UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE FILOSOFIA E CIÊNCIAS HUMANAS
DEPARTAMENTO DE CIÊNCIA POLÍTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA POLÍTICA
MESTRADO EM CIÊNCIA POLÍTICA

GILLS LOPES MACÊDO SOUZA

REFLEXOS DA DIGITALIZAÇÃO DA GUERRA NA POLÍTICA INTERNACIONAL DO SÉCULO XXI: UMA ANÁLISE EXPLORATÓRIA DA SECURITIZAÇÃO DO CIBERESPAÇO NOS ESTADOS UNIDOS, BRASIL E CANADÁ

RECIFE
2013

GILLS LOPES MACÊDO SOUZA

REFLEXOS DA DIGITALIZAÇÃO DA GUERRA NA POLÍTICA INTERNACIONAL DO SÉCULO XXI: UMA ANÁLISE EXPLORATÓRIA DA SECURITIZAÇÃO DO CIBERESPAÇO NOS ESTADOS UNIDOS, BRASIL E CANADÁ

Dissertação de Mestrado Acadêmico apresentada como requisito obrigatório para a obtenção do título de Mestre em Ciência Política – área de concentração em "Relações Internacionais" – pelo Programa de Pós-Graduação em Ciência Política da Universidade Federal de Pernambuco (PPGCP-UFPE).
Orientador: Prof. Dr. Marcelo de Almeida Medeiros.

RECIFE
2013

Catalogação na fonte

Bibliotecária, Divonete Tenório Ferraz Gominho, CRB4- 985

S729r 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.
133 f.,: il. ; 30 cm.

Orientador: Prof. Dr. Marcelo de Almeida Medeiros.
Dissertação (mestrado) – Universidade Federal de Pernambuco, CFCH. Programa de Pós-Graduação em Ciência Política, 2013.
Inclui bibliografia, anexo e apêndices.

1. Ciência Política. 2. Cibernética. 3. Política Internacional. 4. Ciberespaço - Securitização. I. Medeiros, Marcelo de Almeida. (Orientador). II. Titulo.

320 CDD (22.ed.) UFPE (BCFCH 2013-25)

Ata da Reunião da Comissão Examinadora para julgar a Dissertação do aluno **GILLS LOPES MACEDO SOUZA**, intitulada: "**REFLEXOS DA DIGITALIZAÇÃO DA GUERRA NA POLÍTICA INTERNACIONAL DO SÉCULO XXI: UMA ANÁLISE EXPLORATÓRIA DA SECURITIZAÇÃO DO CIBERESPAÇO NOS ESTADOS UNIDOS, BRASIL E CANADÁ"**, para obtenção do grau de Mestre em Ciência Política.

Às 10:00 horas do dia 20 de fevereiro de 2013, no Auditório do Programa de Pós-Graduação em Ciência Política da Universidade Federal de Pernambuco, reuniram-se os membros da Comissão Examinadora para defesa de Dissertação do Mestrando **GILLS LOPES MACEDO SOUZA**, intitulada: "**REFLEXOS DA DIGITALIZAÇÃO DA GUERRA NA POLÍTICA INTERNACIONAL DO SÉCULO XXI: UMA ANÁLISE EXPLORATÓRIA DA SECURITIZAÇÃO DO CIBERESPAÇO NOS ESTADOS UNIDOS, BRASIL E CANADÁ"**, para obtenção do grau de Mestre em Ciência Política, composta pelos professores doutores: **MARCELO DE ALMEIDA MEDEIROS** (Orientador), **RICARDO BORGES GAMA NETO** (Examinador Titular Interno) e **JOSÉ ALEXANDRE FERREIRA FILHO** (Examinador Titular Externo). Sob a presidência do primeiro, realizou-se a arguição do candidato **GILLS LOPES MACEDO SOUZA**. Cumpridas todas as disposições regulamentares, a Comissão Examinadora considera a Dissertação **APROVADA COM DISTINÇÃO**. E nada mais havendo a tratar, eu, Daniel Neto Bandeira, secretário do Programa de Pós-Graduação em Ciência Política da Universidade Federal de Pernambuco, lavrei a presente Ata que dato e assino com os membros da Comissão Examinadora. Recife, 20 de fevereiro de 2013.

_____

DANIEL NETO BANDEIRA (Secretário)

_____

Prof. Dr. **MARCELO DE ALMEIDA MEDEIROS** (Orientador)

_____

Prof. Dr. **RICARDO BORGES GAMA NETO** (Examinador Titular Interno)

_____

Prof. Dr. **JOSÉ ALEXANDRE FERREIRA FILHO** (Examinador Titular Externo)

_____

GILLS LOPES MACEDO SOUZA (Aluno)

Dedico às memórias de
Ayrton Senna, Sérgio Vieira
de Mello e Jaime Lopes,
provas de que meus heróis
não morreram de *overdose*.

AGRADECIMENTOS

Ao meu Orientador, prof. Marcelo de Almeida Medeiros (CP-UFPE), por todas as oportunidades dadas a mim, ao longo desses dois anos, e por nunca ter negado uma orientação, seja ela acadêmica, profissional ou pessoal.

Aos membros da Banca Examinadora: professores Ricardo Borges (CP-UFPE), José Alexandre Ferreira Filho (DEA/UNICAP), Enivaldo Rocha (CP-UFPE) e Eugênia Barza (CCJ/UFPE), por acreditarem no potencial deste trabalho. Ao prof. Rafael Villa (RI-USP), pelas críticas construtivas, quando da Banca de Qualificação.

Aos que, enviando-me textos das mais diversas áreas, ajudaram a moldar este trabalho: Antonio Henrique Lucena Silva (CP-UFF), prof. Augusto Wagner M. Teixeira Jr (RI-UFPB), Elton Gomes (CP-UFPE), Igor Daniel P. Acácio (CP-UERJ), prof. Marcos Alan Ferreira (RI-UFPB), prof. Marcos A. Guedes de Oliveira (CP-UFPE), prof. Paulo Kuhlmann (RI-UEPB) e Rodrigo Albuquerque (CP-UFPE).

Sou grato também à Força de Peterson F. da Silva (RI-USP), à ajuda de Tiago Freire (SERPRO-PB) e à atenção dos professores Amanda Aires (UFPE), Andrea Steiner (UFPE), Jonathan Paquin (*Université Laval*, Canadá) e Marcus André Melo (UFPE).

Ao prof. Joseph S. Nye (*Harvard University*, EUA), pelo envio de seus textos.

Ao prof. Kevin Newmeyer (*National Defense University* – NDU, EUA) pela atenção.

Aos entrevistados: Leonard Kleinrock (*University of California, Los Angeles* – UCLA, EUA), prof. André Martin (USP, Brasil), prof. Alan Woodward (*University of Surrey*, Inglaterra), prof. Rudibert Kilian Jr. (Escola de Guerra Naval, Brasil), prof. Eduardo Guerra (ITA, Brasil), prof. Walfredo Ferreira Neto (AMAN, Brasil), prof. Érico Duarte (UFRGS, Brasil), prof. Gunther Rudzit (FIRB, Brasil) e Emanuel Rodrigues (Brasil).

Ao prof. Antonio Jorge Ramalho da Rocha (RI-UnB), pelas críticas a meu artigo apresentado no 6º Seminário sobre Livro Branco de Defesa Nacional do Ministério da Defesa.

Ao prof. Colin S. Gray (*University of Reading*, Inglaterra) que, mesmo sem obrigação, respondeu meu *e-mail*, enfatizando que estava produzindo trabalho sobre estratégia e ciberespaço para o *U.S. Army* e que, por isso, não poderia omitir opiniões sobre o assunto.

Ao Núcleo de Estudos de Política Comparada e Relações Internacionais (NEPI/UFPE/CNPq) e ao Programa de Pós-Graduação em Ciência Política da UFPE (PPGCP-UFPE), pela imprescindível infraestrutura acadêmica.

Aos Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), Organização dos Estados Americanos (OEA) e *Center for Hemispheric Defense Studies* da *National Defense University* (CHDS/NDU), pelo apoio financeiroinstitucional.

Sou deveras grato também a Nicolas Diotte e ao *Ministère des affaires étrangères et Commerce international Canada* (MAECI), por me proporcionar um período-sanduíche no *Institut québécois des hautes études internationales* (HEI) da *Université Laval*, em Québec.

Aos meus professores da Graduação em Redes de Computadores, no Instituto Federal de Educação, Ciência e Tecnologia da Paraíba (IFPB), pelos conhecimentos técnicos, na pessoa do prof. Thiago Gouveia.

À minha família Lopes, principalmente a meu padrinho, prof. Roberto Sidnei A. Macedo (UFBA), por "pré-orientar" este trabalho, ainda quando o mesmo não passava de um rabisco num papel.

E, em especial, às eternas mulheres da minha vida: Lita Lopes, Rhana Lopes, Mariinha Lopes e Dalliana Vilar (Lopes), por tudo.

Sem vocês, jovens, eu não teria conseguido.

A partir do momento em que a gente fica dependente das redes de computadores, tudo é possível. (General José Carlos dos Santos, comandante do CDCiber, *apud* SÁ, 2012).

[...]nada substitui o envolvimento do povo brasileiro no debate e na construção da sua própria defesa. (BRASIL, 2008a).

RESUMO

O tema deste trabalho gira em torno dos impactos da securitização militar do ciberespaço na política internacional do século XXI. Escolhe-se como objeto de estudo a defesa cibernética, justamente por ela possibilitar inferências sobre a materialização politicoinstitucional de tal temática, buscando-se sustentação na teoria da securitização, proposta pela Escola de Copenhague. Nesse sentido, a presente Dissertação objetiva: (i) identificar as principais ameaças (ciber)existenciais para o setor militar, revelando o porque de esse processo se intensificar no século XXI; (ii) projetar quais as condições para tal securitização; e (iii) explicar os efeitos dela na política internacional, com fulcro nos casos estadunidense, brasileiro e canadense. Para tal, engendra-se o Espectro da Securitização Militar do Ciberespaço (ESMC), um *framework* de análise baseado na teoria da securitização com foco na defesa cibernética num determinado tempo e espaço. Quanto à revisão da literatura, autores brasileiros e estrangeiros de Ciência Política e de Relações Internacionais figuram majoritariamente no corpo deste trabalho. No que se refere à metodologia, utilizam-se a lógica dedutiva popperiana e o estilo qualiquantitativo de análise, no que pese à utilização de entrevistas, estudos de caso, análise de discursos e documentos, bem como o auxílio de *softwares*. Sua conclusão busca corroborar a hipótese de que, além de haver a securitização do ciberespaço pelo setor militar, tal processo tem reflexos na política internacional hodierna. Como consequência, é possível situar os três casos aqui selecionados no ESMC.

Palavras-chave: Defesa cibernética. Política Internacional e Comparada. Espectro da Securitização Militar do Ciberespaço.

ABSTRACT

The theme of this work revolves around the impacts of the cyberspace's military securitization on 21st century international politics. It is chosen as object of study the cyber defense, precisely because it is both the political and institutional materialization of this phenomenon. It is understood that from the moment that Information features an Age or a society, it becomes relevant to comprehend some of its political effects. For this, it seeks support on the securitization theory, proposed by the Copenhagen School. In this sense, this thesis aims to: (i) identify the main (cyber) existential threats to the military sector, revealing the reasons this process intensifies in the 21st century, (ii) designing the conditions for such securitization, and (iii) understand its effects on the international politics, paying special attention to the U.S., Brazilian and Canadian cases. To that end, the Spectrum of Cyberspace's Military Securitization is created. Regarding the literature review, the Political Science and / or International Relations' authors appear mostly in this work's body. As regards the methodology, it uses the Popperian deductive logic and both qualitative and quantitative analysis styles, albeit the use of interviews, case studies, speech and documents analysis, as well as the help of software. Its conclusion seeks to corroborate the hypothesis that, besides having the cyberspace by the military sector, such a process can have repercussions in nowadays international politics today.

Keywords: *Cyber defense*. *International and comparative politics*. *Spectrum of Cyberspace's Military Securitization*.

RÉSUMÉ

Le thème de ce travail tourne autour de l'impact de la sécurisation militaire du cyberespace dans la politique internationale du XXIe siècle. Il est choisi comme objet d'étude la cyberdéfenseprécisément parce qu'elle permet des inférences sur l'expression institutionnelle de ce thème, visant à soutenir la théorie de sécurisation, proposé par l'École de Copenhague. En ce sens, cette thèse vise à: (i) identifier les principales menaces (cyber) existentiels de les militaires pour révéler la raison de ce processus se révèle dans le XXIe siècle, (ii) concevoir ce que les conditions de la sécurisation, et (iii) expliquer ces effets dans la politique internationale, basées sur les cas américaine, canadienne et brésilienne. À cette fin, il est engendré le Spectre de la Sécurisation Militaire du Cyberespace (ESMC), un cadre d'analyse basé sur la théorie de sécurisation concentrant sur la cyberdéfense en un moment et dans um espace donnés. En ce qui concerne l'examen de la littérature, les auteurs brésiliens et étrangers de sciences politiques et de relations internationales contenues dans le corps de ce travail. En ce qui concerne la méthodologie, il est utilisé la logique déductive de Popper et de style qualiquantitatif, principalement au moyen d'entrevues, études de cas, l'analyse des discours et des documents, ainsi que l'aide des logicieux. Sa conclusion vise à corroborer l'hypothèse selon laquelle, en plus d'avoir la sécurisation du cyberespace par les militaires, ce processus se traduit dans la politique internationale aujourd'hui. Par conséquent, il est possible de situer les trois cas sélectionnés ici au ESMC.

***Mots clés** : Cyberdéfense. Politique internationale et comparée. Spectre de la Sécurisation Militaire du Cyberespace.*

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ARPA	*U.S. Advanced Research Projects Agency*
ARPANET	*Advanced Research Projects Agency Network*
BRA-AMAN	Academia Militar das Agulhas Negras
BRA-CCOMGEX	Centro de Comunicações e Guerra Eletrônica do Exército [Brasileiro]
BRA-CDCiber	Centro de Defesa Cibernética do Exército [Brasileiro]
BRA-EB	Exército Brasileiro
BRA-END	Estratégia Nacional de Defesa [do Brasil]
BRA-ITA	Instituto Tecnológico de Aeronáutica
BRA-PCD	Política Cibernética de Defesa [do Brasil]
BRA-MD	Ministério da Defesa [do Brasil]
BRA-Nu CDCiber	Núcleo do Centro de Defesa Cibernética do Exército
BRA-SMDC	Sistema Militar de Defesa Cibernética [do Brasil]
CAN-CCRIC	*Centre canadien de réponse aux incidents cybernétiques*
CAN-CSCC	*Un cadre de sécurité civile pour le Canada*
CAN-MD	*Ministère de la Défense nationale et les Forces canadiennes*
CAN-SCC	*Stratégie de cybersécurité du Canada*
CAN-SNIE	*Stratégie nationale sur les infrastructures essentielles*
CERN	*Conseil Européen pour la Recherche Nucléaire*
CERT	*Computer Emergency Response Team*
C&T	Ciência e Tecnologia
CrySyS	*Laboratory of Cryptography and System Security at Budapest University of Technology and Economics*
DDoS	Ataque(s) distribuído(s) de negação de serviço
DoS	Ataque(s) de negação de serviço
ESMC	Espectro da Securitização Militar do Ciberespaço
EUA	Estados Unidos da América
EUA-DHS	*U.S. Department of Homeland Security*
EUA-DoD	*U.S. Department of Defense*
EUA-ISC	*International Strategy for Cyberspace*
EUA-NSS	*U.S. National Security Strategy*
EUA-NSSC	*National Strategy to Secure Cyberspace*
EUA-SOC	*Strategy for Operating in Cyberspace*
EUA-USCYBERCOM	*U.S. Cyber Command*
GPL	*Graphical Production Language*
IEC	*International Electrotechnical* Commission
IPdDC	Índice de Politização Documental da Defesa Cibernética

IPiDC	Índice de Politização Institucional da Defesa Cibernética
IPvDC	Índice de Politização Virtual da Defesa Cibernética
ISO	*International Organization for Standardization*
NTIC	Novas tecnologias de informação e comunicação
OEA	Organização dos Estados Americanos
ONU	Organização das Nações Unidas
OTAN	Organização do Tratado do Atlântico Norte
P&D	Pesquisa e Desenvolvimento
RI	Relações Internacionais
RMA	*Revolution in Military Affairs*
SCADA	*Supervisory Control and Data Acquisition*
SIC	Segurança da Informação e Comunicações
SQL	*Structured Query Language*
TI	Tecnologia da Informação
TIC	Tecnologias da informação e comunicação
URL	*Uniform Resource Locator*
VANT	Veículos aéreos não tripulados

LISTA DE SÍMBOLOS

a.a.	Ao ano
D	Variável da diferença entre períodos (ano posterior menos ano anterior)
$\overline{D}$	Média da variável D
Σ	Somatório
$\sum(X-\bar{X})^2$	Fórmula da soma dos desvios quadráticos
gl	Grau(s) de liberdade
H_0	Hipótese nula ou de trabalho
H_1	Hipótese alternativa
n	Tamanho da amostra
N	Tamanho da população
S_D	Desvio padrão da variável D
S_X	Desvio padrão de uma variável
μ_{antes}	Interesse médio nos sítios virtuais, antes da filtragem dos termos
μ_{depois}	Interesse médio nos sítios virtuais, depois da filtragem
x'	Um valor padronizado
x	Um valor da variável X
X	Uma variável
$\overline{X}$	Média aritmética de uma variável

SUMÁRIO

1 INTRODUÇÃO

> O estudioso sempre otimista, se estudando o trabalho do impacto social ou artístico da computação, busca a luz além do nevoeiro e a(s) verdade(s) atrás dos disfarces. (MARX, 2008, p. vii, tradução nossa[1]).

A presente Dissertação possui, em última instância, a informação – mensurada por meio de *bits*(*)[2] – e o poder como sua unidade nuclear, pois entende que, a partir do momento em que o termo Informação caracteriza uma Era ou Sociedade global, torna-se relevante explicar alguns de seus efeitos políticos.

Assume-se, então, que: (i) o poder militar deriva do político (BRASIL, 2012d, p. 260; FUCCILLE, 2007, p. 104, 127; PROENÇA JR; DINIZ, 1998, p. 15; VON CLAUSEWITZE, 2007, *passim*); (ii) o ciberespaço é a informação em trânsito; e (iii) a utilização militar deste ambiente pode dizer algo a respeito do atual estado de coisas – *state of affairs* – internacional.

Portanto, não se trata de um trabalho sobre Ciência da Informação ou da Computação. Disserta-se, sim, sobre elementos que são a *raison d'être* da Ciência Política e das Relações Internacionais (RI), como: poder, Estado, guerra, política externa e segurança internacional.

A fim de situar tematicamente a presente obra, admite-se que, "no estrito senso da conduta da guerra, a digitalização significaria a capacitação por intermédio de computadores e redes de todos os armamentos e soldados, de maneira que todos saibam o que todos estão fazendo" (DUARTE, 2012a, p. 8). Nesse sentido, absorve-se também a assertiva de que:

> [...] a digitalização de simuladores e o desenvolvimento de ferramentas e modelagens têm permitido a construção de diversas formas e instâncias de guerra virtual. Os ganhos de aprendizado e a possibilidade de avaliação da atividade combatente decorrente destas tecnologias *acenam com a possibilidade de uma aferição inédita da capacidade de combate das forças armadas*. (PROENÇA JR; DINIZ, 1998, p. 54, grifo nosso).

De acordo com von Clausewitz (2007, p. 64, grifo nosso, tradução nossa[3]), a questão da informação na guerra está inexoravelmente atrelada à da inteligência:

> Por "inteligência", entendemos cada tipo de informação sobre o inimigo e seu país – a base, em resumo, de nossos próprios planos e operações. Se consideramos *a atual base dessa informação, quão duvidosa e transitória ela é*, logo percebemos que a guerra é uma estrutura frágil que pode facilmente entrar em colapso e nos enterrar.

Agora, considera-se um ambiente que se expande como o Big Bang e, no qual, informações são obtidas diretamente de bancos de dados não muito duvidosos, mas cujo

---

[1] Texto original: "*The ever optimistic scholar, whether studying the work of the artist or social impact of computer technology, seeks the light beyond the fog and the truth(s) behind the masks"*.

[2] O asterisco entre parênteses – (*) – identifica termos cujas definições estão no Glossário, ao final do trabalho.

[3] Texto original: "*By 'intelligence', we mean every sort of information about the enemy and his country – the basis, in short, of our own plans and operations. If we consider the actual basis of this information, how unreliable and transient it is, we soon realize that war is a flimsy structure that can easily collapse and bury us in its ruins*". Ver também von Clausewitz (2007, p. 88-89).

caráter transitório ainda persiste. Esse é o espaço que o pensamento original de Clausewitz – e de tantos outros que não presenciaram a Revolução da Informação(*) – não leva em conta e que engendra, no alvorecer do século XXI, um novel estágio: a Era da Informação, em que uma Sociedade da Informação se articula em redes (CASTELLS, 2007, *passim*) cada vez mais transnacionais (HELD; MCGREW, 2001, *passim*). Trata-se, portanto, do ciberespaço.

Já no final do século XX, Proença Jr e Diniz (1998, p. 25), compactuando com o pensamento clausewitziano, atêm-se que os arranjos de comando, controle, comunicações, computação e inteligência (C^4I)[4] sofrem "de uma dupla discriminação": (i) são "quase invisíveis e, portanto, pouco percebidos" e (ii) tendem "a ser preteridos em favor de meios mais conspícuos: os armamentos". Eles também enfatizam, *in verbis*, que:

> Não é admissível que os arranjos e meios de $C^3I.C$, que são a materialidade do uso da guerra como ferramenta política e das forças [armadas] como instrumentos, sejam relegados a um segundo plano. Ao contrário, devem ser objeto de prioridade em qualquer proposta séria de política de defesa. (PROENÇA JR; DINIZ, 1998, p. 25).

Assim, é também a guerra – no sentido de continuação da política por outros meios (VON CLAUSEWITZ, 2007, p. 30, 252, 258) – que interessa aqui, seja nos desdobramentos de como evitá-la, superá-la ou, mesmo, preparar-se para sua chegada.

Tal assertiva não denota que atores não governamentais sejam irrelevantes para os temas aqui abordados. *Hackers*(*), *crackers*(*), hacktivistas(*), extremistas e empresas privadas assumem papéis cada vez mais relevantes no desenrolar da política internacional[5] hodierna, tal qual ocorre no "mundo real" com os extremistas, mercenários, ativistas, terroristas e corporações[6]. Todavia, reafirma-se aqui que o Estado não "[...]está condenado a desaparecer, apesar da investida dos globalistas" (MIYAMOTO, 2003, p. 721).

Por causa da limitação textual e da recente imersão do setor militar no ciberespaço, afunilam-se as inferências para a atuação especificamente estratégica[7] nesse ambiente.

Portanto, a digitalização da guerra implica um leque de possibilidades sobre questões que envolvem o planejamento doutrinário e o *modus operandi* da própria arte da guerra, tais como: defesa cibernética, veículos aéreos não tripulados (VANT)[8] e mísseis (tele)guiados[9].

---

[4] Tais autores preferem "$C^3I.C$", enfatizando o elemento humano da inteligência sobre o da computação.
[5] Utiliza-se "política internacional" ("*international politics*") com o mesmo sentido de "relações internacionais" ("*international relations*"), *i.e.*, enquanto objeto de estudo de RI (*International Relations*).
[6] Exemplos: a participação hacktivista na Primavera Árabe e a Organização do Tratado do Atlântico Norte (OTAN) considerar o grupo Anonymous uma ameaça governamental (LOPES, 2011c; LOPES; AZEVEDO NETO, 2012, *passim*). O caso do Partido Pirata também é emblemático (UNIÃO EUROPEIA, [201-]).
[7] Usa-se aqui "estratégia" e suas derivações para designar concepções doutrinárias e/ou operacionais do setor militar. Crê-se que a utilização dos seguintes termos se vale dessa mesma acepção: "estratégico" (ARON, 2012, *passim*; PROENÇA JR; DINIZ, 1998, p. 6, 15, 22), "estratégico-militar(es)" (MIYAMOTO, 1998, p. 284; 2001, p. 15) e "político-estratégica" (PROENÇA JR; DINIZ, 1998, p. 55).
[8] Cf. DUARTE, 2012a, p. 42-51, 72-73, 77-78, 91-92; SANGER, 2012a, p. xiv-xv.

O tema principal deste trabalho versa sobre as duas primeiras palavras desse leque. Individualmente, elas são bastante analisadas, respectivamente, pelos Estudos de Segurança Internacional[10] e pela Ciência da Computação, a saber: defesa e cibernética. Já sua junção forma um termo que ganha relevância nos *fora* de discussão nacionais e internacionais recentes. Cuida-se, portanto, da defesa cibernética ou ciberdefesa/*cyber defense*.

Quanto à justificativa desta Dissertação, utiliza-se a assertiva de King *et al.* (1996, p. 15, tradução nossa[11]), quando eles salientam que uma pesquisa em ciências sociais deve satisfazer a dois critérios: (i) "[...]colocar uma questão que é 'importante' no mundo real"; e (ii) "[...]fazer uma contribuição específica para uma literatura acadêmica identificável". Nesse sentido, objetiva-se contribuir para a diminuição, no Brasil, de "[...]um déficit de quadros de pessoas [...] que tenham alto grau de conhecimento do mundo" (VIOLA, 2010). Neste caso, busca-se conhecer o mundo das novas tecnologias de informação e comunicação (NTIC)(*) atrelado ao pensamento estratégico.

Ademais, pelo fato de a literatura brasileira de Ciência Política/RI, nessa temática, ser ainda deveras escassa (LOPES, 2010), objetiva-se pleitear seu espaço, enquanto fonte acadêmica, sobre alguns dos intrigantes fenômenos da atual política internacional.

Busca-se também ser crítico, partindo-se do pressuposto de que apenas comprovar se o ciberespaço é ou está sendo securitizado num dado Estado, por si só, não lhe confere relevância acadêmica, ainda mais numa ciência social. Tal comprovação deve lançar um olhar nevrálgico sobre as nuances dos processos políticos, implicando, assim, numa avaliação de como Estados securitizam militarmente o ciberespaço.

A literatura pertinente ao tema em apreço é relativamente nova: de acordo com Acácio e Lopes, (2012, p. 5), os primeiros escritos canônicos sobre a imersão estratégica no ciberespaço se encontram em Arquilla e Ronfeldt (1993). Nele, os autores apontam que, para as Forças Armadas se defenderem das ameaças articuladas em rede, devem agir assim também, e não na forma clássica/hierarquizada. A obra supracitada é apenas uma das poucas sobre o ciberespaço que foge das áreas de computação, linguística ou ciência da informação, no final do século XX. Isso se deve, em grande medida, ao desenvolvimento civil da Internet: somente a partir do momento em que ela se populariza e se torna quase ubíqua, é possível

---

[9] Cf. DUARTE, 2012a, p. 59-65.

[10] Estudos de Segurança Internacional é um subcampo de RI (BUZAN; HANSEN, 2009, p. 1, 256) e possui outros sinônimos, como "Estudos de/sobre Segurança" (BUZAN *et al.*, 1998, p. 1) e, como vistos em Mahnken e Maiolo (2008, *passim*) e Miyamoto (2001, *passim*), "Estudos Estratégicos".

mensurar seus reais impactos na economia e na política internacional.

Em contrapartida, não se negligencia, aqui, a noção de que três perspectivas sobre a função da tecnologia na guerra ganham relevância no âmbito dos Estudos de Segurança Internacional: "a revolução nos assuntos militares (*revolution on military affairs* – RMA), a proposta de guerras de quarta geração (G4Gs) e a teoria da guerra de Clausewitz" (DUARTE, 2012a, p. 9, grifo do autor). Embora pactue com alguns pressupostos da terceira perspectiva, o caminho teórico deste trabalho é iluminado por uma quarta: a securitização.

Nesse sentido, tem-se o seguinte problema de pesquisa: como os processos nacionais de securitização militar do ciberespaço influenciam a política internacional no século XXI?

Para responder à precitada indagação, parte-se da hipótese principal de que, no século XXI, a securitização militar do ciberespaço, por parte de um Estado, pode tornar-se internacionalmente relevante quando outro Estado a subentende de forma tal a influenciar suas próprias ações naqueles mesmos ambiente e setor[12].

Essa tese geral se divide em três hipóteses secundárias:

1. o ciberespaço retorna à pauta militar a partir do momento em que Estados passam a utilizar NTIC de forma estratégica contra outros Estados[13];
2. a sucessiva empreitada militar no ambiente cibernético pode ser evidenciada mediante o estudo comparado, no que pese a comparação de poucos países[14]; e
3. a securitização militar nacional do ciberespaço influencia a política internacional, no século XXI.

Buzan *et al.* (1998, p. 29) salientam que, em certo casos, securitizar questões é inevitável, como no enfrentamento de calamidades públicas ou de um agressor bárbaro. Assim, seria até esperado que um dos objetivos deste trabalho fosse o de analisar se a securitização militar do ciberespaço nos Estados aqui escolhidos se enquadra em tais casos. Mas, como os próprios autores apontam, mesmo que tal pesquisa encontre meios de mensurar se uma questão foi securitizada – de forma correta ou não –, o que realmente importa é o fato político, que tem consequências fulcrais na vida do Estado, "pois essa securitização permitirá

---

[12] Essa hipótese deriva de um dos possíveis casos tratados por Buzan *et al*. (1998, p. 30) para demonstrar sob quais pontos de vista – objetivos, subjetivos e intersubjetivos – uma questão securitizada deve e pode ser encarada. Eis aí a razão do termo "subentende", ao invés de "entende", para enfatizar o caráter intersubjetivo que envolve o processo de securitização (cf. BUZAN *et al.*, 1998, p. 29-31).

[13] Em parte, tal premissa repousa numa espécie de silogismo análogo ao de Villa e Reis (2006, p. 37), quando estes afirmam que uma "[...] importante transformação [no pós-Guerra Fria] está no fato de que o direito das grandes potências de adquirir territórios não é mais reconhecido". Nesse sentido, o "território" ciberespacial se mostra apto para tais empreitadas (LEMAN-LANGLOIS, 2012, p. 7).

[14] Sobre a comparação entre poucos países (*comparing few countries*), ver Landman (2008, p. 27-29, 67-83).

ao ator [securitizador] operar em um modo diferente que, de outra forma, ele não poderia fazê-lo" (BUZAN *et al.*, 1998, p. 30, tradução nossa[15]).

Porém, tem-se em mente também que:

> [...]a decisão de buscar explicações causais é que leva o cientista a caracterizar seu objetivo[...]. O objetivo é o de encontrar teorias explicativas[...]; em outras palavras, teorias que descrevam certas propriedades estruturais do mundo e que nos permitam deduzir, com auxílio de condições iniciais, os efeitos que se pretende explicar. (POPPER, 2008, p. 64).

Nesse sentido, o objetivo geral desta Dissertação é analisar as causas e os efeitos de uma possível securitização militar do ciberespaço na política internacional hodierna. Com isso, unem-se, num mesmo intento, a lógica objetiva popperiana e o fato político intersubjetivo copenhagueano.

Para orientar o objetivo geral, pactua-se com a seguinte assertiva:

> [...]os estudos de securitização objetivam obter um entendimento cada vez mais preciso de quem securitiza, sobre quais questões (ameaças), para quem[...], por que, com quais resultados e[...] sob quais condições (ou seja, o que explica quando securitização é bem sucedida). (BUZAN *et al.*, 1998, p. 32, tradução nossa[16]).

Assim, com tais premissas, configuram-se os seguintes objetivos específicos, que, assim como – e em consonância com – as hipóteses secundárias, são três:

1. identificar as principais ameaças (ciber)existenciais para o setor militar, revelando os motivos de esse processo se intensificar no século XXI;
2. projetar quais as condições para tal fenômeno político, em três estudos de caso e, posterior, comparação entre eles; e
3. explicar os resultados dessa securitização para a política internacional.

Assim, essa arquitetura científica tem como fio condutor não "[...] repetir o erro de banalização, muito comum nos estudos sobre tecnologia militar, de fixar a atenção *simplesmente* a armamentos e equipamentos e suas plataformas associadas [...]" (DUARTE, 2012a, p. 36, grifo nosso).

