder negativamente a determinados estímulos quando entrassem em contato com VANTs ou aeronaves específicas, no caso as israelenses. Mesmo entre os especialistas em programação é reconhecida a dificuldade de se identificar linhas de código maliciosas em softwares complexos como os que compõem os sistemas de defesa aérea. Uma terceira opção, menos provável, porém longe de ser descartada, é que tenha havido uma interceptação de alguma fibra óptica que veicula os dados que alimentam a rede antiaérea síria. Embora seja improvável que agentes circulem pelo território sírio em busca de fibras ópticas para "emendar", é de conhecimento dos dois países que a prática da espionagem ativa acontece tanto na Síria quanto em Israel (CLARK; KNAKE, 2010, p.314-366).

O ataque israelense, segundo Richard Clark, provavelmente foi inspirado em feito americano datado de 1990, por ocasião da primeira guerra contra o Iraque. Na ocasião os primeiros guerreiros cibernéticos se uniram aos comandos das forças especiais, cuja missão consistia em assumir o controle de uma base de radares ao sul do Iraque. Para tanto, foram levados a campo *hackers* da Força Aérea Americana (USAF), os quais, uma vez dentro da base de radares, teriam a tarefa de "rodar" um software capaz de travar todos os computadores iraquianos, tornando-os impossíveis de reiniciar (CLARK; KNAKE, 2010, p.377).

Treze anos mais tarde, em 2003, novamente antes do início de um conflito bélico, os americanos invadiram as redes de computadores iraquianas e emitiram de dentro do próprio Ministério da Defesa um e-mail com a seguinte mensagem aos oficiais das Forças Armadas do Iraque:

> "Esta é uma mensagem do Comando Central dos Estados Unidos. Como você sabe, nós podemos ser instruídos para invadir o Iraque num futuro próximo. Se o fizermos, nós iremos sobrepujar as forças que se opõem a nós, como fizemos anos atrás. Nós não queremos prejudicar você ou suas tropas. Nosso objetivo é destituir Saddam e seus dois filhos. Se você deseja permanecer ileso, coloque seus tanques e outros veículos blindados em formação e abandone-os. Afaste-se. Você e suas tropas devem ir para suas casas. Você e as outras forças iraquianas serão reconstituídas após o regime ser alterado em Bagdá." (CLARK; KNAKE, 2010, p.398)

Muitos dos oficiais iraquianos obedeceram às instruções americanas e posicionaram seus blindados e demais veículos ordenadamente na parte exterior de suas Unidades, o que facilitou a destruição feita por bombas lançadas por aviões americanos. Alguns comandantes deram licença a seus subordinados poucas horas antes da guerra começar.

Os dois exemplos, onde os Estados Unidos utilizam o espaço cibernético para obter vantagem antes da utilização de tropas, mostram duas formas de sobreposição ao "inimigo" por intermédio do espaço cibernético. A primeira, em 1990, tinha como objetivo obter comandamento sobre as defesas iraquianas, desativando-as, o que facilitaria um eventual ataque cinético[13]; na segunda, o espaço cibernético iraquiano foi condutor de ações psicológicas com o objetivo de desmoralizar o inimigo, dando-lhe a opção de facilitar sua própria derrota.

Diferentemente dos casos anteriores, onde ataques cibernéticos precederam ataques militares, Estados-Nações e grupos ativistas podem se utilizar do *hacking* para fins políticos e diplomáticos. Em 17 de maio de 2007 a cidade de Tallinn, que se tornou a capital da Estônia em 1991 após a dissolução da União Soviética, foi palco de ataques cibernéticos em larga escala.

Durante a Segunda Guerra Mundial a cidade foi "libertada" dos alemães pelos soldados soviéticos, que expulsaram as tropas nazistas que ali resistiam. Em uma área central da cidade foi construída uma estátua, um "Monumento aos Libertadores de Tallinn", que consistia na estátua de um soldado do exército vermelho, em memória aos *soviets* que tombaram no entrave com os nazistas. Em 2007 o parlamento estoniano aprovou a lei de Estruturas Proibidas[14], que indicava a derrubada imediata de qualquer objeto público que denotasse a ocupação russa, por entender que o período representou grande opressão política e desrespeitos aos grupos étnicos minoritários. A decisão do legislativo gerou revolta e conflito entre grupos étnicos, culminando, em 27 de abril de 2007, no ato que ficou conhecido como *Bronze Night*[15], quando as autoridades estonianas, no intuito de cessar o

[13] Ofensiva militar onde existe mobilização e movimento de tropas convencionais.
[14] http://www.baltictimes.com/news/articles/17342/. Acesso em 02 de maio de 2016.
[15] https://en.wikipedia.org/wiki/Bronze_Night. Acesso em 02 de maio de 2016.

conflito, removeram o monumento para um cemitério militar em local protegido. A remoção gerou indignação tanto nas mídias quanto no próprio Legislativo da Federação Russa. Foi então que os conflitos e retaliações saíram do mundo real e partiram para o espaço cibernético (CLARK; KNAKE, 2010, p.445).

A Estônia é um dos países mais conectados do mundo, possuindo uma estrutura de *e-government*[16] (governo eletrônico) sólida[17], o que consiste dizer que utiliza de forma sistemática as tecnologias de comunicação e informação em seus processos internos, tanto para os serviços do Estado quanto aos cidadãos, o que inclui a prestação de serviços públicos por meio eletrônico, como prestação de contas, requisições diversas, espaços abertos para discussões, serviços de ouvidoria, cadastro e serviços online[18]. Após a Noite de Bronze os servidores que hospedavam os sites mais utilizados na Estônia entraram em colapso e pararam devido aos milhares de pedidos de acesso simultâneos. Outros sites ficaram inacessíveis devido à sobrecarga de *pings*[19]*,* impedindo o acesso de cidadãos aos aplicativos bancários online e aos serviços eletrônicos do governo (CLARK; KNAKE, 2010, p.456).

O que ocorreu na Estônia é chamado de *Distributed Denial of Service* (DDoS), ou Ataque Distribuído de Negação de Serviço, que ocorre quando centenas de milhares de computadores enviam solicitações e *pings* a sítios na internet, excedendo os limites do servidor, o que inutiliza suas funcionalidades. Os computadores que promovem os ataques são chamados de *botnets,* uma coleção de programas conectados à internet que se comunica com outros programas

---

[16] O E-GOV pode ser entendido como uma das principais formas de modernização do estado e está fortemente apoiado no uso das novas tecnologias para a prestação de serviços públicos, mudando a maneira com que o governo interage com os cidadãos, empresas e outros governos. O conceito não se restringe a simples automação dos processos e disponibilização de serviços públicos através de serviços on-line na Internet [Abramson, 2001], mas sim na transformação da maneira com que o governo, através da TIC, atinge os seus objetivos para o cumprimento do papel do estado. Acesso em 02 de maio de 2016.

[17] Estonia: A Model for e-Government. Disponível em: http://cacm.acm.org/magazines/2015/6/187320-estonia/fulltext. Acesso em 02 de maio de 2016.

[18] http://www.governoeletronico.gov.br/o-gov.br/historico. Acesso em 02 de maio de 2016.

[19] Dicionário de TI: "**Ping**» Pequeno utilitários empregado para verificar se uma determinada ligação encontra-se ativa e qual o tempo que uma mensagem leva para ir de um ponto ao outro da ligação." Disponível em: http://www.bandtec.com.br/index.php/dicionario-de-ti/. Acesso em 02 de maio de 2016.

similares a fim de executar tarefas[20]. De forma simplificada, os *botnets* “consistem em uma rede robótica de computadores zumbis controlados remotamente” (CLARK; KNAKE, 2010, p.466). As ameaças que difundem os *botnets* pela internet escondem-se em *links* e no plano de fundo de botões em sites desprotegidos.

Os DDoS na Estônia foram os maiores já registrados. Eles se direcionaram aos servidores que davam base ao sistema telefônico, às operadoras de cartão de crédito, aos diretórios de gestão da internet, fazendo até mesmo o *Hansa Bank*[21] interromper suas atividades. Os ataques duraram semanas ininterruptas. Os especialistas afirmaram que os computadores de controle dos ataques estavam localizados na Rússia, que por sua vez, negou[22]. Mas o fato é que os ataques cibernéticos paralisaram a rotina de setores críticos da sociedade estoniana.

Outro caso a ser abordado de forma sumária, mas de suma importância para a compreensão de ataques cibernéticos a sistemas e infraestruturas críticas de países, trata do perigo oferecido por hackers a sistemas operacionais como os de transmissão de energia elétrica. Esses sistemas merecem atenção especial de governos e autoridades especializadas em segurança, dada sua importância estratégica para o funcionamento dos sistemas de informação e para o próprio dia-a-dia dos cidadãos.

No ano de 2005 o Brasil sofreu um “apagão”, ou seja, teve parte do fornecimento de energia elétrica interrompido. A imprensa noticiou que o ocorrido se deu por conta da falha de operação de um funcionário, que na tentativa de reparar um defeito técnico, acabou por contribuir para o desligamento de algumas linhas de transmissão operadas pela Eletrobrás-Furnas[23]. O incidente atingiu cerca de 3

---

[20] https://pt.wikipedia.org/wiki/Botnet. Acesso em 02 de maio de 2016.
[21] Hoje Swedbank. Na época, o Hansa Bank era o maior banco da Estônia. https://www.swedbank.com/about-swedbank/our-history/hansabank-history/. Acesso em 02 de maio de 2016.
[22] www.bbc.com/portuguese/.../070517_estoniaataquesinternetrw.shtml. Acesso em 02 de maio de 2016.
[23] Furnas Centrais Elétricas S.A., é uma empresa brasileira de economia mista subsidiária da Eletrobras, vinculada ao Ministério de Minas e Energia, atuando no segmento de geração e transmissão de energia em alta e extra-alta tensão. Está sediada em Botafogo, na cidade do Rio de Janeiro. Fonte: https://wikipedia.org/wiki/Eletrobras_Furnas

milhões de pessoas nos estados do Rio de Janeiro e Espírito Santo, o que rendeu a Furnas uma multa de R$ 4,1 milhões de reais[24].

Três anos mais tarde, em 2008, foi noticiada a ocorrência de falha em uma subestação da Companhia de Transmissão de Energia Elétrica Paulista (CTEEP), atingindo vinte e quatro bairros do estado de São Paulo. O blecaute afetou o funcionamento de empresas, residências, e sistemas de segurança, como a sinalização semafórica de vias paulistas importantes, como as Avenidas Paulista, Nove de Julho e Brasil, atentando, claramente, contra a segurança pública e de trânsito[25].

Curiosamente, o presidente dos Estados Unidos Barak Obama, em discurso datado de maio de 2009, afirmou, ao se referir ao ciberterrorismo, "(...) saber que esses invasores cibernéticos têm colocado à prova nosso sistema interligado de energia (SIN) e que, em outros países, ataques assim jogaram cidades inteiras na escuridão". Segundo a emissora de televisão americana CBS, fontes ligadas aos setores militar, de inteligência e de segurança afirmaram que o presidente Obama estava se referindo aos casos brasileiros de 2005 e 2008. Uma menção pública aos casos foi proferida por John Grines enquanto Secretário-Assistente de Defesa dos Estados Unidos, em conferência em Paris[26], afirmando que "não muito tempo atrás houve um ataque ao sistema de energia no Brasil, em sua rede de Supervisão e Aquisição de Dados (Supervisory Control and Data Acquisition - SCADA), o que causou grandes perturbações". Richard Clarke, autor mencionado diversas vezes neste trabalho e assessor especial sobre cibersegurança do ex-presidente dos Estados Unidos George W. Bush, em entrevista à revista *Wired*[27], também mencionou o Brasil, quando se referia ao grau de seriedade que a administração Obama está aplicando a cibersegurança, envidando esforços para que não aconteça aos EUA o que aconteceu com o Brasil, onde hackers obtiveram sucesso na invasão de sistemas de distribuição de energia.