Quanto a seus aspectos metodológicos, opta-se pelos dois estilos de análise – o qualitativo e o quantitativo –, com a pretensão de criar um *framework* que auxilie na análise da securitização das ameaças cibernéticas num dado tempo (século XXI) e espaço (Estado). A tal ferramenta se dá o nome de Espectro da Securitização Militar do Ciberespaço (ESMC), que compreende três índices e é detalhada na Seção 3.

---

[15] Texto original: "[...]*because this securitization will cause the actor to operate in a different mode than he or she would have otherwise*".

[16] Texto original: "[...]*securitization studies aims to gain an increasingly precise understanding of who securitizes, on what issues (threats), for whom*[...], *why, which results, and, not least, under what conditions (i.e., what explains when securitization is successful)*".

Assim, selecionam-se três Estados para submissão ao ESMC: Estados Unidos da América (EUA), Brasil e Canadá, com base principalmente em fatores geopolíticos e logísticos.

Dados secundários, como estratégias e políticas de defesa, estão presentes. No que tange aos primários, entrevistas e análises de discursos robustecem o aspecto pragmático deste trabalho, haja vista que ele não se sustentaria com uma visão puramente normativa – algo bem tentador quando se trata de um ambiente tão "líquido" ou "pós-moderno" como o ciberespaço.

O esquema das Seções desta Dissertação segue as diretrizes do *Índice como hipótese de trabalho*, de Eco (1996, p. 81-87). Assim, além desta Introdução, há mais três Seções:

- *A emergência do debate sobre "defesa cibernética" na política internacional*: apresenta a hipótese principal e o que se sabe sobre ela, bem como revisa a literatura sobre o tema. É aqui também que se apresentam as questões teóricas e epistêmicas acerca do surgimento, conceituação e debate sobre defesa cibernética;
- *Análise exploratória da securitização militar do ciberespaço: os casos estadunidense, brasileiro e canadense*: analisa os dados e demonstra como a hipótese principal opera. O objetivo principal dessa seção é demonstrar como a caserna dos três Estados selecionados dramatizam as ameaças ciberexistenciais e ofertar um *framework* próprio para mensurar tal securitização, o ESMC; e
- *Conclusão*: corrobora ou não o enunciado da hipótese principal. Após análise sobre os sítios virtuais, documentos e instituições militares de defesa cibernética, é possível responder se tal processo político tem relevância ou não na política internacional hodierna. Ademais, é nessa seção também que se ponderam considerações acerca dos resultados da mensuração do ESMC.

Ademais, ofertam-se elementos pós-textuais – Glossário, Apêndices e Anexo –, com o intuito de complementar as argumentações postas.

Frisa-se, antemão, que todas as opiniões dos entrevistados aqui publicadas não representam a posição oficial das instituições a que eles pertencem.

Observa-se também que, a fim de não prejudicar a leitura, as referências das citações indiretas que ocupam mais de duas linhas figuram em notas de rodapé.

Por fim, acresce-se a sigla do Estado às abreviações de instituições e documentos oficiais militares relacionadas à defesa cibernética. Acredita-se que, assim, torna-se mais fácil associar a instituição/documento ao seu país de origem.

2 A EMERGÊNCIA DO DEBATE SOBRE "DEFESA CIBERNÉTICA" NA POLÍTICA INTERNACIONAL[17]

> Muita pesquisa científica é também conduzida utilizando noções não examinadas de crime cibernético, guerra cibernética, fraude cibernética [...] e similares (LEMAN-LANGLOIS, 2012, p. 4, tradução nossa[18]).

Da teoria à prática: no início da década de 1990, Arquilla e Ronfeldt (1993, *passim*) já mencionam o termo "*cyberwar*"; no século XXI, o presidente estadunidense autoriza secretamente o uso de armas e ataques cibernéticos para sabotar o programa nuclear iraniano (SANGER, 2012a, *passim*; 2012b).

Defesa cibernética, ataques cibernéticos, guerra cibernética e armas cibernéticas são termos cada vez mais presentes em noticiários internacionais, artigos acadêmicos sobre segurança internacional e falas de autoridades, mundo afora.

Porém, entender simplesmente o que *são* tais objetos e *onde* eles podem ser empregados no campo de batalha sem atinar para *como* eles são transformados em questões "de segurança" tornaria este trabalho limitado.

Gagnon (2008, p. 50) sustenta que, há alguns anos, o ciberespaço se prostra como um assunto pertinente à caserna de vários países, com notoriedade para os Estados Unidos da América (EUA). Porém, a defesa desse ambiente, envolta num *ethos* militar, constitui-se algo deveras recente e que, outrossim, pode ser considerado como uma das características inerentes do século XXI (GAGNON, 2008, p. 63; NYE, 2008; LOPES, 2011d, *passim*).

Nada obstante, percebe-se que as ações militares no ciberespaço não se dão abruptamente. Um amálgama entre a experiência militar com guerras informacional e eletrônica[19] e a assimilação de novas ameaças parece dar o tom dessa empreitada cibernética, que passa a incluir planejamento estratégico e controle operacional – elementos *ex-ante* e *ex-post*, respectivamente, da defesa cibernética – em seu intento. O presente trabalho enfatiza principalmente a fase anterior às ações militares no ciberespaço, enquadrando-a no processo de securitização.

Grosso modo, o conceito de securitização, proposto pelos pensadores da chamada Escola de Copenhague, é uma crítica à maioria das tentativas de se encaixar determinadas questões como sendo "de segurança". Isso porque, ao etiquetá-las como "urgentes" ou "de defesa", um ator automaticamente acaba por cercear o fluxo natural dos procedimentos

---

[17] Esta Seção conta com fragmentos de Lopes (2011a; 2011b).
[18] Texto original: "*Much scientific research is also conducted on unexamined notions of cybercrime, cyberwar, cyberfraud, cyberharassment, cyberpiracy, cyberloitering and the like*".
[19] Cf. Subseção 2.1.6, *infra*.

políticos habituais (BUZAN *et al.*, 1998, p. 29), mesmo com o aval de uma audiência relevante.

Trazendo Duarte (2012a, p. 36) novamente ao debate, parte-se da premissa de que, embora tentador, o papel da tecnologia bélica – neste caso, associada à "plataforma" cibernética – não deve sobrepor a centralidade do elemento humano[20], no que diz respeito ao planejamento e à execução bélica no ciberespaço.

As próximas subseções introduzem o estado da arte do tema ora em tela.

2.1 Situando as Unidades de Análise

Em Segurança Internacional, duas difundidas escolas de pensamento vêm à tona: a tradicionalista, que restringe segurança a questões meramente político-militares; e a abrangente – ou *widener* –, que a estende a outros setores[21] (BUZAN *et al.*, 1998, p. 1, 239)[22]. Assim, a fim de comparar essas duas abordagens[23] e de explicar como as questões (*issues*) são securitizadas, Buzan *et al*. (1998, p. 1) buscam prover uma classificação do que é e do que não é uma questão de segurança.

É nesse mesmo sentido de separação e reagrupamento que a presente subseção define os principais objetos e temas desta Dissertação, com o intuito de iniciar a (a)provação da hipótese principal.

2.1.1 Poder político e poder militar

O poder – tema central em muitas obras clássicas de Teoria Política e de RI, ao longo dos anos – ganha espécies que permitem a seus analistas o enquadrar sob um determinado nível de análise. São exemplos os poderes político[24], econômico e militar.

Utilizando a teoria da guerra clasewitziana, Proença Jr e Diniz (1998, p. 15) apregoam que "[...]não existem considerações ou critérios 'puramente militares', e qualquer decisão relacionada ao emprego ou à possibilidade de emprego de força armada tem inevitavelmente

---

[20] Tal centralidade é uma das cinco dinâmicas que instruem a própria capacidade combativa das forças armadas – sendo estas uma das quatro componentes de uma política de defesa (PROENÇA JR; DINIZ, 1998, p. 25).

[21] Setores são pontos de vista inseparáveis do todo – sistema internacional –, que selecionam determinado tipo de interação, separando-o entre militar, político, societário (*societal*), econômico e ambiental (BUZAN *et al.*, 1998, p. 1-2, 27). Eles possuem uma engenharia retroalimentar: desagregam um todo, para fins de análise, escolhendo alguns de seus diferentes padrões de interação e, então, reagrupam-nos (BUZAN *et al.*, 1998, p. 8).

[22] Seguindo a classificação de Nye (2011b, p. 3-109), pode-se dizer que essas duas abordagens lidam com setores relacionados respectivamente ao *hard* e ao *soft powers*, sendo o setor econômico um transeunte. Por exemplo, a Política de Defesa Nacional brasileira pactua explicitamente com a vertente abrangente (BRASIL, 2005).

[23] Buzan *et al.* (1998, p. 2-5) fazem isso em sua obra seminal.

[24] Assaz atrelado à questão democrática eleitoral – "poder das urnas" –, muito embora, em regimes autoritários ou não democráticos, seus governantes também detenham "o poder em suas mãos".

aspectos não apenas táticos e estratégicos, mas também políticos". Assim, como já mencionado, assume-se que o poder militar deriva do político, embora "nem todas as metas políticas podem ser alcançadas pela via militar" (PROENÇA JR; DINIZ, 1998, p. 51).

Sabe-se que, ao longo da história, houve países que lideraram o mundo. Nesse sentido, "essa sucessão de eventos que periodicamente modela o sistema internacional […] mostra que o poder tem se convertido em instrumento central em torno do qual os Estados formulam suas políticas" (MIYAMOTO, 2003b, p. 686).

Nota-se, então, que a manutenção de um diálogo estreito e permanente entre as políticas exterior e de defesa de um Estado é questão já pacificada na literatura consultada[25].

Todavia, como derivado do poder político, o poder militar pode sofrer influências ideológicas daquele, no que Saint-Pierre (2009, p. 3, tradução nossa[26]) chama de *destino das paralelas*, que, "[...]dependendo da ideologia do setor burocrático que se encontre à frente de cada corpo diplomático e militar, pode existir coincidência ou não entre os objetivos da política exterior". Assim ocorrendo, as tênues linhas que devem existir entre as políticas exterior e de defesa não se cruzam; elas vivem num eterno paralelismo. Esta, porém, parece ser a exceção nos assuntos sobre defesa cibernética no século XXI.

O que importa frisar é que o poder político impregna o militar, e a forma mais perceptível disto é relacionar as políticas nacionais exterior e de defesa.

2.1.2 A política internacional do século XXI

Poder militar e política internacional sempre andaram juntos, principalmente "[...]quando os interesses de um Estado ou de um grupo" estão "em jogo" (MIYAMOTO, 1998, p. 278).

Vislumbra-se uma nova ordem global engendrada no/pelo fim da Guerra Fria (BUZAN *et al*., p. 7; 1998, p. MARIANO, 2007, p. 123, 127; VAZ, 2012, p. 15; VILLA; REIS, 2006, p. 36) e ainda em construção (SARAIVA, 2012, p. 20, 78, 80-81). Tal ordem tem influência, dentre outros, nos principais desdobramentos da Revolução da Informação, que propicia a interconectividade entre pessoas físicas e jurídicas num grau inimaginável (ARQUILLA; RONFELDT, 1993, p. 141-143; VILLA; REIS, 2006, p. 37), muito

---

[25] ALSINA JÚNIOR, 2009, *passim*; ARON, 2002, p. 29-30, 52-55, 64; Celso Amorim *apud* BRASIL, 2007b, p. 301; 2008a; FUCCILLE, 2007, p. 104; Henry Kissinger *apud* SANTOS, 1998, p. 4; MIYAMOTO, 2001, p. 5; PROENÇA JR; DINIZ, 1998, p. 6, 22, 36-37. Cf. GAIO, 1998, p. 50-51; MIYAMOTO, 1981, p. 75; OLIVEIRA, 2004, p. 92; SAINT-PIERRE, 2009, p. 16; WINAND; SAINT-PIERRE, 2010, p. 16, 30.

[26] Texto original: "[...]*dependiendo de la ideología del sector burocrático que se encuentre al frente de cada una de esas corporaciones* [diplomática e militar], *pueda que exista coincidencia o no entre los objetivos de la política exterior*".

"[...]embora o quadro atual das relações internacionais seja distinto do que perdurou dos anos [19]40 ao final dos [19]80, e no imediato pós-guerra fria[...]" (MIYAMOTO, 2003, p. 720).

Em outras palavras:

> Durante décadas, armas nucleares e poder tornaram-se praticamente sinônimos. O novo cenário rompeu essa identidade, fazendo com que novas dimensões de poder e novos atores emergissem no cálculo de poder internacional. (VILLA; REIS, 2006, p. 36).

Nesse ínterim, o ambiente cibernético se torna um amálgama de interdependência complexa e dependência tecnológica de sistemas informacionais interconectados em redes de computadores (CARVALHO, 2011, p. 5).

Para efeitos comparativos, em 1995, há cerca de cinco milhões de internautas no mundo todo; já em 2012, quase dois bilhões e meio de pessoas se cnectam à Internet (INTERNET WORLD STATS, 2012b).

Por isso, não é novel o fato de que, ao longo da história humana, os avanços tecnológicos ajudem a moldar percepções, estratégias e a própria organização militar (ARQUILLA; RONFELDT, 1993, p. 141-142; KEEGAN, 2006, p. 306-307). Mas, assim como o mundo real, o virtual também projeta novas possibilidades de interação social e de inferência acerca do poder político.

No alvorecer do século XXI, as ameaças cibernéticas transbordam do setor societário e atingem os político e militar. A consequência para a política internacional hodierna, dentre outras, é a formulação de políticas exteriores e de defesa nacional que elevam o *status* das ameaças cibernéticas à alçada de assuntos pertinentes à segurança nacional.

2.1.3 Segurança e defesa

À primeira vista, os termos "segurança" e "defesa" parecem assemelhar-se semanticamente (TEIXEIRA JR, 2011, p. 143), pois, para garantir o primeiro, é necessário ter o segundo. Villa e Reis (2006, p. 20) lembram que, "de um modo geral, pode-se dizer que o conceito de segurança tem uma referência defensiva[...]".

Porém, há uma forte corrente – em cujo benefício se advoga aqui – que diz respeito à separação entre Estudos de Segurança e Estudos de Defesa[27]. Tal bipartição possibilita, por exemplo, analisar, mais detalhadamente, assuntos relacionados ao desempenho dos principais atores e instituições – como ministros, parlamentares, ministérios, polícias e Forças Armadas – em determinado(s) assunto(s) e ameaça(s) ou sua(s) iminência(s).

---

[27] Cf. BRASIL (2005); LOPES; MEDEIROS, 2011; PROENÇA JR; DINIZ, 1998, p. 20-22; TEIXEIRA JR 2011, p. 143; WINAND; SAINT-PIERRE, 2010, p. 10, 16.

Rudzit (2005, p. 308), utilizando definição de Buzan *et al.* (1998, p. 23), aponta que segurança é o movimento que conduz a política (*politics*) para além das regras já estabelecidas do jogo e enquadra uma questão como um tipo especial de política.

Embora compartilhem algumas qualidades, a segurança do contexto internacional é bem diferente e extrema da do nacional (BUZAN *et al*., 1998, p. 21): ela lida com a tradicional questão da política do poder (BULL, 2002, *passim*; WIGHT, 2002, *passim*) e da sobrevivência do Estado (BUZAN *et al*., 1998, p. 21, 27, 46).

Já segurança nacional é um conceito que não deve ser idealizado e que geralmente é emanado para tratar uma ameaça doméstica como um álibi, a fim de reivindicar um poder para manobrar, sem muito controle e restrição democrática, algo ou alguém (BUZAN *et al*., 1998, p. 29).

Quando se cuida de defesa, fala-se da atuação do setor militar na vida estatal, no que pese suas Forças Armadas. Geralmente, seus três componentes – ou forças combatentes/singulares ou, ainda e simplesmente, armas – são o Exército, a Marinha e a Aeronáutica, embora países como EUA e Canadá acrescentem outros corpos às suas macroestruturas militares. A função básica das Forças Armadas é pensar e prevenir a defesa de um país (MIYAMOTO, 2003, p. 683), planejando, preparando-se e atuando conjuntamente entre si (PROENÇA JR; DINIZ, 1998, p. 50, 54). Assim, elas são meios ou instrumentos fundamentais de força do Estado (FUCCILLE, 2007, p. 104; PROENÇA JR; DINIZ, 1998, p. 44).

Sobre defesa nacional, Buzan *et al.* (1998, p. 22) asseveram que, "para muitas democracias avançadas, a defesa do Estado está se tornando apenas uma [...] das funções das forças armadas", que incluem atividades militares não ligadas diretamente a uma ameaça existencial externa – como operações de paz – ou, mesmo, a uma ação emergencial que venha a suspender regras normais. Mesmo assim, quando se fala em "defesa", está também se remetendo implicitamente à segurança e à prioridade/urgência (BUZAN *et al*., 1998, p. 27, 28).

Quanto à "[...]atividade de preparação da defesa nacional de um país", de acordo com Duarte (2012a, p. 7), "é uma necessidade intrínseca em consequência da condição anárquica do sistema internacional".

Portanto, quando se menciona sistema e política internacionais, fala-se concomitantemente em segurança nacional, a qual é tratada como uma questão relacional pelos teóricos da Escola de Copenhague (BUZAN *et al*., 1998, p. 10).

2.1.4 Segurança cibernética e defesa cibernética

Assim como nos Estudos de Segurança e de Defesa, cabe agora diferenciar segurança cibernética de defesa cibernética.

Segurança cibernética se refere ao combate e à prevenção dos chamados crimes cibernéticos na esfera da segurança pública. Em outras palavras, segurança cibernética é uma questão de investigação policial ou mesmo por parte de ministérios públicos.

Já defesa cibernética é o "conjunto de ações defensivas, exploratórias e ofensivas, no contexto de um planejamento militar, realizadas no espaço cibernético[...]" (CARVALHO, 2011, p. 8). Assume-se, então, que defesa cibernética significa a salvaguarda da segurança nacional contra ameaças ciberexistenciais.

Dessas definições, obtém-se que defesa cibernética diz respeito ao setor militar. No que tange a seus aspectos operacional e tático, são as Forças Armadas que aplicam a estratégia, com a finalidade de prevenir ou contra-atacar, por exemplo, numa situação de guerra cibernética.

Todavia, tanto segurança cibernética quanto defesa cibernética são duas espécies do gênero segurança da informação, que é levada a cabo tanto por agentes públicos quanto por privados. No âmbito internacional, a *International Organization for Standardization* (ISO) e a *International Electrotechnical* Commission (IEC) padronizam as regras sobre boas práticas de Segurança da Informação: confidencialidade, integridade e disponibilidade (ISO/IEC, 2005, *passim*).

Dentre os três países a ser analisados, o Brasil é o único que recepciona tal norma internacional por meio de uma nacional: a NBR ISO/IEC 27002:2005 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005, *passim*). Indo mais além, o Gabinete de Segurança Institucional da Presidência da República (GSI-PR) do Brasil disciplina a gestão de Segurança da Informação e Comunicações (SIC) na Administração Pública Federal (APF), direta e indireta (BRASIL, 2008b). Assim, no que tange à segurança da informação na esfera pública federal, utiliza-se o conceito de SIC, ou seja, "ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações" (BRASIL, 2008b, p. 6). Em outras palavras, a SIC "[...]é a base da Defesa Cibernética [no Brasil] e depende diretamente das ações individuais; não há Defesa Cibernética sem ações de SIC" (BRASIL, 2012e, p. 11).

A Tabela 1 demonstra como tal diferenciação ocorre no Brasil.

Tabela 1 – A questão das defesa e segurança cibernéticas no Brasil

NÍVEL	DENOMINAÇÃO	ÓRGÃO DE COORDENAÇÃO
Político	Segurança da Informação e Comunicações (SIC) Segurança Cibernética	Gabinete de Segurança Institucional da Presidência da República (GSI-PR)
Estratégico	Defesa Cibernética	Ministério da Defesa
Operacional	Guerra Cibernética	Forças Armadas
Tático		

Fonte: Carvalho (2011, p. 8).

Já nos EUA, essa diferença, há poucos anos, era imperceptível, pelo fato de aquele Estado ter suas finanças praticamente baseadas em sistemas virtuais, com produção de *softwares*, serviços *web*, pagamentos eletrônicos e bolsa de valores eletrônica – a NASDAQ. Entretanto, Gagnon (2008, p. 53) enfatiza o fato de projetos de defesa cibernética terem ajudado a combater delitos menores, como o crime cibernético.

No que tange ao Canadá, por outro lado, há uma ênfase muito grande na segurança cibernética, que, amiúde, tem servido de provedora para se pensar a defesa cibernética.

A Subseção 3.3 realiza a análise desses três casos quanto à defesa cibernética.

2.1.5 Ciberespaço e Internet[28]

A afirmação de que "gerações diferentes pensam o ciberespaço de formas diferentes" (CLARKE; KNAKE, 2012, p. xii, tradução nossa[29]) se baseia no termo "ciberespaço/*cyberspace*" cunhado pelo escritor William Gibson no seu famoso livro de ficção-científica *Neuromancer*, de 1984[30]. Desde então, o prefixo ciber/*cyber* passa a exprimir atividades relacionadas ao espectro eletromagnético e computacional (NYE, 2011a, p. 19), bem como "a total interconexão de seres humanos através de computadores e [de] telecomunicação sem considerações de geografia física" (THING, 2003, p. 200).[31] Portanto, vislumbra-se o ciberespaço nas diversas relações homem-máquina, bem como nos serviços de telemática(*).

---

[28] Opta-se, aqui, por "Internet", ao invés de seus homônimos: WWW, *World Wide Web*, rede mundial de computadores, grande rede, rede das redes, *Web* etc. Porém, vale notar que tais codinomes têm motivos, os quais, por sua vez, estão relacionados a descobertas de protocolos – como o TCP/IP – e de linguagens de marcação – como a HTML. Para mais detalhes, ver Thing (2003, *passim*) e Subseção 2.2.1.

[29] Texto original: "*Different generations think of cyberspace differently*".

[30] ARQUILLA; RONDELFT, 1993, p. 163; BENEDIKT, 1991, p. 1; LEMAN-LANGLOIS, 2008b, p. 3; LOPES, 2011a, p. 3; LOPES; AZEVEDO NETO, 2012, p. 1.

[31] Para estudo filológico da palavra ciber, enquanto derivada do latim, ver Arquilla e Ronfeldt (1993, p. 162).

A Internet do jeito que se conhece hoje – sob o codinome de WWW – surge apenas no final dos anos 1980[32], como um projeto paralelo de Sir Tim Berners-Lee (LOPES; MACIEL, 2010), quando este ainda trabalhava no Conselho Europeu para a Pesquisa Nuclear (CERN).

Assim, apesar de a Internet está contida no ciberespaço – e, portanto, serem coisas tecnicamente diferentes –, empregam-se ambos os termos aqui sem prejuízo de compreensão.

2.1.6 Infraestruturas críticas, cyber warfare *e guerra cibernética*

De acordo com a literatura consultada – em que pese Clarke e Knake (2012) –, as infraestruturas críticas de um Estado são o principal alvo que pode potencializar uma guerra cibernética. Daí, a necessidade de a defesa cibernética as abarcar.

Ao longo deste trabalho, utiliza-se deveras tal termo, principalmente no intuito de demonstrar que os danos causados por um ataque cibernético ou por uma arma cibernética podem ir muito além do *software* e atingir também o *hardware*.

Para fins metodológicos, utiliza-se a definição fornecida pelo governo canadense, o qual afirma, *in verbis*, que:

> Infraestruturas críticas são o conjunto de processos, sistemas, instalações, tecnologias, redes, bens e serviços necessários para garantir a saúde, a segurança ou o bem-estar da sua população, bem como a eficácia do seu governo. Esse conjunto pode ser tanto infraestruturas autônomas quanto dependentes, dentro de uma província ou território, ou para além das fronteiras do país. O rompimento dessas infraestruturas pode resultar em perda de vidas e efeitos econômicos adversos, além de prejudicar significativamente a confiança do cidadão. (CANADÁ, 2009, p. 2, tradução nossa[33]).

No que tange à *cyber warfare*, é muito comum encontrar entendimentos equivocados entre os não anglófonos sobre tal conceito, sobretudo por que, na língua inglesa, há duas palavras que, dependendo do caso, significam literalmente "guerra": *war* e *warfare*.

Em termos gerais, *warfare* é tudo o que envolve a vida militar, incluindo, por exemplo, as batalhas, as incursões em solo inimigo e a própria guerra. Migrando-se para a seara cibernética, *cyber warfare* também possui tal sentido abrangente e inclui, por conseguinte, a utilização de armas e ataques cibernéticos (cf. próxima subseção) e a própria

---

[32] Cf. Subseção 2.2.1.

[33] Texto original: "*On entend par infrastructures essentielles l'ensemble des processus, des systèmes, des installations, des technologies, des réseaux, des biens et des services nécessaires pour assurer la santé, la sûreté, la sécurité ou le bien-être économique des Canadiens et des Canadiennes ainsi que l'efficacité du gouvernement. Il peut s'agir d'infrastructures autonomes ou caractérisées par des interdépendances au sein d'une province ou d'un territoire, entre eux ou au-delà des frontiéres du pays. La perturbation de ces infrastructures essentielles pourrait se traduire en pertes de vie et en effets économiques néfastes, et pourrait considérablement ébranler la confiance du grand public*".

guerra cibernética (*cyber war*)[34]. Assim, *cyber warfare*, por ser um campo em rápido desenvolvimento (ANDRESS; WINTERFELD, 2011, p. 80), designa tanto ações governamentais quanto não governamentais no ciberespaço, utilizando-se de técnicas *hacker*.

Por causa dessa questão semântica, mantém-se, aqui, sua grafia na língua original[35].

Nesse sentido, guerra cibernética não é a mesma coisa que *cyber warfare*, que guerra informacional[36] ou mesmo guerra eletrônica (ARQUILLA; RONFELDT, 1993, p. 146).

Grosso modo, guerra informacional diz respeito ao setor societário, em que governo e/ou meios de comunicação e/ou *lobbies* desempenha(m) objetiva(m) "desinformar" determinado público (ARQUILLA; RONFELDT, 1993, p. 141, 144-146).

Já guerra eletrônica é o bloqueio ou ruptura de sinais de comunicação no espectro eletromagnético[37]. A título de exemplo, o Brasil dispõe tanto do Centro de Comunicações e Guerra Eletrônica do Exército (BRA-CCOMGEX) quanto do Centro de Defesa Cibernética do Exército (BRA-CDCiber), sendo este último analisado na Subseção 3.3.2.

Em relação ao uso de ataques cibernéticos, Rudzit (2012), em entrevista a este autor, aponta que, "com o passar do tempo, outros governos também começaram a utilizar este instrumento contra outros Estados, deflagrando o que alguns chamam de 'guerra cibernética'".

Como se verá neste trabalho, o conceito de guerra cibernética ainda não está pacificado, pois a literatura diverge sobre sua natureza. Porém, é possível encontrar relações entre os autores, sobretudo no que tange aos danos a infraestruturas críticas baseadas em novas tecnologias de informação e comunicação (NTIC) e ao uso sistemático de documentos e instituições militares para essa área.

Numa visão mais holística, Bezerra ([2009]) afirma que a guerra cibernética é o "uso da Internet como ferramenta de ação política ou militar".

Arquilla e Ronfeldt (1993, p. 30), por sua vez, entendem que essa é apenas mais uma forma de os Estados guerrearem.

Já para Clarke e Knake (2012, p. xi) e Demeterco (2011, *passim*), ela é entendida como uma alternativa à guerra convencional, que pode, *de facto*, aumentar a ocorrência de combates tradicionais, cujos principais alvos são majoritariamente civis, justamente por estes

---

[34] O Anexo A oferece um breve histórico da *cyber warfare* na política internacional, proposto por Lewis University (2010). Já University of Washington (2013) elenca várias referências sobre o tema.

[35] A mesma indagação que serve de critério para diferenciar "ciberespaço" de "Internet" é utilizada aqui: a troca das palavras modifica também o contexto? Entende-se que na relação "*cyber warfare*-guerra cibernética", sim, pois os atores e níveis de análise podem ser totalmente diferentes, resultando em conclusões igualmente distintas.

[36] São suas equivalências: *infowar* ou *information war*. Arquilla e Ronfeldt (1993, *passim*) utilizam *netwar*.

[37] Cf. DUARTE, 2012a, p. 72.

dependerem de infraestruturas críticas (CARVALHO, 2011, p. 7; DEMETERCO, 2011, p. 6-7; MANDARINO JR, 2009, p. 19-22) baseadas em NTIC.

A possibilidade real de interrupção, sabotagem ou mesmo de dano a essas infraestruturas pode potencializar o curso de uma guerra ou mesmo de um ataque não declarado[38], sobretudo em uma era contextualizada pela informação compartilhada em redes de computadores.

É nesse sentido que Lopes e Teixeira Jr (2011) conceituam guerras cibernéticas como:

> [...]modalidades estratégicas que se caracterizam por objetivos como o de obter informações privilegiadas e/ou desestabilizar determinado sistema gerenciador de informações baseadas em redes de computadores de um ou mais ente estatal, utilizando, para tal, o ambiente cibernético.

Segundo Gagnon (2008, p. 53), o advento da guerra cibernética se dá em 1991, quando, no âmbito da Guerra do Golfo[39], as Forças Armadas estadunidenses exploram as vulnerabilidades informacionais do Iraque. Porém, Duarte (2012a, p. 25) tem uma opinião diferente quanto à sobrevalorização meramente tecnológica, principalmente em tal guerra:

> Assim, da mesma maneira que a tecnologia nuclear não marcou uma revolução na natureza da guerra e na sua conduta, não existem evidências de que a Guerra do Golfo tenha correspondido a essa mudança[...]. O sucesso desta guerra foi gerado pela aplicação de uma capacidade bélica orientada a confrontar uma versão branda de um oponente muito mais capaz e poderoso que os iraquianos: o Exército Vermelho na Europa. O exército de Saddam adotava arsenal, doutrina e organização soviéticas, no entanto, em um terreno muito distinto, elemento que, somado a erros crassos de conduta, foi explorado pelos Estados Unidos e seus aliados. Talvez seja este o grande ganho das tecnologias de sensoriamento e ataque a distância: apesar de não serem substitutas do confronto terrestre e de choque, elas potencializam a capacidade de identificação e exploração de erros de organização, posicionamento e capacidade do oponente.

Para Kilian Jr (2012), em entrevista a este autor, a guerra cibernética

> […] está dentro da panóplia de sistemas de armas (multiplicador do poder de combate) utilizadas para degradar o poder de combate do inimigo. Ela tão somente não efetiva a destruição do inimigo ou quebra a sua vontade de lutar, mas o seu uso é essencial na redução do poder de combate do inimigo. Outro dado importante [é] que ela só pode ser usada contra um antagônico que esteja na era da informação, ou seja em rede. O seu uso contra um ator que esteja na fase agrária e que não dependa de redes é ineficaz.

Woodward (2012, tradução nossa[40]), por seu turno e também em entrevista a este autor, atenta para o fato de que nem todo ataque cibernético a um Estado pode ser considerado uma guerra cibernética e, portanto, "[...]dependerá do contexto geral em que ele é conduzido". Assim, concordando com Kilian, ele afirma que "o objetivo de uma guerra cibernética é causar danos ou impedir a capacidade de combate de um alvo inimigo".

---

[38] Cf. Subseção 2.2.4.1.

[39] Em entrevista a este autor, Ferreira Neto (2011) também aponta tal conflito como emblemático para o tema.

[40]Texto original: "*[...] I tend to favour those where the objective of the operation is to do damage, or to impede the fighting capability of the target. [...] depending on the overall context in which it is conducted.*".

Como se percebe, formam-se duas correntes sobre (i) o papel revolucionário e (ii) a natureza da guerra cibernética na seara bélica. Porém, como aponta Richard A. Clarke (*apud* RAMIREZ, 2010, p. 1, tradução nossa[41]), "a questão principal não é saber as chances de uma guerra cibernética ocorrer, mas as reais chances de ocorrer uma guerra". Se depender das armas e dos ataques cibernéticos ocorridos no século XXI, este debate tende a crescer ainda mais.

2.1.7 Armas e ataques cibernéticos

Quanto às armas cibernéticas, como o Stuxnet[42], Ferreira Neto (2011, grifo nosso) – em entrevista a este autor – informa que elas não possuem ainda uma definição clara e, por isso, ele parte do pressuposto de que elas "são vírus(*), *worms*(*) e programas semelhantes capazes de derrubar sistemas, roubar informações e dar informações falsas". Uma grande diferença das armas cibernéticas de outrora para as atuais está no contexto global em que foram utilizadas. Portanto, para ele,

> Os novos vírus/*worms*/Cavalos de Tróia podem passar sem ser percebidos por antivírus e programa semelhantes, ficar adormecidos até serem ativados, coletar informações, afetar e destruir *hardware*, etc ... [os *worms*] StuxNet e o Flame são o máximo em sofisticação, tão complexos que somente países podem tê-los desenhados. (FERREIRA NETO, 2011, grifo nosso).

Mais que isso, indagado se a possível utilização de tais armas por parte de Estados como EUA e Israel pode ser considerada uma prévia de uma guerra ainda não declarada contra o Irã, Ferreira Neto (2011) informa que ambos os países têm não só a tecnologia necessária, mas também os recursos e a motivação política para tal, acrescentando que:

> Um ataque deste tipo pode no mínimo atrasar o programa nuclear do Irã ou ser tão eficaz que pode até destruir as centrífugas de enriquecimento. Mas também pode ser o primeiro tipo de ataque em uma guerra de verdade. O primeiro alvo são sempre estações do tipo C^{4}ISTAR (Comunicação, Comando, Controle, Computadores, Inteligência, Sobrevivência, Aquisição de Alvos e Reconhecimento). Numa guerra tipo da Líbia onde não houve uma ataque (*sic*) com sistemas maliciosos antes o serviço foi feito por Tomahawks, depois os aviões de guerra eletrônica e por fim caças comuns. Mas sempre algo fica em pé. Numa situação ideal o ataque deve começar pela inutilização dos sistemas por contaminação de vírus/*worms*, deixando tudo inoperante, impossibilitando qualquer tipo de contra ataque. (FERREIRA NETO, 2011, grifo nosso).

Nessa mesma linha de raciocínio está Woodward (2012, tradução nossa[43]), quando este faz a seguinte indagação: "por que bombardear um país quando você pode neutralizá-lo a ponto de ele ter de capitular"?

---

[41] Texto original: "*The question isn't what are the chances of a cyberwar.* […]*is what are the chances of a war*".
[42] Cf. Subção 2.2.4.2.
[43] Texto original: "*Why bomb a country when you can incapacitate it to the extent that it has to capitulate.*".

Como se vê, os ataques e armas cibernéticas exigem um profissional militar diferenciado, comumente chamado, na literatura, de guerreiro cibernético (*cyber warrior*) (CLARKE; KNAKE, 2012, *passim*; SANGER, 2012a, p. xi).

Com esses conceitos em mente, é possível lançar luz a questões que preocupam o setor militar, neste século, como se vê na próxima subseção.

2.2 Securitização do Ciberespaço e Segurança Nacional

As extraordinárias possibilidades trazidas pelos recursos das redes de computadores são reconhecidas desde cedo pelos militares (GAGNON, 2008, p. 49).

Antes do século XXI, os próprios teóricos da Escola de Copenhague já adentram na relação entre segurança cibernética e setor militar, ao explicar pormenores da utilização do processo de securitização em casos específicos: "[...]o Pentágono define *hackers* como 'uma ameaça catastrófica' e 'uma grave ameaça à segurança nacional'[...], que poderia levar a ações no campo da informática, mas sem transbordar para outras questões de segurança" (BUZAN *et al.*, 1998, p. 25, ênfase nossa, tradução nossa[44]).

De fato, essa tentativa do Departamento de Defesa estadunidense (EUA-DoD) não reverbera em outros setores, naquela época. Em contrapartida, no século atual, parece que o discurso das ameaças cibernéticas se intensifica por parte da caserna de alguns países, conforme se defende neste trabalho e colocando essa afirmação copenhagueana por terra.

Nesse sentido cronológico, Gagnon (2008, 49-50) sugere uma linha do tempo para demarcar a influência do ciberespaço na política de segurança estadunidense – e, consequentemente, mundial –, a saber: (i) infância, com o desenvolvimento militar-acadêmico da *Advanced Research Projects Agency Network* (ARPANET); (ii) adolescência, marcada pela chegada comercial dos provedores de serviços de Internet ou (ISP, do inglês, *Internet Service Providers*), fazendo com que "o centro original de poder se dividisse em dois oceanos de novos atores, cada um com novos níveis de poder dentro da Internet" (GAGNON, 2008, p. 50, tradução nossa[45]); e (iii) maioridade, quando o ciberespaço vira um ambiente estratégico.

---

[44] Texto original: "[...] *the Pentagon designating hackers as 'a catastrophic threat' and 'a serious threat to national security'*[...], *which could possibly lead to actions within the computer field but with no cascading effects on other security issues.*".

[45] Texto original: "*The original centre of power divided into a sea of new players, each with new levels of power inside the web.*".

Assim, compreender a evolução e o papel da Internet no ambiente da política internacional[46] e analisar, à luz da teoria da securitização, sua relação com o setor militar são, respectivamente, os objetivos das duas próximas subseções[47].

2.2.1 Evolução da Internet e seus impactos à segurança nacional

A Internet, embora imprescindível para os diversos tipos de transações entre as sociedades atuais, tem servido, dentre outras possibilidades, de base para mensurar o grau de liberdade de expressão num dado Estado[48] e ainda como ambiente de transação econômico-financeiro (HELD; MCGREW, 2011, p. 12). Porém, essa popular ferramenta carrega consigo um interessante histórico: em meio à Cortina de Ferro, ela se desenvolve sob o espectro da Revolução da Informação e se populariza pelos processos globalizantes atrelados a elas (LOPES; TEIXEIRA JR, 2011), como comunicação instantânea, processamento de dados a distância e revolução dos *microchips*.

Ainda no que diz respeito à Guerra Fria, ressalvam-se a busca por meios comunicacionais mais seguros e o engendramento da agência estadunidense *Advanced Research Projects Agency* (ARPA)[49], na década de 1950, com o intuito de superar os soviéticos, no que se refere à Ciência e Tecnologia (C&T) avançada[50].

Assim, cria-se o projeto que origina a Internet sob o codinome ARPANET (GAGNON, 2008, p. 48, 63; LOPES, 2011a, p. 3-4), o qual obtém forte aporte da seara militar (DUARTE, 2012a, p. 27).

Embora engendrada nesse contexto, a ARPANET, segundo um de seus primeiros desenvolvedores, não é concebida para ser um projeto militar. De acordo com Kleinrock (2011, tradução nossa[51]), em entrevista a este autor, o objetivo dos que estavam envolvidos na sua elaboração era o de:

> […]prover um projeto entre nossos muitos computadores de pesquisas. Com o forte apoio dos gestores da ARPA, nossos pesquisadores naturalmente promoveram um

---

[46] Esta frase é em alusão a curso *online* oferecido pelo prof. Daniel Oppermann, em 2010.

[47] Isso é necessário, tendo em vista que, nos últimos anos, vê-se a alegação de que "[...]governos que não estejam se preparando para enfrentar esta nova ameaça à sua Segurança Nacional, poderão ter sério problemas em futuro não muito distante" (RUDZIT, 2012).

[48] *Vide*, por exemplo, o *Google Transparency Report*, em: www.google.com/transparencyreport.

[49] Aualmente *Defense Advanced Research Projects Agency* (DARPA).

[50] Àquela época, o *leitmotiv* de ambas as superpotências gira em torno da corrida espacial, como um transbordamento da disputa por novas formas de transportar ogivas nucleares, como consequência, por sua vez, da utilização dos foguetes nazistas V2 na Segunda Guerra Mundial.

[51] Texto original: "*Neither we nor ARPA considered the Arpanet to be a military project. The goal was to provide connectivity among our many research computers. With the strong support of the ARPA managers, our team of researchers naturally fostered an environment of openness, trust, sharing, and creativity. We did not expect it to grow as dramatically as it has, but we did see its enormous value from the earliest days*".

> ambiente de abertura, confiança, partilha e criatividade. Nós não esperávamos que a ARPANET crescesse tão drasticamente como de fato ocorreu, mas conseguíamos ver seu enorme valor desde aqueles primeiros dias.

Já na visão geopolítica de Martin (2012), também em entrevista a este autor, historicamente, a criação da ARPANET é:

> [...]a resposta de John Kennedy ao "Sputnik" o que desencadeou isto que temos agora, onde conquista espacial, controle da informação via satélite, e digitalização de alvos são passos no aprimoramento do Exército do imperialismo[...], manifestada por Donald Rumsfeld, de que 'uma nova geração de armas' propiciará o domínio do século XXI para o Império Americano[...].

Da tese de doutoramento de Kleinrock, no *Massachusetts Institute of Technology* (MIT), sai um dos maiores subsídios para viabilizar as redes de computadores: uma teoria matemática para a troca de pacotes de dados (*packet switching*). Tal comutação consiste, basicamente, em dividir um arquivo digital – como vídeo, imagem e texto – em pedaços sistemáticos e eficientes, chamados de pacotes, os quais carregam o endereço da máquina de destino. Somente por meio dessa engenharia é que arquivos de tipos e tamanhos diferentes podem trafegar numa rede de computadores[52].

Em outras palavras, se "as redes [de computadores] são sistemas que permitem a comunicação entre vários locais e várias pessoas" (HAYDEN, 1999, p. 21), a ARPANET, *per se*, possui uma estrutura autoexpansível e descentralizada. Assim, a Internet – enquanto herdeira dessa mesma tecnologia – mantém, até os dias atuais, tais características que lhe possibilitam ser, por natureza, livre e anárquica.

Entretanto, como aponta Gagnon (2008, p. 49, 63), o monopólio da caserna sobre as redes de computadores não dura muito, pois a disciplina de Redes de Computadores passa a ser ensinada e difundida em todo o mundo.

Não obstante, a ARPANET sozinha não seria capaz de fazer com que sua utilização fosse realidade para mais de dois bilhões de usuários (ESTADOS UNIDOS, 2011a, p. 1). E esse fato está atrelado a outro: o desenvolvimento da Internet é um resultado marcante da Revolução da Informação ou Terceira Revolução Industrial.

Como seu nome já aponta, trata-se de uma revolução, e não de uma simples mudança ou ruptura trivial de paradigmas. Basta lembrar que a Primeira Revolução Industrial principia na Inglaterra, no final do século XVIII, e marca o início da história mundial contemporânea (VIZENTINI, 2006, p. 13, 21, 24-30, 54). A Segunda Revolução Industrial, datada do último quartel do século XIX, tem como signo o crescente processo de industrialização, bem como o "acirramento do imperialismo, [...]a formação de blocos militares antagônicos, [...] duas

---

[52] Para uma explicação mais detalhada acerca da comutação de pacotes, *vide*: Hayden (1999, p. 23-26), Kleinrock (2008, *passim*) e Thing (2003, p. 624-625).

guerras mundiais[...]". (VIZENTINI, 2006, p. 15, 73, 98-100, 135). Essa segunda revolução também acelera "tecnicamente as comunicações", criando "novos meios de difusão de ideias" (VIZENTINI, 2006, p. 147).

Já a Terceira Revolução Industrial – que tem início na década de 1970 – carrega consigo o modelo científico-tecnológico e baliza o desgaste hegemônico dos EUA, coincidindo com o fim da URSS, ao mesmo tempo em que impulsiona áreas como a informática e a comunicação (VIZENTINI, 2006, p. 16, 273).

No mesmo período em que o Império Soviético começa a se dissolver, dois fatos importantes para o desenvolvimento da Internet ocorrem: a ARPANET engendra a *Militar Network* ou MILNET e o Protocolo de Controle de Transmissão (TCP, de *Transmission Control Protocol*)(*) é implementado.

É importante citar esses dois acontecimentos por que eles demonstram um contínuo interesse militar no campo das comunicações seguras e por que, uma vez implantado um protocolo universal para comunicação em redes de computadores, o próximo passo para se chegar a um verdadeiro espaço cibernético ou uma "rede das redes" é a concretização do hipertexto – possível apenas com o advento do Protocolo de Controle de Transmissão/ Protocolo de Internet (TCP/IP, de *Transmission Control Protocol/Internet Protocol*).

Assim, entre o final dos anos 1980 e início dos 1990, o pesquisador britânico Tim Berners-Lee, escreve sobre uma possível e viável proposta[53] sobre interconectar redes de computadores numa única rede mundial de computadores. Surge, assim, teórica e empiricamente, a Internet.

Os trabalhos de Bernes-Lee sobre a concretização do hipertexto[54] são fulcrais para o desenvolvimento da Internet como ela é conhecida e utilizada até hoje. Aliada ao fato de que a ARPANET possibilita a conexão de computadores em redes, a criação, por parte de Berners-Lee, do Protocolo de Transferência de Hipertexto (HTTP, de *Hypertext Transfer Protocol*) e da Linguagem de Marcação de Hipertexto (HTML, de *HyperText Markup Language*) fornece vida à rede mundial de computadores ou simplesmente WWW (*World Wide Web*)(*)[55].

Ao longo dos anos 1990 e 2000, a Internet é impulsionada, dentre outros, graças à diminuição do preço dos computadores e do acesso à Internet, possibilitando sua popularização em escala planetária. Assim, a última Revolução Industrial – agora, já aportada

---

[53] Para ler a proposta original de Berners-Lee, acessar: http://w3.org/History/1989/proposal.html.

[54] Lembra-se que a concepção do hipertexto é centenária, remontando a autores da linguística. A nota de rodapé é, assim, um exemplo de hipertexto todo. Cf. LOPES; MACIEL, 2010.

[55] A título de demonstração dessa concepção teórica, os endereços na Internet possuem tais elementos aqui tratados: o "http", o "www" e, em alguns casos, terminam com um ".html". Ex.: *http*://*www*.nasa.gov/index.*html*.

no fenômeno da globalização[56] – impele um ritmo enorme à pesquisa e desenvolvimento (P&D) e à C&T baseadas nos fantásticos avanços da microcomputação e da possibilidade de interconectar os sistemas financeiros e econômicos, tendo a Internet como plataforma.

A partir do século XXI, o número de internautas também acompanha quantitativamente a evolução da rede mundial de computadores: quase 300 milhões, ainda no final do ano 2000 (LUPI, 2001, p. 199). A Tabela 2 apresenta um panorama sobre tal aumento até os dias atuais.

Tabela 2 – Uso da Internet em relação à população mundial (2000-2012)

Região	Estimativa populacional (2012)	Nº de internautas (2000)	Nº de internautas (2012)	Penetração populacional na Internet[a)]	Crescimento internautas (2000-2012)[b)]	Utilizadores da tabela[c)]
África	1.073.380.925	4.514.400	167.335.676	15.6 %	3.606,7 %	7,0 %
Ásia	3.922.066.987	114.304.000	1.076.681.059	27.5 %	841,9 %	44,8 %
Europe	820.918.446	105.096.093	518.512.109	63,2 %	393,4 %	21,5 %
Oriente Médio	223.608.203	3.284.800	90.000.455	40,2 %	2.639,9 %	3,7 %
América do Norte	348.280.154	108.096.800	273.785.413	78,6 %	153,3 %	11,4 %
Am. Central e do Sul	593.688.638	18.068.919	254.915.745	42,9 %	1.310,8 %	10,6 %
Oceania e Austrália	35.903.569	7.620.480	24.287.919	67,6 %	218,7 %	1,0 %
Total Mundial	**7.017.846.922**	**360.985.492**	**2.405.518.376**	**34,3 %**	**566,4 %**	**100,0 %**

Fonte: INTERNET WORLD STATS, 2012a, tradução nossa.
Legenda: a) A fórmula leva em conta a Estimativa populacional (2012) e o Nº de internautas (2012).
b) Leva-se ponderadamente em conta o Nº de internautas (2012) e o Nº de internautas (2010).
c) Leva-se em conta o Total Mundial do Nº de internautas (2012) e o Nº de internautas (2012) de cada região.

Logo, como exposto até aqui, "o nascedouro da Internet se forma com uma característica intrinsecamente descentralizada, anárquica e em autoexpansão, permanecendo assim até os dias atuais" (LOPES, 2011d, p. 2). Em outras palavras, por ser "uma rede sem centro, sem dono, cuja inteligência encontra-se nas máquinas dos usuários" (MERCADANTE, 2011), a Internet é um ambiente propício para a disseminação de todos os tipos de relações sociais, transações, possibilidades e, concomitantemente, de mazelas e ameaças, tanto para os indivíduos quanto para os Estados.

A próxima subseção enfoca justamente o *modus operandi* de como se dá uma securitização e, mais especificamente, como o setor militar securitiza as questões provenientes desse ambiente autoexpansível, descentralizado e anárquico.

[56] Held e McGrew (2001, p. 12) apontam que, ao lado da vitória do capitalismo sobre o socialismo soviético, a "rápida difusão da revolução da informação" ajuda a alargar os debates acerca do fenômeno da globalização.

2.2.2 O processo de securitização: reflexos para o campo cibernético

O vocabulário que envolve a teoria ora em tela possui algumas palavras-chave: segurança, setor, objeto referente, ameaça existencial, medidas emergenciais, ator securitizador, ato de fala, movimento securitizador, politização e questão de segurança. Portanto, torna-se imprescindível para os objetivos deste trabalho situá-los agora.

Como visto, para os teóricos da Escola de Copenhague, segurança é um tipo particular de política que é aplicável a uma variedade de questões (BUZAN *et al.*, 1998, p. 239). Com esta definição ampla e oferecendo um método operacional construtivista[57], para diferenciar o processo de securitização do de politização (BUZAN *et al.*, 1998, p. vii, 5, 239), tais pensadores são situados na vertente crítica dos Estudos de Segurança Internacional[58], *i.e.*, entre tradicionalistas e abrangentes (BUZAN *et al.*, 1998, p. 4, 11, 22, 239).

O *framework* elaborado por esses autores para analisar a segurança leva em conta cinco setores: o militar, o político, o econômico, o ambiental e o societário (BUZAN *et al.*, 1998, p. vii). Tais teóricos salientam ainda que "segurança significa sobreviver em face às ameaças existenciais, porém o que constitui uma ameaça existencial não é o mesmo entre os setores" (BUZAN *et al.*, 1998, p. 27, tradução nossa[59]).

Tendo-se em mente o problema de pesquisa desta Dissertação, as argumentações aqui apresentadas se centram apenas no setor militar, no qual o objeto referente é geralmente o Estado, embora possam ser também outros tipos de entidades políticas (BUZAN *et al.*, 1998, p. 22, tradução nossa). Isso, porém, não implica dizer que se parte de um viés estritamente tradicionalista; pelo contrário, reconhece-se que as ameaças e questões de defesa cibernética podem transbordar para os demais setores e vice-versa[60].

Segurança é uma prática autorreferencial, ou seja, algo só se torna uma questão de segurança não por que uma ameaça existencial realmente existe, mas por que ela é dramatizada e apresentada como tal (BUZAN *et al.*, 1998, p. 24, 26). Assim, um ator securitizador[61] reivindica uma necessidade e um direito de tratá-la por intermédio de meios

---

[57] Cf. (BUZAN *et al.*, 1998, p. 26.

[58] Quanto ao posicionamento epistêmico dos teóricos da Escola de Copenhague, ver Buzan *et al.* (1998, p. 2, 20).

[59] Texto original: "*Security means suvirval in the face of existential threats, but what constitutes an existential threat is not the same across diferent sectors*".

[60] Basta, por exemplo, notar a literatura sobre proteção das infraestruturas críticas baseadas em sistemas *Supervisory Control and Data Acquisition* (SCADA)(*), como hidroelétricas, gasodutos e reatores nucleares. Dependendo dos ataques virtuais a tais infraestruturas – como os ocorridos no Irã –, as consequências ao meio ambiente podem atingir a mais de um país, transbordando, assim, para os demais setores.

[61] São seus outros sinônimos: "agente securitizador" e "securitizador" (BUZAN *et al.*, 1998, *passim*).

extraordinários (BUZAN *et al*., 1998, p. 26). É nesse sentido que securitização se torna sinônimo de ato de fala (*speech act*), ou seja, ao falar, algo é feito (BUZAN *et al.*, 1998, p. 26).

Com tal definição de segurança, os teóricos da Escola de Copenhague elaboram um espectro, contendo três tipos de política, que vai da não politizada até a securitizada, passando pela politizada. Basicamente, uma questão pública – que se diz – de segurança é: (i) não politizada, quando não está na pauta do Estado ou não se encontra nas esferas públicas de discussão e decisão; (ii) politizada, quando é parte de política pública (*policy*), requerendo decisão e alocação de recursos do governo; e (iii) securitizada, quando a questão é apresentada como uma ameaça existencial, exigindo medidas emergenciais e justificando ações fora do escopo normal do processo político (BUZAN *et al*., 1998, p. 23-24).

Politização, em outras palavras, "significa fazer uma questão parecer estar aberta a opiniões, uma matéria de escolha, alguma coisa que é decisiva e que, por isso, vincula responsabilidades" (BUZAN *et al*., 1998, p. 29, tradução nossa[62]).

Assim, o processo de securitização de uma questão de segurança é uma visão mais extrema/intensificada da politização, a qual pode variar entre Estados e no tempo[63] (BUZAN *et al*., 1998, p. 23-24, 29; RUDZIT, 2005, p. 308).

Nesse sentido, securitizar uma questão no setor militar tem sido utilizado como um álibi para legitimar o uso da força (BUZAN *et al*., 1998, p. 21). Em termos de defesa cibernética, é esse teor reivindicatório da máxima weberiana que parece nortear parte da política de defesa estadunidense, haja vista que:

> O Pentágono entende que sabotagem de computadores vindo de outro país pode constituir um ato de guerra, uma descoberta que pela primeira vez abre a porta para os EUA responder [ataques virtuais], usando força militar tradicional. (GORMAN; BARNES, 2011, tradução nossa[64]).

Outro exemplo da tentativa de securitização do ciberespaço por parte dos EUA é visto na *National Strategy to Secure Cyberspace* (EUA-NSSC) (ESTADOS UNIDOS, 2003, *passim*), quando esta imprime mais de 40 vezes o termo "*national cyberspace*" e faz a explícita diferença entre os ciberespaços estadunidense e não estadunidense – "*our*" e "*their*", respectivamente (GAGNON, 2008, p. 51) –, dando poderes especiais ao *U.S. Department of Homeland Security* (EUA-DHS).

---

[62] Texto original: "*Politicization means to make an issue appear to be open, a matter of choice, something that is decided upon and that therefore entails responsibility*[...]".

[63] O ESMC busca demonstrar isso (cf. Seção 3).

[64] Texto original: "*The Pentagon has concluded that computer sabotage coming from another country can constitute an act of war, a finding that for the first time opens the door for the U.S. to respond using traditional military force*".

Em continuidade, questões são consideradas securitizadas quando:

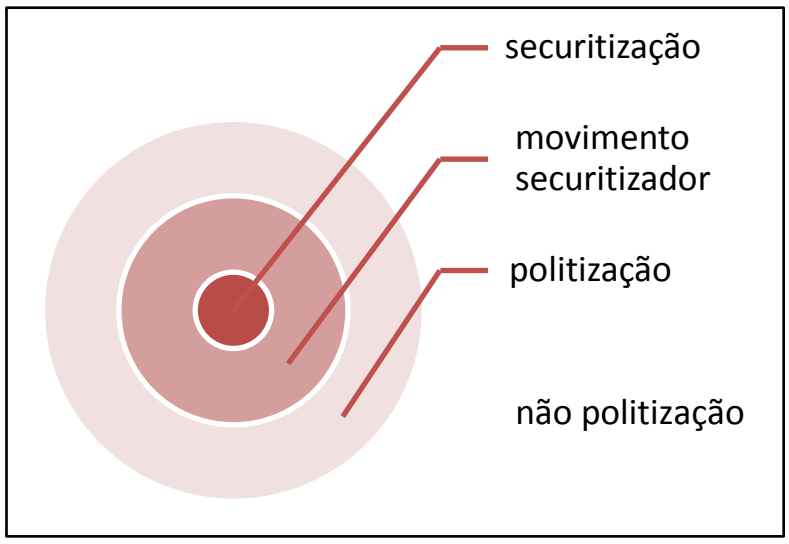
> São encaradas como ameaças existenciais para um objeto referente por um ator securitizador que gera, assim, aprovação de medidas emergenciais que estão além das regras que, de outra forma, se relacionariam. (BUZAN *et al.*, 1998, p. 5, tradução nossa[65]).

Todavia, deve-se observar que o fato de um discurso/argumento apresentar uma questão como uma ameaça existencial para um objeto referente não cria, *per se*, securitização. Isto é o que Buzan *et al.* (1998, p. 25) denominam "movimento securitizador" (*securitizing move*). Para que haja, *de facto*, securitização, mais um estágio é necessário: a audiência deve aceitar a questão como tal. Tendo em mente que uma securitização não pode ser imposta[66], a sutil diferença entre um movimento securitizador e um objeto que está sendo securitizado reside no fato de que, no primeiro caso, não há sinais de aceitação de uma audiência relevante (BUZAN *et al.*, 1998, p. 25, 27).

Em resumo, para a teoria da securitização, um ato de segurança sempre deve ser legitimado por uma audiência, por meio de um ato de fala realizado por um ator securitizador (VILLA; SANTOS, 2010, p. 122).

O Esquema 2 demonstra graficamente os níveis desse processo político.

Esquema 1 – Espectro da securitização, segundo a Escola de Copenhague



Fonte: Elaboração própria.

[65] Texto original: "*They have to be staged as existential threats to a referent object by a securitizing actor who thereby generates endorsement of emergency measures beyond rules that would otherwise bind.*".
[66] No caso da securitização mais extrema – a guerra –, as contrapartes não negociam uma questão entre si, como ocorre normalmente no interior de uma unidade, mas uma busca eliminar a outra (BUZAN *et al.*, 1998, p. 26).

A seguir, listam-se três conjecturas na política internacional envolvendo *cyber warfare* e que têm servido de subsídio para setores militares de alguns Estados dramatizarem suas questões de segurança do ciberespaço.

2.2.3 O debate teórico: o ciberespaço enquanto domínio militar?

Como visto na Subseção 2.2.1, a Internet engendra muitas possibilidades que, antes dela, não eram passíveis de ocorrer. Porém, ela gera também uma série de desafios àqueles que buscam dominar, se apropriar ou limitá-la.

Há autores que compreendem que o ciberespaço é um novo domínio ou topologia – como terra, mar e ar – (CLARKE; KNAKE, 2012, p. 36; PROENÇA JR, 2009, p. 4; Nick Harvey *apud* HOPKINS, 2011b) e outros que não aceitam tal analogia, como Carr (2012, *passim*).

Talvez uma comparação[67] interessante não seja uma topologia limitada ou limitadora na ação ou exploração de seu próprio ambiente, conquanto sua mensuração seja praticamente impossível de ser precisada também.

Este trabalho parte do pressuposto de que não é plausível precisar o ciberespaço. Não é possível, por exemplo, saber onde começam e terminam determinados lugares no ciberespaço. É possível, sim, identificar o endereço IP(*) de aparelhos conectados à Internet. Assim, a melhor analogia que se vislumbra, aqui, é comparar o ciberespaço ao espaço sideral, em toda sua plenitude autoexpansível, onde é possível identificar seus corpos e fenômenos, não seus limites.

Tal assertiva deriva de Proença Jr (2009, p. 4, grifo nosso) quando este argumenta que:

> *Assim como a topologia da órbita próxima à Terra*, a certeza de que algo se pode fazer para influenciar a vontade de outros ou para resguardar a nossa vontade contra a influência de outros ainda não encontrou uma expressão clara [no ciberespaço]. Assim como foi o caso do uso do ar para fins bélicos nas primeiras décadas do Século XX, por exemplo, tem-se ambições, receios e militâncias mais ou menos corporativas, mais ou menos mercadológicas, e *não se tem como saber qual dentre estas visões, se é que alguma, antecipa o que revelará mais adiante*.

De fato, como aponta Proença Jr, é muito complexo afirmar com precisão quais os reais interesses que movem um Estado no ciberespaço: *lobby*, defesa da soberania nacional, controle da ordem interna, *misperception* sobre o papel da polícia ou do funcionamento da Internet, dentre outros. Entretanto, Clarke e Knake (2012, *passim*) dão dois indícios sobre esta resposta: o primeiro diz respeito à proteção das infraestruturas críticas nacionais; e o segundo

---

[67] Vale frisar que Proença Jr sugere tal comparação não em termos físicos ou geográficos, mas relativos às atividades de inteligência, levando-se em conta também o exposto por Clausewitz (cf. Seção 1, *supra*).

– em decorrência do primeiro –, ao fato de que a sociedade civil é quem está na mira de fogo das ameaças provenientes do ciberespaço, como uma extensão do terrorismo.

Os debates civis e militares acerca da *cyber warfare* aumentam à medida que armas e ataques cibernéticos provocam danos cada vez maiores ao Estado – e também ao setor privado. São alguns exemplos desta máxima: os sucessivos ataques virtuais a redes de computadores de vários órgãos governamentais, em todo o mundo – liderados pelo grupo de hacktivistas Anonymous e pelo grupo de *crackers* LulzSec –, em meados de 2011; ao aumento do número de eventos relacionados à defesa cibernética; a criação de instituições e disciplinas militares voltadas ao estudo da defesa cibernética (FERREIRA NETO, 2011).

O General da força aérea estadunidense e ex-Diretor do *Cyberspace Operations Task Force*, Bob Elder (*apud* CLARKE; KNAKE, 2012, p. 36, tradução nossa[68]), é mais efusivo e apregoa que "se você não dominar no ciberespaço, não pode dominar em outros domínios".

Gagnon (2008, p. 50) enfatiza que as novas doutrinas de segurança que tratam do ciberespaço o percebem a partir de um ponto de vista estratégico, levando à criação de novas ideias sobre o papel das Forças Armadas nesse novo ambiente. Para o setor militar estadunidense, o ciberespaço é mais um ambiente para projeção de poder; o "novo 'espaço estratégico', tão importante quanto terra, mar, ar e espaço extra-atmosférico" (GAGNON, 2008, p. 58).

Por outro lado, o setor militar brasileiro entende que é vital "revisar os planejamentos das Hipóteses de Emprego (HE) para considerar as ações no espaço cibernético" (BRASIL, 2012d, p. 12).

Como se vê mais adiante, o Brasil alça as questões de defesa cibernética à categoria de setor estratégico (cf. Subseção 3.3.2.2), o qual, para Rudzit (2012),

> [...]não pode ser da alçada exclusiva da caserna. Se os militares agirem desta forma, estão perdendo a melhor oportunidade para estreitar as relações civil-militares no Brasil, uma vez que é justamente em ambientes livres de hierarquias e abertos à inovação [...]que se conseguirá os melhores indivíduos aptos a se adaptar à realidade cibernética.

2.2.4 O debate empírico: ataques e armas cibernéticas

Episódios envolvendo o uso de NTIC atreladas a antigas formas de se guerrear[69] destacam-se na quase debutante política internacional do século XXI.

---

[68] Texto original: "*If you do not dominate in cyberspace, you cannot dominate in other domains*".

[69] Cf. CARR, 2012, *passim*; CLARKE; KNAKE, 2012, *passim*; LOPES, 2011a, p. 8; NYE, 2008; OPPERMANN, 2009, p. 15-18.

Alguns desses episódios permeiam uma literatura que envolve temas como segurança internacional, política externa e segurança da informação. Nesse ponto, utilizam-se três casos para evidenciar o embate empírico por trás da defesa cibernética.

O primeiro diz respeito aos ataques cibernéticos sofridos pela Estônia, em 2007, e imputados, pelo governo daquele Estado, à Rússia.

O segundo tem a ver com o conflito internacional envolvendo Rússia e Geórgia, em 2008, onde ataques cibernéticos potencializam os tradicionais no território georgiano.

O último caso se refere aos impactos do verme virtual (*worm*) Stuxnet, em 2010, quando tal praga virtual atrasa o programa nuclear iraniano. Pela complexidade do seu código-fonte(*) e pela destreza de seus objetivos políticos, desde então, esse verme é considerado a primeira arma cibernética, *i.e.*, o primeiro instrumento de guerra projetado especificamente para o ciberespaço.