---

[24] Conforme notícia publicada pelo site da Rede Globo em 23 de junho de 2012. Disponível em: http://redeglobo.globo.com/globoecologia/noticia/2012/06/relembre-os-apagoes-que-ocorreram-no-brasil-nas-ultimas-decadas.html. Acesso em 03 de maio de 2016.
[25] Idem à nota anterior.
[26] http://www.foreignpolicyjournal.com/. Acesso em 03 de maio de 2016.
[27] www.wired.com. Acesso em 03 de maio de 2016.

Do lado brasileiro, o então Diretor do Departamento de Segurança da Informação e Comunicação do Gabinete de Segurança Institucional da Presidência da República (DSIC/GSI-PR), Raphael Mandarinno Júnior, afirmou ter checado o assunto junto das empresas de energia sem encontrar rastros. Mandarinno disse, ainda, que o Brasil está "protegido", de certa forma, por ter entrado tardiamente nos avanços tecnológicos. Afirma que parte das empresas não têm seus sistemas operacionais conectados diretamente à rede mundial de informações, o que, segundo ele, dificulta sobremaneira um hacker invadir uma rede interna[28].

É fácil presumir a relutância de um governo em assumir ter sido alvo de ataques cibernéticos bem sucedidos. Uma vez divulgada a notícia oficialmente, inúmeros ataques se voltariam aos sistemas e sites governamentais. Seria um tipo de "certificado de insegurança", o que rapidamente difundiria as tentativas de invasão a sistemas e redes.

Os exemplos expostos acima mostram o quão nocivos podem ser os ataques realizados no espaço virtual. Seja para viabilizar operações militares, ou em retaliação a divergências ideológicas e culturais, até mesmo para causar prejuízo ao fornecimento de serviços básicos de países, a segurança de infraestruturas emerge como uma missão do Estado, dada sua ramificação e penetrabilidade, mediante regulação, nos setores estratégicos nacionais.

---

[28] Entrevista sob o título: "Hacker pode causar apagão, mas não é provável, diz chefe de segurança de Lula", concedida ao jornalismo de tecnologia do site www.globo.com, datada de 27 de novembro de 2009.

3 REQUISITOS PRÉ-PESQUISA

3.1 Pergunta de Pesquisa

Que políticas públicas, estratégias, atores e interações são relevantes para compreender os esforços do Estado brasileiro na tentativa de alcançar a segurança e defesa do seu espaço cibernético?

3.2 Justificativa

A comunidade internacional se depara com uma nova ameaça, esta, intangível e assimétrica. Os ataques advindos do espaço cibernético não respeitam protocolos, limites geográficos, Constituições, ou mesmo o poderio bélico de seus alvos. Eles são irregulares, podendo durar dias ou semanas, além de seus rastros serem facilmente dissimulados. Diante dessas ameaças, países têm formulado novas medidas para a segurança e defesa de seus ciberespaços.

A revolução tecnológica, ao passo que permitiu a inserção de comodidades ao cotidiano de cidadãos e organizações, abriu caminho para ameaças diversas, que podem desestruturar um Estado em seus pilares mais básicos, como a prestação de serviços energéticos, operações financeiras, telecomunicação, transportes, entre outras. Esse quadro cria a motivação necessária para governantes pensarem políticas públicas que visem se antecipar a quaisquer potenciais fragilidades no ciberespaço que possam se converter em danos e prejuízos no mundo real.

A relevância da temática em tela se sustenta na necessidade de países proverem a segurança e defesa de seus espaços cibernéticos como forma de garantia e manutenção das liberdades de seu corpo burocrático (governo, empresas públicas, agências e atores que contribuem para a máquina pública) e de seus cidadãos. Logo, esta pesquisa visa compreender como o Brasil tem buscado a proteção do seu ciberespaço, o que abre caminho para que especialistas em tecnologia da informação, cientistas políticos e estrategistas pensem a capacidade do Estado de implementar políticas que assegurem a sociedade da informação existente.

Admitindo a possibilidade de o Brasil enfrentar uma situação de conflito no ciberespaço, ou seja, o vislumbre de possíveis ataques às infraestruturas lógicas que possam culminar em uma situação de guerra cibernética, esta pesquisa toma por base a premissa constitucional de que é dever do Estado prover ações para sua segurança e defesa (CONSTITUIÇÃO, 1988, Art. 21; 22; 142). Logo, o Estado deve garantir as condicionantes que integram os ciclos de difusão da informação que permeiam o cotidiano do país, adotando políticas públicas para a segurança e defesa do espaço cibernético.

Ciberespaços seguros emergem como uma necessidade mundial aplicável a todas as sociedades da informação. Essa segurança permeia a manutenção de interesses diversos, existentes nas áreas estratégicas elementares de países. A não adoção dessas premissas de segurança e defesa seria um retrocesso, onde países deixariam de acompanhar o exponencial movimento das revoluções tecnológicas que se inserem transversalmente nas relações entre Estado e sociedade, o que fica claro com o advento das governanças eletrônicas.

Na intenção de proceder a uma análise das ações voltadas para a segurança e defesa de espaços cibernéticos, este trabalho tem por motivação o caso brasileiro, analisando as políticas, atores e ações adotadas, abordando sumariamente cada uma delas.

3.3 Objetivo Geral

Diante do contexto tecnológico atual, aliado à constatação de que imprescindivelmente países precisam pensar políticas para o provimento da segurança e defesa de seus espaços cibernéticos, este trabalho tem como objetivo geral elucidar as políticas, estratégias e inovações voltadas para a segurança e defesa do espaço cibernético brasileiro, ressaltando quais ações, leis, mecanismos, processos e instituições foram relevantes para que a proteção do espaço cibernético se transformasse em uma política de abrangência nacional.

3.4 Objetivos Específicos

- Conceituar segurança e defesa de espaços cibernéticos e suas infraestruturas críticas;
- Identificar possíveis danos que um ataque cibernético pode causar a países;
- Revisar parte da bibliografia sobre políticas públicas;
- Identificar quais os aspectos que são contemplados quando se pensa a proteção do espaço cibernético brasileiro;
- Identificar as legislações que possibilitaram a adoção de políticas para a segurança e defesa do ciberespaço brasileiro;
- Identificar as principais instituições responsáveis pela segurança e defesa do ciberespaço brasileiro;

3.5 Metodologia

Para alcançar tanto o objetivo geral quanto os objetivos específicos, este trabalho utilizará os seguintes métodos de pesquisa: revisão bibliográfica, análise documental, coleta de dados qualitativos e quantitativos, e análise comparativa de dados.

A revisão bibliográfica se dará na parte conceitual da temática sobre segurança e defesa cibernética, bem como na análise de exemplos de incidentes e atentados à cibersegurança de países, assim como da teoria de políticas públicas, que fundamentam as decisões de governo que atinjam segmentos diversos da nação. Para compreender as ações de governos em prol da cibersegurança, será procedida análise de documentos oficiais e legislações sobre segurança e defesa cibernética. A análise comparativa se dará entre as ações de países expressas em documentos oficiais, tais como políticas, estratégias, resoluções e leis em geral.

4 REFERENCIAL TEÓRICO

Ao tratar a questão da segurança e defesa cibernética como uma necessidade do Estado, atribuindo a ele a capacidade de convergir esforços para o alcance dos objetivos necessários, é cabível compreender que tais medidas traduzam-se em políticas públicas.

Dada a distância existente entre as disciplinas que abarcam as tecnologias da informação e as propostas da ciência política, este trabalho compreende ser plausível a observação do fenômeno tecnológico, aqui tratado pela exploração do ciberespaço, sob a ótica das ações do Estado, ou seja, das políticas públicas. Para tanto, é mister compreender o que são políticas públicas, qual a sua natureza, e, mesmo que brevemente, compreender como os estudos de políticas públicas começaram a ser pensados dentro da Academia. Para isso serão abordados conceitos clássicos que ainda hoje fundamentam pesquisas e desdobramentos teóricos, como os estudos de difusão de inovações, a fim de ressaltar a atuação do Estado na concepção de políticas de segurança e defesa.

Os estudos de políticas públicas tem seu nascimento nos EUA, onde há uma quebra da tradição europeia de se estudar apenas o Estado e suas instituições, iniciando uma análise do produto de suas ações, ou seja, as políticas públicas. Enquanto ferramenta de análise do “mundo público” pode-se dizer que a disciplina surgiu guiada por três caminhos. O primeiro mantém a ideia de Madison, que focalizava nas instituições como agentes limitadores das paixões humanas, estas traduzidas e compreendidas como sendo os intentos dos governantes e suas decisões. O segundo segue a tradição de Paine e Tocquevile, que acreditavam que nas instituições residiam a virtude e a capacidade cívica para a prática de boas políticas. O terceiro caminho trata as políticas públicas como um ramo da ciência política disposto a elucidar como e por que governos optam ou não por certos cursos de ações/decisões (SOUZA, 2006, p.22).

A difusão do tema na Academia teve início na década de 1930, tendo como expoentes iniciais quatro grandes nomes, a saber, Harold Laswell, Herbert Simon, Charles Edward Lindblom e David Easton. Estes quatro estudiosos são considerados os pais fundadores dos estudos de políticas públicas.

Laswell (1936) é o precursor, introduzindo a expressão *policy analisis*, como ferramenta vinculadora de cientistas sociais, grupos de interesse e governo. Simon (1957) tratou do conceito de racionalidade limitada dos *policy makers*, argumentando que ela poderia ser minimizada pelo conhecimento racional dos atores. A tomada de decisão seria prejudicada pela falta de informações ou por estarem elas incompletas, pelo tempo que o gestor dispõe para a tomada de decisão, o próprio auto interesse dos atores é compreendido como dificultador. Lindblom (1959; 1979) dá partida à sua análise e conceituação incluindo variáveis ignoradas por seus antecessores. Para ele devem ser consideradas as relações de poder e de integração entre as fases do processo decisório. Easton (1965) sistematiza a compreensão de política pública, concebendo um conceito que relaciona a formulação, resultados e o ambiente político que tangenciam a política. Dessa forma, as políticas são *outputs* das pressões exercidas dos partidos políticos, pelos grupos midiáticos e pelos grupos de interesses específicos (SOUZA, 2006, p. 24).

O objeto de estudo dos autores citados está longe de possuir uma definição ideal, sendo muitos os conceitos atribuídos a políticas públicas. Entre os conceitos que fundamentam a concepção do termo, vale destacar os que se seguem.

Thomas Dye (1976) traz uma abordagem mais sucinta, definindo política pública como “aquilo que o governo escolhe fazer ou não fazer, por que faz e que diferença tal ação traz”. A definição de Dye, por vezes, é considerada simplista demais, pois desconsidera aspectos comportamentais dos agentes do governo no processo de decisão. Essa definição não distingue as ações triviais das significativas, carecendo de um aprofundamento na questão comportamental dos tomadores de decisão (HOWLETT, 1995, p. 04).

Willians Jenkins (1978), de maneira um pouco mais complexa, afirmou que uma política pública é “uma conjunção de decisões tomadas por atores políticos ou grupo de atores em relação a metas e recursos para se atingir uma determinada situação”. Contrapondo-se à afirmativa de Dye, para ele uma política pública se caracteriza como um processo, não uma escolha. Ela envolve uma série de

decisões, tomadas por diferentes atores em certo nível de diálogo e deliberação sobre o assunto, decisões essas que se inter-relacionam (HOWLETT, 1995, p. 05).

James Anderson (1984) problematiza a questão ao afirmar que “a política pública é o curso de uma ação proposta por um ator ou grupo de atores empenhados na solução de um problema ou uma questão de interesse (dos atores)”. Indica que não somente problemas públicos ou sociais se tornam objeto de decisões governamentais. Indo além do que Dye e Jenkins propõem, Anderson afirma que as decisões sobre políticas emanam de um grupo de atores em comunicação com o governo, seu interlocutor. Sinaliza ainda que a tomada de decisão de um governo parte da identificação de um problema no seio da sociedade que necessita de uma solução política.

Peters (1986) fala que “política pública é a soma das atividades do governo que agem diretamente ou por intermédio de delegação, e que influenciam a vida dos cidadãos”. Enquanto Mead (1995) define políticas públicas como “um campo dentro do estudo da política que analisa o governo à luz de grandes questões públicas”.