2.2.4.1 Os ataques cibernéticos à Estônia (2007)[70] e à Geórgia (2008)[71]

Ocorrido em 2007, o caso em que o governo da Estônia imputa ao da Rússia a responsabilidade pelos vultosos ataques cibernéticos – principalmente com o uso de ataques distribuídos de negação de serviço (DDoS, de *distributed denial-of-service attack*)(*) – às suas infraestruturas críticas de informação e comunicação. Pela possibilidade de se deslumbrar, pela primeira vez, alguns anseios negativos quanto ao uso de NTIC contra um Estado, este caso fica conhecido como a Primeira Guerra Virtual (CLARKE; KNAKE, 2012, p. 30; SUTHERLAND, 2012, p. 161).

Todo o imbróglio se origina com a remoção de uma antiga estátua soviética – em memória ao soldado morto – do centro para uma região afastada da capital estoniana, Tallinn. Os descendentes russos e parte da própria população russa entendem tal ato como uma afronta à sua história e, no mesmo dia da remoção, iniciam manifestações nas ruas, que acabam em grande violência e repressão policial. Concomitantemente, uma série de ataques cibernéticos faz com que os sítios virtuais (*sites*) estonianos saiam do ar, ilhando o país do restante do mundo. Sistemas bancários e serviços aos cidadãos saem do ar, bem como os de

---

[70] A presente Subseção é um resumo deste caso relatado em: Bezerra ([2009]); Clarke e Knake (2012, p. 30); Gagnon (2008, p. 46-48); Leman-Langlois (2012, p. 1); Lopes (2010, *passim*; 2011a, p. 7-8); Lopes e Teixeira Jr (2011); Nye Jr (2008; 2011b); Oppermann (2009, p. 12-15), Rumer (2007, p. 8).

[71] Esta subseção é um resumo dos acontecimentos que envolvem este caso, obtidos em: Clarke; Knake (2012, p. 17-21); Geórgia (2008); Gorman e Barnes (2011); Saalbach (2012, p. 16-17); Lopes (2010; 2011a, p. 8); Lopes e Teixeira Jr (2011).

troca/solicitação de informação são danificados de forma tal que a Estônia pede ajuda à OTAN e aos EUA.

Embora mesmo com especialistas em informática relatando que tal episódio está mais ligado à atuação de pessoas físicas do que a governos – por meio de *bots*(*) e *botnets*(*) –, desde então, a OTAN mantém, na capital estoniana, seu centro de defesa cibernética, o *Cooperative Cyber Defence Centre of Excellence* (NATO CCD COE).

Segundo Leman-Langlois (2012, p. 6), tanto os ataques cibernéticos quanto a cooperação entre OTAN, FBI e Estônia não foram totalmente explicados.

Um ano após o ocorrido na Estônia, especialistas em TIC se espantam com os danos causados pelos ataques virtuais russos causados contra a Geórgia, no âmbito do conflito bélico pela independência da Ossétia do Sul (OPPERMANN, 2009, *passim*; LOPES, 2010; 2011a, p. 5).

O que marca este caso, em especial, é o fato de que ataques cibernéticos – muito semelhantes aos contra a Estônia – provenientes dos militares russos precedem ataques bélicos tradicionais ao território georgiano. É pacífico na literatura que o fato de a infraestrutura crítica baseada em NTIC georgiana ter sido danificada impossibilita o governo e os militares daquele país a se organizarem adequadamente. Em outras palavras, a guerra cibernética potencializou a tradicional.

Sobre este fato, Nye (2008) afirma que se tratam dos primeiros ataques cibernéticos significativos que acompanham um conflito armado e que essa idiossincrasia da segurança internacional será a nova tônica dos conflitos bélicos do século XXI.

O próximo caso torna a afirmação de Nye um pouco equivocada, pois, como se vê, é possível utilizar ataques cibernéticos para se evitar ataques tradicionais.

2.2.4.2 A primeira arma cibernética atinge o Irã: Stuxnet (2010)[72]

Em 2010, sistemas computacionais de infraestrutura crítica nuclear iraniana sofrem sérios danos. A causa: a atuação sistemática e imperceptível do verme denominado Stuxnet (CLARK; KNAKE, 2012, p. 291; LOPES, 2011a; IRÃ, 2011; SANGER, 2012a, p. ix).

Especialistas em segurança da informação do mundo todo se surpreendem com a sofisticação da engenharia dessa praga virtual (SUTHERLAND, 2012, p. 164), a qual, atacando o sistema SCADA – ou sistema de controle de supervisão e aquisição de dados –

[72] Boa parte do que é apresentado aqui, corrobora com: Broad *et al.* (2011); Falliere *et al.* (2011); Hopkins (2011); Irã (2010; 2011); Sanger (2012a; 2012b, p. ix-xiii, xvii); Lopes (2011a, p. 8).

desenvolvido pela Siemens, atrasa o programa nuclear iraniano em muitos meses (CLARKE; KNAKE, 2012, p. 291-296; FERREIRA NETO, 2011; SANGER, 2012a, p. 188-225).

Muito se cogita acerca da autoria desse *malware*(*) (SUTHERLAND, 2012, p. 168). Em entrevista a este autor, Woodward (2012), que chega a analisar o código-fonte do verme, afirma que é praticamente improvável que o Stuxnet tenha sido desenvolvido por uma empresa ou universidade, pois seu alvo é assaz incomum: o sistema SCADA da Siemens de centrífugas enriquecedoras de urânio (CLARKE; KNAKE, 2012, p. 291). Mas é no livro de um professor de Harvard que o que parecia ser apenas cogitações - como posto, por exemplo, em Hopkins (2011b) – mostra-se uma surpreendente questão de política externa para sabotar o programa nuclear iraniano, sem o uso de ataques bélicos convencionais.

Segundo Sanger (2012a, p. ix, 188), o Stuxnet é o resultado de uma parceria entre os governos estadunidense e israelense engendrada sob o manto do programa ultrassecreto *Olympic Games* (Jogos Olímpicos), no final do segundo governo W. Bush. Tal programa tem um objetivo estratégico e outro político: sabotar o programa nuclear iraniano e convencer Israel de que é possível lidar com essa questão sem ser por meio de ataques aéreos (SANGER, 2012a, p. 190-192). Ainda, segundo esse autor, o presidente Obama tinha a real noção de "[...]que, com cada ataque, ele empurrava os EUA para um novo território" (SANGER, 2012a, p. xi, tradução nossa[73]).

É também Sanger (2012a) que figura a mais detalhada narrativa de como o programa que dá origem ao Stuxnet é política, jurídica e tecnicamente arquitetado: "[...] a confecção do verme demandou meses, sobretudo para que a equipe jurídica se certificasse de que seu código-fonte não violava nenhuma lei de conflito armado" (SANGER, 2012a, p. 193, tradução nossa[74]).

A explicação de como o verme cai na Internet e, assim, fica mundialmente conhecido, deriva mais de uma falta de planejamento do que de um erro operacional:

> Um cientista iraniano plugou seu *notebook* no controlador computacional de uma das centrífugas e o verme saltou para sua máquina. Quando, mais tarde, ele conecta o mesmo *notebook* na Internet, o verme se liberta e começa a se replicar. (SANGER, 2012a, p. xii).

Cogita-se também que alguma parte que cabia aos israelenses – vale lembrar que o código-fonte do *software* contém milhares de milhões de linhas de programação – não é compartilhada com os EUA. Mas a falha, sim, é compartilhada entre ambos.

---

[73] Texto original: "*He also acutely aware that with every attack he was pushing the United States into new territory.*".
[74] Texto original: "[...]*much of it [time] spent with lawyers trying to make sure that the code they were writing did not violate the laws of armed conflict.*".

Se o que é exposto pela literatura, acerca do papel dos EUA na confecção do Stuxnet, se confirmar daqui a algumas décadas – quando os documentos do *Olympics Games* se tornam públicos –, ter-se-á também a corroboração de que, após a Guerra Fria, os EUA tomam "algumas vantagens dentre elas o fato de o poder militar" (GAIO, 1998, p. 50) ser utilizado "como um instrumento de política externa [...]contra os que pretendem desafiar importantes interesses seus[...]" (Dimitri Simes *apud* GAIO, 1998, p. 50-51).

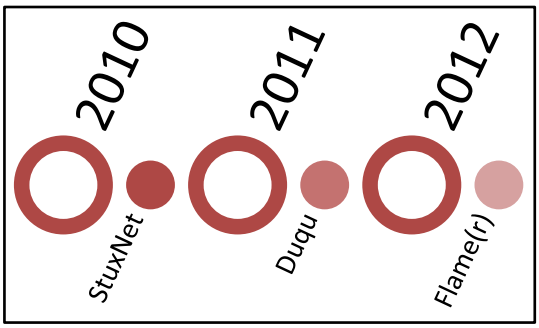
Uma vez na Internet, o Stuxnet é alterado, compartilhado e direcionado para diferentes alvos[75].

Uma variante bastante conhecida do Stuxnet é o Duqu, descoberto em 2011, quando o *Laboratory of Cryptography and System Security* da *Budapest University of Technology and Economics* (CrySyS) emite um relatório sobre os resultados da análise no código-fonte do Duqu: segundo o documento, tais resultados abrem um novo capítulo na história dos ataques cibernéticos que são direcionados a alvos específicos (BENCSÁTH *et al.*, 2011, p. 2).

Em meados de 2012, uma segunda variante do Stuxnet, ainda mais complexa, vem à tona: Flame(r) ou sKyWIper (BENCSÁTH *et al*., 2011, *passim*). Até o mês de maio de 2012, quando da criação de sua vacina, nenhum dos 43 antivírus testados pela equipe de respostas a incidentes informáticos (CERT, de *computer emergency response team*)(*) iraniana pôde detectá-lo (IRÃ, 2012).

O Esquema 2 demonstra a linha do tempo do StuxNet e de suas variantes.

Esquema 2 – Linha do tempo do StuxNet e de suas variantes



Fonte: Elaboração própria.

Desde então, o Stuxnet é considerado a primeira arma cibernética projetada para, por intermédio de incursão cibernética, produzir danos a infraestruturas de um país estrangeiro

[75] Daí o grande temor que os EUA têm de que a cria se volte contra seu criador.

(CLARKE; KNAKE, 2012, p. 291; HOPKINS, 2011a; SANGER, 2012a, p. x, 188; SUTHERLAND, 2012, p. 164-165; WOODWARD, 2011).

Para o Ministro da defesa britânico, Nick Harvey, embora as armas cibernéticas não substituam as convencionais, é certo que ações no ciberespaço farão parte do futuro campo de batalha (HOPKINS, 2011b). É nesse mesmo viés que Lopes e Teixeira Jr (2011) proclamam que o ciberespaço é um novo *front*.

Assim, tem-se percebido que o setor militar de muitos Estados atenta aos acontecimentos que envolvem o mundo das NTIC, sobretudo no que concerne ao ciberespaço.

A próxima seção busca demonstrar como esse processo intersubjetivo de assimilação e dramatização militar quanto às ameaças ciberexistenciais opera nos EUA, Brasil e Canadá, de forma isolada, conjunta e comparativa. Embora trate de aspectos epistêmicos à concretização dos objetivos deste trabalho, a arquitetura por traz da próxima seção está relacionada intrinsecamente a aspectos conceptuais abordados nesta seção.

3 ANÁLISE EXPLORATÓRIA DA SECURITIZAÇÃO MILITAR DO CIBERESPAÇO: OS CASOS ESTADUNIDENSE, BRASILEIRO E CANADENSE

> Guerra cibernética implica também desenvolver novas doutrinas sobre os tipos de forças necessárias, onde e como implantá-los e o que e como atacar o lado inimigo (ARQUILLA; RONFELDT, 1993, p. 146, tradução nossa[76]).

Como se expõe na Seção 1, o segundo objetivo específico corresponde à projeção das condições necessárias ao processo de securitização militar na política internacional hodierna, sendo seus resultados – ou consequências internacionais – o derradeiro objetivo específico, visto apenas na quarta seção "Conclusão".

Por ora, para que a presente Seção atinja o segundo objetivo específico – explicar quando a securitização militar do ciberespaço é considerada bem sucedida (BUZAN *et al.*, 1998, p. 32) –, é preciso esboçar uma análise que leve em conta idiossincrasias militares e cibernéticas, permanecendo fiel aos pressupostos da Escola de Copenhague.

Para tanto, explicam-se os motivos para a utilização dos casos ianque, tupiniquim e canadiano, bem como o porquê de aglutinar os dois estilos de pesquisas numa só perspectiva. Em seguida, oferta-se o Espectro da Securitização Militar do Ciberespaço (ESMC), quando é possível analisar detalhadamente sítios virtuais, documentos e instituições de defesa cibernética de cada um dos Estados selecionados.

3.1 As escolhas dos casos e do estilo de análise

Tem-se em mente que o tamanho da amostra é deveras baixo (n = 3), se comparado à população de Estados do sistema internacional (N = 195) (ESTADOS UNIDOS, 2013).

Tal seleção se explica, primeiro, pelo fato de que, a partir do momento em que se opta pela teoria da securitização, avalia-se cada Estado de maneira bem meticulosa, buscando compreender não só os dados em si, mas também os processos políticos pelos quais eles são gerados – pois é o fato político que realmente importa para a teoria da securitização. Isso impede, por exemplo, que, em dois anos – período de feitura da pesquisa e da escritura desta Dissertação –, possam-se satisfatoriamente entender processos securitizatórios de um número maior de casos[77].

---

[76] Texto original: "*Cyberwar may also imply developing new doctrines about the kinds of forces needed, where and how to deploy them, and what and how to strike on the enemy's side*".

[77] Em Lopes (2011b), a amostra é acrescida de mais dois países (n = 5). Mesmo assim, a análise se limita apenas a questões institucional e documental superficiais.

Os três países selecionados estão entre as 10 maiores economias do mundo, possuem grandes territórios e desempenham papéis, cada vez mais, de protagonistas no cenário internacional. A seleção de EUA, Brasil e Canadá se dá também por razões geopolíticas e logísticas: o fato de os três Estados se situarem no mesmo continente possibilita um recorte geral dos principais e maiores atores estatais americanos, no que tange à defesa cibernética[78]; e a possibilidade de realizar pesquisas *in loco*, tendo acesso a fontes ligadas diretamente aos temas em apreço.

Especificamente, o caso estadunidense se projeta como particular, pois é o que figura em praticamente todos os *frameworks* e análises relacionados à defesa cibernética[79], bem como é um dos primeiros atores a tratar as ameaças ciberespaciais como "de segurança nacional". Ademais, por ser o nascituro da Internet (cf. Subseção 2.2.1), o Estado ianque "[...]atualmente, exerce uma 'ciber-hegemonia' sobre a Internet" (GAGNON, 2008, p. 63, tradução nossa[80]). É nesse sentido que Duarte (2012a, p. 37) também se direciona, ao analisar a digitalização na guerra: "os Estados Unidos são a principal referência desse esforço".

No que tange ao caso brasileiro, nota-se um crescente interesse do setor militar pela defesa cibernética, no que pese à guerra cibernética. Provas disso são os vários eventos que a própria caserna promove[81] e/ou nos quais se faz ativamente presente[82]. Os lançamentos da Estratégia Nacional de Defesa (BRA-END) e da Política Cibernética de Defesa (BRA-PCD), bem como a criação do Centro de Defesa Cibernética do Exército (BRA-CDCiber) parecem indicar um interesse militar pelas questões de segurança que envolve o ciberespaço. Esse interesse é posto a provas na Subseção 3.3.2.

Já o caso canadense se prostra como uma incógnita no que tange aos assuntos pertinentes ao uso estratégico do ciberespaço: suas relações militares com os EUA podem enviesar sua própria política de defesa cibernética. Como as políticas exterior e de defesa estão estritamente associadas, a securitização do ciberespaço, por parte dos militares canadenses, pode ajudar a explicar seu dilema entre autonomia estatal, em face às relações assimétricas com os EUA (PAQUIN, 2009, *passim*), e a busca por uma identidade própria no cenário internacional.

---

[78] Lopes e Medeiros (2011) analisam as segurança e defesa cibernéticas no âmbito da OEA e concluem que a mesma negligencia a última, em razão da primeira.

[79] O mais famoso é o *Cyber War Strenght*, de Clarke e Knake (2012, 148-149), que leva em conta apenas aspectos objetivos.

[80] Texto original: "*The USA currently exercises 'cyberhegemony' over the web*[...]".

[81] Como a realização do Seminário de Defesa Cibernética (BRASIL, 2012b; 2012c) e da Jornada de Trabalho de Defesa Cibernética (BRASIL, 2011b), ambos pelo Ministério da Defesa (MD) do Brasil.

[82] Ver participação de militar do Exército na palestra "Guerra Cibernética e Ameaças" (BRASIL, 2013b).

Quanto aos critérios que levam à seleção de um estilo misto de análise, atribui-se à influência da própria complexidade dos: (i) tema, que, por ser recente, carece, ainda, de muitas fontes de dados e de análise, principalmente, sobre Brasil e Canadá; e (ii) *frameworks* de análise utilizado e proposto – o espectro da securitização e o ESMC, respectivamente.

Como já antecipado, Buzan *et al.* (1998, p. 30) informam que mensurar objetivamente a securitização de uma questão é quase impossível, haja vista que cada Estado possui seus próprios limites para definir o que é uma ameaça. Entrementes, King *et al.* (1996, p. 5, tradução nossa[83]), por sua vez, asseveram que "se quisermos entender o mundo em rápida mudança social, temos de incluir informações que não podem ser facilmente quantificadas, bem como as que podem".

Munindo-se de tais recomendações, a presente Dissertação busca, então, ofertar uma alternativa de superação ao desafio proposto pela Escola de Copenhague, que, ao mesmo tempo, dialogue com dados e análises de estilos diferentes.

Propõe-se, então, o ESMC, que leva em conta tanto aspectos intersubjetivos quanto objetivos, a fim de esboçar um panorama o mais próximo possível do processo de securitização das ameaças cibernéticas no nível nacional e de seus eventuais reflexos no internacional.

Um dos pressupostos dessa ferramenta repousa no fato de que algumas consequências dessa securitização podem ser evidenciadas também objetivamente, como ocorre com as instituições militares de defesa cibernética[84]. Alerta-se para o fato de que apenas contar quantas instituições há, não atinge aos objetivos propostos. Deve-se levar em conta os pormenores da criação de tal instituição, respeitando-se, portando, o processo político.

Com isso, também não se perde de vista o fato de que a parte mais importante numa análise sobre securitização, como já exposto, consiste em explicar *como* ela ocorre, isto é, de que forma um ator securitizador securitiza uma questão para uma audiência relevante.

Nessa linha de raciocínio, opta-se pelo estilo qualiquantitativo de pesquisa, indo de encontro, assim, ao que Flick (2009) defende: que a pesquisa qualitativa é superior à quantitativa. Também, não se sustenta aqui que o contrário é verdadeiro. Para satisfazer aos desafios ensejados pelo problema de pesquisa desta Dissertação, vai-se, sim, ao encontro de uma conciliação entre ambos[85].

---

[83] Tradução livre de: "*If we are to understand the rapidly changing social world, we will need to include information that cannot be easily quantified as well as that which can*".

[84] "Mmilitar de defesa cibernética", sob um viés mais rígido, pode ser considerado pleonasmo, uma vez que quem cuida da defesa de um Estado é o poder militar. Pelo fato de o tema ser recente, usa-se tal expressão.

[85] Cf. ECO, 1996, p. 25; GÜNTHER, 2006, *passim*; KING *et al.*, 1996, p. 5; LANDMAN, 2008, p. 20-21, 78-81.

Todavia, realizam-se três considerações sobre determinadas fontes de dados que podem impactar um trabalho sobre defesa cibernética, como este.

A primeira se refere à descrição de objetos: bastantes dados relevantes ao tema em tela, por se situarem na seara militar, estão classificados como secretos ou ultrassecretos. Muitos deles, portanto, não são revelados, deixando de ser analisados sob um enfoque mais comparativo. Restam, então, documentos publicados, os quais, amiúde, não revelam todos os dados, apresentando ambiguidades e generalizações com outras áreas correlatas às NTIC, mas que não dizem respeito especificamente à defesa cibernética. Segue-se um exemplo teórico dessa problemática: adquirir equipamentos e serviços informáticos em geral e desenvolver *softwares* para fins administrativos, de um lado; e investir em equipamentos e serviços – como cursos – voltados exclusivamente à questão da defesa cibernética. Um exemplo empírico sobre o exposto está em Brasil (2007a), onde não é possível identificar tal separação com a aquisição de equipamentos que podem ser tanto para manutenção tecnicoadministrativa quanto para defesa cibernética, por parte do Exército Brasileiro (BRA-EB).

A segunda consideração pode ter relação com a primeira, mas não é uma regra: é prática comum de Estados utilizarem o chamado orçamento negro (*black budget*) para camuflar, sob pseudônimos, projetos que precisam ser desenvolvidos com dotação de recursos públicos, mas que não podem ser detalhadamente publicados, já que põem em risco a segurança nacional ou a de uma autoridade, por exemplo[86]. Mais uma vez, muito dado deixa de ser revelado ou, num outro sentido, pouco dado é revelado sobre o projeto/programa em si.

A terceira e última observação se relaciona mais especificamente à questão orçamentária de defesa[87]. Pactua-se com a hipótese de que comparar investimentos[88] em P&D e C&T de defesa cibernética é uma tarefa deveras complexa, pois envolve questões não somente quantitativas, mas também qualitativas que, caso não analisadas conjuntamente, podem enviesar uma análise ou, simplesmente, não revelar todas as nuances da amostra.

Arquilla e Ronfeldt (1993, p. 141-142) arguem que a guerra atual não gira mais em torno apenas de quem coloca capital, homens e tecnologia (elementos quantitativos) no campo de batalha, mas também e, principalmente, de quem tem a melhor informação (elemento qualitativo) sobre ele. É o que von Clausewitz (2007, p. 64) também já ressalta há mais de 150 anos. Só que, na Era da Informação e no que tange à defesa cibernética, o fato de um

---

[86] Buzan *et al*. (1998, p. 28) vinculam-os aos "*black programs*".

[87] Para uma visão holística sobre distinção de orçamento consolidado de defesa, *vide* Proença Jr e Diniz (1998, p. 52-53, 56). Para um exemplo empírico desta problemática, ver Apêndice A.

[88] A literatura na área de defesa prefere utilizar a expressão "investimento" a "gasto" militar.

Estado investir mais ou menos em *software* e/ou *hardware* do que outro se torna praticamente irrelevante, se a análise for puramente quantitativa.

Por exemplo, ao contrário do poder persuasório de porta-aviões, que, quanto maior/potente, melhor; uma pequena divisão militar – ou, mesmo, um só oficial – pode obter informações ultrassecretas ou mesmo auferir danos a bases informacionais, utilizando-se apenas de um ultrapassado computador e de uma conexão à Internet bastante limitada[89]. Em outras palavras: o pressuposto de que o elemento humano domina a tecnologia, e não o contrário[90], estende-se à defesa cibernética de uma forma ainda mais extremada.

Há que se comparar, conjunta e qualiquantitativamente, as componentes que envolvem a defesa cibernética. Talvez, uma possível brecha para países, como Coreia do Norte, tomarem partido em relação a seu atraso tecnológico[91] resida na capacidade de, ciberneticamente, obterem informações privilegiadas e/ou produzirem danos a infraestruturas.

O documento que mais se aproxima da idealização/reivindicação desse *orçamento consolidado de defesa cibernética* aqui defendido é a BRA-PCD, que propõe a "[...]criação de programa orçamentário para viabilizar as ações e atividades do[...]" setor cibernético (BRASIL, 2012e, p. 12). Com isso, é possível mensurar, por exemplo, quanto, de fato, o País investe nessa área, e não realizar pressuposições.

Ratifica-se também o fato de que tais empecilhos podem até limitar o objeto de um estudioso de defesa cibernética, mas não a problematização do tema.

Com estas ressalvas, parte-se agora para explicar como os dados referentes a este trabalho são coletados e analisados.

3.2 A coleta e a análise dos dados

Qualquer coleta de dados busca conhecer certas características dos elementos de uma amostra ou população (BARBETTA, 1994, p. 10). Aqui, não é diferente. Porém, como já mencionado, o simples fato de se coletar os dados, *per se*, não satisfaz aos objetivos deste trabalho; é preciso assimilar o que eles representam e como foram para lá.

---

[89] A China, por exemplo, já demonstra essa preocupação, desde o início deste século, quando passa a revisar suas políticas de segurança, em face das ameaças atuais, como a atuação de *crackers* (WALLER, 2000). Já a Coreia do Norte pode ser enquadrada na situação descrita.

[90] Cf. ARQUILLA; RONFELDT, 1993, p. xx; BRASIL, 2008a; PROENÇA JR; DINIZ, 1998, *passim*; DUARTE, 2012a, *passim*; 2012b, *passim*.

[91] Quanto a esta questão, Duarte (2013), em entrevista a este autor, numa visão sociológica, entende que "[...] o maior problema [...] é disponibilidade de capital para investimento e uma cultura de inovação para alocação mais produtiva desse investimento". Nessa visão, o atraso bélico norte-coreano ainda permanece, mesmo se se utilizar de artifícios ciberespaciais para obter dados e/ou causar danos.

Como observado por Buzan *et al.* (1998, p. 25, 30), a forma mais eficaz de se estudar securitização é por meio do discurso e de abordagens não objetivas. Esse discurso se traduz, aqui, por meio de argumentos de formuladores de políticas (*policy makers*) e de documentos oficiais. Em alguns casos, é possível perceber relações entre eles. Para a Escola de Copenhague, a fonte de justificativa final da securitização está na argumentação. Em outras palavras, "se, por meio de um argumento sobre a prioridade e a urgência de uma ameaça existencial, o ator securitizador conseguiu se libertar dos procedimentos ou regras a que ele estaria vinculado, estamos testemunhando um caso de securitização" (BUZAN *et al*., 1998, p. 25, tradução nossa[92]).

Tendo em vista essas ressalvas e, embora a securitização possa ser estudada diretamente e sem indicadores (BUZAN *et al.*, 1998, p. 25), busca-se situar pontos comuns entre os dados, como se defende na subseção anterior. Assim, este trabalho se mune também de meios mensuráveis/objetivos para concretizar o objetivo geral.

Como já apontado, tais meios se baseiam em índices, já que não há como mensurar a securitização em si mesma, mas sobre o grau/nível de politização em determinado elemento correlato ou, ainda, sobre certos comportamentos desses elementos que se operam na fase mais extremada da politização, que é a securitização.

Entende-se que a questão da defesa cibernética pode ser analisada objetiva e intersubjetivamente[93], com vistas a evidenciar um espectro da securitização específico para o ciberespaço, o Espectro da Securitização Militar do Ciberespaço (ESMC). Parte-se, portanto, de um mesmo conjunto de medidores para situar a securitização militar do ciberespaço para cada caso selecionado.

Assim, três índices[94] ajudam nessa empreitada, buscando explicar as politizações da defesa cibernética[95], no que tange a três atributos: virtual, documental e institucional.

Ao final da análise, busca-se enquadrar, no período compreendido entre janeiro de 2000 e dezembro de 2012, os três casos, naquilo que se epiteta ESMC.

---

[92] Texto original: "*If by means of an argument about the priority and urgency of an existential threat the securitizing actor has managed to break free of procedures or rules he or she would otherwise be bound by, we are witnessing a case of securitization*.".

[93] Cf. BUZAN *et al.*, 1998, p. 29-31.

[94] Projetam-se inicialmente quatro índices, de forma que os estilos qualitativo e quantitativo fossem distribuídos igualitariamente. Porém, e como já previsto na Subseção 3.1, dados orçamentários relacionados à defesa cibernética ainda são escassos ou mal distribuídos. A título de melhorias para futuras atualizações do ESMC, um esboço do Índice de Politização Orçamentária da Defesa Cibernética (IPoDC) se apresenta no Apêndice A.

[95] Utiliza-se "defesa cibernética", ao invés de "ciberespaço", porque, como demonstrado nas Subseções 2.1.4 e 2.1.5, este último abrangeria áreas outras não ligadas ao setor militar.

A fim de alcançar o segundo objetivo específico deste trabalho – o de explicar quando a securitização do ciberespaço é bem sucedida nos três casos aqui analisados –, as próximas três subseções explicam como ocorre a *descrição dos dados*, com base nos índices propostos, partindo-se, em seguida, para a *análise exploratória* dos mesmos.

3.2.1 O Índice de Politização Virtual da Defesa Cibernética (IPvDC)

O presente índice possui o seguinte problema de pesquisa: no século XXI, é possível constatar um aumento do interesse militar pelas ameaças cibernéticas, tendo como plataforma o próprio ciberespaço?

Portanto, a amostra se compõe dos sítios virtuais oficiais das Forças Armadas e Ministérios da Defesa de cada um dos Estados, agrupados por ano.

A metodologia de análise consiste em medir a quantidade de palavras relacionadas à defesa cibernética produzida e/ou adicionada na/à amostra, no que pese aos 13 primeiros anos do século XXI.

Para a extração dos dados, prosseguem-se as seguintes escolhas:

a) motor de busca (*search engine*) que (i) abranja o maior número de pesquisas possível e (ii) permita filtrar, em suas opções personalizadas, os resultados por ano e domínio. Assim, apenas o Google Search (http://google.com.br) se credencia.
b) palavras-chave que estejam de acordo com (i) a temática deste trabalho[96] e (ii) o(s) idioma(s) oficial(is) dos três países[97]. Excetuando-se "Stuxnet", que é um nome próprio, as palavras-chave selecionadas, por Estado e em ordem alfabética, são:
    - para os EUA: *cyber arsenal*, *cyber attack*, *cyber attacks*, *cyber defense*, *cyber war*, *cyber warfare*, *cyber wars*, *cyber weapon*, *cyber weapons*, *cyberarsenal*, *cyberattack*, *cyberattacks*, *cyberdefense*, *cybernetic war*, *cybernetic warfare*, *cybernetic wars*, *cyberspace*, *cyberwar*, *cyberwarfare*, *cyberwars*, *cyberweapon* e *cyberweapons*, totalizando 22 palavras-chave;
    - para o Brasil: arma cibernética, armas cibernéticas, ataque cibernético, ataques cibernéticos, ciber arsenal, ciber defesa, ciberataque, ciberataques, ciberdefesa, ciberespaço, ciberguerra, ciberguerras, cyber arsenal, cyberataque, cyberataques, cyberespaço, cyberguerra, cyberguerras, defesa

[96] Cf. Seção 2.

[97] Inglês americano; português brasileiro; e inglês e francês (*québécois*) canadenses.

cibernética, espaço cibernético, guerra cibernética e guerras cibernéticas, totalizando 22 palavras-chave; e

- para o Canadá: *arsenal cybernétique*, *arme cybernétique*, *armes cybernétiques*, *attaque cibernétique*, *attaques cibernétiques*, *cyber arme*, *cyber armes*, *cyber attaque*, *cyber attaques*, *cyber defence*, *cyber défense*, *cyber guerre*, *cyber guerres*, *cyberarme*, *cyberarmes*, *cyberdefence*, *cyberdéfense*, *cyberguerre*, *cyberguerres*, *defence cybernetic*, *défense cybernétique*, *guerre cybernétique* e *guerres cybernétiques*, totalizando 23 palavras-chave[98].

c) partes de URL (*Uniform Resource Locator*) militares oficiais que abranjam o Ministério da Defesa e as Forças Singulares dos três Estados. Para tais critérios, sete URL se credenciam:

- para o Brasil:
  1) .mil.br: Exército Brasileiro (BRA-EB) (eb.mil.br), Marinha do Brasil (mar.mil.br) e Força Aérea Brasileira (fab.mil.br);
  2) .exercito.gov.br: o BRA-EB, por razão desconhecida a este autor, também utiliza tal URL; e
  3) .defesa.gov.br: Ministério da Defesa do Brasil (BRA-MD).
- para os EUA:
  4) .mil: que engloba *US Air Force* (af.mil), *US Army* (army.mil), *US Marine Corps* (marines.mil) e *US Navy* (navy.mil); e
  5) .defense.gov: EUA-DoD.
- e para o Canadá:
  6) forces.ca: englobando *Marine royale canadienne* (navy.forces.ca e marine.forces.ca), *Armée de terre canadienne* (army.forces.ca) e *Aviation royale canadienne* (airforce.forces.ca); e
  7) forces.gc.ca: *Ministère de la Défense nationale et les Forces canadiennes* (CAN-MD).

d) para cada um dos três Estados, realiza-se uma pesquisa com as mesmas palavras acima, a fim de obter seus resultados nacionais.