Na literatura brasileira, Celina Souza (2006) resumiu o conceito de política pública como “o campo do conhecimento que busca, ao mesmo tempo, colocar o governo em ação, ou analisar essa ação, e, quando necessário, propor mudanças no rumo dessas ações”. Salienta ainda que, em governos democráticos, as políticas públicas se traduzem no cumprimento dos programas e plataformas eleitorais, ou seja, é a materialização das soluções propostas às questões sociais passivas de solução (SOUZA, 2006, p. 26).

Outra autora que trata o tema é Maria das Graças Rua (1998), que em um trabalho preliminar, conceitua dizendo que:

> “As políticas públicas (policies), por sua vez, são outputs, resultantes da atividade política (politics). Elas compreendem o conjunto das decisões e ações relativas à alocação imperativa de valores. Nesse sentido é necessário distinguir entre política pública e decisão política. Uma política pública geralmente envolve mais do que uma decisão e requer diversas ações estrategicamente selecionadas para implementar as decisões

> tomadas. Já uma decisão política corresponde a uma escolha dentre um leque de alternativas, conforme a hierarquia das preferências dos atores envolvidos, expressando em maior ou menor grau - uma certa adequação entre os fins pretendidos e os meios disponíveis. Assim, embora uma política pública implique decisão política, nem toda decisão política chega a constituir uma política pública. Um exemplo encontra-se na emenda constitucional para reeleição presidencial. Trata-se de uma decisão, mas não de uma política pública. Já a privatização de estatais ou a reforma agrária são políticas públicas."

Diante de tantas formas de interpretação e conceituação do que seriam as políticas públicas, é possível chegar a uma compilação básica sobre o tema. Dessa forma, as *policies* se traduzem em um processo, este, composto por decisões e diálogos entre atores diversos. Esse processo nasce após a identificação de um problema no seio da sociedade, carente de uma ação governamental para sua solução. As soluções possíveis podem chegar aos gestores do governo por intermédio de interlocutores na sociedade civil (grupos, atores específicos), partidos políticos ou dentro do próprio governo, oriundas de sua plataforma política proposta por ocasião das eleições. Nesse caso as políticas são a materialização da plataforma política proposta.

Aliando a teoria com o objeto da pesquisa, este trabalho considera apropriada a teoria que emerge das análises neoinstitucionalistas sobre políticas públicas. Não é objetivo deste trabalho aprofundar-se nas vertentes neoinstitucionalistas de análise de políticas públicas, apenas trazer à tona a centralidade do Estado na hora de formular políticas, ou seja, o próprio Estado/instituições como ponto de partida para a solução de problemas e questões sociais. Para a compreensão das abordagens para o alcance do tema desse trabalho, faz-se plausível que se observe o Estado como o centro analítico para explicação das políticas governamentais abordadas.

A abordagem sobre um posicionamento mais autônomo do Estado na hora de formular ações governamentais se contrapõe à perspectiva de Robert Dahl (1988), que afirma ser o corpo institucional do Estado algo próximo de uma neutralidade, pronto para promover a conciliação de demandas que emergem da sociedade. Nessa linha, Skocpol (2005) retoma a compreensão de Weber e Hintze,

trazendo o entendimento que os governantes, quando dotados de ferramentas institucionais adequadas, são capazes de mirar objetivos e concluí-los, mesmo que eles sejam impopulares ou em desacordo com as prioridades de grupos da sociedade civil organizada.

A compreensão das ações do Estado enquanto centro analítico de políticas públicas perpassa por três perspectivas amplamente consolidadas na Academia, a saber, o neoinstitucionalismo histórico e o neoinstitucionalismo da escolha racional.

O institucionalismo histórico remonta como objeto de análise o conjunto de atores institucionais cuja interação é permanente, sendo esse vínculo firmado sob a concepção de serem as instituições procedimentos, regras e normas formais próprias da estrutura formal da política (HALL; TAYLOR, 2003, p.196). O modelo reedita modelos de cunho histórico-estruturais, como as propostas de Weber e Marx, a fim de elucidar o funcionamento das instituições com base em um legado histórico que configura os arranjos que as guiam (STEINMO; THELEN, 1992).

A abordagem do institucionalismo da escolha racional interpreta as instituições a partir do arranjo Estado-Sociedade-Decisões, firmando os atores que figuram os círculos de decisão que implicam diretamente nas escolhas. Esta estrutura considera a interação entre atores, levando em consideração as preferências individuais dos mesmos, estas exógenas ao processo (SHEPSLE, 2008, p. 24). Dessa forma, os indivíduos lançam sobre as instituições suas preferências, uma vez que estão dotados das ferramentas que lhes proporcionam a possibilidade de moldá-las, forjando estratégias de acordo com suas preferências e de posse das informações necessárias para saber se os seus intentos são viáveis ou não.

5 AGENDA DE SEGURANÇA E DEFESA CIBERNÉTICA BRASILEIRA

A agenda brasileira para proteção do espaço cibernético contempla dois campos distintos, embora complementares: o da Segurança Cibernética, a cargo da Presidência da República (PR); e a Defesa Cibernética, a cargo do Ministério da Defesa/Forças Armadas (MD/FFAA).

Para compreender as ações realizadas pelo governo brasileiro no tocante à segurança e defesa cibernética, este trabalho elucidará medidas delegadas a setores do Estado diretamente vinculados à implantação dessa inovação no âmbito nacional. Primeiramente, a Presidência da República (PR), por se tratar da mais alta autoridade brasileira efetivamente capaz de produzir políticas públicas. O Gabinete de Segurança Institucional da Presidência da República (GSI/PR), órgão de assessoramento essencial, por ser sua atribuição, por intermédio do Departamento de Segurança da Informação e Comunicações (DSIC), a condução de ações para a segurança da informação e comunicação no âmbito da Administração Pública Federal (APF). O Ministério da Defesa (MD), por ser o órgão do primeiro escalão do Executivo responsável pela organização e atuação das Forças Armadas, às quais, natural e constitucionalmente, compete qualquer assunto afeto à defesa nacional, inclusive a concepção de defesa cibernética. No escopo da organização do Ministério da Defesa, figura como ator-chave na condução dos trabalhos para a defesa cibernética o Exército brasileiro (EB), conforme será elucidado mais adiante, depreendendo pessoal e material em larga escala para esse projeto.

5.1 Medidas para a Segurança Cibernética

5.1.1 Gabinete de Segurança Institucional da Presidência da República (GSI/PR)

No escopo da área governamental, o tema passou a ser tratado com a inclusão da necessidade de prover a segurança da informação no âmbito da Presidência da República., passando a ser possível através da Medida Provisória (MP) nº 2.216-37, de 31 de agosto de 2001, que alterou dispositivos da Lei nº 9.649, de 27 de maio de 1998, atribuindo ao GSI/PR a coordenação das atividades de segurança da informação, como se segue:

> “ANEXO I
> ESTRUTURA REGIMENTAL DA CASA MILITAR DA PRESIDÊNCIA DA REPÚBLICA
> CAPÍTULO I
> DA NATUREZA E COMPETÊNCIA
> Art. 1o À Casa Militar da Presidência da República, órgão essencial da Presidência da República, compete:
> I - assistir direta e imediatamente o Presidente da República no desempenho de suas atribuições;
> II - realizar o assessoramento pessoal em assuntos militares e de segurança;
> III - coordenar atividades de segurança da informação no âmbito da administração pública federal;”

Para cumprir o que determina a Lei n° 9.649/98, foi inserido na estrutura regimental do GSI o Departamento de Segurança da Informação e Comunicação, o que demonstra a importância e seriedade que o tema seria tratado pela APF.

5.1.2 Departamento de Segurança da Informação e Comunicação (DSIC-GSI/PR)

Por intermédio do Decreto nº 5.772, de 8 de maio de 2006, foi criado o Departamento de Segurança da Informação e Comunicações (DSIC), no GSI/PR, cuja missão é planejar e coordenar as ações para a Segurança da Informação e Comunicações (SIC) no âmbito da Administração Pública Federal (APF).

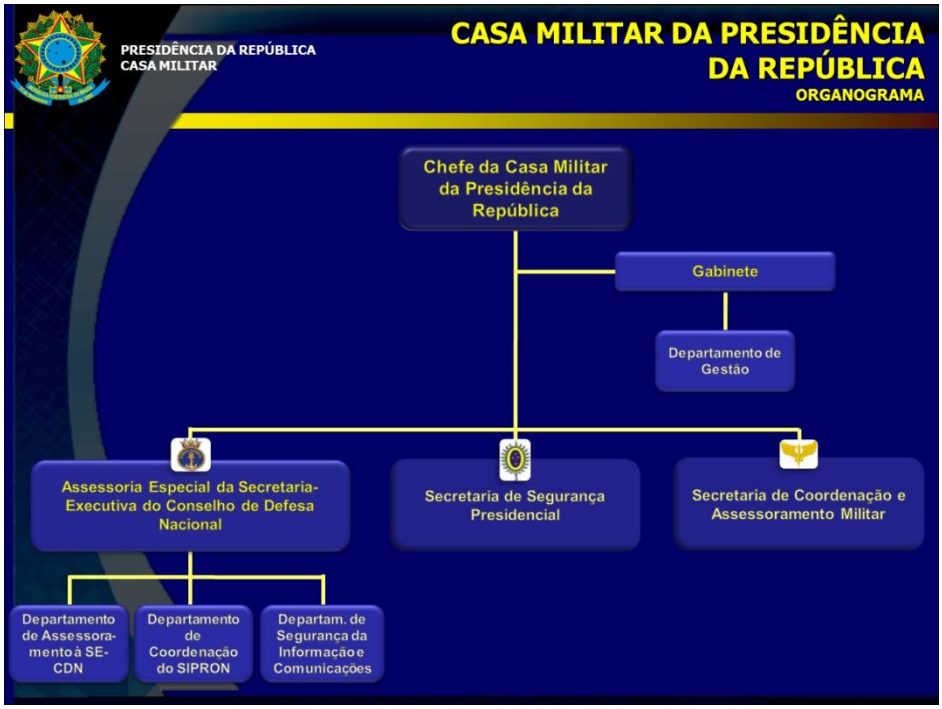
As competências do DSIC foram explicitadas pelo Decreto nº 7.411, de 29 de dezembro de 2010, atribuindo ao Departamento a competência para:

> “I - orientar a implementação de ações de segurança da informação e comunicações, inclusive as de segurança cibernética, no âmbito da administração pública federal;
> II - definir normativos e requisitos metodológicos para implementação de ações de segurança da informação e comunicações pelos órgãos e entidades da administração pública federal, no âmbito da Secretaria-Executiva do Conselho de Defesa Nacional;
> III - operacionalizar e manter o centro de tratamento e resposta a incidentes ocorridos nas redes de computadores da administração pública federal;
> IV - avaliar tratados, acordos ou atos internacionais relacionados ao tratamento e à troca de informação classificada;
> V - exercer, por meio do Núcleo de Segurança e Credenciamento, na qualidade de Órgão de Registro Central, atividades relacionadas ao credenciamento de segurança e ao tratamento de informação classificada; e

> VI - exercer outras atribuições que lhe forem determinadas pelo Assessor Chefe da Assessoria Especial da Secretaria-Executiva do Conselho de Defesa Nacional."

A estrutura da Casa Militar da Presidência da República, que abriga os dois principais órgãos responsáveis pela segurança cibernética da APF, passa a ficar da seguinte maneira:

Figura 1 – Organograma da Casa Militar da Presidência da república.



Fonte: http://www.gsi.gov.br/sobre/estrutura. Acesso em 02 de junho de 2016.

O DSIC agrega à sua rotina intensas atividades de segurança atividades de orientação e aperfeiçoamento dos quadros da APF, a fim de disseminar a cultura de segurança da informação e comunicação. Uma de suas principais atividades consiste na operacionalização e manutenção do Centro de Tratamento e Resposta a Incidentes[29] (CTIR Gov) em redes de computadores da APF (Dec 5.772/06, Art.8°, Inciso IV). O CTIR Gov atua de maneira corretiva, ou seja, atende demandas após indicações e relatórios de incidentes em redes de computadores, buscando sua origem, natureza e possíveis intentos. Sua atuação garante ação-resposta às redes da APF.