---

[98] Escolhem-se apenas palavras-chave exatas, e não genéricas. Toma-se como exemplo o caso estadunidense: para o ano de 2011 e apenas na URL .mil, a busca por "*cyber weapon*" resulta oito ocorrências; já para "*cyber weapons*", 47; se remover as aspas da última palavra-chave, são 1.870 resultados.

A etapa seguinte consiste em aumentar o nível da linguagem(*), fazendo com que todos esses requisitos se transformem em linhas de comando e resultem em dados quantitativos para alimentar o banco de dados. Somente assim, os dados podem ser operacionalizados pelo presente índice.

É preciso, então, transformar as palavras-chave em termos de busca (*search terms*) a serem lidos pelo buscador do Google. Para isso, sabe-se que: (i) o uso de aspas duplas permite encontrar o termo exato; (ii) em linguagem SQL (*Structured Query Language*)(*) – de cuja sintaxe os comandos de busca do Google derivam –, a conjunção disjuntiva "ou" se expressa por seu equivalente em inglês e em maiúsculo "*OR*"; (iii) para se pesquisar apenas em determinado URL, é preciso inserir o comando "site:" antes do endereço eletrônico, por exemplo: "site:.mil.br"; e (iv) para pesquisar em determinado país, remove-se o parâmetro "site:" e, na página virtual da Busca Avançada do Google[99], escolhe-se cada um dos três Estados, no campo "Região".

Com essa arquitetura, as variáveis que armazenam cada um dos treze resultados – um para cada ano entre 2000 e 2012 – de cada país são: *EUA_MIL*[100], *BRA_MIL* e *CAN_MIL*. A soma dos valores dessas variáveis é guardada em *TOTAL_MIL*. Por fim, remove-se toda filtragem de URL, armazenando os resultados obtidos, por ano, na variável *TOTAL_MIL*.

Com tais diretrizes, configuram-se:

i. quatro conjuntos de comandos – um para cada Estado mais um auxiliar para a somatórios –, sendo que cada um deles contém os mesmos 67 termos (22 brasileiros, 22 estadunidenses e 23 canadenses);
ii. sete comandos de entrada – um para cada URL selecionado na etapa "c", acima –, pois o Google não permite pesquisar em mais de um URL ao mesmo tempo; e
iii. como se quer filtrar os resultados por cada ano do século XXI, para cada um dos 13 resultados, há 13 filtragens manuais, que correspondem aos anos de 2000 a 2012.

Por conseguinte, criam-se 17 variáveis para a operacionalização dos dados, conforme se mostra na Tabela 3.

---

[99] http://www.google.com/advanced_search.

[100] Não se levam em conta URLs de sítios virtuais militares oficiais de recrutamento dos US Army (goarmy.com), US Navy (navy.com), US Air Force (airforce.com), US Marines (marines.com) e US Coast Guard (gocoastguard.com).

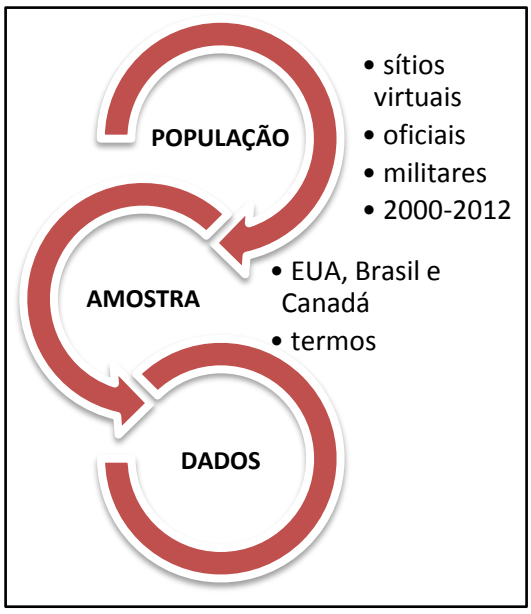
Tabela 3 – Variáveis do IPvDC de EUA, Brasil e Canadá

ID	VARIÁVEL	FUNÇÃO
1	ANO	Exibe o ano da geração do dado
2	BRA_.mil.br	Exibe os resultados referentes ao domínio .mil.br
3	BRA_.exercito.gov.br	Exibe os resultados referentes ao domínio .exercito.gov.br
4	BRA_.defesa.gov.br	Exibe os resultados referentes ao domínio .defesa.gov.br
5	BRA_MIL	Soma os valores de BRA_.mil.br, BRA_.exercito.gov.br e BRA_.defesa.gov.br
6	BRA_NAC	Exibe os resultados referentes a todos os domínios brasileiros
7	CAN_.forces.ca	Exibe os resultados referentes ao domínio .forces.ca
8	CAN_.forces.gc.ca	Exibe os resultados referentes ao domínio .forces.gc.ca
9	CAN_MIL	Soma os valores de CAN_.forces.ca e CAN_.forces.gc.ca
10	CAN_NAC	Exibe os resultados referentes a todos os domínios canadenses
11	EUA_.defense.gov	Exibe os resultados referentes ao domínio .defense.gov
12	EUA_.mil	Exibe os resultados referentes ao domínio .mil
13	EUA_MIL	Soma os valores de EUA_.defense.gov e EUA_.mil
14	EUA_NAC	Exibe os resultados referentes a todos os domínios estadunidenses
15	TOTAL_MIL	Soma os valores de BRA_MIL, CAN_MIL e EUA_MIL
16	TOTAL_NAC	Soma os valores de BRA_NAC, CAN_NAC e EUA_NAC
17	TOTAL_MUNDO	Exibe os resultados referentes a toda a Internet (população)

Fonte: Elaboração própria.

O Apêndice B detalha comandos e outros aspectos mais técnicos da busca. Já o Esquema 3 mostra resumidamente a técnica por trás da obtenção dos dados para este Índice.

Esquema 3 – Técnica de extração dos dados para o IPvDC



Fonte: Elaboração própria.

Realiza-se a análise e validação dos dados por meio do chamado *teste t para dados pareados*[101], o qual busca falsear a seguinte *hipótese nula* ou *de trabalho* (H_0): em média, os sítios virtuais oficiais militares tendem a não alterar seu interesse pelas questões de defesa cibernética, no século XXI. Por conseguinte, a *hipótese alternativa* (H_1) – que se defende aqui – é a de que: com o passar do século XXI, o interesse da população em estudo aumenta. Em termos estatísticos, tem-se que:

- H_0: $\mu_{depois} = \mu_{antes}$; e
- H_1: $\mu_{depois} > \mu_{antes}$,

onde:

- μ_{antes}: interesse médio nos sítios virtuais, antes da filtragem dos termos; e
- μ_{depois}: interesse médio nos sítios virtuais, depois da filtragem.

Tendo em vista que os dados a serem obtidos são agrupados em 12 intervalos que correspondem aos 13 primeiros anos do século XXI – e não pelos três casos selecionados –, tem-se que a *amostra observada* é 12 (n = 12). Nesse sentido, é possível comparar se o interesse se modifica a cada ano ou não, conforme o modelo da Tabela 4, abaixo.

Tabela 4 – Tabela-modelo para o IPvDC

ID	**período**	**Resultados das buscas dos termos (interesse = μ)**		
		anterior (X_{ano1})	**posterior (X_{ano2})**	**diferença ($D = X_{ano2} - X_{ano1}$)**
1	2000-2001	X_{2000}	X_{2001}	$X_{2001} - X_{2000}$
...	...	...	...	...
12	2011-2012	X_{2011}	X_{2012}	$X_{2012} - X_{2011}$

Fonte: Elaboração própria.
Nota: Utiliza-se a variável *ID* apenas para fins didáticos neste exemplo.

Com o valor da diferença (D), é possível realizar a *estatística do teste* (*t*), que verifica se uma tendência pode ser ou não explicada, apenas, pela casualidade (BARBETTA, 1994, p. 205). Assim, para que H_0 se confirme, os valores de D ou sua média ($\overline{D}$) devem se aproximar de zero. Para fins matemáticos, utiliza-se uma função da média mencionada ($f(\overline{D})$), conforme a Equação 1.

[101] É uma alternativa dentre os *testes de hipótese* ou *de significância* (cf. LANDMAN, 2008, p. 4, 6-10). Opta-se por *t de Student* por causa do tamanho pequeno da amostra utilizada no IPvDC (n = 12). Sobre tal, cf. Barbetta (1994, p. 204-213).

Equação 1 – Equação da estatística *t* para dados pareados

$$t = \frac{\overline{D} \cdot \sqrt{n}}{S_D} \quad (1)$$

Para se chegar até ela, é preciso obter a média das diferenças (D) observadas e o desvio padrão (S_D) entre elas, ou seja, as Equações 2 e 3.

Equação 2 – Equação da média

$$\overline{D} = \frac{\sum D}{n} \quad (2)$$

Equação 3 – Equação do desvio padrão

$$S_D = \sqrt{\frac{\sum D^2 - n.\overline{D}^2}{n-1}} \quad (3)$$

Para o escore do presente índice, em cada Estado, utiliza-se o resultado individual da *estatística do teste t*, se e somente se ele for aprovado quanto à *probabilidade de significância* (P) de aproximadamente 0,10, ou seja, $\alpha = 0{,}10 = 10\%$[102]. Em outras palavras, é possível refutar ou aceitar a hipótese nula (H_0) com 90% de certeza.

Para este índice, utiliza-se o resultado do *teste t*, se e somente se ele for aprovado quanto a seu P. Caso o valor de um determinado Estado não passe nesta prova, seu escore para o presente índice é zero.

3.2.2 O Índice de Politização Documental da Defesa Cibernética (IPdDC)

Busca-se auferir este índice por meio da análise qualitativa de documentos oficiais emanados pelo setor militar ou a ele endereçados e que, necessariamente, referem-se à defesa cibernética.

Aqui, três critérios são assegurados: possuir documento oficial nacional de defesa que abarque, ainda que de maneira geral, o tema em tela (2 pontos); possuir documento oficial nacional de defesa cibernética que inclua medidas extraordinárias, como criação de instituições e delegação de poder nessa área (3 pontos); e conter, no corpo textual de tal(is) documento(s), referência a Stuxnet e/ou a armas/ataques cibernéticos por parte de Estados

[102] Cf. Apêndice D.

estrangeiros, com o fito de potencializar a dramatização (1 ponto)[103]. Observa-se que, pela pontuação, um documento de cunho geral que contenha tal(is) termo(s) se equipara a um documento específico. Mais uma vez, o que é testado aqui não é a eficácia das propostas do(s) documento(s), mas o poder de alcance do seu ato de fala em dramatizar uma ameaça ciberexistencial.

Igualmente, entende-se que, por mais importante que um documento oficial desse cunho seja – como uma política ou estratégia nacional de defesa –, ele, por si só, não garante a securitização da questão; apenas satisfaz *parte* da audiência relevante[104]. É nesse sentido que o presente índice concede o grau de *movimento securitizador*[105], e não de *securitizado*, à pontuação máxima.

Os valores possíveis em cada variável figuram na Tabela 5.

Tabela 5 – Valores possíveis do IPdDC

ID	VARIÁVEL	VALORES POSSÍVEIS	DESCRIÇÃO DA PONTUAÇÃO
1	*DOC_stux*	0 | 1	Não possui ou possui, pelo menos, um documento nacional que se refira ao StuxNet ou a armas/ataques cibernéticos estrangeiros
2	*DOC_geral*	0 | 2	Não possui ou possui documento(s) nacional(is) que trate(m), de forma geral, sobre defesa cibernética
3	*DOC_espec*	0 | 3	Não possui ou possui documento(s) nacional(is) que trate(m), de forma específica, sobre defesa cibernética
4	*DOC_total*	0 | 2 | 3 | 5 | 6	Soma os valores de *DOC_stux*, *DOC_geral* e *DOC_espec*

Fonte: Elaboração própria.

Assim, quando o valor de *DOC_total* de um Estado é zero, diz-se que a ameaça ciberexistencial não está sequer em pauta; é do tipo não politizada. Quando a pontuação atinge 2 pontos, diz-se que tal questão é politizada. O Estado que conseguir um escore acima de 2 pontos no presente índice, demonstra ocorrer uma politização do tipo movimento securitizador.

Na sequência, a Tabela 6 apresenta o exposto no parágrafo anterior, mostrando os possíveis *status* das ameaças existenciais que provêm do ciberespaço.

[103] Tal ponto extra pode ser obtido apenas uma vez, já que o objetivo final é um só: securitizar o ciberespaço.

[104] Como afirmam Buzan *et al.* (1998, p. 30), politização e securitização são processos essencialmente intersubjetivos.

[105] Subseção 2.2.2.

Tabela 6 – *Status* possíveis para o IPdDC

Escore	*Status* das ameaças ciberexistenciais
0	Não politizada
2	Politizada
3, 5, 6	Movimento securitizador

Fonte: Elaboração própria.

As análises de cada um dos três Estados para este índice se encontram nas Subseções 3.3.1.2, 3.3.2.2. 3.3.3.2 e 3.3.4.2.

3.2.3 O Índice de Politização Institucional da Defesa Cibernética (IPiDC)

Percebe-se que "as instituições militares têm pensado o ciberespaço como um potencial teatro de operações; um local onde deva haver o domínio estratégico" (GAGNON, 2008, p. 50, tradução nossa[106]).

Buzan *et al*. (1998, p. 27) apregoam que a securitização pode ser institucionalizada como uma resposta urgente a um dado tipo de ameaça persistente ou recorrente. Ainda segundo esses autores, no setor militar tal manifestação se torna mais visível.

É neste sentido comprobatório que o presente índice de opera qualitativamente, elencando as principais instituições militares de defesa cibernética, tomando por base os processos que as engendram. Sua variação leva em conta instituições militares de defesa cibernética que já estejam em funcionamento[107].

Assim, excluem-se instituições militares de guerra eletrônica – como o BRA- Centro de Comunicações e Guerra Eletrônica do Exército (BRA-CCOMGEX) – e de telemática, cujo escopo de atuação, de tão abrangente, acaba por abarcar parte da defesa cibernética.

Ademais, sabe-se que: (i) Brasil possui três armas; (ii) EUA e Canadá têm mais de três cada um (ESTADOS UNIDOS, [20--]); e (iii) todos eles também possuem ministérios da defesa – embora, no caso canadense, seu ministério de segurança pública jogue papel relevante também nos assuntos de defesa.

Para uma padronização dos resultados, realizam-se os seguintes aperfeiçoamentos: (i) aglutinam-se as respostas do *US Marine Corps* com as do *US Navy*, uma vez que, em última instância, os fuzileiros navais estão associados à Marinha; e (ii) omitem-se as respostas do *US Coast Guard*, haja vista que ele é a única força armada estadunidense que não se reporta ao

[106] Texto original: "*Military institutions have started to think about cyberspace as another potential theatre of operations, a space where strategic dominance must be achieved*".
[107] Esta última etapa é vital para o IPiDC, pois documentos nacionais de defesa cibernética podem apontar a criação de tais instituições, mas muitas podem levar anos para concretizar tal empreitada.

EUA-DoD, mas sim ao *U.S. Department of Homeland Security* (EUA-DHS) (ESTADOS UNIDOS, [20--])[108].

Assim, o presente índice busca auferir uma resposta categórica binária – sim ou não – para cada ministério da defesa ou órgão centralizador (0 ou 3 pontos) e força armada (0 ou 1 ponto) de cada um dos Estados, no que tange às suas instituições voltadas exclusivamente para a defesa cibernética. Nesse sentido, um Estado que possua apenas um órgão centralizador equivale a ter três singulares.

A pontuação total vai de 0 a 6 pontos, sendo que acima de 0 é possível apontar que há politização.

Com este índice, não se pode ainda afirmar com certeza que há uma securitização, mas, pelo menos, quando o índice é acima de 2, diz-se que uma politização do tipo movimento securitizador acontece. Isso por causa de um exemplo que vem dos EUA. Sua primeira força combatente a criar uma instituição voltada à defesa cibernética é a Força Área (CLARKE; KNAKE, 2012, p. 34-41). Porém, essa questão não é securitizada por todo o setor militar daquele Estado; mas apenas pela própria força, que toma para si o direito de ser, ela própria, o órgão centralizador. Após muitas discussões acerca de qual das armas combatentes conduziria as operações estratégicas no ciberespaço, os EUA engendram seu órgão centralizador. Até esta criação se tem um movimento securitizador, não uma securitização. Já a criação de uma instituição militar voltada à defesa cibernética em qualquer uma das forças, garante, no mínimo, o *status* de politização.

As respostas são obtidas por intermédio dos documentos oficiais dos Estados e o escore é referendado conforme a Tabela 7. Subseções, mais abaixo, analisam cada um dos três casos selecionados.

Tabela 7 – Valores do IPiDC

Órgão centralizador	Exército	Marinha	Aeronáutica	Total possível
Não = 0 Sim = 3	Não = 0 Sim = 1	Não = 0 Sim = 1	Não = 0 Sim = 1	0: não politização 1 |-- 2: politização 3 |-- 6: mov. securitizador

Fonte: Elaboração própria.
Notas: Se o total possível for maior que zero, diz-se que há uma politização da defesa cibernética. Caso contrário, não há politização institucional.
"Não" e "Nenhum" são sinônimos. Esta informação se torna pertinente na análise gráfica dos dados.

[108] Só quando há guerra no território ianque é que a Guarda Costeira estadunidense se reporta ao EUA-DoD.

3.3 Mensurando o impacto da securitização militar do ciberespaço

Conforme Buzan *et al.* (1998, p. 32, tradução nossa[109]) apregoam, "[...]ninguém pode tornar os atores da securitização o ponto fixo da [sua] análise – a prática da securitização é o centro de análise".

À luz dessa recomendação, busca-se dar ênfase nos processos em si mesmos, analisando os três casos abaixo com o fito de explicar seus processos nacionais de securitização militar do ciberespaço. O preenchimento dos índices propostos na Subseção anterior reforça tal ênfase, e não o de partir de uma lógica indutiva, incoerente com os objetivos deste trabalho.

Ao final desta Subseção, é possível, enfim, evidenciar o Espectro da Securitização Militar do Ciberespaço (ESMC).

3.3.1 O caso estadunidense

Conforme Gagnon (2008, p. 48-49, tradução nossa[110]) afirma, "a importância das atividades *web* nos EUA tem levado suas autoridades a desenvolver doutrinas estratégicas sobre a Internet, suas possibilidades e suas potenciais ameaças". Ainda, segundo o autor, apesar do pioneirismo militar estadunidense quanto às questões cibernéticas, suas primeiras diretrizes doutrinárias, como a *National Strategy to Secure Cyberspace* (EUA-NSSC), parecem advir dos novos desafios ciberespaciais com antigas táticas do período da Guerra Fria. Ele ainda afirma que a EUA-NSSC "[...]é estabelecida na mesma linguagem territorial, soberana e centrada no Estado-Nação que demonizou a doutrina da Guerra Fria, mas o [ciber]espaço referido por ela é estritamente virtual, não nacional, flexível e dinâmico" (GAGNON, 2008, p. 51, tradução nossa[111]).

Há dois fatos que merecem ser notados, quanto aos EUA: (i) como já frisado, possuem cinco Forças Armadas (ESTADOS UNIDOS, [20--]): Exército (*US Army*), Marinha (*US Navy*), Força Aérea (*US Air Force*), Corpo de Fuzileiros Navais (*US Marine Corps*) e Guarda Costeira (*US Coast Guard*); e, conforme aponta GAGNON (2008, p. 53, tradução nossa[112]), "[...]são a única nação cujas autoridades de segurança admitem publicamente o uso de armas

---

[109] Texto original: "[...] *one can not make the actors of securitization the fixed point of analysis – the practice of securitization is the center of analysis*".

110 Texto original: "*The importance of web activities in the USA has led authorities to develop strategic doctrines about the Internet, its possibilities and the potential threats that might emerge from it*".

[111] Texto original: "*The strategy is set out in the same territorial, sovereign, national-state language that dominated Cold War doctrine, but the space it refers to is strictly virtual, non-national, flexible and dynamic.*".

[112] Texto original: "*The USA is probably the only nation in which security authorities have publicly admitted the use of cyberweapons in recent conflicts.*".

cibernéticas em recentes conflitos", utilizadas pela primeira vez em 1999, na Guerra do Kosovo.

Com isso em mente, parte-se para a inferência do caso estadunidense, tomando por base os três índices de politização da defesa cibernética já explicados.

3.3.1.1 IPvDC

A Tabela 8 apresenta os dados estadunidenses referentes às buscas nos sítios virtuais militares oficiais entre os anos de 2000 e 2012.

Tabela 8 – Resultados das buscas nos sítios virtuais militares oficiais dos EUA (2000-2012)

ANO	EUA_.mil	EUA_.defense.gov	EUA_MIL
2000	2.119	3.065	5.184
2001	2.906	3.729	6.635
2002	1.232	1.035	2.267
2003	931	705	1.636
2004	1.079	1.085	2.164
2005	1.604	1.348	2.952
2006	2.292	1.432	3.724
2007	2.468	2.319	4.787
2008	4.310	2.970	7.280
2009	5.267	3.216	8.483
2010	7.754	3.453	11.207
2011	11.225	5.271	16.496
2012	12.353	4.876	17.229
Σ	**55.540**	**34.504**	**90.044**

Fonte: Elaboração própria.

Observa-se que há um interesse militar anormal no ano de 2001, ano dos atentados às Torres Gêmeas. Como os ataques ao *World Trade Center* ocorrem na metade do segundo semestre daquele ano, sua reverberação só ocorre entre o final de 2001 e o primeiro semestre de 2002, trazendo consigo perspectivas sobre os futuros focos de ameaças terroristas aos EUA, incluindo o ciberespaço. Daí, defende-se, o porquê de os valores referentes a 2002 serem maiores que os de 2003, ano em que eles se normalizam – tomando-se por base os valores a partir de 2004.

Para se ter uma ideia, o número de páginas/documentos virtuais que cita, pelo menos, um dos 67 termos buscados, em 2001, só é superado, em média, mais de seis anos depois. Mesmo assim, um possível aumento do interesse militar se mostra crescente, pois, a partir de 2003, os valores tendem a incrementar em média 7,7% a.a.

Agora, busca-se comparar o interesse virtual militar estadunidense, em cada ano. Para tanto, é necessário expor os dados na Tabela 9.

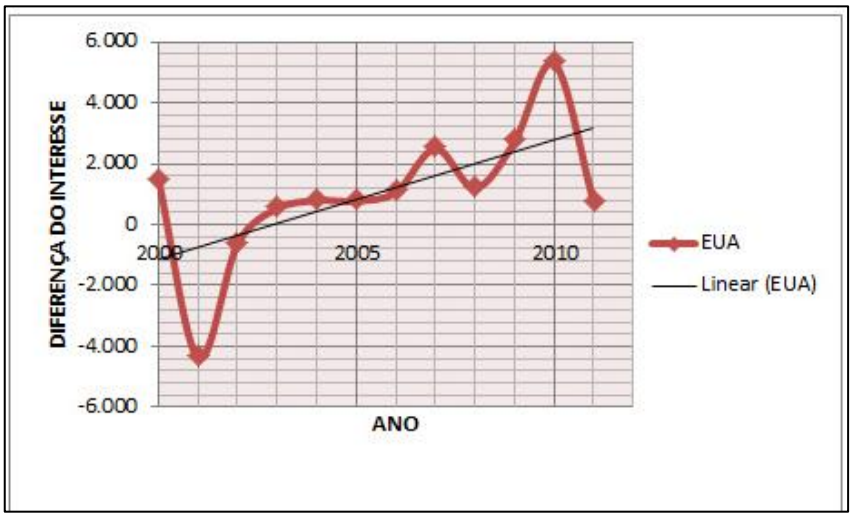
Tabela 9 – Cálculo da diferença de interesse virtual militar dos EUA na defesa cibernética (2000-2012)

período	Resultados das buscas dos termos (interesse = μ) anterior (X_{ano1})	posterior (X_{ano2})	diferença ($D = X_{ano2} - X_{ano1}$)
2000-2001	5.184	6.635	1.451
2001-2002	6.635	2.267	-4.368
2002-2003	2.267	1.636	-631
2003-2004	1.636	2.164	528
2004-2005	2.164	2.952	788
2005-2006	2.952	3.724	772
2006-2007	3.724	4.787	1.063
2007-2008	4.787	7.280	2.493
2008-2009	7.280	8.483	1.203
2009-2010	8.483	11.207	2.724
2010-2011	11.207	16.496	5.289
2011-2012	16.496	17.229	733
Total	**72.815**	**84.860**	**12.045**

Fonte: Elaboração própria.

Percebe-se que a diferença final apresenta um valor muito alto. Utilizando um diagrama de pontos, é possível analisar a variação dessa amostra. É o que exibe o Gráfico 1.

Gráfico 1 – Variação do interesse virtual militar dos EUA (2000-2012)



Fonte: Elaboração própria.

Pelo diagrama de pontos acima, identifica-se que a maioria dos valores se situa acima do eixo X – valores positivos – e o valor final é bem elevado, o que, *a priori*, pode levar a inferir que há um grande interesse do setor militar por tais questões.

Com as informações acima e utilizando o teste t[113], obtém-se o valor de 1,55 pontos para o caso estadunidense. Após se constatar que seu P = 0,10, aprova-se, então, tal escore para o presente índice. Em outras palavras: assume-se com 90% de certeza que há um interesse sobre temas que envolvem a defesa cibernética, por parte dos sítios virtuais oficiais militares dos EUA.

3.3.1.2 IPdDC

Para auferir o presente índice, consultam-se a *National Security Strategy* (EUA-NSS), de 2010, e a *Strategy for Operating in Cyberspace* (EUA-SOC), de 2011.

É interessante notar que tais documentos atualizam outros relacionados à defesa cibernética, como a EUA-NSSC, de 2003, criado ainda sob a Administração W. Bush. Outro documento referente aos temas aqui abordados é o *International Strategy for Cyberspace* (EUA-ISC), lançado em 2011. Pelo fato de este último (i) ser uma estratégica internacional, e não nacional, e, portanto, (ii) ser um documento de política externa, e não de defesa nacional, o presente índice não o leva em consideração[114].

Os EUA lançam a EUA-NSS, no sentido de atualizar as últimas estratégias de segurança nacional dos dois governos W. Bush. De plano, a EUA-NSS afirma que estratégias para a proteção das redes cibernéticas estadunidenses constituem uma das mais altas prioridades de segurança nacional (ESTADOS UNIDOS, 2010b, p. 4).

No que tange aos propósitos deste trabalho, a EUA-NSS busca conscientizar a nação e a esfera pública estadunidenses de que o ciberespaço faz parte de um conjunto de setores dependentes – como o espacial – que estão na mira de seus inimigos e dentro das chamadas ameaças assimétricas (ESTADOS UNIDOS, 2010b, p. 17). Além disso, ela traz o conceito de segurança interna (*security at home*), o qual consiste, dentre outras ações estratégicas, em proteger as infraestruturas críticas baseadas em TIC e o próprio ciberespaço estadunidense (ESTADOS UNIDOS, 2010b, p. 18).

Essa Estratégia considera o ciberespaço como um domínio – ao lado do espaço, mar, ar e terra –, onde as ameaças cibernéticas "representam um dos mais graves desafios de

[113] Cf. Seção 3.2.1 e Apêndice D.

[114] O EUA-ISC fornece fortes indícios de que há, pelo menos, um movimento securitizador do ciberespaço para o setor político daquele Estado, no que pese seu corpo diplomático.

segurança nacional, segurança pública e econômica que os EUA enfrentam enquanto nação" (ESTADOS UNIDOS, 2010b, p. 27, tradução nossa[115]).

Até este ponto, a EUA-NSS faz levantamentos referentes à segurança cibernética, e não à defesa cibernética. Entretanto, um elemento novo surge: os EUA consideram outros Estados como potenciais inimigos que tiram proveito do ambiente cibernético para tentar invadir/sabotar suas infraestruturas críticas digitais ou mesmo obter informações privilegiadas (ESTADOS UNIDOS, 2010b, p. 27).

Assim, a EUA-NSS prevê duas formas de prevenção a tais ameaças: (i) investir em pessoal e tecnologia; e (ii) reforçar as parcerias entre as esferas pública e privada nacionais e internacionais, conforme já ocorre com alguns países da Ásia (ESTADOS UNIDOS, 2010b, p. 42).

Um ano após o lançamento da EUA-NSS, os EUA dão vida à EUA-SOC, no âmbito do seu departamento de defesa[116]. Ela é fortemente influenciada pela EUA-NSS, citando-a frequentemente, estando assim dividida:

i. *Introdução*: conceitua o ciberespaço para o EUA-DoD, bem como explicita a dependência desse espaço, no intuito de que operações militares, de inteligência e logísticas possam ocorrer (ESTADOS UNIDOS, 2011a, p. 1);
ii. *Contexto estratégico*: demonstra os pontos fortes e as oportunidades do EUA-DoD no ciberespaço, elencando as principais ameaças cibernéticas à segurança nacional, incluindo-se aí governos estrangeiros (ESTADOS UNIDOS, 2011a, p. 2-4);
iii. *Cinco iniciativas estratégicas* em que o EUA-DoD deve: (i) tratar o ciberespaço como um domínio operacional de organização, treinamento e equipagem, de modo que se possa tomar completa vantagem do potencial ciberespacial; (ii) empregar novos conceitos operacionais de defesa para proteger suas redes e sistemas; (iii) fazer parcerias com outros departamentos e agências nacionais, bem como acionar a esfera privada para permitir uma estratégia de segurança cibernética que envolva todo o governo; (iv) construir robustos relacionamentos com aliados e parceiros internacionais para fortalecer a segurança cibernética coletiva; e (v) alavancar a engenhosidade da nação por meio de uma excepcional força de trabalho e rápida inovação tecnológica (ESTADOS UNIDOS, 2011a, p. 5-12); e

---

[115] Texto original: "*Cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation*".
[116] Daí o nome oficial dessa estratégia ser *Department of Defense Strategy for Operating in Cyberspace*.

iv. *Conclusão*: resume a Estratégia, acrescentando que ela deve guiar os interesses do EUA-DoD no ciberespaço, de modo que os EUA e seus aliados possam continuar beneficiando-se das inovações da era da informação (ESTADOS UNIDOS, 2011a, p. 13).

Ademais, a EUA-SOC menciona que uma instituição voltada à defesa cibernética será responsável por garantir grande parte do que é exposto e também organizar as ações das suas Armas. O subterfúgio da dramatização estadunidense fica por conta, sobretudo, da proteção às infraestruturas críticas, de dominar o ciberespaço e de livrar "seu" ciberespaço das tentativas de sabotagem/dano de Estados estrangeiros. Portanto, somam um ponto na variável *DOC_stux*.

Assim, a Tabela 10 mostra a pontuação final dos EUA para este índice.

Tabela 10 – IPdDC dos EUA (2000-2012)

DOC_stux	DOC_geral	DOC_espec	DOC_total	*Status*
1	2	3	6	Movimento securitizador

Fonte: Elaboração própria.

3.3.1.3 IPiDC

Para dar suporte às questões cibernéticas mais corriqueiras – como crimes cibernéticos –, o EUA-DoD conta ainda com a arquitetura apresentada na Tabela 11.

Tabela 11 – Atores-chave do EUA-DoD envolvidos em contenções cibernéticas corriqueiras (2008)

Organizações	Suborganizações	Responsabilidades
Defense criminal and counterintelligence investigative organizations	*- Department of Defense Criminal Investigative Service (DCIS)* *- Air Force Office of Special Investigation (AFOSI)* *- Naval Criminal Investigative Service (NCIS)*	Representa as principais agências de segurança do DoD para a investigação da criminalidade cibernética
Department of Defense Cyber Crime Center (DC3)	*- Defense Computer Forensics Laboratory* *- Defense Computer Investigations Training Program* *- Defense Cybercrime Institute*	Realiza atividades forenses para a defesa criminal e para organizações de contra-investigação
Joint Task Force – Global Network Operations	*Global network operations*	Detecta e dissuade a criminalidade cibernética que poderia atrapalhar o DoD *Global Information Grid* (GIG)

Fonte: GAGNON, 2008, p. 55-56, tradução nossa (com adaptações).

Porém, quando o assunto é defesa cibernética, o EUA-DoD se mune de uma estrutura mais robusta, como se vê a partir de agora.

Como já mencionado, os EUA se lançam institucionalmente no ciberespaço com viés militar em 2006, quando sua Força Aérea cria o *Air Force Cyber Command* ou AFCYBER (CLARKE; KNAKE, 2012, p. 34). As outras forças seguem seus passos e criam também seus órgãos específicos de defesa cibernética.

Em 2009, o subcomando responsável por coordenar os órgãos de defesa cibernética é ativado, o *U.S. Cyber Command* (EUA-USCYBERCOM) (ESTADOS UNIDOS, 2010a; 2011a, p. 5)[117].

Embora o engendramento de tal órgão não se dê por uma estratégia pensada nem por debates públicos (CLARKE; KNAKE, 2012, p. x), o USCYBERCOM já nasce composto pelos: *Army Forces Cyber Command*; *24th US Air Force*; *Fleet Cyber Command*; e *Marine Forces Cyber Command* (ESTADOS UNIDOS, 2010a).

Com essas informações, é possível observar a Tabela 12.

Tabela 12 – Resultado escalar do IPiDC dos EUA (2000-2012)

Órgão Centralizador	Exército	Marinha	Aeronáutica	Total
Sim	Sim	Sim	Sim	--
3	1	1	1	6

Fonte: Elaboração própria.

Como se vê, pela segunda vez, os EUA obtêm a pontuação máxima possível. Esses dados são analisados em conjunto com os de Brasil e Canadá mais abaixo, momento em que ajudam a compreender o ESMC.

Parte-se, agora, para a exploração do caso brasileiro quanto aos mesmos três índices aplicados aos EUA.

3.3.2 O caso brasileiro[118]

Em entrevista a este autor, Rudzit (2012) aponta que "as universidades podem oferecer [...] ambiente [de inovação tecnológica] que dificilmente se consegue replicar na área militar".

Um exemplo dessa mescla entre os mundos acadêmico e militar é visto em Guerra (2012), quando este informa – também em entrevista a este autor – que uma das linhas de

[117] Vale salientar que, embora aglutine as operações cibernéticas das armas estadunidenses, o EUA-USCYBERCOM é originalmente dirigido pelo Diretor da NSA, a agência de segurança nacional dos EUA,.

[118] Esta subseção é uma expansão de Lopes (2011a; 2011b).

pesquisa do Programa de Pós-graduação em Aplicações Operacionais (PPGAO) e do Laboratório de Comando e Controle (LAB-C2) do Instituto Tecnológico de Aeronáutica (BRA-ITA) é sobre guerra cibernética. Lá, os "[...]alunos de mestrado e doutorado [...] estão trabalhando em temas ligados a Guerra Cibernética e [...] são apoiados pelo [supracitado] laboratório" (GUERRA, 2012)[119].

Outro tema que faz parte das corriqueiras informações sobre defesa cibernética no cenário brasileiro é sobre a possibilidade de contratar *hackers* – uma das principais fontes para se projetar armas cibernéticas. Em atenção a esse tema, Coronel Luis Cláudio pondera que isso é, sim, uma possibilidade (LUPION, 2011).

Tal afirmação encontra respaldo também na fala do então Ministro da Ciência, Tecnologia e Inovação, Aluízio Mercadante – hoje na Educação –, informando querer dialogar com os *hackers* para, juntos com o Ministério, ajudar a identificar e corrigir eventuais falhas de segurança e modernizar portais da pasta (D'ANDRADE, 2011). Mercadante (2011, grifo nosso) escreve que "[...]a internet tem sua inteligência distribuída, é completamente aberta, o que permite que *hackers* continuem criando soluções inovadoras" e que "a experiência e a genialidade dos criadores de códigos[-fonte] não podem ser ignoradas".

Já o BRA-EB, desde 2010, assume que "guerra cibernética" é um dos estágios setoriais a ser disponibilizado aos Cadetes do 4º Ano da Academia Militar das Agulhas Negras (BRA-AMAN) (BRASIL, 2010b, p. 96-97).

Quanto a esta iniciativa, o professor da BRA-AMAN, Walfredo Ferreira Neto, em entrevista a este autor, informa que é favorável e ainda afirma que a especialidade em comunicações é que: "[...]deva ter uma maior carga horária relativa à cibernética. Existem também os tempos de aula referentes aos Assuntos da Atualidade. Nesses tempos poderemos ter como objeto transversal o estudo desse setor" (FERREIRA NETO, 2011)[120].

Em fase de preparação para sediar grandes eventos, o governo brasileiro amplia ainda mais a discussão sobre as ameaças ciberexistenciais.

3.3.2.1 IPvDC

O primeiro passo para auferir este índice ao caso brasileiro é conhecer os resultados das buscas virtuais. As Tabelas 13 e 14 empreendem tal tarefa.

---

[119] Um exemplo de como a seara civil pode dialogar com a militar se encontra na leitura conjunta de Brasil (2012a) e Duarte (2012b).

[120] Nesse mesmo sentido, cf. Brasil (2012d, p. 12).

Tabela 13 – Dados do IPvDC do Brasil (2000-2012)

ANO	BRA_.mil.br	BRA_.exercito.gov.br	BRA_.defesa.gov.br	BRA_MIL
2000	0	0	0	0
2001	2	0	0	2
2002	0	0	0	0
2003	1	0	0	1
2004	2	0	0	2
2005	1	0	1	2
2006	4	0	1	5
2007	5	0	1	6
2008	13	0	3	16
2009	29	0	6	35
2010	48	3	2	53
2011	132	53	11	196
2012	210	168	76	454
TOTAL	**447**	**224**	**101**	**772**

Fonte: Elaboração própria.

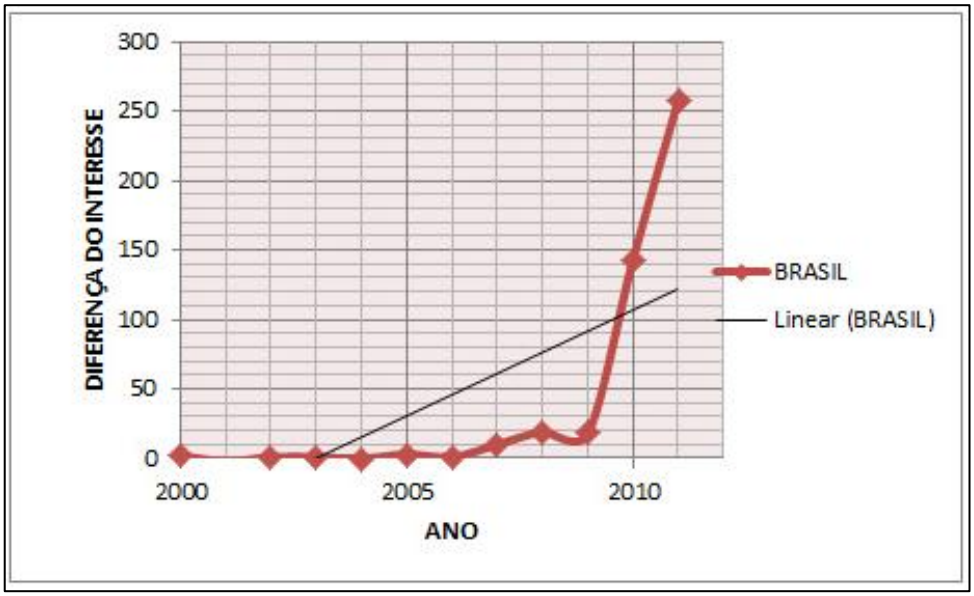
Tabela 14 – Cálculo da diferença de interesse virtual militar do Brasil na defesa cibernética (2000-2012)

período	Resultados das buscas dos termos (interesse = μ) anterior (X_{ano1})	posterior (X_{ano2})	diferença ($D = X_{ano2} - X_{ano1}$)
2000-2001	0	2	2
2001-2002	2	0	-2
2002-2003	0	1	1
2003-2004	1	2	1
2004-2005	2	2	0
2005-2006	2	5	3
2006-2007	5	6	1
2007-2008	6	16	10
2008-2009	16	35	19
2009-2010	35	53	18
2010-2011	53	196	143
2011-2012	196	454	258
Total	**378**	**772**	**454**

Fonte: Elaboração própria.

Com isso, é possível ter uma visão geral da variação do interesse militar brasileiro, expressada em seus sítios virtuais. O Gráfico 2, *infra*, auxilia nessa empreitada.

Gráfico 2 – Variação do interesse virtual militar do Brasil (2000-2012)



Fonte: Elaboração própria.

Como retratado acima, o caso brasileiro aparenta ter graficamente um interesse crescente em politizar militarmente o ciberespaço.

Essas informações são suficientes para auferir o escore provisório brasileiro para o presente índice: 1,64 pontos, que se confirma somente após verificar que o seu P = 0,10. Portanto, o IPvDC brasileiro é 1,64.

3.3.2.2 IPdDC

Levam-se em conta dois documentos que se enquadram nos critérios deste índice: a Estratégia Nacional de Defesa (BRA-END) e a Política Cibernética de Defesa (BRA-PCD), de 2008 e 2012, respectivamente. Para preencher algumas lacunas deixadas por tais documentos, requer-se auxílio a Decretos Federais (BRASIL, 2010a; 2011a) e ao Boletim do Exército (BRASIL, 2010b; 2010c).

Antemão, frisa-se que o próprio Ministério da Defesa (BRA-MD) já trata especificamente do termo "guerra cibernética" desde 2008, quando incorpora oficialmente a abreviação "G Ciber" ao jargão militar tupiniquim (BRASIL, 2008c, p. 71, 181). Isso não quer dizer que as guerras convencionais são subvalorizadas por parte deste Estado; pelo contrário, a BRA-END assume que "a tecnologia, por mais avançada que seja, jamais será alternativa ao combate", rejeitando "a tentação de ver na alta tecnologia alternativa ao combate" (BRASIL, 2008a). É o que se defende aqui também.

Contrariamente ao caso estadunidense, no Brasil, os debates sobre a criação de uma estratégia nacional de defesa que vinculasse Forças Armadas e independência nacional se dão de forma ampla, abrangendo-se vários *fora* de discussão. Ao se findar o trabalho do Comitê Ministerial, formado para elaborar e apresentar a BRA-END, submete-se à Presidência da República um Projeto de Decreto que aprova o texto final da estratégia de defesa tupiniquim. Após apreciação, o Chefe do Executivo brasileiro sanciona o Decreto nº 6.703, de 18 de dezembro de 2008, e, assim, o seu Anexo – a íntegra da BRA-END – é aprovado.

O principal objetivo da BRA-END é modernizar a estrutura de defesa nacional. Para isso, busca atuar em três *eixos estruturantes*, a saber: (i) reorganização das Forças Armadas; (ii) reestruturação da indústria brasileira de material de defesa; e (iii) política de composição dos efetivos das Forças Armadas (BRASIL, 2008a).

O primeiro eixo estratégico, dentre outros, enumera 23 *diretrizes estratégicas*, resultantes da junção entre "capacidade de improvisação e adaptação" e "sentido do compromisso nacional no Brasil" (BRASIL, 2008a), as quais são atinentes a cada uma das três forças. Para lograr essas diretrizes, a BRA-END dá nova postura às Forças Armadas.

A sexta dessas 23 precitadas diretrizes, por sua vez, elenca três *setores estratégicos*: o nuclear, o espacial e o cibernético. Em outras palavras, a BRA-END lista três domínios imprescindíveis para a defesa nacional do País, uma vez que, segundo o próprio documento, "não é independente quem não tem o domínio das tecnologias sensíveis, tanto para a defesa como para o desenvolvimento" nacional (BRASIL, 2008a).

Cada força singular se responsabiliza, então, pelo desenvolvimento de um setor estratégico. Nesse sentido, a Força Aérea Brasileira deve liderar as pesquisas na área espacial; a Marinha do Brasil, no que concerne ao desenvolvimento da tecnologia nuclear[121]; e, por fim, o BRA-EB é o responsável pelo setor cibernético.

Como a BRA-END não explicita a guarda do setor cibernético ao BRA-EB, cabe à Portaria do Comandante do Exército nº 03-RES, de 2009, fazê-lo (BRASIL, 2010b, p. 96).

Deve-se pesar sobre as atribuições do BRA-EB, no que tange ao setor cibernético, um importante – e igualmente complexo – papel: o de defender o território cibernético nacional – ou o que se pensa ser ele – dos diversos tipos de ameaças ciberexistenciais.

O Esquema 4 situa o setor cibernético na BRA-END, em associação aos dois Boletins do Exército, que distribuem os três setores estratégicos entre as três armas brasileiras.

---

[121] Respeitando-se o Tratado de Não Proliferação de Armas Nucleares e o Art. 21, XXIII, *a*, da Carta Magna brasileira: "toda atividade nuclear em território nacional somente será admitida para fins [...]" (BRASIL, 1998).

Esquema 4 – O setor estratégico cibernético brasileiro à luz da BRA-END

Fonte: LOPES, 2011a, p. 11.

Além disso, a BRA-END projeta a criação de uma "organização encarregada de desenvolver a capacitação cibernética nos campos industrial e militar" (BRASIL, 2008), a qual é criada em 2010 e analisada na próxima subseção.

Em novembro de 2010, a Presidência da República publica o Decreto nº 7.364, que, dentre outros, aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão do Grupo-Direção e Assessoramento Superiores do BRA-MD (BRASIL, 2010a).

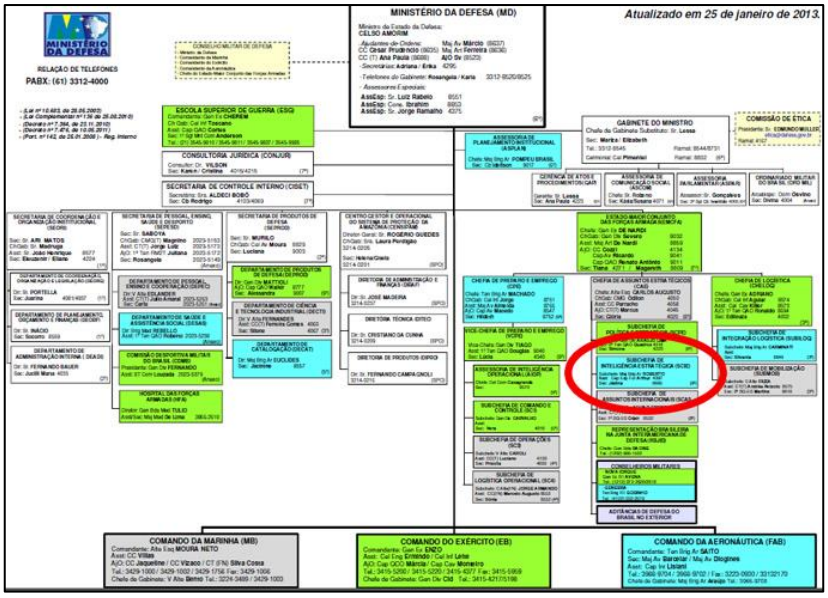
A estrutura organizacional do BRA-MD passa a ter: (i) quatro órgãos de assistência direta e imediata; (ii) dois órgãos de assessoramento; (iii) quatro órgãos específicos singulares; (iv) três órgãos de estudo, de assistência e de apoio; e (v) três Forças Armadas (BRASIL, 2010a).

Um desses órgãos de assessoramento é o Estado-Maior Conjunto das Forças Armadas que possui três Chefias, sendo uma delas a de Assuntos Estratégicos (BRASIL, 2010a). Esta última, por sua vez, é formada por três unidades ou Subchefias, sendo uma delas a que interessa aqui: a de Inteligência Estratégica. Dentre suas dez competências, a sétima informa que ela deve "desenvolver capacidade de integração dos conhecimentos, para os fins de defesa, nos campos científico, tecnológico, *cibernético*, espacial e nuclear" (BRASIL, 2010a,

grifo nosso). Portanto, a Subchefia de Inteligência Estratégica do BRA-MD, desde 2010, passa a desempenhar papel vital para as questões de defesa cibernética no Brasil.

O Esquema 5 posiciona a Subchefia de Inteligência Estratégica no BRA-MD.

Esquema 5 – Localização da Subchefia de Inteligência Estratégica no organograma do BRA-MD



Fonte: BRASIL, 2013a (com adaptações).

Em dezembro de 2012, o BRA-MD publica a Portaria Normativa nº 3.389, dispondo sobre a BRA-PCD.

Ao contrário do texto da BRA-END, o da BRA-PCD é assaz curto, haja vista que esta trata apenas de um dos inúmeros temas daquela.

Em linhas gerais, este documento específico "[...]tem a finalidade de orientar, no âmbito do Ministério da Defesa[...], as atividades de *Defesa Cibernética*, no nível estratégico, e de *Guerra Cibernética*, nos níveis operacional e tático, visando à consecução dos seus objetivos" (BRASIL, 2012e, p. 11, grifo nosso).

Nota-se ainda uma espécie de chamado às armas cibernéticas, por parte do BRA-MD, ao afirmar que um dos pressupostos básicos da BRA-PCD é o de que:

> a eficácia das ações de Defesa Cibernética depende, fundamentalmente, da atuação colaborativa da sociedade brasileira, incluindo, não apenas o MD, mas também a comunidade acadêmica, os setores público e privado e a base industrial de defesa. (BRASIL, 2012e, p. 11).

Pela primeira vez, um documento oficial brasileiro afirma que o País pode não só se defender no ciberespaço, mas também atacar (BRASIL, 2011d, p. 11). Cita, ainda, poder trabalhar na construção de suas próprias armas cibernéticas, ao "atuar no reconhecimento de

artefatos e desenvolvimento de ferramentas cibernéticas, em conjunto com a PR [Presidência da República], contribuindo para a proteção dos ativos de informação" da administração pública federal (BRASIL, 2012e, p. 12, grifo nosso).

Como posto na primeira Seção desta Dissertação, a informação possui seu chamariz próprio neste século. Não por menos, a BRA-PCD argui que "a eficácia das ações de Defesa Cibernética no [BRA-]MD depende diretamente do grau de conscientização alcançado junto às organizações e pessoas acerca do *valor da informação* que detêm ou processam" (BRASIL, 2011d, p. 11, grifo nosso).

Assim, é possível preencher o IPdDC para o caso brasileiro, conforme a Tabela 15.

Tabela 15 – IPdDC do Brasil (2000-2012)

DOC_stux	DOC_geral	DOC_espec	DOC_total	*Status*
0	2	3	5	Movimento securitizador

Fonte: Elaboração própria.

3.3.2.3 IPiDC

No que tange à segurança da informação em instituições governamentais brasileiras, o especialista em segurança da informação Rodrigues (2012), em entrevista a este autor, afirma que elas:

> [...]sofrem milhares de ataques todos os dias, muitos [deles] são detectados e neutralizados, uma parte tem sucesso e é do conhecimento da organização e uma pequena parte tem sucesso e a organização não sabe o que está acontecendo.

Também em entrevista a este autor, o militar Kilian Junior (2012) concorda com a afirmação de que, embora haja esforços, há também lacunas expostas: "[...]o Brasil precisa se preparar, pois possui infraestruturas críticas da nação que hoje são vulneráveis a ataques cibernéticos".

Se a segurança cibernética do Estado tupiniquim recai sobre seus policiais e especialistas em segurança da informação, sua defesa cibernética é conduzida pelo braço forte e pela mão amiga do BRA-EB, como frisado na subseção anterior.

Em entrevista a este autor, Guerra (2012) informa que a descoberta das armas cibernéticas "[...]pode ajudar no entendimento dos mecanismos de ataque e ajudar na criação de mecanismos de defesa". Ele vê ainda como positivo o fato de o Brasil possuir um centro de defesa cibernética para esses fins.

Para se entender o papel do Centro de Defesa Cibernética do Exército (BRA-CDCiber), torna-se necessário contextualizar sua criação, a qual se dá, por exemplo, de maneira diferente da do EUA-USCYBERCOM.

Embora a BRA-END esteja focada em ações estratégicas de médio e longo prazo, a supracitada organização é engendrada em menos de dois anos da publicação do Decreto que dá vida à BRA-END.

Com a publicação das Portarias n^{os} 666 e 667, ambas de 4 de agosto de 2010, o Comandante do BRA-EB – ouvindo o Departamento de C&T do Exército – cria o BRA-CDCiber, ativa o Núcleo do Centro de Defesa Cibernética do Exército (BRA-Nu CDCiber[122]) e dá outras providências (BRASIL, 2010c, p. 7-8).

Segundo o Comandante do BRA-CDCiber, General José Carlos dos Santos, R$ 10 milhões são investidos, em 2010, para a implantação do Centro, e outro R$ 1,5 milhão é estimado para o seu pleno funcionamento (LOYOLA, 2011). Lupion (2011), ao entrevistar o Coordenador do BRA-Nu CDCiber, Coronel Luis Cláudio Gomes Gonçalves, lembra que, embora subordinado ao BRA-EB, o BRA-CDCiber "irá coordenar as ações de defesa cibernética das Forças Armadas". Portanto, o BRA-CDCiber tem, pelo menos até o final de 2012, o mesmo papel que o EUA-USCYBERCOM[123].

Logo, o engendramento do BRA-CDCiber aloca discussões sobre como o setor militar brasileiro, e em especial, seu Exército, encara o setor cibernético, buscando subentendê-lo e respeitando suas – do ciberespaço e da caserna – próprias possibilidades e limitações. Mais que isso, tal criação demonstra a percepção *presente* de um *futuro* que já começa a se materializar, pois, como lembra Hopkins (2011b) e Lopes e Teixeira Jr (2011), ações no ciberespaço farão parte do futuro campo de batalha.

Medeiros (2002, p. 147) afirma que "não há fronteiras demarcadas no ambiente cibernético" e que esse fato "derruba um dos principais pilares do chamado Estado Moderno". Na mesma linha de raciocínio, o Comandante do BRA-CDCiber, General José Carlos, demonstra um alto grau de percepção realista do ciberespaço, quando pondera que "no conflito convencional, as fronteiras estão bem definidas. No espaço cibernético, essa fronteira não existe, uma vez que a arquitetura da internet é livre" (LOYOLA, 2011).

A fim de "[...]assegurar, de forma conjunta, o uso efetivo do espaço cibernético – preparo e emprego operacional – pelas Forças Armadas (FA) e impedir ou dificultar sua

---

[122] Órgão encarregado por implantar o BRA-CDCiber.
[123] Essa afirmação é refutada com a publicação da BRA-PCD, vista na subseção anterior.

utilização contra interesses da Defesa Nacional" (BRASIL, 2012e, p. 12), a BRA-PCD visa, dentre outros, criar o Sistema Militar de Defesa Cibernética (BRA-SMDC) e um órgão centralizador para coordenar as ações das três armas no ciberespaço.

Essas implementações demandam recursos materiais e humanos, e a BRA-PCD atina para isso, ao informar que pretende "criar cargos e funções específicos e mobilizá-los com pessoal especializado para atender às necessidades do[…]" setor cibernético.

Tal órgão ainda não possui nome, mas sabe-se que será o órgão central do BRA-SMDC, mantendo, assim, permanente diálogo com os órgãos centrais das Forças Armadas e "responsável por propor as inovações e atualizações de doutrina para o [...] [setor cibernético] no âmbito da Defesa" (BRASIL, 2012d, p. 12).

A partir dessas informações, é possível, portanto, preencher a Tabela 16.

Tabela 16 – Resultado do IPiDC do Brasil (2000-2012)

Órgão centralizador	Exército	Marinha	Aeronáutica	Total
Não	Sim	Não	Não	--
0	1	0	0	1

Fonte: Elaboração própria.

3.3.3 O caso canadense

Apesar de fronteiriço com os EUA, o Canadá sabe da natureza assimétrica de suas relações com aquele Estado, *i.e.*, sabe "[...]que a balança entre sua autonomia e a harmonia política com os EUA é vital, mas precária" (PAQUIN, 2009, p. 99, tradução nossa[124]).

Desde os atentados de 2001 e a consequente política global da Guerra ao Terror estadunidense, vê-se que a cooperação na área de segurança entre ambos os países se adapta totalmente às ameaças do século XXI (PAQUIN, 2009, p. 100, 105). Não obstante, tal reformulação é vista como indecisa e mesmo inconsistente por parte da academia canadiana (PAQUIN, 2009, p. 102).

Talvez, seja por isso que os assuntos de defesa e segurança cibernéticas, dentro do Canadá, não são totalmente separados, como se vê nas próximas subseções.

[124] Texto original: "[...]*that the balance between Canada's autonomy and political harmony with the United States is vital but precarious*".

3.3.3.1 IPvDC

Conforme os procedimentos explanados na Subseção 3.2.2.1, obtêm-se os dados canadenses referentes ao presente índice, por meio da busca *online* em seus sítios virtuais oficias militares.

Tais meios de comunicação e de armazenamento de informações do setor militar canadense possuem partes de seus URL associadas a dois domínios: .forces.ca e .forces.gc.ca.

A Tabela 17 mostra os resultados da busca para o caso canadense.

Tabela 17 – Dados do IPvDC do Canadá (2000-2012)

ANO	CAN_.forces.ca	CAN_.forces.gc.ca	CAN_MIL
2000	0	0	0
2001	0	0	3
2002	2	6	8
2003	1	2	3
2004	1	1	2
2005	0	4	4
2006	0	3	3
2007	1	2	3
2008	0	3	3
2009	0	2	2
2010	0	66	66
2011	4	207	211
2012	0	187	187
TOTAL	**9**	**486**	**495**

Fonte: Elaboração própria.

Em seguida, a Tabela 1 calcula a diferença do interesse militar canadense, conforme os parâmetros estabelecidos na Subseção 3.2.

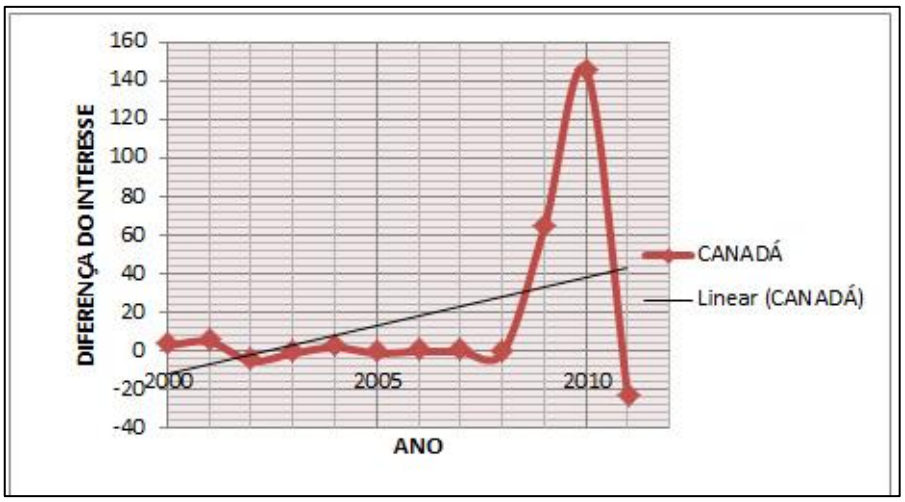
Tabela 18 – Cálculo da diferença de interesse virtual militar do Canadá na defesa cibernética (2000-2012)

período	Resultados das buscas dos termos (interesse = μ) anterior (X_{ano1})	posterior (X_{ano2})	diferença ($D = X_{ano2} - X_{ano1}$)
2000-2001	0	3	3
2001-2002	3	8	5
2002-2003	8	3	-5
2003-2004	3	2	-1
2004-2005	2	4	2
2005-2006	4	3	-1
2006-2007	3	3	0
2007-2008	3	3	0
2008-2009	3	2	-1
2009-2010	2	66	64
2010-2011	66	211	145
2011-2012	211	187	-24
Total	**308**	**495**	**187**

Fonte: Elaboração própria.

Com isso, é possível analisar superficialmente a tendência canadense para uma provável politização do ciberespaço, conforme se vê no Gráfico 3.

Gráfico 3 – Variação do interesse virtual militar do Canadá (2000-2012)



Fonte: Elaboração própria.

Como se vê, o Canadá tende a manter seu interesse de forma homogênea até o final dos anos 2000, quando há dois picos bem assimétricos, que colocam em xeque uma tentativa superficial de auferir se há, de fato, ou não aumento no seu interesse. Porém, essas informações são imprescindíveis para a obtenção do escore provisório deste índice para o caso canadense: 1,18.

Porém, como seu P = 0,25, automaticamente se aceita a hipótese nula de que, *de facto*, não há interesse militar visto em seus sítios virtuais oficiais sobre os temas que envolvem a securitização do ciberespaço. Assim, seu escore é zero para o IPvDC.

Busca-se agora auferir o índice de politização documental da defesa cibernética para o caso canadense.

3.3.3.2 IPdDC

Um adendo a este caso se faz imperioso: o documento canadense analisado e, portanto, validado para o presente índice é a *Stratégie de cybersécurité du Canada* (CAN-SCC), a qual é lançada em 2010 (CARR, 2012, p. 244; DEIBERT, 2012, p. 3; UNIÃO EUROPEIA, 2012, p. 7). Ela não é uma publicação do ´Ministério da Defesa canadense (CAN-MD), mas sim do seu Ministério da Segurança Pública.

Todavia, leva-se tal documento em consideração, sob quatro alegações: (i) cita explicitamente o CAN-MD, tendo, portanto, reverberações no setor militar canadense; (ii) é a única estratégia nacional voltada às ameaças cibernéticas daquele país; (iii) trata dos principais assuntos aqui explanados, inclusive sobre a atuação de Estados estrangeiros no ciberespaço; e (iv) evidencia a não separação canadense entre defesa e segurança cibernéticas.

A CAN-SCC faz parte de um conjunto de estratégias que visa à concretude da *Stratégie nationale sur les infrastructures essentielles* (CAN-SNIE), de 2009, que, por sua vez, reflete as ponderações do *Un cadre de sécurité civile pour le Canada* (CAN-CSCC), cuja décima edição é lançada em 2011.

Como já frisado, para auferir o escore canadense neste índice, considera-se apenas o CAN-SCC, embora os outros dois documentos – assim como ocorre no caso brasileiro – permitam lançar luz sobre algumas questões que ajudam a entender melhor sobre o porquê de a CAN-SCC dar tamanha relevância à segurança cibernética, e negligenciar a defesa cibernética.

Em primeiro lugar, utilizando-se o *software* de análise qualitativa de dados ATLAS.ti (2012), evidencia-se que o CAN-SCC se refere apenas uma única vez, em todo seu corpo textual, às ameaças ciberespaciais, quando versa a questão dos perigos e catástrofes causados pelo ser humano – *d'origine anthropique* –: "eles incluem os eventos intencionais que englobam uma parte do espectro de certos tipos de conflitos humanos, como os ataques terroristas e *cibernéticos*" (CANADÁ, 2011, p. 8, ênfase nossa, tradução nossa[125]).

Já a CAN-SNIE trata da "[...]natureza interconectada das infraestruturas críticas" daquele país (CANADÁ, 2009, p. 2, tradução nossa[126]). Por isso, seu principal objetivo é o de construir um Canadá mais seguro e resiliente, por meio de ações coerentes e complementares entre todas as iniciativas de governo – federal, provincial e territorial – e entre os 10 setores de infraestruturas críticas daquele país, a saber: (i) energia e serviços públicos; (ii) finanças; (iii) alimentação; (iv) transporte; (v) governo; (vi) TIC; (vii) saúde; (viii) água; (ix) segurança; e (x) setor manufatureiro (CANADÁ, 2009, p. 2, 6).

De acordo com o governo canadense, resiliência é a capacidade de um sistema, comunidade ou sociedade potencialmente exposto(a) a riscos de se adaptar, resistindo ou mudando, a fim de alcançar e manter sua estrutura e seu nível de funcionamento aceitáveis (CANADÁ, 2009, p. 4; 2011, p. 8-9).

---

[125] Texto original: "*Ils incluent les événements intentionnels qui englobent une partie du spectre de certains types de conflits humains, comme les attaques terroristes ou cybernétiques*".
[126] Texto original: "[...]*des interconnexions qui existent entre les infrastructures essentielles*[...]".