[29] http://www.ctir.gov.br/sobre-CTIR-gov.html#abrangencia

Os documentos que se seguem são formulações apresentadas à APF como diretrizes, devendo cada órgão integrante designar equipe capaz de implementar os objetivos assinalados nos documentos do DSIC. A ideia é incrementar os quadros funcionais com seções específicas e responsáveis pela manutenção do nível de segurança alcançado após determinação da instância superior.

5.1.2.1 Livro Verde de Segurança Cibernética

Um dos principais guias brasileiros para a segurança cibernética é o Livro Verde de Segurança Cibernética (2010)[30]. Desenvolvido pelo DSIC, ele reúne um compilado de informações que norteiam a atividade se segurança da informação no Brasil, abordando o papel brasileiro tanto em âmbito interno quanto no cenário internacional, destacando "oportunidades e desafios nos vetores: político-estratégico, econômico, social e ambiental, e segurança de infraestruturas críticas" (Livro Verde, 2010, p. 15). Além disso, o Livro Verde expressa potenciais diretrizes para o estabelecimento de uma cultura de segurança cibernética a serem alcançadas em curto (2-3 anos), médio (5-7 anos) e longo (10-15 anos) prazo.

Entre as diretrizes estipuladas, vale ressaltar as que dão ênfase ao fomento de uma mudança de concepção do setor cibernético pela sociedade e à segurança de infraestruturas críticas. Para a educação, o documento aborda a necessidade de desenvolvimento e inclusão de práticas de segurança cibernética no campo acadêmico, como se segue:

> "EDUCAÇÃO
>
> DESENVOLVER programa nacional de capacitação em segurança cibernética e de recrutamento, que seja construído a partir da visão interdisciplinar que o tema requer, no curto, médio e longo prazo, nos níveis: básico, técnico, graduação, especialização, mestrado e doutorado;
>
> DESENVOLVER programa de conscientização nacional no tema de forma a atingir, especialmente, no curto e médio prazo, diferentes comunidades do país, desenvolvendo material apropriado para os públicos: infantil; de adolescentes e jovens; de baixa renda; da terceira idade; de educadores em todos os níveis de formação educacional; e, de gestores e legisladores públicos, dentre outros segmentos a serem atendidos, no médio e longo prazo;

[30] http://dsic.planalto.gov.br/documentos/publicacoes/1_Livro_Verde_SEG_CIBER.pdf

> INCLUIR nos currículos de ensino de nível fundamental e médio do País a obrigatoriedade de temas como segurança da informação e correlatos.” (Livro Verde, 2010, p. 46)

No tocante à segurança de ICI, o documento é bastante ambicioso, lançando propostas em grande escala, que se implantadas, trarão grandes benefícios aos setores de importância estratégica para o país. As propostas são as seguintes:

> “DAS INFRAESTRUTURAS CRÍTICAS
> LANÇAR a Política Nacional de Segurança das Infraestruturas Críticas no curto prazo;
> CONHECER E MAPEAR o grau de vulnerabilidade do país em relação aos seus sistemas de informação e as suas infraestruturas críticas de informação por meio de programa específico, no médio e longo prazo, que compreenda: a) a macro-coordenação do mapeamento dos ativos de informação das infraestruturas críticas; b) o apoio ao processo de auditoria de segurança das infraestruturas críticas da informação, definindo requisitos mínimos de segurança; e, c) a macro-coordenação e o desenvolvimento de sistema de monitoramento de ameaças cibernéticas e divulgação de alertas de suporte às infraestruturas críticas;
> ELABORAR E/OU ADAPTAR metodologia, no médio e longo prazo, para avaliações de risco e de continuidade de negócio em segurança cibernética, o que inclui dentre outras ações: a) identificar o grau de interdependência dos serviços das infraestruturas críticas do país; b) desenvolver e/ou adaptar metodologia comum para avaliar as vulnerabilidades das infraestruturas críticas de informação, dos seus sistemas e de seus serviços; e, c) conceber um sistema dinâmico de medidas preventivas, próativas, e reativas contra ameaças e ataques cibernéticos;
> DESENVOLVER PROGRAMA de capacitação de gestores atuantes nas infraestruturas críticas que contemple dentre outras competências: análise e gestão de riscos, segurança das infraestruturas críticas da informação, resiliência operacional e organizacional, monitoramento e resposta a ataques cibernéticos.” (Livro Verde, 2010, p. 47)

A principal meta do Livro se mostra como a criação de um ambiente propício para uma cultura de segurança da informação e comunicação. A sua sugestão para uma Política Nacional de Segurança Cibernética que alcance transversalmente todos os atores que compõem a APF.

5.1.2.2 Estratégia de Segurança da Informação e Comunicação e Segurança Cibernética da Administração Pública Federal (Est SIC Seg Ciber APF)

A partir das propostas estabelecidas pelo Livro Verde de Segurança Cibernética, o DSIC formulou um segundo documento, este estabelecendo um curso estratégico para a segurança da informação e comunicação no âmbito da APF. Trata-se da Estratégia da Segurança da Informação e Comunicação (2015-2018)[31], uma ferramenta de apoio ao planejamento estratégico do governo para o quadriênio 2015-2018. Está dividido em objetivos estratégicos e metas, que buscam a excelência da segurança da informação e comunicação e da segurança cibernética. Quanto às metas, elas são designadas para cada ano, de 2015 a 2018, além de existir metas contínuas, a serem seguidas ao longo dos quatro anos de vigência do documento (Est SIC Seg Ciber APF, 2010, p. 11).

Os Objetivos Estratégicos estipulados pelo documento representam a motivação para o alcance da missão de segurança estabelecida, a fim de estabelecer uma forma de Governança Sistêmica de SIC e de SegCiber, institucionalizando o tema ora proposto.

Na tabela abaixo é possível visualizar cada um dos objetivos desenhados pelo documento.

Tabela 1 – Objetivos Estratégicos de Segurança da Informação e Comunicações.

OE I - INSTITUCIONALIZAR O TEMA DE SIC E DE SEGCIBER NO PLANEJAMENTO E ORÇAMENTO FEDERAL.
OE II - GARANTIR CONTINUAMENTE O APRIMORAMENTO DO QUADRO DE PESSOAL DA APF EM SIC E SEGCIBER, DE FORMA QUALITATIVA E QUANTITATIVA.
OE III - GARANTIR CONTINUAMENTE A PESQUISA, O DESENVOLVIMENTO E A INOVAÇÃO EM SIC E SEGCIBER NA APF.
OE IV - INSTITUIR MODELO DE GOVERNANÇA SISTÊMICA DE SIC E DE SEGCIBER NA APF, COM COORDENAÇÃO EXECUTIVA, ACOMPANHAMENTO E AVALIAÇÃO DO ÓRGÃO CENTRAL (GSI/PR)
OE V - ALINHAR O PLANEJAMENTO DE SIC E DE SEGCIBER AO PLANEJAMENTO ESTRATÉGICO DOS ÓRGÃOS E ENTIDADES DA APF.
OE VI - AMPLIAR E FORTALECER AÇÕES COLABORATIVAS EM SIC E SEGCIBER COM A ACADEMIA, SETORES PÚBLICO, PRIVADO E TERCEIRO SETOR, NO PAÍS E NO EXTERIOR.
OE VII - ELEVAR O NÍVEL DE MATURIDADE DE SIC E DE SEGCIBER NA APF.
OE VIII - REFORÇAR A SIC E A SEGCIBER COMO ALTA PRIORIDADE NA AGENDA DE GOVERNO.

[31] http://dsic.planalto.gov.br/documentos/publicacoes/4_Estrategia_de_SIC.pdf

OE IX - VALORIZAR E AMPLIAR AÇÕES QUE FORTALEÇAM A SEGURANÇA DAS INFRAESTRUTURAS CRÍTICAS DA INFORMAÇÃO.
OE X - PROMOVER MECANISMOS DE CONSCIENTIZAÇÃO DA SOCIEDADE SOBRE SIC E SEGCIBER.

(Est SIC Seg Ciber APF, 2010. Design do autor.)

O documento detalha as atribuições de vários atores-chave do Estado brasileiro no quesito segurança cibernética, descrevendo as ferramentas que possibilitarão maior integração entre empresas, Academia e cidadãos. Incita, ainda, a consolidação de uma base industrial de equipamentos de defesa, assim como a END preconiza. Um exemplo já em curso são as redes privativas desenvolvidas pelo SERPRO para possibilitar a comunicação de informações caras à segurança e soberania nacional[32].

5.1.2.3 Guia de Referência para a Segurança das Infraestruturas Críticas da Informação (Guia Seg ICI)

Objeto central dos esforços para a segurança e proteção de espaços cibernéticos, as infraestruturas críticas da informação brasileiras foram contempladas com um estudo amplo e detalhado. Os trabalhos foram desenvolvidos pelo Grupo de Trabalho de Segurança das Infraestruturas Críticas da Informação (GT SICI), instituído no seio do Comitê Gestor de Segurança da Informação (CGSI), regidos pela Portaria n° 34 do Conselho de Defesa Nacional - CDN/SE de 05/08/2009, que lhe atribuiu:

> **"**I - levantar e avaliar as potenciais vulnerabilidades e riscos que possam afetar a Segurança das Infraestruturas Críticas da Informação, o que requer a identificação e monitoramento das interdependências;
> II - propor, articular e acompanhar medidas necessárias à Segurança das Infraestruturas Críticas da Informação;
> III - estudar, propor e acompanhar a implementação de um sistema de informações que conterá dados atualizados das Infraestruturas Críticas da Informação, para apoio a decisões; e,
> IV - pesquisar e propor um método de identificação de alertas e ameaças da Segurança de Infraestruturas Críticas da Informação."

[32] http://www.defesanet.com.br/cyberwar/noticia/19669/Nova-Estrategia-Nacional-de-Seguranca-Cibernetica/

O Grupo de Trabalho foi subdividido para o desenvolvimento de tópicos necessários para o início da análise de vulnerabilidade das ICI brasileiras, a saber:

1) Mapeamento de Ativos de Informação das Infraestruturas Críticas da Informação;

2) Requisitos mínimos necessários à Segurança das Infraestruturas Críticas da Informação: visando aumentar a segurança, resiliência e capacitação; e,

3) Método de Identificação de Ameaças e Geração de Alertas de Segurança das Infraestruturas Críticas da Informação.

O documento contribui sobremaneira para a gestão de riscos e vulnerabilidades de infraestruturas caras ao funcionamento da sociedade brasileira. Conforme este trabalho mostrou anteriormente, tanto no caso estoniano como no próprio caso brasileiro, infraestruturas críticas como os setores de energia, abastecimento e bancário, quando afetados por ataques oriundos do espaço cibernético, causam danos exponenciais à população e aos sistemas de segurança de um país.

5.2 Medidas para a Defesa Cibernética

5.2.1 Política Nacional de Defesa (PND)

O primeiro documento oficial a tratar a necessidade de uma agenda para o ciberespaço brasileiro se materializou no Decreto nº 5.484 de 30 de junho de 2005, quando o governo do então presidente Luís Inácio Lula da Silva aprovou a Política Nacional de Defesa, documento que introduziu a necessidade da defesa cibernética no âmbito do planejamento político da Administração Pública Federal.

A PND refere-se claramente a possíveis ameaças externas que o Brasil possa sofrer, atribuindo ao Ministério da Defesa a prerrogativa de planejamento e coordenação. Está dividida em duas partes, sendo a primeira um referencial político, abordando: os conceitos relativos à defesa; os ambientes nacional e internacional onde o Brasil pretende assumir papel de destaque; e os objetivos da Defesa. A

segunda parte refere-se à estratégia a ser adotada, fornecendo orientações e diretrizes a serem seguidas.