Essa resiliência se relaciona intrinsecamente às várias intempéries internas e externas. Dentre os exemplos de riscos a que as infraestruturas críticas canadenses estão sujeitas, a CAN-SNIE destaca desde catástrofes naturais – como o furacão Katrina, de 2005 – aos atentados terroristas de 2001 (CANADÁ, 2009, p. 4-5).

Assim, ao estender, num só documento, o rol de setores a se resguardar, o Canadá não só abarca a esfera pública, mas também a privada – no que pese também empresários, operadores e cidadãos comuns – para defender suas infraestruturas críticas.

Em resumo, os civis, por serem os primeiros a relatar as informações iniciais sobre danos a infraestruturas críticas, desempenham papel fundamental para que o governo possa responder à altura de cada situação.

Nesse sentido e ainda de acordo com o documento, dois fatos unem todos os setores: (i) o complexo sistema de interdependências entre infraestruturas críticas aumenta tais riscos e vulnerabilidades, podendo resultar em efeitos em cascata; e (ii) a crescente dependência da sociedade em TI acentua, cada vez mais, os efeitos da interdependência entre setores e suas infraestruturas críticas (CANADÁ, 2009, p. 5).

Já a CAN-SCC assemelha-se em parte à EUA-NSS, no que tange à importância dada às infraestruturas críticas digitais para o dia a dia de suas sociedades.

As palavras do Ministro da Segurança Pública canadense, Vic Toews, assinalam que, dentre outros grupos de interesses, forças militares estrangeiras estão interessadas nos sistemas digitais canadenses (CANADÁ, 2010, p. 1). Ele ainda informa que a CAN-SCC é o "plano canadense para conhecer de perto as ameaças virtuais" (CANADÁ, 2010, p. 1, tradução nossa[127]); daí o teor deste documento ser mais geral do que específico, no que tange às ameaças ciberexistenciais.

Com aproximadamente 75% dos lares acessando a Internet, o Canadá ainda presta mais de 130 tipos de serviços públicos virtuais à sua população (CANADÁ, 2010, p. 2). Com esses números, não é de se espantar que o sucesso no ciberespaço é um dos grandes patrimônios do Canadá e que proteger tal sucesso é proteger igualmente os sistemas cibernéticos, já que a segurança cibernética afeta não só o governo, mas também toda sua população (CANADÁ, 2010, p. 2).

Embora enfatize o combate ao crime cibernético – e, consequentemente, dê mais ênfase à segurança cibernética –, a CAN-SCC afirma que "as ameaças cibernéticas mais

[127] Texto original: "[...]*constitue notre plan pour combattre les cybermenaces*".

sofisticadas vêm dos serviços militares e de inteligência de Estados estrangeiros" (CANADÁ, 2010, p. 5, tradução nossa[128]), com o objetivo de obter algum tipo de vantagem.

Mais que isso, esse documento adentra na seara da defesa cibernética ao tomar conhecimento de que determinados Estados assumem publicamente que os ataques cibernéticos são um elemento central às suas estratégias militares, citando implicitamente o caso Rússia-Geórgia: "alguns [Estados] foram amplamente acusados de conduzir ataques cibernéticos paralelamente a algumas operações militares tradicionais justamente para enfatizar as consequências destas" (CANADÁ, 2010, p. 5, tradução nossa[129]).

Apenas uma subseção de meia página deste documento é dedicada à defesa cibernética, que termina por indicar que uma estratégia de defesa cibernética canadense está por vir (CARR, 2012, p. 145):

> O Canadá e seus aliados sabem que eles precisam *modernizar sua doutrina militar* para enfrentar tais riscos. Por essa razão, a OTAN adota vários documentos estratégicos sobre *defesa cibernética*. Assim como as forças militares de nossos aliados mais próximos, o *CAN-MD estuda quais os passos* que o Canadá pode tomar *para responder de forma otimizada a futuros ataques cibernéticos*. (CANADÁ, 2010, p. 8, grifo nosso, tradução nossa[130]).

Assim, com base em três pilares – proteger os sistemas governamentais, promover parcerias públicas e privadas e ajudar os canadenses a estarem seguros *online* –, a CAN-SCC pretende fortalecer os sistemas virtuais de infraestrutura crítica, apoiar o crescimento econômico e proteger os canadenses quando eles se conectam uns aos outros e ao mundo (CANADÁ, 2010, p. 7; CARR, 2012, p. 244; UNIÃO EUROPEIA, 2012, p. 7).

Com essas informações, então, é possível avaliar a pontuação do caso canadense para este índice e constatar que, com três pontos de escore, o *status* da ameaça ciberexistencial é politizado do tipo movimento securitizador, como se aponta na Tabela 19.

Tabela 19 – IPdDC do Canadá (2000-2012)

País	DOC_stux	DOC_geral	DOC_espec	DOC_total	*Status*
Canadá	1	2	0	3	Movimento securitizador

Fonte: Elaboração própria.

[128] Texto original: "*Les services militaires et du renseignement étrangers sont à l'origine des cybermenaces les plus évoluées*".
[129] Texto original: "*Certains ont été largement accusés de mener des cyberattaques parallèlement à des opérations militaires traditionnelles pour accentuer les conséquences de ces dernières*".
[130] Texto original: "*Le Canada et ses alliés savent qu'ils doivent moderniser leur doctrine militaire pour affronter ces risques. Pour cette raison, l'Organisation du Traité de l'Atlantique Nord (OTAN) a adopté plusieurs documents stratégiques sur la cyberdéfense. Comme les forces militaires de nos plus étroits alliés, le ministère de la Défense nationale et les Forces canadiennes étudient les mesures que peut prendre le Canada pour réagir de manière optimale aux cyberattaques futures*".

Conforme a possibilidade vista de o setor militar canadense criar suas diretrizes doutrinárias e/ou operacionais para o ciberespaço, é importante salientar que uma proposta de estratégia cibernética nacional é apresentada por Deibert (2012)[131]. Em seu artigo, ele busca demonstrar que o ciberespaço está mais para um ecossistema, um ambiente em que o Canadá deve se fazer presente, como outros países já fazem (DEIBERT, 2012, p. 2). Ele salienta que, embora a CAN-SCC seja uma alternativa válida, se comparada com outras Estratégias estrangeiras, ela é ainda "tímida quanto a seus compromissos e especificidades, bem como deixa muitas questões sem respostas" (DEIBERT, 2012, p. 2, tradução nossa[132]). É uma conclusão a que aqui também se chega.

3.3.3.3 IPiDC

A busca por uma maior autonomia canadense em suas relações com os EUA se expressa de forma latente na afirmação de Paquin (2009, p. 105, grifo nosso, tradução nossa[133]): "nas questões de segurança, o Canadá deve aprofundar o perímetro de segurança norte-americano, institucionalizando a cooperação bilateral acerca das questões que estão *diretamente* relacionadas à [sua]segurança nacional".

Como apontado na subseção anterior, o setor militar canadense buscará em seus aliados mais próximos, como os EUA, a ajuda necessária para poder evoluir em suas questões de defesa cibernética. O dilema entre sua autonomia e a dependência estadunidense pode ser transbordado também para as questões cibernéticas.

O Canadá cria seu órgão nacional voltado às ameaças cibernéticas antes de a CAN-SCC ser engendrada. Trata-se do *Centre canadien de réponse aux incidents cybernétiques* (CAN-CCRIC), cujo objetivo é "monitorar e prestar aconselhamento sobre redução de ameaças cibernéticas e coordenar respostas nacionais a qualquer incidente de segurança cibernética" (CANADÁ, 2010, p. 3, tradução nossa[134]).

Vale frisar que o CAN-CCRIC nada mais é que um CERT, *i.e.*, uma organização governamental que lida com praticamente toda a sorte de incidentes que envolvem computadores ou redes computacionais num dado território nacional. Assim como o Canadá,

---

[131] Ron Deibert é professor de Ciência Política e diretor do *Canada Centre for Global Security Studies* e do *Citizen Lab* da *University of Toronto*.

[132] Texto original: "[...] [a CAN-SCC] *was thin on both commitments and specifics and left many issues unaddressed*".

[133] Texto original: "*In the security realm, Canada must deepen the North American security perimeter by institutionalizing bilateral cooperation over the issues that are directly related to national security*".

[134] Texto original: "[...]*to monitor and provide mitigation advice on cyber threats, and coordinate the national response to any cyber security incident*".

os EUA possuem o seu US-CERT e o Brasil possui o CERT.br. Embora o CAN-CCRIC seja o primeiro a reagir a ataques cibernéticos, ele não possui autoridade suficiente para respondê-los diretamente, triando-os às agências canadenses competentes (CARR, 2012, p. 245), como o Serviço Canadense de Inteligência de Segurança e o CAN-MD (ANDRESS; WINTERFELD, 2011, p. 74).

É interessante frisar que o curso de Engenharia Elétrica e de Computação do Real Colégio Militar do Canadá já prepara especialistas em *cyber warfare* e redes de computadores (CANADÁ, [201-]), o que pode ser uma possível fonte para a formação do profissional – guerreiro cibernético – que venha a atuar em tal instituição militar de defesa cibernética.

Nesse sentido, o Canadá ainda não tem um órgão voltado especificamente à defesa cibernética. Como já frisado, pela própria CAN-SCC, o CAN-MD buscará meios de melhor responder a futuros ataques cibernéticos, o que implicitamente um órgão.

Assim, é possível preencher a Tabela 20, em relação a estes índice e caso.

Tabela 20 – Resultado do IPiDC do Canadá (2000-2012)

Órgão centralizador	Exército	Marinha	Aeronáutica	Total
Não	Não	Não	Não	--
0	0	0	0	0

Fonte: Elaboração própria.

3.3.4 Análise conjunta dos três casos

Como já mencionado, o segundo objetivo específico deste trabalho é projetar quais as condições para a securitização militar do ciberespaço de EUA, Brasil e Canadá. Sua meta, portanto, não é comparar, mas explorar essas condições. Todavia, como alguns dados possibilitam a comparação entre eles, oferta-se também tal análise na presente subseção.

3.3.4.1 IPvDC

A Tabela 21 apresenta os resultados das buscas nos sítios virtuais oficiais militares agrupados pelo total de cada Estado, respeitando-se o período proposto.

Tabela 21 – Resultados das buscas nos sítios virtuais militares de EUA, Brasil e Canadá (2000-2012)

ANO	EUA_MIL	BRA_MIL	CAN_MIL	TOTAL_MIL
2000	5.184	0	0	5.184
2001	6.635	2	3	6.640
2002	2.267	0	8	2.275
2003	1.636	1	3	1.640
2004	2.164	2	2	2.168

2005	2.952	2	4	2.958
2006	3.724	5	3	3.732
2007	4.787	6	3	4.796
2008	7.280	16	3	7.299
2009	8.483	35	2	8.520
2010	11.207	53	66	11.326
2011	16.496	196	211	16.903
2012	17.229	454	187	17.870
TOTAL	**90.044**	**772**	**495**	**91.311**

Fonte: Elaboração própria.

Como se vê, há um aumento pelo interesse militar nas questões de segurança do ciberespaço em todos os três países. Nos EUA, os valores aumentam 70% entre 2000 e 2012. No Brasil, não há sequer uma única menção em 2000, mas em 2012, já são 454. Já o caso canadense não é estatisticamente relevante.

Com essas informações é possível, por exemplo, comparar os dados dos três casos com os nacional e mundial.

A Tabela 25, na sequência, exibe tais comparações por setor, no nível nacional e no mundial. Esta última pode ser considerada a população de todas as páginas e/ou documentos virtuais no mundo que apresentam, pelo menos, um dos 67 termos de busca.

Tabela 22 – Resultados das buscas nos sítios virtuais de EUA, Brasil e Canadá em relação ao mundo (2000-2012)

ANO	TOTAL_MIL	TOTAL_NAC	TOTAL_MUNDO
2000	5.184	85.820	121.445
2001	6.640	110.933	161.375
2002	2.275	44.911	69.920
2003	1.640	30.628	49.999
2004	2.168	41.043	67.407
2005	2.958	60.274	100.313
2006	3.732	84.817	140.950
2007	4.796	115.209	205.470
2008	7.299	210.398	373.270
2009	8.520	332.313	1.063.600
2010	11.326	919.031	1.432.300
2011	16.903	1.582.230	3.150.900
2012	17.870	2.471.213	5.687.000
TOTAL	**91.311**	**6.088.820**	**12.623.949**

Fonte: Elaboração própria.

A partir da Tabela 22, atenta-se para três comportamentos uniformemente variados em *TOTAL_MIL*, *TOTAL_NAC* e *TOTAL_MUNDO*:

i. em 2001, há um enorme interesse pelas questões que envolvem o ciberespaço. Duas razões podem ajudar a explicar isso: uma diz respeito aos atentados terroristas do 11 de setembro, já mencionado na Subseção 3.3.1.1; e a outra se refere ao fato de que, a partir desse ano, a Convenção de Budapeste sobre Cibercrimes é assinada na Hungria, fazendo com que o ciberespaço seja visto como objeto de análise estatal enquanto fonte de ameaças (LOPES; PEREIRA, 2009, p. 5);

ii. a partir de 2003 vê-se um aumento crescente não só do interesse militar (*TOTAL_MIL*), mas também do civil-militar (*TOTAL_NAC*) dos três países, bem como do mundial (*TOTAL_MUNDO*), com uma taxa crescente de aproximadamente 11,1% a.a. para as três variáveis[135]; e

iii. a partir de 2010, quando da descoberta do Stuxnet, tanto o interesse militar quanto o civil se elevam de maneira anormal (média de aproximadamente 33,3% a.a.).

Como o foco aqui é o setor militar, e não o societário, parte-se agora para a aglutinação dos resultados. Assim, é possível calcular a diferença do interesse dos três países, em relação ao século XXI, como se vê na Tabela 23.

Tabela 23 – Cálculo da diferença de interesse virtual militar de EUA, Brasil e Canadá na defesa cibernética (2000-2012)

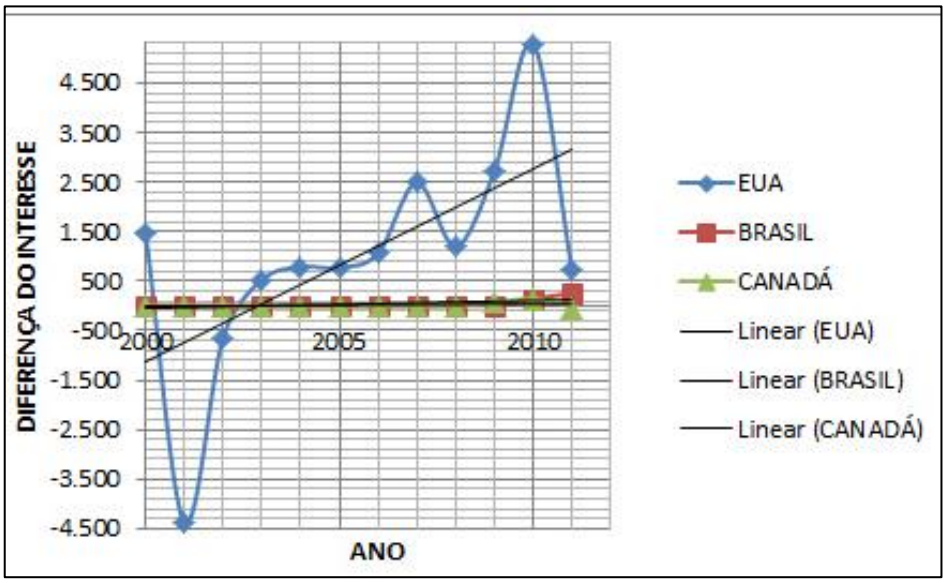
Período	Resultados das buscas dos termos (interesse = μ)		
	anterior (X_{ano1})	posterior (X_{ano2})	diferença ($D = X_{ano2} - X_{ano1}$)
2000-2001	5.184	6.640	1.456
2001-2002	6.640	2.275	-4.365
2002-2003	2.275	1.640	-635
2003-2004	1.640	2.168	528
2004-2005	2.168	2.958	790
2005-2006	2.958	3.732	774
2006-2007	3.732	4.796	1.064
2007-2008	4.796	7.299	2.503
2008-2009	7.299	8.520	1.221
2009-2010	8.520	11.326	2.806
2010-2011	11.326	16.903	5.577
2011-2012	16.903	17.870	967
Total	**73.441**	**86.127**	**12.686**

Fonte: Elaboração própria.

Os Gráficos 4 e 5 exibem as tendências dos interesses desses três países.

[135] Muito se deve, em verdade, ao aumento concomitante do número de internautas, que passa de quase 361 milhões, em 2000, para quase 2,5 bilhões em 2012, conforme a Tabela 1.

Gráfico 4 – Variação do interesse virtual militar individual de EUA, Brasil e Canadá (2000-2012)



Fonte: Elaboração própria.

Gráfico 5 – Variação do interesse virtual militar agrupado de EUA, Brasil e Canadá (2000-2012)

Fonte: Elaboração própria.

Vê-se que tanto no Brasil quanto no Canadá o interesse militar apresenta tendência homogênea; enquanto que nos EUA, não. Já com a consolidação dos dados, é possível perceber que a tendência final possui uma projeção bem semelhante à dos EUA.

3.3.4.2 IPdDC

Tendo como base a literatura da área e os resultados das análises aqui realizados, percebe-se que as ameaças existenciais oriundas do ciberespaço são, primeiro, assinaladas por uma comunidade epistêmica – que, muitas vezes, está fora do setor militar, como peritos e técnicos em segurança da informação – por meio de relatórios e/ou pareceres técnicos.

Em seguida, tem-se a dramatização, por parte do setor militar, da mesma questão, partindo-se de uma percepção mais abrangente e doutrinária de como as Forças Armadas – ou, mesmo, de uma ou mais força combatente – *compreenderão* sua participação no ciberespaço. Em outras palavras: sobre *o que* o Estado busca nacionalmente e *do que* ele se defende internacionalmente. As EUA-NSS, BRA-END e CAN-CCSS são exemplos dessas premissas.

Como numa espécie de terceiro estágio ou etapa, vislumbra-se um período de curta duração – aproximadamente três anos – para a "digestão" ou incubação das questões cibernéticas em forma de projetos e/ou de documentos militares cujo foco estratégico e/ou operacional mostra mais especificamente como as Forças Armadas *atuarão* no ciberespaço, orientando *como* se dará a defesa nacional frente às ameaças cibernéticas. É o que ocorre, por exemplo, nas EUA-SOC e BRA-PCD.

Em parecida direção de orientação – da político/doutrinária para a operacional/logística –, Duarte (2012a, p. 74) segue a expectativa "[...]de que uma política orienta os programas de tecnologias militares, e não o contrário[...]".

As três etapas acima não devem ser encaradas como um dogma; apenas como uma tendência que se observa em fenômenos ligados à securitização – sobretudo, as que projetam instituições específicas, como nos casos estadunidense e brasileiro – do ciberespaço pelo setor militar de alguns países e também de organizações internacionais[136].

Esses passos se encaixam no caso brasileiro, que marca um ponto a menos que os EUA e dois pontos a mais que o Canadá, neste índice.

O Canadá e os EUA são os únicos que pontuam na variável sobre a dramatização explícita de guerras cibernéticas, em seus documentos oficiais. Embora os canadenses não utilizem literalmente o termo "Stuxnet" – como o fazem, por exemplo, Alemanha e Holanda (LOPES, 2011b, p. 14) –, a dramatização militar evoca casos-chave na literatura da área, envolvendo ataques tradicionais conjugados com virtuais.

---

[136] Cf. LOPES, 2011d; LOPES; MEDEIROS, 2011.

Já os EUA se mantêm na primeira posição, marcando seis pontos de seis possíveis para este índice.

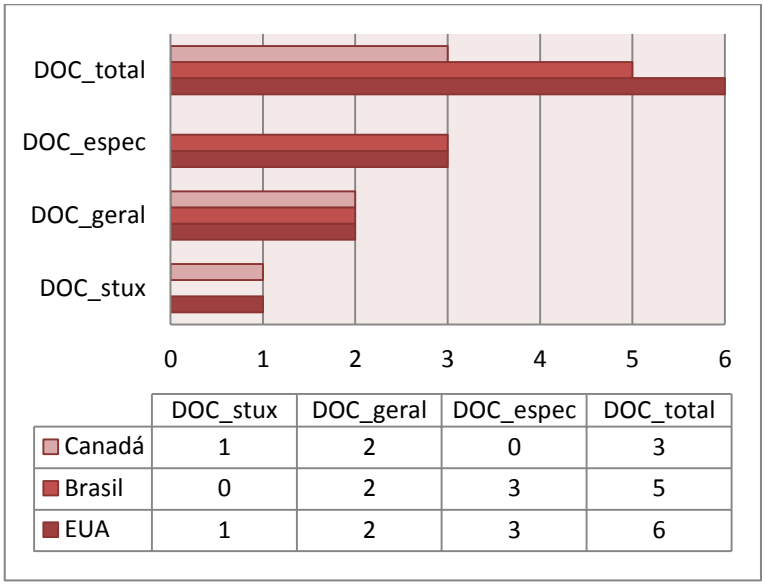
A Tabela 24 e o Gráfico 6 apresentam o exposto nos parágrafos anteriores.

Tabela 24 – IPdDC de EUA, Brasil e Canadá (2000-2012)

País	DOC_stux	DOC_geral	DOC_espec	DOC_total	*Status*
EUA	1	2	3	6	Movimento securitizador
Brasil	0	2	3	5	Movimento securitizador
Canadá	1	2	0	3	Movimento securitizador

Fonte: Elaboração própria.

Gráfico 6 – IPdDC de EUA, Brasil e Canadá (2000-2012)



Fonte: Elaboração própria.

Graças aos dados supramencionados e com o auxílio da Tabela 25[137], projeta-se a distribuição de frequências dos/entre os três xasos.

Tabela 25 – Distribuição de frequências do IPdDC de EUA, Brasil e Canadá (2000-2012)

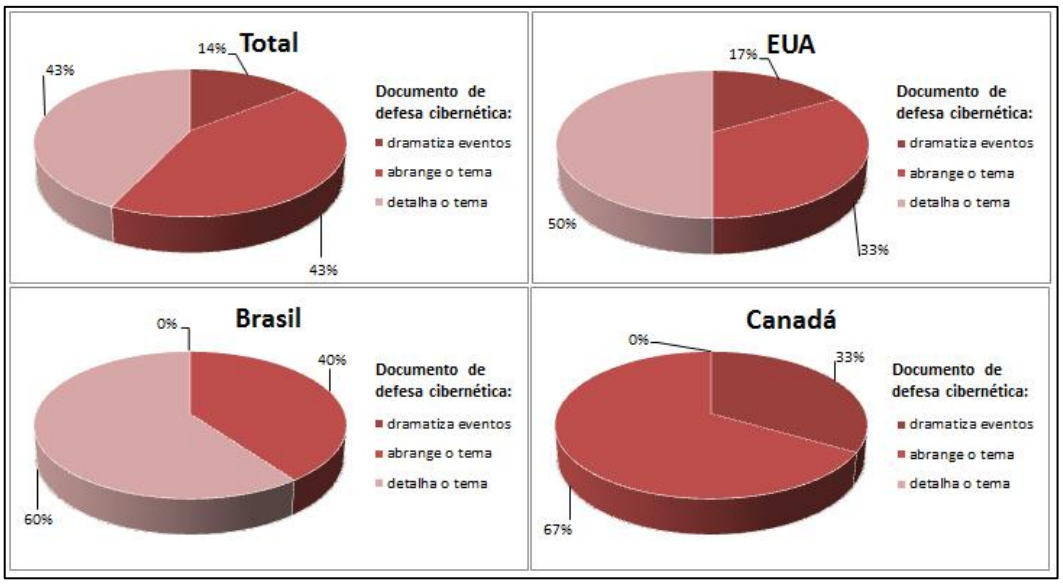
Documento de defesa cibernética	EUA (%)	Brasil (%)	Canadá (%)	Total (%)
dramatiza eventos internacionais	1 (33)	0 (0)	1 (33) [a)]	2 (14)
abrange o tema	2 (17)	2 (40)	2 (67) [a)]	6 (43)
detalha o tema	3 (50)	3 (60)	0 (0)	6 (43)
Total	**6 (100)**	**5 (100)**	**3 (100)**	**14 (100)**

Fonte: Elaboração própria.
Nota: a) Valor aproximado.

[137] Por sua natureza, a Tabela 28 pode ser considerada uma tabela de dupla entrada ou de contingência (cf. BARBETTA, 1994, p. 67).

Já o Gráfico 7 desempenha o mesmo papel que a Tabela 25, só que de forma mais intuitiva.

Gráfico 7 – Distribuição de frequências dos resultados do IPdDC de EUA, Brasil e Canadá (2000-2012)



Fonte: Elaboração própria.

Os EUA chegam ao ápice do escore possível, pois apresenta todas as variáveis testadas. Já o caso brasileiro alcança um índice satisfatório, embora a tabela e o gráfico imediatamente acima apresentem que o escore brasileiro possui 0% de dramatização de eventos internacionais. É possível afirmar também que, para o índice presente, o escore canadense é o mais baixo por que não possui ainda um documento específico de defesa cibernética, e sim um documento que apenas a abrange de forma a não atribuir poderes nem constituir instituições militares nesta seara.

3.3.4.3 IPiDC

Os dados consolidados deste índice para os três Estados selecionados são mostrados na Tabela 26.

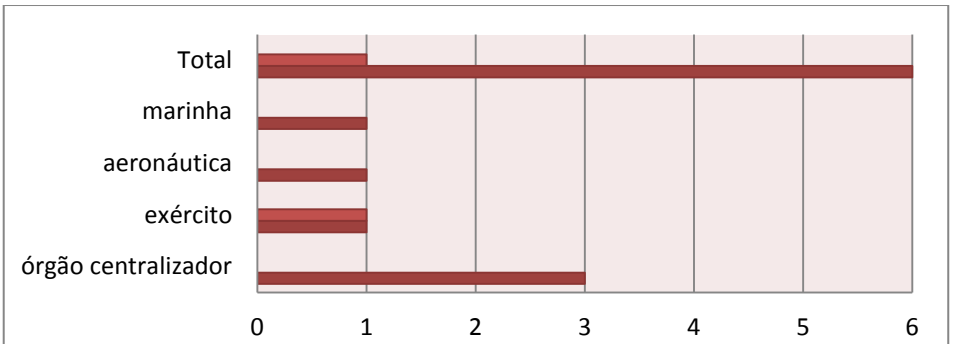
Tabela 26 – Resultados da institucionalização da defesa cibernética de EUA, Brasil e Canadá (2000-2012)

País	Órgão Centralizador	Exército	Marinha	Aeronáutica
EUA	Sim	Sim	Sim	Sim
Brasil	Não	Sim	Não	Não
Canadá	Não	Não	Não	Não

Fonte: Elaboração própria.

Transpondo os valores nominais para escalares, é possível realizar a pontuação de cada Estado, conforme exibem os Gráficos 8 e 9, sendo o último gerado a partir de R Core Team (2012).

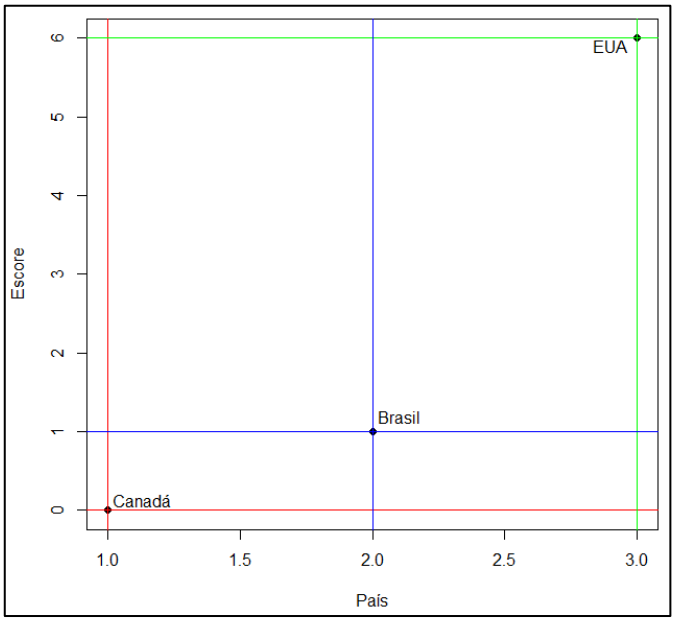
Gráfico 8 – Projeção em barras do IPiDC de EUA, Brasil e Canadá (2000-2012)



	órgão centralizador	exército	aeronáutica	marinha	Total
Canadá	0	0	0	0	0
Brasil	0	1	0	0	1
EUA	3	1	1	1	6

Fonte: Elaboração própria.

Gráfico 9 – Projeção em *plot* do IPiDC de EUA, Brasil e Canada (2000-2012)



Fonte: Elaboração própria.

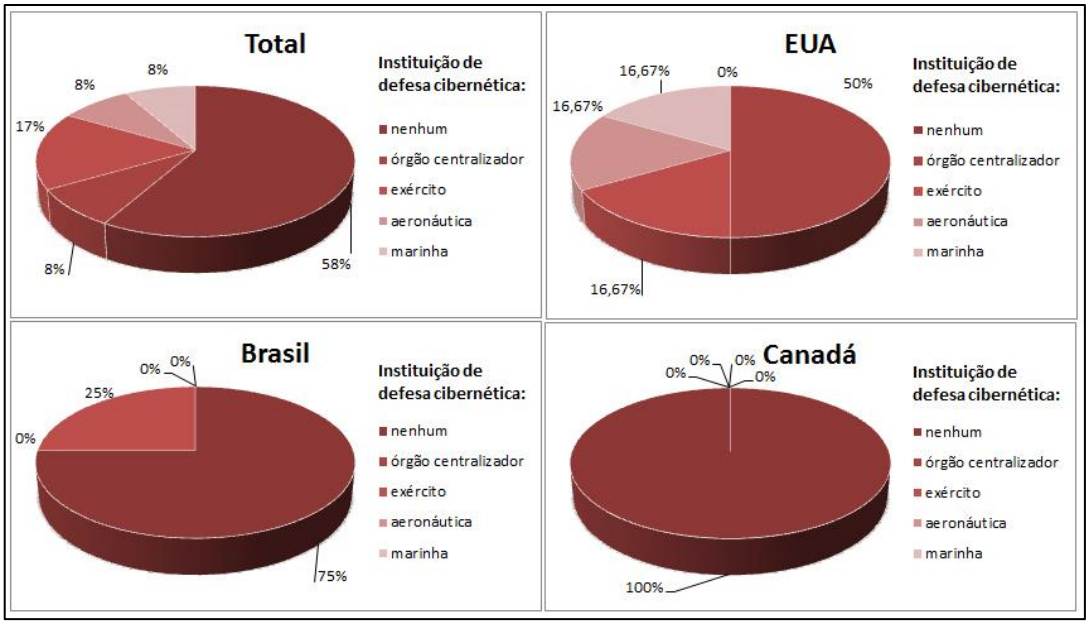
Por meio dos dados apontados acima, é possível traçar a distribuição de frequências entre os três países, conforme a Tabela 27 e o Gráfico 10.

Tabela 27 – Distribuição de frequências do IPiDC de EUA, Brasil e Canadá (2000-2012)

Instituição de defesa cibernética	EUA (%)	Brasil (%)	Canadá (%)	Total (%)
nenhum	0	3 (75)	4 (100)	7 (58,33) [a)]
órgão centralizador	3 (50)	0	0	1 (8,33) [a)]
exército	1 (16,67) [a)]	1 (25)	0	2 (16,7) [a)]
marinha	1 (16,67) [a)]	0	0	1 (8)
aeronáutica	1 (16,67) [a)]	0	0	1 (8)
Total	**6 (100)**	**4 (100)**	**4 (100)**	**12 (100)**

Fonte: Elaboração própria.
Legenda: a) Valor aproximado da segunda casa decimal.

Gráfico 10 – Distribuição de frequências do IPiDC de EUA, Brasil e Canadá (2000-2012)



Fonte: Elaboração própria.

Como se vê, os EUA são o Estado que possui o maior IPiDC entre os três casos, marcando pontos em todos os quatro atributos. Isso se deve, bem verdade, pelo fato de ele ser um potencial alvo de armas e ataques cibernéticos.