A estratégia oferecida orienta a tomada de ações que minimizem a possibilidade de ataques ao ciberespaço brasileiro. Isto posto, o alcance desse objetivo se dará com permanente aperfeiçoamento de setores internos específicos e quadros de pessoal, reduzindo a vulnerabilidade de sistemas essenciais. A consecução dessa estratégia está diretamente ligada ao pressuposto básico de modernização, balanceamento e aprestamento das Forças Armadas. Suas diretrizes indicam o fortalecimento e aumento na segurança de dispositivos e sistemas diretamente ligados às infraestruturas dotadas de valores estratégicos, como o setor energético, de transporte e comunicação.

As orientações e diretrizes para o setor cibernético previstas na PND se aliam a outros dispositivos do documento que localizam o Brasil como país integrante das agendas de combate ao terrorismo (cyber terrorismo) no cenário internacional, de estabilidade regional e de manutenção da paz e segurança interna da ONU .

5.2.2 Estratégia Nacional de Defesa

Concebida no corpo do Decreto n° 6.703 de 18 de dezembro de 2008, a END se caracteriza pela criação de um vínculo entre a necessidade de independência do Brasil enquanto país soberano, de um lado, e a necessidade de FFAA capacitadas e prontas para garantir essa soberania, de outro.

Está organizada em torno de três eixos estruturantes considerados essenciais para o desenvolvimento, a saber, 1) Organização das FFAA; 2) Reorganização da Indústria Nacional de Defesa; e 3) Otimização do efetivo das FFAA (END, 2010).

Com base nessas premissas, suas diretrizes visam fortalecer três setores de importância estratégica para a defesa nacional: o espacial, o cibernético e o nuclear. O primeiro ficou a cargo da Força Aérea Brasileira, o segundo a cargo do Exército, e o terceiro sob a guarda da Marinha. A intenção é direcionar as ações das

Forças para uma atuação em rede, visando fortalecer e aprimorar a tecnologia nacional, diminuindo a dependência tecnológica externa (END, 2012, p.12). Outra diretriz relevante diz respeito à interação e integração da América do Sul a essas políticas setoriais, de modo que haja uma relação de mútuo-aprendizado e desenvolvimento na região, que ao longo do tempo se traduzirão em acordos e declarações oficiais de fortalecimento no setor cibernético.

Quanto às medidas de implantação efetiva do setor cibernético, a estratégia preza pelo condicionamento da compra de produtos de defesa somente em caso de transferência de tecnologia, incluindo parcerias em pesquisas (END, 2012, p. 45). Prevê, ainda, a alocação de recursos financeiros específicos de forma continuada, de modo que a inovação seja implantada dentro de agendas sólidas tanto na política quanto na área financeira. É possível visualizar o desdobramento de recursos financeiros para o setor cibernético a partir de pesquisas nas Leis de Orçamento Anuais (LOA) compreendidas entre os anos 2012-2016, conforme o quadro que se segue.

Tabela 2 - Recursos anuais destinados à Implantação do Sistema de Defesa Cibernética (em Milhões de R$). Brasil. LOA (2012 - 2016).

	2012	2013	2014	2015	2016
Despesas com a PND	83,6	90	70	96	42
Despesas com TI	28,5	67,5	7,4	1,1	0
Total	112,1 Mi	157,5 Mi	77,4 Mi	97,1 Mi	42 Mi

Fonte: http://www.orcamentofederal.gov.br/orcamentos-anuais

A END figura como documento norteador das ações para a implantação do setor, visando a consecução de autonomia e independência nacional no tocante a essa área de atuação. Consequência disso, o Ministério da Defesa, por intermédio da Diretriz Ministerial nº 14, de 9 de novembro de 2009, delegando ao Exército a responsabilidade de coordenação do Setor Cibernético do MD (POMPEU, 2012, p. 06). Para tanto, definiu em duas fases a estruturação do Setor, a saber:

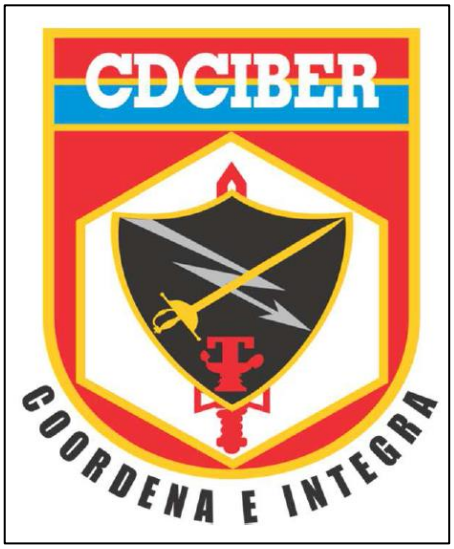
1ª fase - abrangência do tema e objetivos setoriais;

2ª fase – desdobramento dos objetivos setoriais em ações estratégicas.

5.2.3 Centro de Defesa Cibernética (CDCiber)

Em cumprimento ao prescrito na END, tendo como norte a Diretriz Ministerial n° 14-MD, por intermédio das Portarias do Comandante do Exército n° 666 e n° 667, de 4 de agosto de 2010, foi criado o Centro de Defesa Cibernética (CDCiber), Unidade militar responsável pelas atividades de coordenação e integração entre as Forças, ataque, defesa e exploração do espaço cibernético brasileiro. Foi incluído na estrutura regimental do Exército somente em 20 de setembro de 2012, por meio do Decreto Presidencial n° 7.809[33]. Possui instalações próprias e funciona no Quartel-General do Exército, em Brasília, contando com militares da Marinha, Exército e Aeronáutica, coordenados por um Estado-Maior Conjunto.

Figura 2 – Logo do Centro de Defesa Cibernética do Exército Brasileiro.



Fonte: http://www.cert.br/forum2014/slides/ForumCSIRTs2014-CDCiber.pdf

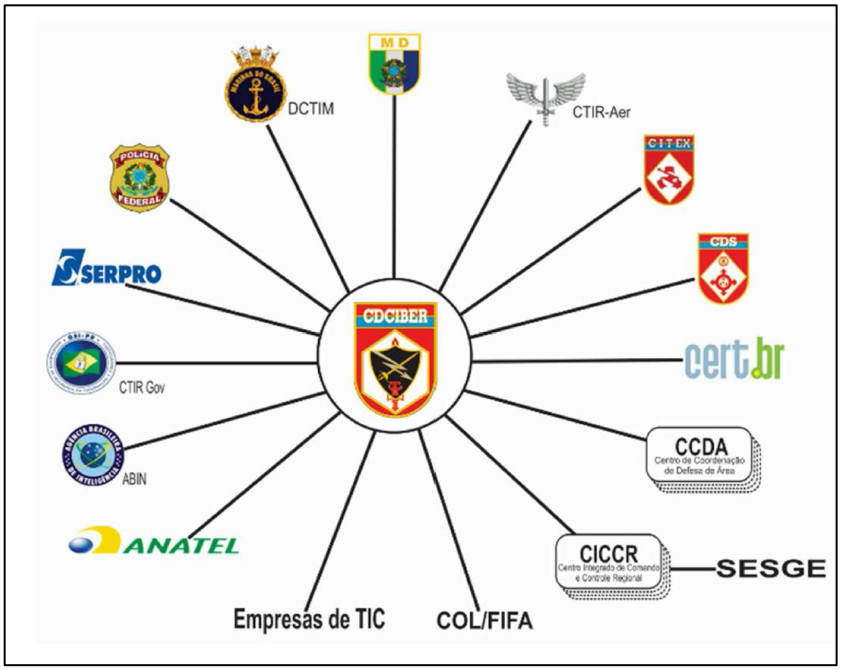
O CDCiber teve grande visibilidade por ocasião dos grandes eventos organizados em solo brasileiro, como a RIO+20, Copa das Confederações de 2013, Jornada Mundial da Juventude, Copa do Mundo da FIFA 2014 e, no corrente ano, atuará nas Olímpiadas Rio 2016.

---

[33] Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Decreto/D7809.htm

Quanto à sua atuação nos grandes eventos, é possível verificar alguns resultados do CDCiber em ações durante a Copa do Mundo de 2014, conforme foi exposto pelo Coronel José Ricardo Souza Camelo no 3° Fórum Brasileiro de CSIRTS[34]. A estratégia adotada pelo Centro consistiu em operar com treze destacamentos de defesa cibernética, um em cada capital anfitriã, sendo dois em Brasília. A atuação coordenada contou com a colaboração de diversos órgãos governamentais e empresas de TIC, atingindo um número de cento e doze militares e civis empregados, reflexo da interação exemplificada pela figura abaixo.

Figura 3 - Atuação colaborativa na Copa.



Fonte: http://www.cert.br/forum2014/slides/ForumCSIRTs2014-CDCiber.pdf

Entre os incidentes observados e tratados pelos destacamentos, merece destaque o caso de vazamento de informações da rede do Itamaraty, que resultou na divulgação de cerca de 500 documentos sigilosos contendo informações e contatos de autoridades, além do conteúdo de relatórios de corpos diplomáticos. A

[34] Disponível em: http://www.cert.br/forum2014/slides/ForumCSIRTs2014-CDCiber.pdf.

responsabilidade pelos ataques foi requerida pelo grupo hackitivista[35] *Anonymous*, como forma de retaliação contra a Copa[36].

Importante aquisição realizada pelo CDCiber consiste no Simulador de Operações de Guerra Cibernética (SIMOC), um programa de simulação de ambiente de conflito cibernético destinado para a preparação de recursos humanos para eventuais litígios em rede.

O SIMOC foi desenvolvido pela empresa RustCon[37], empresa brasileira de tecnologia e defesa responsável por diversos projetos em parceria com as FFAA. Desenvolvido com 100% de tecnologia nacional, o Simulador

> "(...) utiliza tecnologia de virtualização, que executa vários sistemas operacionais em um único equipamento, e componentes de software de código livre para atender aos requisitos identificados. Com isso, vamos gerar um produto completo no mesmo nível das principais soluções estrangeiras disponíveis no mercado. E ainda existe a vantagem de termos 100% do controle da solução" (Carlos Rust – presidente da RustCon)[38].

Entre os objetivos a serem alcançados com a adoção do SIMOC pode-se destacar a capacitação de recursos humanos para pronta resposta de proteção e defesa, treinamento com base em cenários realistas (desastres, invasão de infraestruturas críticas, etc), comparação de eficácia de ações diante diversas possibilidades de exploração do espaço cibernético.

---

[35] Hacking + ativismo político.
[36] Disponível em: http://www.parana-online.com.br/editoria/politica/news/803187/?noticia=INVASORES+VAZARAM+DOCUMENTOS+SECRETOS+DO+ITAMARATY. Acesso em 04 de junho de 2016.
[37] www.rustcon.com.br
[38] Disponível em: http://www.rustcon.com.br/portfolio/guerra-eletronica/. Acesso em 06 de junho de 2016.

Figura 4 – Simulador de Guerra Cibernética da RustCon.

Fonte: http://www.rustcon.com.br/portfolio/guerra-eletronica/

5.2.4 Política Cibernética de Defesa

Com a finalidade de nortear a atuação de defesa cibernética nos níveis estratégico, operacional, tático e de guerra cibernética, a Portaria Normativa nº 3.389/MD, de 21 de dezembro de 2012, aprovou a Política Cibernética de Defesa (PCD), que possui entre seus objetivos a manutenção e desenvolvimento da doutrina de emprego do Setor Cibernético.

A PCD aplica-se a todos os componentes do poder nacional envolvidos nas atividades de defesa cibernética, obedecendo sempre aos seguintes pressupostos básicos:

- Interação entre entidades e setores de defesa com a Academia, setores público e privado, e a base industrial de defesa;
- As atividades de Defesa Cibernética no MD são orientadas para atender às necessidades da Defesa Nacional;
- Harmonização entre o setor cibernético com a Política de Ciência, Tecnologia e Inovação para a Defesa Nacional (C,T&I);
- Conscientização da sociedade quanto à necessidade de uma cultura de segurança da informação;

- Correlação e dependência entre Defesa Cibernética e Segurança Cibernética, valorizando as ações individuais de SIC;
- As ações cibernéticas no contexto do MD visam a assegurar o uso do espaço cibernético, impedindo ou dificultando seu uso contra os interesses do País e garantindo, dessa forma, a liberdade de ação (PCD, 2012, p. 13/20).

O modelo brasileiro dá ênfase a cinco áreas prioritárias para a consolidação da defesa cibernética: recursos humanos, inteligência, operacionalidade, doutrina, ciência e tecnologia. A PCD, em seus objetivos, abarca esses cinco pontos, esboçando linhas gerais para seu alcance, conforme o quadro abaixo.

Tabela 3 – Diretrizes atinentes aos objetivos da Política Cibernética de Defesa.

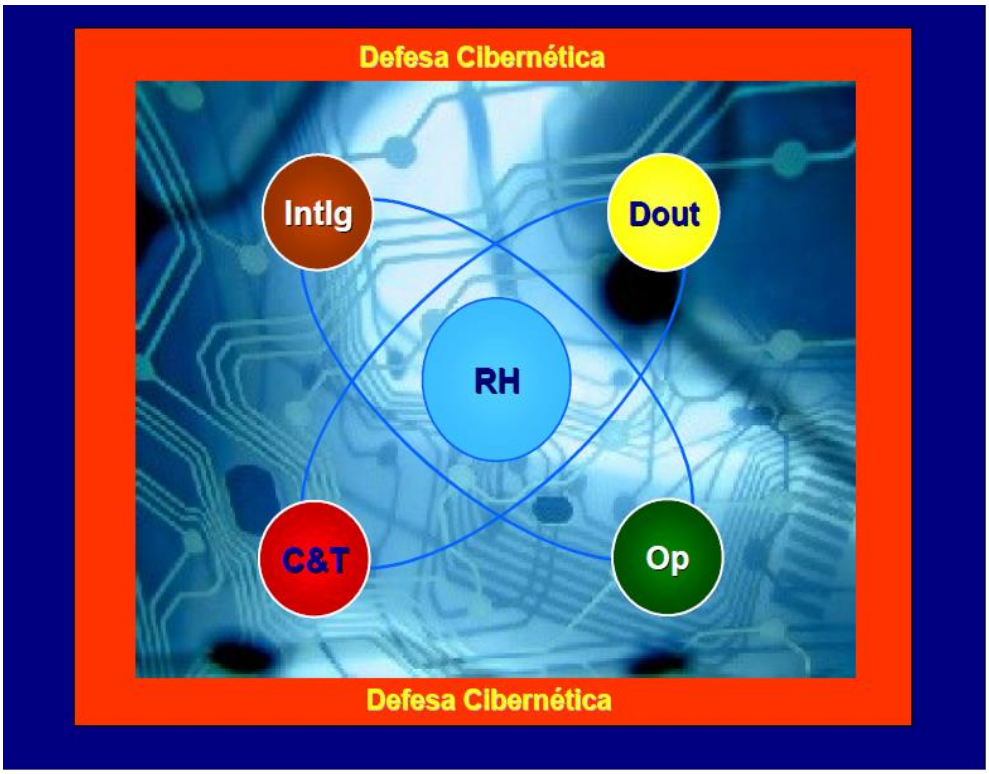
Objetivo Nr I - assegurar, de forma conjunta, o uso efetivo do espaço cibernético (preparo e emprego operacional) pelas Forças Armadas (FA) e impedir ou dificultar sua utilização contra interesses da Defesa Nacional;
Objetivo Nr II - capacitar e gerir talentos humanos necessários à condução das atividades do Setor Cibernético (St Ciber) no âmbito do MD;
Objetivo Nr III - colaborar com a produção do conhecimento de Inteligência, oriundo da fonte cibernética, de interesse para o Sistema de Inteligência de Defesa (SINDE) e para os órgãos de governo envolvidos com a SIC e Segurança Cibernética, em especial o Gabinete de Segurança Institucional da Presidência da República (GSI/PR);
Objetivo Nr IV - desenvolver e manter atualizada a doutrina de emprego do St Ciber;
Objetivo Nr V - implementar medidas que contribuam para a Gestão da SIC no âmbito do MD;
Objetivo Nr VI - adequar as estruturas de C,T&I das três Forças e implementar atividades de pesquisa e desenvolvimento para atender às necessidades do St Ciber;
Objetivo Nr VII - definir os princípios básicos que norteiem a criação de legislação e normas específicas para o emprego no St Ciber;
Objetivo Nr VIII - cooperar com o esforço de mobilização nacional e militar para assegurar a capacidade operacional e, em consequência, a capacidade dissuasória do St Ciber; e
Objetivo Nr IX - contribuir para a segurança dos ativos de informação da Administração Pública Federal (APF), no que se refere à Segurança Cibernética, situados fora do âmbito do MD.

(PCD, 2012, p. 15/20)

A Figura 5 retrata a convergência existente entre as prioridades do MD para o setor cibernético. Detalhe para a importância dada ao elemento “recurso humano”, central para o funcionamento e manutenção do projeto. A partir desses

elementos, as ações complementares adotadas pelo Estado brasileiro terão por base a potencialização de cada uma delas.

Figura 5 – Elementos prioritários para a Defesa Cibernética.



Fonte: CDCiber.

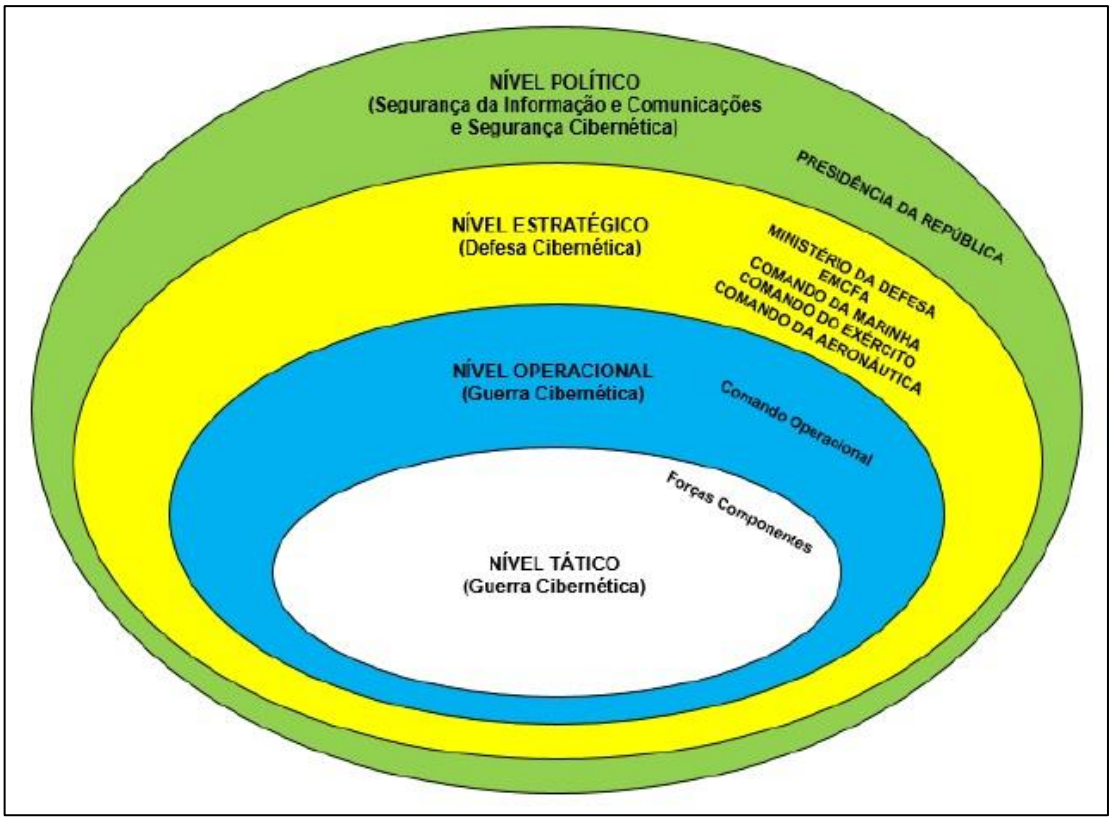
5.2.5 Doutrina Militar de Defesa Cibernética

Outra medida de grande importância para a unidade de pensamento sobre o tema, a Doutrina Militar de Defesa Cibernética, apresentada pela Portaria Normativa nº 3.010/MD de 18 de novembro de 2014, emerge como o documento-base para a atuação conjunta das Forças Armadas.

A Doutrina estabelece os níveis de decisão competentes para a autorização de ações no espaço cibernético, a saber: nível político, nível estratégico, nível operacional e tático. O nível político compreende o círculo de decisão a quem compete a atuação para provimento da segurança da informação e comunicação e segurança cibernética no âmbito da APF, a Presidência da República, orientada pelo DSIC-GSI/PR. A capacidade de decisão no âmbito estratégico refere-se às ações de defesa cibernética, ficando a cargo do Ministério da Defesa, seu Estado-Maior Conjunto das Forças Armadas, e Comando das FFAA. Apesar de a decisão partir de

atores políticos no primeiro escalão dessas instituições, toda a ação é feita em interação com a PR e a APF. Por último, o nível de decisão operacional e tático decide frente à iminência de uma guerra cibernética. Nesse caso as decisões se voltam para a atuação de ataque, defesa e exploração do espaço cibernético quando da existência de atores com intentos hostis à segurança nacional, tal qual ocorreu à Estônia, como este trabalho narra em páginas anteriores. A figura abaixo elucida de forma sistemática os níveis de decisão para ações no espaço cibernético.

Figura 6 – Níveis de Decisão.



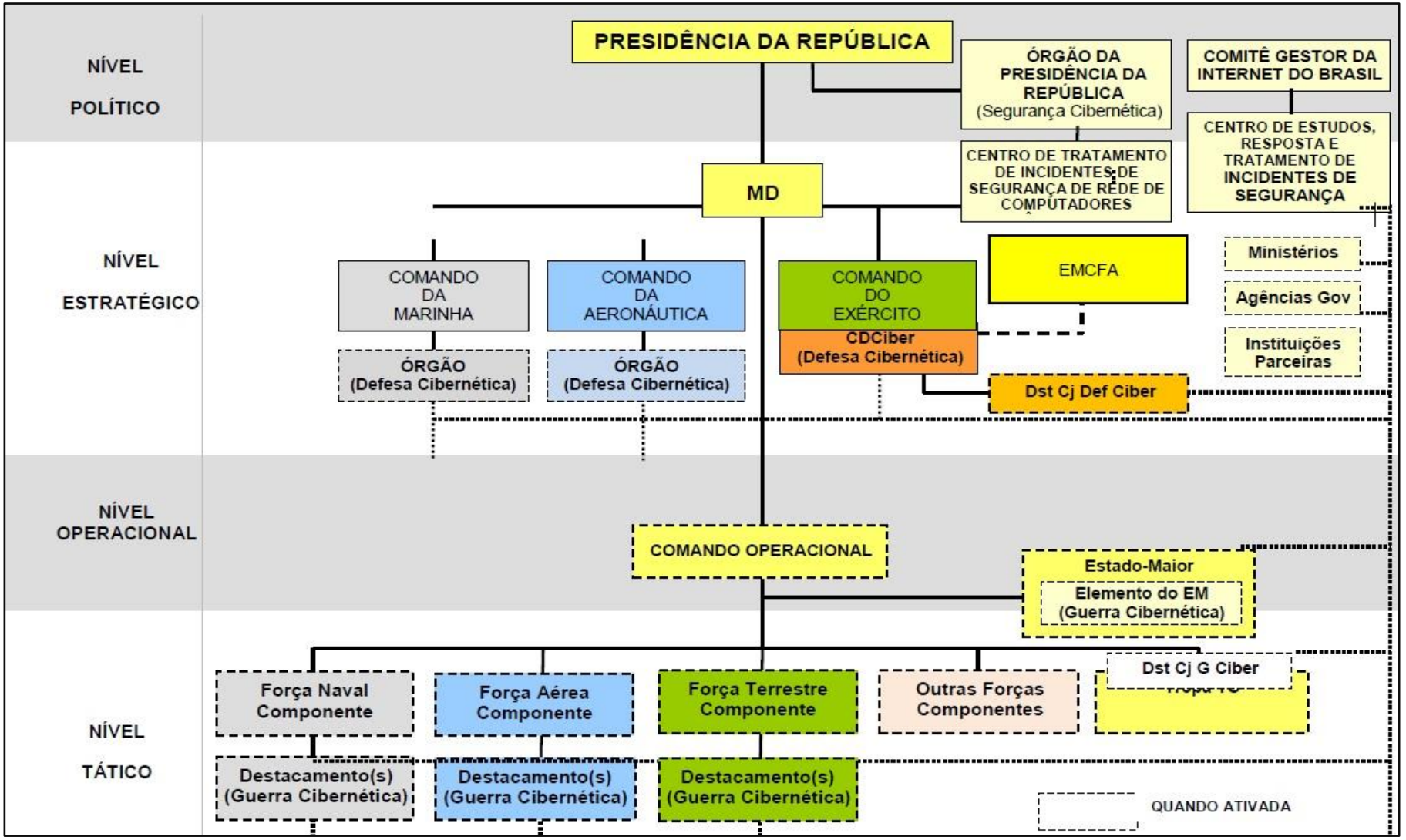
(Dout Mil Def Ciber, 2014, p. 17)

Todas essas instâncias compõem o Sistema Militar de Defesa Cibernética (SMDC), que compreende o “conjunto de instalações, equipamentos, doutrina, procedimentos, tecnologias, serviços e pessoal essenciais para realizar atividades de defesa no espaço cibernético” (Dout Mil Def Ciber, 2014, p. 25). Ao SMDC compete a coordenação e integração da segurança das infraestruturas críticas da informação definidas pelo Ministério da Defesa. A ele se somam militares e civis de diferentes áreas de atuação que, concomitantemente às suas atribuições, devem

sempre interagir pela manutenção do SMDC. Seu órgão central é o CDCiber, que mantém constante comunicação com os demais órgãos e instâncias do Sistema, cuja estrutura pode ser observada pelo organograma abaixo.

O SMDC figura como o objetivo maior de todo esse escopo de políticas e estratégias de governo, pois ele inclui elementos de segurança e defesa do ciberespaço, o que obrigatoriamente carece de interação entre atores da APF como um todo.

Figura 7 – Sistema Militar de Defesa Cibernética



(Dout Mil Def Ciber, 2014, Anexo)

5.2.6 Comando de Defesa Cibernética (ComDCiber)

Em 27 de outubro de 2014, o Ministério da Defesa resolveu, por intermédio da Portaria Normativa nº 2.777-MD, aprovar diretrizes visando à potencialização da Defesa Cibernética Nacional. Essas medidas se traduzem na criação do Comando de Defesa Cibernética e da Escola Nacional de Defesa Cibernética.

Essa diretriz foi acolhida, culminando na Portaria nº 001-Cmt Ex, de 02 de janeiro de 2015, que não só criou o ComDCiber já ativou seu Núcleo de funcionamento, um tipo de "embrião" da Organização que o Comando virá a ser.

O ComDCiber está subordinado ao CDCiber e ocupa as instalações do Comando Militar do Planalto, em Brasília. A intenção é que o Comando seja responsável pelo Sistema de Homologação e Certificação de Produtos de Defesa Cibernética, medida a ser desenvolvida em ato contínuo à reestruturação da Indústria Nacional de Defesa, conforme orienta a Estratégia Nacional de Defesa.

Essa Organização Militar será a responsável por todas as atividades e desdobramentos para a defesa cibernética em âmbito nacional, assim como é o USCyberComm para os EUA[39]. A implantação do Comando é recente e os primeiros militares começaram a ser lotados na Unidade no corrente ano, mas a previsão é que haja desdobramentos financeiros que permitam a consolidação do projeto para os próximos anos[40].

5.2.7 Escola Nacional de Defesa Cibernética (ENaDCiber)

Com datas de criação e ativação do Núcleo iguais ao do ComDCiber, a Portaria nº 002-Cmt Ex criou a Escola Nacional de Defesa Cibernética. Esse projeto visa cumprir as diretrizes da END e PCD, que determinam a capacitação de recursos humanos para a atuação de segurança e defesa do espaço cibernético brasileiro, além de operar o Observatório de Defesa Cibernética.

---

[39] www.cybercomm.mil
[40] Informações adquiridas pelo autor diretamente no Estado-Maior Conjunto de Defesa Cibernética do CDCiber.

Enquanto não são concluídas as instalações físicas, quadro de pessoal e estrutura interna da Escola, está em funcionamento o Instituto de Defesa Cibernética (IDCiber), responsável pela promoção e capacitação de civis e militares. O Instituto é fruto de uma parceria entre o CDCiber e a Universidade de Brasília, que em um primeiro momento proporcionam a formação de pessoal na modalidade à distância, orientando os interessados na área de segurança e defesa cibernética. Além disso, em uma visão de futuro, o IDCiber buscará formar quadros em diferentes níveis de especialização, presenciais e EAD, fortalecendo a cultura de segurança da informação no seio da sociedade, conforme proposta da END.

Figura 8 - Layout da página do IDCiber-UnB.

http://www.idciber-eb.unb.br/

5.2.8 Política Setorial de Defesa

Em 2015 o Ministério da Defesa lançou dois importantes documentos para a realização das ações estratégicas previstas na END. Pela Portaria Normativa n° 2.624 /MD de 07 dezembro de 2015, ficou instituída a Política Setorial de Defesa (PSD). O documento divide a atuação da Defesa em áreas temáticas, sendo uma delas, o setor cibernético. Cada área temática possui seus respectivos Objetivos Setoriais de Defesa (OSD) que, por sua vez, referem-se a cada uma das Ações Estratégicas abordadas na END.

Atentando para a importância da cibernética para a defesa nacional, o documento ressalta a necessidade de “(ODS 7) utilização efetiva do espaço cibernético pelo Ministério da Defesa e a negação de tal uso contra os interesses da defesa e segurança nacionais” (Pol Set Def, 2015, p.6). Esses objetivos dialogam diretamente com as ações estratégicas para a inteligência de defesa e segurança nacional, ambas estabelecidas pela END.

5.2.9 Estratégia Setorial de Defesa

Admitindo que a Política Setorial de Defesa aborde “o que fazer” para alcançar os objetivos preceituados na END, a Portaria Normativa n° 2.621 /MD de 07 de dezembro de 2015 estabelece a Estratégia Setorial de Defesa (ESD), que diz respeito ao “como fazer” para alcançar esses objetivos. Para isso, estabelece Ações Setoriais de Defesa (ASD).

Figura 9 – Ações Setoriais de Defesa – Cibernética.

CIBERNÉTICA	
OSD 7	**Utilização efetiva do espaço cibernético pelo Ministério da Defesa e a negação de tal uso contra os interesses da defesa e segurança nacionais.**
ASD 6	Implantar o Sistema Militar de Defesa Cibernética (SMDC).
ASD 7	Promover a interoperabilidade do setor cibernético na Defesa Nacional.
ASD 8	Criar e implantar o Comando de Defesa Cibernética.
ASD 9	Criar e implantar a Escola Nacional de Defesa Cibernética.
ASD 10	Criar e implantar o Sistema de Homologação e Certificação de Produtos de Defesa Cibernética.
ASD 11	Desenvolver o Observatório Nacional de Defesa Cibernética.
ASD 12	Capacitar e gerir recursos humanos necessários à condução das atividades do Setor Cibernético (St. Ciber) no âmbito da Defesa Nacional.
ASD 13	Implantar o Sistema de Informações Seguras, com enfoque na área de Segurança da Informação e Comunicações.
ASD 14	Contribuir para o fomento da pesquisa e do desenvolvimento de produtos de defesa cibernética.
ASD 15	Contribuir para a produção do conhecimento de inteligência oriundo da fonte cibernética.

(Estratégia Setorial de Defesa, 2015, p.14)

Entre as ações determinadas pela ESD, conforme citado anteriormente, algumas já estão concluídas, enquanto outras se encontram em fase de implantação. Entre as ações concluídas, porém em fase de aprimoramento, destaque para a criação do ComDCiber e ENaDCiber. As demais ações dependem de questões orçamentárias e procedimentais.

6 CONSIDERAÇÕES FINAIS

Diante do exposto na primeira seção do trabalho, fica claro o interesse de variados atores pelo espaço cibernético, local onde as ações ofensivas e defensivas passam a figurar as disputas por controle e manipulação do espaço real. A sociedade da informação se depara com a necessidade de seguir seu ciclo evolutivo paralelamente à necessidade de autopreservação, que reside nas garantias desse novo ambiente de interação.

O ciberespaço pode ser compreendido a partir de sua funcionalidade ambígua: como facilitador da difusão de boas práticas democráticas (e-Gov, mecanismos de accountability, etc) e, contra as mesmas, como canal para a interrupção desses serviços. A exploração do espaço cibernético por atores com intenções hostis fomenta a necessidade de se pensar a sua segurança. Os casos ocorridos na Estônia e na Síria, e mesmo os supostos casos de ataques ao setor energético brasileiro, ajudam a compreender a elevada capacidade de conferir danos que reside em ataques assimétricos, como os apresentados, onde um único ator, munido de tecnologia e intenção hostil, é capaz de causar prejuízos em larga escala, desde a segurança pública até setores estratégicos como os setores energéticos e de abastecimento de água. Outra característica que suscita a atenção de governos é a possibilidade de ações no espaço cibernético antecederem operações militares, contribuindo para seu êxito, como ficou evidente na segunda investida dos EUA no Iraque, em 2003.

Analisando as ações voltadas para a segurança e defesa cibernética enquanto políticas de Estado, o papel do governo/instituições enquanto detentores da premissa de formulação e implementação de políticas públicas merece destaque. No caso de medidas para o espaço cibernético, é clara a centralidade que reside no papel das instituições para a consecução desses objetivos. Os indivíduos que compõem as instituições, dotados de conhecimento técnico específico, ajudam a demarcar as possibilidades e limites das políticas, atuando em conjunto com interlocutores diversos, que vão da sociedade civil até grupos empresariais munidos de interesses meramente econômicos. Essas concepções possuem ligação com a

teoria de Willians Jenkins (1978) quando este afirma serem as *policies* o resultado de processos burocráticos e complexos nascidos no interior do governo.

O governo brasileiro tem depreendido esforços consideráveis para alcançar o objetivo de possuir um espaço cibernético seguro, bem como estar preparado para defendê-lo caso se faça necessário, de modo à reestabelecer sua seguridade. Admitindo a separação conceitual entre segurança e defesa abordada pelos formuladores das políticas para a cibersegurança no Brasil, a Presidência da República, atuando por intermédio do Departamento de Segurança da Informação e Comunicações, figura como ator central no que compete a segurança cibernética no âmbito da APF. Sua atribuição possui larga escala, alcançando setores públicos a privados, estes, em constante comunicação e interação. As propostas lançadas pelo Departamento visam alcançar certo grau de maturidade em segurança cibernética, a partir do fomento de uma "cultura de segurança", que passa pelos seguintes pontos: incluir na educação uma disciplina sobre o tema; fortalecimento e fomento de proteção de ICs e ICIs, a cibersegurança na APF, indução de boas práticas; manter um debate contínuo sobre o tema com a Academia; institucionalizar o tema no âmbito do governo; e incluir no orçamento do governo recursos exclusivos para a manutenção e aprimoramento do setor cibernético.

Quanto à defesa cibernética, figuram como atores centrais ao processo de adoção dessas políticas o Ministério da Defesa e o Exército Brasileiro. Já se passaram mais de dez anos desde que o termo "defesa cibernética" assumiu lugar de destaque nos principais documentos norteadores da defesa nacional. Os alcances tem se mostrado promissores, com políticas e estratégias específicas para a área, além da reformulação de parte da indústria de defesa brasileira. As principais mudanças se dão na estrutura regimental do Exército que, historicamente destacado pelo aprimoramento e emprego do combate convencional (cinético), a Força se viu diante do desafio de repensar seus quadros, inserindo dentro da lógica militar as tecnologias de informação e comunicação em graus elevados, criando um Centro específico para o tratamento de incidentes que ameacem a defesa nacional.

A criação do Comando de Defesa Cibernética, bem como a Escola Nacional de Defesa Cibernética, deixam claras as intenções do Brasil enquanto ator

que busca ser uma potência no cenário internacional. A partir dessas medidas o país poderá ascender ao papel de protagonista sobre o assunto, uma vez que iniciou uma política isenta de influência tecnológica estrangeira, sendo 100% nacional. Essa condição facilita a ascensão do Brasil posto de difusor de políticas de segurança e defesa cibernética, como já se estabeleceu em relação a políticas de transferência condicionada e orçamento participativo. A Estratégia Nacional de Defesa revela essa intenção, estipulando condições para que haja intercâmbio de conhecimento com países amigos, sendo uma delas a transferência de tecnologia.

Pode-se concluir que tanto as políticas de segurança quanto as de defesa cibernética fazem parte do objetivo maior da agenda brasileira: a implantação de um Sistema de Defesa Cibernética. Nele, tanto a APF quanto organizações militares convergem para objetivos comuns, uma vez que representam a complementaridade intrínseca aos próprios termos “segurança” e “defesa”.

Portanto, o Brasil parece ter compreendido a necessidade de prover a segurança e defesa do seu ciberespaço como vetor de desenvolvimento e ascensão internacional. O fomento da pesquisa científica com vistas à tecnologia e inovação se mostram centrais para que o projeto de solidificação do setor cibernético. Os primeiros passos foram dados e espera-se que o projeto resista às mudanças políticas e orçamentárias que a Defesa sempre está passiva de sofrer.

REFERÊNCIAS BIBLIOGRÁFICAS

ABRAMSON, M; MEANS, G. E. E-Government 2001 IBM Endowment for the Bussiness of Government. Rowman & Littlefield Publishers, Inc. 2001.

BRASIL. Conselho de Defesa Nacional. Portaria n° 34-CDN/SE, de 05 de agosto de 2009.

_____. Constituição (1988). Constituição da República Federativa do Brasil; Promulgada em 5 de outubro de 1988: atualizada até a Emenda Constitucional nº 67, de 22 de dezembro de 2010. Disponível em: < http://www.planalto.gov.br/ ccivil_03/Constituicao/Constituicao.htm>. Acesso em: 01 de junho de 2016.

_____. Decreto nº 5.484, de 30 de junho de 2005. Aprova a Política de Defesa Nacional, e dá outras providências. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 1º de julho de 2005.

_____. Decreto nº 5.484, de 30 de junho de 2005. Aprova a Política de Defesa Nacional, e dá outras providências. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 1º de julho de 2005.

_____. Decreto nº 5.772, de 8 de maio de 2006. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Gratificações de Exercício em Cargo de Confiança do Gabinete de Segurança Institucional da Presidência da República, e dá outras providências. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 9 de maio de 2006.

_____. Decreto nº 6.703, de 18 de dezembro de 2008. Aprova a Estratégia Nacional de Defesa, e dá outras providências. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 19 de dezembro de 2008.

_____. Decreto nº 7.411, de 29 de dezembro de 2010. Dispõe sobre remanejamento de cargos em comissão do Grupo-Direção e Assessoramento Superiores - DAS, aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Gratificações de Exercício em Cargo de Confiança do GSI-PR, e dá outras providências. DOU. Brasília, DF, 30 de dezembro de 2010.

_____. Decreto nº 7.809, de 20 de setembro de 2012. Altera os Decretos nº 5.417, de 13 de abril de 2005, nº 5.751, de 12 de abril de 2006, e nº 6.834, de 30 de abril de 2009, que aprovam as estruturas regimentais e os quadros demonstrativos dos cargos em comissão e das funções gratificadas dos Comandos da Marinha, do Exército e da Aeronáutica, do MD. DOU. Brasília, DF, 21 de setembro de 2012.

_____. Exército Brasileiro. Portaria nº 001-Cmt Ex, de 02 de janeiro de 2015.

_____. Exército Brasileiro. Portaria nº 002-Cmt Ex, de 02 de janeiro de 2015.

_____. Exército Brasileiro. Comandante do Exército. Portaria nº 666, de 4 de agosto de 2010. Cria o Centro de Defesa Cibernética do Exército e dá outras providências. Boletim do Exército nº 31. Brasília, DF, 6 de agosto de 2010.

_____. Exército Brasileiro. Comandante do Exército. Portaria nº 667, de 4 de agosto de 2010. Ativa do Núcleo do Centro de Defesa Cibernética do Exército e dá outras providências. Boletim do Exército nº 31. Brasília, DF, 6 de agosto de 2010.

_____. Gabinete de Segurança Institucional da Presidência da República. Portaria nº 2, de 8 de fevereiro de 2008. Institui Grupos Técnicos de Segurança de Infraestruturas Críticas (GTSIC) e dá outras providências. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 11 de fevereiro de 2008.

_____. Guia de Referência para a Segurança das Infraestruturas Críticas da Informação. v.01. Brasília. Gabinete de Segurança Institucional da Presidência da República. 2010a. Disponível em: http://dsic.planalto.gov.br/documentos/publicacoes/2_Guia_SICI.pdf

_____. Lei nº 9.649, de 27 de maio de 1998. Dispõe sobre a organização da Presidência da República e dos Ministérios, e dá outras providências. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 5 de junho de 1998. BRASIL.

_____. Livro Verde: segurança cibernética no Brasil. Claudia Canongia e Raphael Mandarino Junior (org.). Brasília: GSIPR/SE/DSIC. 2010b. Disponível em: http://dsic.planalto.gov.br/documentos/publicacoes/1_Livro_Verde_SEG_CIBER.pdf.

_____. Medida Provisória nº 2.216-37, de 31 de agosto 2001. Altera dispositivos da Lei no 9.649, de 27 de maio de 1998, que dispõe sobre a organização da Presidência da República e dos Ministérios, e dá outras providências. Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 1 de setembro de 2001.

_____. Ministério da Defesa. Diretriz Ministerial nº 14. Integração e Coordenação dos Setores Estratégicos da Defesa. Brasília, DF, 9 de novembro de 2009.

_____. Ministério da Defesa. Exército Brasileiro. Estado-Maior do Exército. Minuta de Nota de Coordenação Doutrinária relativa ao I Seminário de Defesa Cibernética do Ministério da Defesa. Brasília, 2010. p.9.

_____. Ministério da Defesa. Glossário das Forças Armadas – MD35-G-01.

_____. Ministério da Defesa. Portaria nº 3.028, de 14 de novembro de 2012. Atribui ao Centro de Defesa Cibernética (CDCiber), do Comando do Exército, a responsabilidade pela coordenação e integração das atividades de defesa cibernética, no âmbito do Ministério da Defesa (MD). Diário Oficial [da] República Federativa do Brasil. Brasília, DF, 20 de novembro de 2012.

_____. Ministério da Defesa. Portaria Normativa nº 2.777-MD, de 27 de outubro de 2014.

_____. Ministério da Defesa. Portaria Normativa nº 3.010/MD, de 18 de novembro de 2014.

_____. Ministério da Defesa. Portaria Normativa nº 3.389/MD, de 21 de dezembro de 2012.

_____. Ministério da Defesa. Portaria Normativa nº 2.624/MD, de 07 de dezembro de 2015.

_____. Ministério da Defesa. Portaria Normativa nº 2.621/MD, de 07 de dezembro de 2015.

CARNEIRO, João Marinonio Enke. A Guerra Cibernética: uma proposta de elementos para formulação doutrinária no Exército Brasileiro / João Marinonio Enke Carneiro. 2012. 203 f. : il ; 30 cm. Tese (Doutorado) – Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2012.

CASTELLS, Manuel. A Era da Informação: economia, sociedade e cultura, vol. 3, São Paulo: Paz e terra, 1999.

CLARKE, Richard A.; KNAKE, Robert K. Cyber War: the next threat to national security and what to do about it. 2. ed. New York: HarperCollins, 2012.

DAHL, Robert. Análise política moderna. Brasília: Editora UNB, 1988.

DANTAS, Marcos. A lógica do capital informação: monopólio e monopolização dos fragmentos num mundo de comunicações globais. Rio de Janeiro: Contraponto, 1998.

DYE, Thomas D. Understanding Public Policy. Englewood Cliffs, N.J.: Prentice-Hall. 1984.

EASTON, D. A Framework for Political Analysis. Englewood Cliffs: Prentice Hall.

FERNANDES, A. G. E-governo: o que já fazem estados e municípios. Informe-se [on-line] nº 20, out. de 2000.

HALL, Peter. ; TAYLOR, Rosemery. C. R. As três visões do Neo Institucionalismo. Lua Nova, n. 58, p. 193-223, 2003.

HOWLETT, Michael Patrick. Studying public policy: policy cycles and policy subsystems. Oxford University, 1955.

LASWELL, H.D. Politics: Who Gets What, When, How. Cleveland, Meridian Books. 1936/1958.

LINDBLOM, Charles E. “Still Muddling, Not Yet Through”, Public Administration.

_____. “The Science of Muddling Through”, Public Administration.

LYNN, L. E. Designing Public Policy: A Casebook on the Role of Policy Analysis. Santa Monica, Calif.: Goodyear. 1980.

MANDARINO Jr, Raphael. Um Estudo sobre a Segurança e a Defesa do Espaço Cibernético. Monografia em Especialização em Ciência da Computação: Gestão da Segurança da Informação e Comunicações. Brasília, Universidade de Brasília-UnB.

2009. Disponível em: http://dsic.planalto.gov.br/documentos/cegsic/monografias_1_turma/raphael_mandarino.pdf.

_____. Segurança e a Defesa do Espaço Cibernético Brasileiro. Recife: Cuzbac, 2010. 182p.: il.

MEAD, L. M. “Public Policy: Vision, Potential, Limits”, Policy Currents, Fevereiro: 1-4. 1995.

OLIVEIRA, Antônio Francisco Maia; BAZI Rogério Eduardo Rodrigues. Revista Digital de Biblioteconomia e Ciência da Informação, Campinas, Vol 5, n. 2, p.115-131, jul./dez. 2007.

PETERS, B. G. American Public Policy. Chatham, N.J.: Chatham House. 1986.

POMPEU, Alessandro. A Estratégia Nacional de Defesa e o Setor Cibernético. XI Ciclo de Estudos Estratégicos. Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2012.

SABATIER, Paul e JENKINS-SMITH, Hank. Policy Change and Learning: The Advocacy Coalition Approach. Boulder: Westview Press. 1993.

SHEPSLE, Kenneth A. Rational choice institutionalism. In: RHODES, R. A. W.; BINDER, S. A.; ROCKMAN, B. A. (Orgs.). The Oxford book of political institutions. Oxford: Oxford University Press, 2008.

SIMON, Herbert. Comportamento Administrativo. Rio de Janeiro: USAID. 1957.

SKOCPOL, Theda. Bringing the State back in: Strategies of analysis in current research. In: EVANS, P.; RUESCHMEYER, D.; SCOKPOL, T. Bringing the State back in. New York: Cambridge University Press, 1985.

SOUZA, Celina. Public Policy: a revision of literature. Revista Sociologias, Porto Alegre, ano 8, n° 16, jul/dez 2006, p. 20-45.

SOUZA, Gills Lopes Macêdo. Reflexos da digitalização da guerra na política internacional do século XXI: uma análise exploratória da securitização do ciberespaço nos Estados Unidos, Brasil e Canadá / Gills Lopes Macêdo Souza. – Recife: O autor, 2013.

STEINMO, S.; THELEN, K.; LONGSTRETH, F. Structuring politics: historical institutionalism in comparative analysis. New York, Cambridge University, 1992. 257.

TOFFLER, Alvin; TOFFLER, Heidi. Guerra e Anti-Guerra. Livros do Brasil, Lisboa, 1994.