O Brasil demonstra interesse institucional pela defesa cibernética, oficialmente, desde 2008, quando a BRA-END prevê a criação do BRA-CDCiber, o qual é engendrado em 2010 e posto em funcionamento em 2012 (SÁ, 2012).

O Canadá, por outro lado, está num estágio que pode ser comparado ao que o Brasil apresentava um pouco antes do lançamento da BRA-END, em 2008. Os canadenses reconhecem os riscos e já sinalizam seu setor militar para que promova novos arranjos no âmbito da defesa cibernética. Todavia, seu escore neste índice é zero.

Após a extração e consequente análise do processo de politização da defesa cibernética nos três Estados, parte-se, finalmente, para o desenvolvimento do ESMC, como se vê a partir da subseção abaixo.

3.3.5 O Espectro da Securitização Militar do Ciberespaço (ESMC)

Entende-se que, para a concretude do terceiro objetivo específico[138] desta Dissertação, é preciso analisar os resultados dos três Índices de Politização da Defesa Cibernética conjuntamente. Somente assim, é possível dar vida ao ESMC, *framework* imprescindível para a conclusão desta Dissertação.

A Tabela 28 apresenta os resultados dos três índices propostos para os três casos.

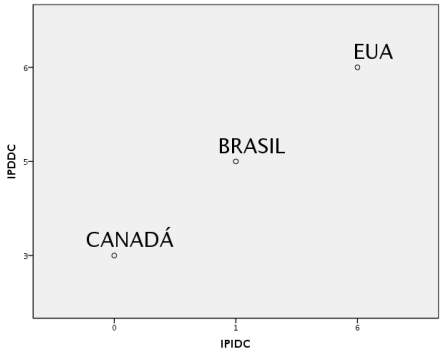
Tabela 28 – Índices de Politização da Defesa Cibernética de EUA, Brasil e Canadá (2000-2012)

País	IPvDC	IPdDC	IPiDC	TOTAL
EUA	1,55	6	6	13,55
Brasil	1,64	5	1	7,64
Canadá	0	3	0	3

Fonte: Elaboração própria.

Tendo essas informações em mente, é possível visualizá-las de forma mais ampla, por meio de diagrama de dispersão. Com a ajuda de IBM SPSS Statistics (2012) e se levando em consideração os índices não zerados dos três casos selecionados, é possível traçar um desses diagramas. O Gráfico 11 projeta tal cenário.

Gráfico 11 – Diagramas de dispersão dos IPdDC pelo IPiDC de EUA, Brasil e Canadá (2000-2012)



Fonte: Elaboração própria.
Nota: Ao todo, IBM SPSS Statistics (2012) gera seis saídas – uma para cada gráfico – na linguagem de produção de gráficos (GPL, de *Graphical Production Language*). O Apêndice E mostra uma das saídas, caso o leitor deseje replicar os resultados obtidos graficamente.

[138] Explicar os resultados da securitização militar na política internacional.

Todavia, o total final dos Índices não garante, ainda, acesso ao ESMC. É preciso, porém, realizar algumas inferências e utilizar silogismos.

Primeiro, se se tomar como base o total dos Índices acima, os escores máximo e mínimo de cada índice são considerados "locais"; já os do total são "globais".

Segundo, levam-se em conta também as seguintes informações: (i) o IPvDC é obtido ponderadamente[139]; (ii) é possível um Estado obter escores máximos nos IPdDC e IPiDC e, mesmo assim, zerar o IPvDC[140]; e (iii) os escores mínimos para se considerar uma questão politizada do tipo movimento securitizador são entre 3 e 6 (IPdDC) e 4 e 6 (IPiDC). Com isso, projeta-se o seguinte escore mínimo para ter acesso ao ESMC: 7 pontos no total dos Índices de Politização da Defesa Cibernética, sendo, pelo menos, 3 pontos no IPdDC e 4 no IPiDC.

Terceiro, para se obter o escore do ESMC, procede-se com o seguinte: (i) reinicia-se a contagem em 1 a partir do sétimo ponto do total final dos índices; e (ii) zera-se o escore dos demais países com menos de 6 pontos, no mesmo total.

Por exemplo, os escores dos três casos analisados são transpostos para o ESMC, como mostra a Tabela 29.

Tabela 29 – Escores no ESMC de EUA, Brasil e Canadá (2000-2012)

País	Total nos Índices	ESMC
EUA	13,55	7,55
Brasil	7,64	1,64
Canadá	3	0

Fonte: Elaboração própria.

Portanto, se, como a literatura aponta, os EUA se encontram atualmente na vanguarda da defesa cibernética, pode-se inferir que o valor de 7,55 pontos é um escore que se aproxima da pontuação máxima possível do ESMC.

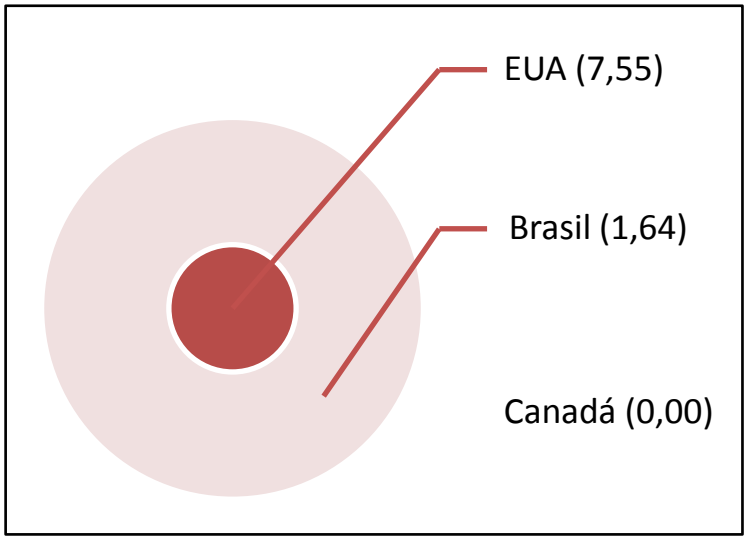
Finalmente, chega-se ao Esquema 6, que apresenta o ESMC para os três casos aqui analisados.

---

[139] Para conhecer o escore máximo deste índice, tem-se que aplicá-lo à população de Estados do sistema internacional (N=195), limitando o período de análise entre 2000 e 2012.

[140] Coreia do Norte é um caso pertinente, mesmo com um restritíssimo acesso à Internet, seu setor/regime militar cibernético detém fortes credenciais entre a literatura especializada (cf. CLARKE; KNAKE, 2012, *passim*; CARR, 2012, *passim*). Leva-se em conta também que "[...]cresce a luta por autonomia no controle da 'rede'. Russos, [...]chineses, e até iranianos se esforçam por fugir do domínio americano na web" (MARTIN, 2012).

Esquema 6 – ESMC de EUA, Brasil e Canadá (2000-2012)



Fonte: Elaboração própria.

Após todo esse esforço para explicar se há e como se procede a securitização militar do ciberespaço em EUA, Brasil e Canadá, no século XXI, é possível agora realizar a conclusão desta Dissertação, em que pese os objetivos inicialmente traçados.

4 CONSIDERAÇÕES FINAIS

> A forma com que o processo de securitização de um ator se encaixa com as percepções de outros sobre o que constitui uma ameaça "real" *importa* na formação da interação de valores dentro do sistema internacional. (BUZAN *et al*., 1998, p. 30-31, grifo nosso, tradução nossa[141]).

A Seção 1 informa que o objetivo principal desta Dissertação é analisar os efeitos de uma possível securitização militar do ciberespaço na política internacional atual. Para tanto, tal meta é dividida em três passos menores e sucessivos.

O primeiro diz respeito à identificação das potenciais ameaças existenciais que o setor militar entende como "de segurança", revelando, concomitantemente, os motivos que a caserna possui para fazê-lo no século atual.

Como se expõe na Seção 2, as ameaças existenciais provenientes do ciberespaço são várias e possuem complexidades de tratamento e resolução diferentes para cada Estado. Porém, duas dessas complexidades chamam a atenção militar: os ataques cibernéticos associados a ataques bélicos e as armas cibernéticas, como demonstrado nos três casos envolvendo Rússia, EUA, Israel, Geórgia, Estônia e Irã. O receio de que os danos causados a estes três últimos Estados não se repitam em seu próprio território – ainda que cibernético – prostra-se como fortes indícios de que a securitização militar do ciberespaço é levada em conta por outros Estados. Já o fato de isso ocorrer e está ocorrendo neste século se explica pela potencialização do caráter anárquico, semiubíquo e autoexpansível da Internet, que igualmente impulsiona as ameaças assimétricas, fazendo com que a caserna desperte, décadas depois, de uma era em que a rede mundial de computadores só lhe trazia benefícios e um sentimento de proteção.

A partir da citação que abre esta última seção, pode-se deduzir que, (i) caso um processo de securitização ocorra num Estado e, uma vez isso se confirmando, (ii) ele influencie o processo político de definir uma ameaça como "de segurança", então (ii) é possível afirmar que esses dois processos intersubjetivos impactam objetivamente a política internacional – que nada mais é do que a interação objetiva, subjetiva e intersubjetiva de atores estatais fora do seu território nacional.

Portanto, assume-se que todos os objetivos desta Dissertação são alcançados e conclui-se, portanto, que: (i) tanto EUA quanto Brasil securitizam as ameaças ciberespaciais no século XXI; (ii) o Canadá, por outro lado, não securitiza, mas demonstra fortes indícios de seguir o

---

[141] Texto original: "*The way the securitization processes of one actor fit with the perceptions of others about what constitutes a 'real' threat matters in shaping the interplay of securities within international system*".

mesmo caminho que os outros dois casos; mais que isso, (iii) o Canadá não só leva em consideração (elemento intersubjetivo) a forma com que outros atores agem no cenário internacional – os quais se utilizam de ataques cibernéticos aliados a bélicos –, como também, a partir deles, dramatiza suas próprias questões "de segurança" cibernética (elemento objetivo); e (iv) tendo em vista a análise exploratória dos casos, na Seção 3, concorda-se com o fato de que os EUA estão na dianteira do desenvolvimento de verdadeiros arsenais cibernéticos (GAGNON, 2008, p. 59).

Sendo assim, o caso canadense – seguindo os mesmos passos dos alemão e holandês, como já frisado – pode ser utilizado aqui não apenas como um *case* da politização em si mesmo (nível de análise: *input* do processo de politização ciberespacial), mas também como um em que os reflexos dessa politização ciberespacial podem ser também auferidos (nível de análise: *output* do processo de politização ciberespacial). É o que está exposto nas estritas palavras de Buzan *et al.* (1998, p. 25, grifo nosso, tradução nossa[142]): "*o processo de securitização* não *se satisfaz* apenas pela quebra de regras [...]nem apenas por ameaças existenciais[...], mas *por casos de ameaças existenciais que legitimam a quebra de regras*".

Os EUA demonstram ser um ator cujas ações internas também influenciam a forma com que outros atores agem perante o ciberespaço (GAGNON, p. 2008, p. 63). Prova disso é que, a partir do incidente com as centrífugas nucleares iranianas, muitos países vão pensar – eis novamente o processo intersubjetivo de que fala a Escola de Copenhague – melhor antes de adquirir um *hardware* de infraestrutura crítica que, mesmo sem ter acesso à Internet, não possua algum *software* de detecção de códigos-fonte maliciosos.

Os teóricos da securitização entendem o sistema internacional em termos relacionais, ou seja, "como coletividades humanas se relacionam entre si em termos de ameaças e vulnerabilidades" (BUZAN *et al*., 1998, p. 10, tradução nossa[143]).

Parece ser também este o caminho adotado por Miyamoto, quando este afirma que "[…] nada é imutável nas relações internacionais" (MIYAMOTO, 2003, p. 704) e que "[...]a segurança é vista sob prismas diferentes conforme o papel que cada um desempenha no cenário mundial" (MIYAMOTO, 2003, p. 707).

Por exemplo, quando se analisa o processo de securitização militar do Brasil, vê-se que, embora se trate de novos arranjos politicodocumentais relacionados a ameaças

---

[142] Texto original: "*Securitization is not fulfilled only by breaking rules* [...] *nor solely by existential threats* [...] *but by cases of existential threats that legitimize the breaking of rules*".
[143] Texto original: "*International security is mostly about how human collectivities relate to each other in terms of threats and vulnerabilities*[…]".

ciberexistenciais, todo ele é marcado por transparência pública e pela proclamação ao legítimo direito de defesa. Por outro lado, o processo securitizatório militar dos EUA, demonstra ser mais agressivo, permeado por um viés tradicionalista da teoria (neo)realista de RI.

Isso implica dizer que um dado Estado pode levar em contar tanto um quanto outro modelo para engendrar o seu próprio. Ou nenhum dos dois. O caso tupiniquim evidencia isto: seu processo de securitização se mostra "autônomo", ou seja, com uma leitura abrangente, infere-se que, ao não marcar na única variável que garante um ponto no IPdDC, o Brasil enfatiza que suas ações no ciberespaço estão associadas principalmente ao seu próprio desenvolvimento nacional. Isso, porém, quem deve subentender é cada um dos Estados que compõem o sistema internacional.

Num mundo onde "tudo, exatamente tudo hoje depende de sistemas em rede, internet e computadores" (FERREIRA NETO, 2011), ou seja, onde tudo está conectado (WOODWARD, 2012), a defesa do espaço ou setor cibernético deixa de ser um enredo de filme de ficção científica e passa a ser uma política de Estado, no que pese a atualização de suas Forças Armadas, que, como já mencionado, é o braço armado do poder político.

Nesse sentido, três considerações também podem ser auferidas, a partir do exposto neste trabalho.

Primeiro, é preciso detalhar melhor os investimentos em defesa cibernética nos orçamentos militares, separando-os dos de segurança cibernética, bem como de meros equipamentos e serviços. É o que conjuga também Brasil (2012d, p. 12).

Segundo, um remédio jurídico internacional também se mostra oportuno. É o que defende Lopes (2011e) e o fundador de uma das maiores empresas de antivírus do mundo:

> O ideal seria proclamar a internet uma zona desmilitarizada. Mas não estou seguro de que o desarmamento seja possível. A oportunidade já foi perdida, os investimentos foram realizados, as armas foram criadas e a paranoia já existe. Mas os países precisam ao menos chegar a um acordo sobre regras e controles quanto às armas cibernéticas. (Eugene Kaspersky *apud* NINIO, 29 jul. 2012).

A relação entre armas cibernéticas e guerreiros cibernéticos também deve ser posta à mesa. É de maneira mais abrangente que Proença Jr e Diniz (1998, 22) afirmam que "armamentos e forças armadas são parte de um contínuo de meios de diálogo entre os Estados, na paz como na guerra, tendo, como disse Clausewitz, sua própria gramática, mas não a sua própria lógica" (PROENÇA JR; DINIZ, 1998, p. 22). Com isso em mente, parte-se para a próxima consideração.

Terceiro e tomando por base a assertiva de que "[...] os estrategistas militares existem exatamente para pensar a guerra" (MIYAMOTO, 1987, p. 22), é fundamental que não só

guerreiros cibernéticos, mas também estrategistas cibernéticos façam parte do corpo de qualquer instituição militar para esses fins. É o que postula também Sanger (2012a, p. 193). Não se deve perder de vista que, assim como em qualquer instituição social, certos direitos fundamentais devem ser observados – se até mesmo na guerra convencional, há regras sobre direitos humanos, por que não estendê-las também ao ambiente cibernético? Um profissional que saiba levar em conta os limites do seu Estado e do próprio ciberespaço se faz imperioso, ainda que se mostre custoso, pois, "[...]em assuntos de defesa, é freqüentemente (*sic*) melhor ter alguns de elite do que ter muitos medíocres" (PROENÇA JR; DINIZ, 1998, p. 39).

Todavia, para qualquer assunto que abranja defesa nacional e ciberespaço, deve-se ter sempre em mente as palavras do Vice-Secretário de Defesa estadunidense, William Lynn: "no século XXI, *bits* e *bytes* podem ser tão ameaçadores quanto balas e bombas" (LYNN III, 2011, grifo nosso, tradução nossa[144]). Embora a tecnologia seja um elemento central na guerra (LEMAN-LANGLOIS, 2008a, p. 243), ela não a governa (ARQUILA; RONFELDT, 1993, p. 142).

Por fim, esta Dissertação conclui que, pelo exposto aqui, Ciência Política e RI se mantêm atualizadas na vanguarda dos estudos internacionais, pois, assim como há um século, quando elas se debruçaram sobre a natureza da guerra e os desafios para se manter a paz, hoje ambas conjugam esses mesmos verbos, só que num outro ambiente: o cibernético.

[144] Texto original: "*In the twenty-first century, bits and bytes are as threatening as bullets and bombs*".

REFERÊNCIAS

ACÁCIO, Igor D. P.; LOPES, Gills. Segurança internacional no século XXI: o que as teorias de Relações Internacionais têm a falar sobre o ciberespaço? In: ENCONTRO ANUAL DA ANPOCS, 36., 2012, Águas de Lindóia. **Anais eletrônicos**. [S.l.]: ANPOCS, 2012. Disponível em: <http://www.anpocs.org/portal/index.php?option=com_docman&task=doc_details&gid=8169&Itemid=76>. Acesso em: 17 dez. 2012.

ALSINA JÚNIOR, João Paulo S. **Política externa e poder militar no Brasil**: universos paralelos. Rio de Janeiro: Editora FGV, 2009. (Série Entenda o Mundo).

ANDRESS, Jason; WINTERFELD, Steve. **Cyber warfare**: techniques, tactics and tools for security practitioners. Boston: Syngress/Elsevier, 2011.

ARON, Raymond. **Paz e guerra entre as nações**. Tradução: Sergio Bath. Brasília e São Paulo: Editora UnB/IPRI/Imprensa Oficial de São Paulo, 2002. v. 1.

ARQUILLA, John; RONFELDT, David. Cyberwar is coming! **Comparative Strategy**, v. 12, n. 2, Spring 1993, p. 141-165.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002:2005**: Tecnologia da informação – Técnicas de segurança – Código de pratica para a gestão da segurança da informação. Rio de Janeiro: 2005. Disponível em: <http://www.abntcatalogo.com.br/norma.aspx?ID=1532>. Acesso em: 20 jan. 2013.

ATLAS.ti. Programa de análise qualitativa de dados. Version 7. Berlim: Scientific Software Development GmbH, 2012.

BARBETTA, Pedro Alberto. **Estatística aplicada às ciências sociais**. Florianópolis: Ed. Da UFSC, 1994.

BENCSÁTH, Boldizsár; PÉK, Gábor; BUTTYÁN, Levente; FÉLEGYHÁZ, Márk. **Duqu**: a Stuxnet-like malware found in the wild. Budapeste: Laboratory of Cryptography and System Security (CrySyS) at the Budapest University of Technology and Economics, 2011.

BENEDIKT, Michael. Introduction. In: _____ (Ed.). **Cyberspace**: first steps. Cambridge, MA: MIT Press, 1991.

BEZERRA, Marcelo. Artigo sobre Guerra Cibernética "Cyberwar". **DSIC/DSI-PR**, Brasília, [2009]. Disponível em: <http://dsic.planalto.gov.br/artigos/71-artigo-sobre-guerra-cibernetica-qcyberwarq>. Acesso em: 29 mar. 2012.

BRASIL. Centro Nacional de Desenvolvimento Científico e Tecnológico – CNPq. Aplicação de Vant na agricultura será apresentada em evento internacional. Brasília, 22 jun. 2012a. Disponível em: <http://www.cnpq.br/web/guest/noticiasviews/-/journal_content/56_INSTANCE_a6MO/10157/299912>. Acesso em: 20 nov. 2012.

_____. Constituição (1988). **Presidência da República**, Brasília, 1998. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 3 dez. 2012.

_____. Decreto nº 5.484, de 30 de junho de 2005. Aprova a Política de Defesa Nacional, e dá outras providências. **Presidência da República**, Brasília, 2005. Disponível: <http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Decreto/D5484.htm>. Acesso em: 8 jan. 2013.

_____. Decreto nº 6.703, de 18 de dezembro de 2008a. Aprova a Estratégia Nacional de Defesa, e dá outras providências. **Presidência da República**, Brasília, 2008a. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Decreto/D6703.htm>. Acesso em: 10 out. 2010.

_____. Decreto nº 7.364, de 23 de novembro de 2010. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão do Grupo-Direção e Assessoramento Superiores - DAS, das Funções Gratificadas - FG, das Gratificações de Exercício em Cargo de Confiança, das Gratificações de Representação pelo Exercício de Função e das Gratificações de Representação - GR do Ministério da Defesa. **Presidência da República**, Brasília, 2010a. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2010/Decreto/D7364.htm>. Acesso em: 20 jan. 2013.

_____. Decreto nº 7.476, de 23 de maio de 2011. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão do Grupo-Direção e Assessoramento Superiores - DAS, das Gratificações de Exercício em Cargo de Confiança e das Gratificações de Representação pelo Exercício de Função da Secretaria de Aviação Civil da Presidência da República, altera dispositivos do Decreto no 7.364, de 23 de novembro de 2010, e dá outras providências. **Presidência da República**, Brasília, 2011a. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Decreto/D7476.htm>. Acesso em: 20 jan. 2013.

_____. Exército Brasileiro. **Boletim do Exército**, Brasília, DF, n. 28, 16 jul. 2010b. Disponível em: <http://www.sgex.eb.mil.br/sistemas/be/copiar.php?codarquivo=812&act=bre>. Acesso em: 17 ago. 2011.

_____. Exército Brasileiro. **Boletim do Exército**, Brasília, DF, n. 31, 6 ago. 2010c. Disponível em: <http://www.sgex.eb.mil.br/sistemas/be/copiar.php?codarquivo=824&act=bre>. Acesso em: 19 ago. 2011.

_____. Exército Brasileiro. Defesa cibernética em grandes eventos é tema de debate em seminário na capital federal. 2012b. Disponível em: <http://www.exercito.gov.br/web/midia-impressa/noticiario-do-exercito?p_p_id=noticias_WAR_noticiasportlet_INSTANCE_cZy7&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=view&p_p_col_id=column-3&p_p_col_count=3&_noticias_WAR_noticiasportlet_INSTANCE_cZy7_journalArticleId=2217012&_noticias_WAR_noticiasportlet_INSTANCE_cZy7_struts.portlet.action=%2Fview%2Farquivo!viewJournalArticle&_noticias_WAR_noticiasportlet_INSTANCE_cZy7_struts.portlet.mode=view#.UP3K4WclqSq>. Acesso em: Acesso em: 9 dez. 2012.

_____. Exército Brasileiro. II Jornada de Trabalho de Defesa Cibernética. 2011b. Disponível em: <http://www.exercito.gov.br/web/midia-impressa/noticiario-do-exercito?p_p_auth=DwUd5pHu&p_p_id=20&p_p_lifecycle=1&p_p_state=exclusive&p_p_mode=view&_20_struts_action=%2Fdocument_library%2Fget_file&_20_folderId=396506&_20_name=DLFE-22210.pdf>. Acesso em: Acesso em: 18 dez. 2012.

_____. Exército Brasileiro. Pregão Presencial 032/2007. 6 dez. 2007a. Disponível em: <http://www.doc.eb.mil.br/docv2/doc_v2/downloads/ciber.xls>. Acesso em: Acesso em: 18 dez. 2012.

_____. Força Aérea Brasileira. INFORMÁTICA – Ministério da Defesa realizará neste mês 3º Seminário de Defesa Cibernética. **Agência Força Aérea**, 15 out. 2012c. Disponível em: <http://www.fab.mil.br/portal/capa/index.php?mostra=13001>. Acesso em: 9 dez. 2012.

_____. Gabinete de Segurança Institucional da Presidência da República. Instrução Normativa GSI Nº 1, de 13 de junho de 2008. Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Poder Executivo, Brasília, DF, 18 jun. 2008b. Seção 1, p. 6-7.

_____. **Livro Branco de Defesa Nacional**. Brasília: Ministério da Defesa, 2012d.

_____. **Manual de abreviaturas, siglas, símbolos e convenções cartográficas das Forças Armadas – MD33-M-02**. 3. ed. Brasília: Ministério da Defesa, 2008c.

_____. Ministério da Defesa. Organograma. Brasília, 25 jan. 2013a. Disponível em: <http://www.defesa.gov.br/arquivos/estrutura/organograma.pdf>. Acesso em: 26 jan. 2012.

_____. Ministério da Defesa. Portaria Nº 3.389/MD, de 21 de dezembro de 2012. Dispõe sobre a Política Cibernética de Defesa. **Diário Oficial [da] República Federativa do Brasil**, Poder Executivo, Brasília, DF, 27 dez. 2012e. Seção 1, p. 11-12.

_____. Ministério das Relações Exteriores. **Repertório de política externa**: posições do Brasil. Brasília: Fundação Alexandre de Gusmão, 2007b.

_____. Software Livre no governo do Brasil. Seminários Tecnológicos - Segurança da Informação. [S.l.], jan. 2013b. Disponível em: <http://softwarelivre.gov.br/eventos/seminarios-tecnologicos-seguranca-da-informacao>. Acesso em: 4 jan. 2013.

BROAD, William J.; MARKOFF, John; SANGER, David E. Israeli test on worm called crucial in Iran nuclear delay. **The New York Times**, 15 January 2011, World. Disponível em: <http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all>. Acesso em: 19 mar. 2012.

BULL, Hedley. **A sociedade anárquica**: um estudo da ordem na política mundial. Tradução: Sergio Bath. Brasília: Editora UnB, 2002.

BUZAN, Barry; HANSEN, Lene. **The evolution of International Security Studies**. Cambridge: Cambridge University Press, 2009.

BUZAN, Barry; WÆVER, Ole; WILDE, Jaap de. **Security**: a new framework for analysis. Boulder: Lynne Rienner, 1998.

CANADÁ. Collège Militaire Royal du Canada. Génie électrique et informatique. Opportunités: Guerre de l'information et réseaux. [201-]. Disponível em: <http://ece-rmc.ca/?page_id=45&lang=fr>. Acesso em: 23 dez. 2012.

_____. Sécurité publique Canada. **Stratégie de cybersécurité du Canada**, Ottawa, 2010. Disponível em: <http://www.publicsafety.gc.ca/prg/ns/cybr-scrty/_fl/ccss-scc-fra.pdf>. Acesso em: 21 jan. 2012.

_____. Sécurité publique Canada. **Stratégie nationale sur les infrastructures essentielles**, Ottawa, 2009. Disponível em: <http://www.publicsafety.gc.ca/prg/ns/ci/_fl/ntnl-fra.pdf>. Acesso em: 2 jan. 2012.

_____. Sécurité publique Canada. **Un cadre de sécurité civile pour le Canada**. 10me. ed. Ottawa, Janvier 2011. Disponível em: <http://publications.gc.ca/collections/collection_2011/sp-ps/PS4-103-2011-fra.pdf>. Acesso em: 4 set. 2012.

CARR, Jeffrey. **Inside cyber warfare**: mapping the cyber underworld. 2. ed. Cambridge: O'Reilly, 2012.

CARVALHO, Paulo Sergio M. de. A defesa cibernética e as infraestruturas críticas nacionais. In: CICLO DE ESTUDOS ESTRATÉGICOS, 10., 2011, Rio de Janeiro. **Apresentações**. Rio de Janeiro: Escola de Comando e Estado-Maior do Exército, 2011. Disponível em: <http://200.20.16.3/seer_ocs/index.php/CEE/XCEE/paper/viewFile/5/7>. Acesso em: 3 abr. 2012.

CASTELLS, Manuel. **Fim do Milênio**. 4. ed. Tradução: Klauss B. Gerhardt e Roneide V. Majer. São Paulo: Paz e Terra, 2007. (A Era da Informação: economia, sociedade e cultura, 3).

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.

D'ANDRADE, Wladimir. Mercadante quer trabalhar com hackers que atacaram sites do governo. **Estadão.com.br**, São Paulo, 27 jun. 2011. Política. Disponível em: <http://www.estadao.com.br/noticias/nacional,mercadante-quer-trabalhar-com-hackers-que-atacaram-sites-do-governo,737600,0.htm>. Acesso em: 17 ago. 2011.

DEIBERT, Ron. **Distributed security as cyber strategy: outlining a comprehensive approach for Canada in cyberspace**. Calgary: Canadian Defence & Foreign Affairs Institute (CDFAI), 2012. Disponível em: <http://www.cdfai.org/PDF/Distributed%20Security%20as%20Cyber%20Strategy.pdf>. Acesso em: 12 jan. 2013.

DEMETERCO, Fernando A. Segurança das infraestruturas críticas. In: CICLO DE ESTUDOS ESTRATÉGICOS, 10., 2011, Rio de Janeiro. **Apresentações**. Rio de Janeiro: Escola de Comando e Estado-Maior do Exército, 2011. Disponível em: <http://200.20.16.3/seer_ocs/index.php/CEE/XCEE/paper/viewFile/2/32>. Acesso em: 31 dez. 2012.

DUARTE, Érico. As falácias em torno da proposta de guerra de quarta geração. In: ENCONTRO NACIONAL DA ABED, 4., 2010, Brasília. **Anais...** Disponível em: <http://abedef.org/encontrosnacionais2/2010-brasilia>. Acesso em: 27 nov. 2012.

_____. Conduta da guerra na era digital e suas implicações para o Brasil: uma análise de conceitos, políticas e práticas de defesa. **Texto para discussão**, Rio de Janeiro, n. 1760, IPEA, ago. 2012a.

_____. **[DISSERTAÇÃO] Perguntas** [mensagem pessoal]. Mensagem recebida por <gills@gills.com.br> em 7 jan. 2013. O entrevistado é professor de Estudos Estratégicos Internacionais da Universidade Federal do Rio Grande do Sul (UFRGS).

_____. Tecnologia militar e desenvolvimento econômico: uma análise histórica. **Texto para discussão**, Rio de Janeiro, n. 1748, IPEA, jun. 2012b.

ECO, Umberto. **Como se faz uma tese**. 14. ed. Tradução: Gilson Cesar C. de Souza. São Paulo: Perspectiva, 1996. (Coleção Estudos).

ESTADOS UNIDOS. Central Intelligence Agency – CIA. The world factbook. Última atualização: 14 Jan. 2013. Disponível em: <https://www.cia.gov/library/publications/the-world-factbook/geos/xx.html>. Acesso em: 20 jan. 2013.

_____. Department of Defense. **Strategy for Operating in Cyberspace**, Washington, DC, July 2011a. Disponível em: <http://defense.gov/news/d20110714cyber.pdf>. Acesso em: 14 dez. 2012.

_____. Department of Defense. **U.S. Cyber Command Fact Sheet**, Washington, DC, 25 May 2010a. Disponível em: <http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf>. Acesso em: 17 ago. 2012.

_____. The White House. **International Strategy for Cyberspace**: prosperity, security, and opennessin a networked world, Washington, DC, May 2011b. Disponível em: <http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>. Acesso em: 5 dez. 2012.

_____. The White House. **National Security Strategy**, Washington DC, May 2010b. Disponível em: <http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf>. Acesso em: 13 out. 2012.

_____. The White House. **National Strategy to Secure Cyberspace**, Washington, DC, 14 Feb. 2003. Disponível em: <http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf>. Acesso em: 15 dez. 2012.

_____. United States Coast Guard. About us. [20--]. Disponível em: <http://www.uscg.mil/top/about/>. Acesso em: 15 jan. 2013.

FALLIERE, Nicolas *et al.* **W32.Stuxnet Dossier**. Cupertino, CA: Symantec Corporation, 2011.

FERREIRA NETO, Walfredo Bento. **Entrevista para artigo LBDN** [mensagem pessoal]. Mensagem recebida por <gills@gills.com.br> em 14 ago. 2011. O entrevistado é professor de Geografia e Relações Internacionais na Academia Militar das Agulhas Negras (AMAN).

FLICK, Uwe. **Introdução à pesquisa qualitativa**. 3. ed. Porto Alegre: Artmed, 2009.

FUCCILLE, Luís Alexandre. Do desafio à acomodação: descaso e tibieza na construção da direção política sobre a Defesa Nacional. **E-Premissas**, n. 2, jan.-jun. 2007, p. 104-130.

GAGNON, Benoît. Cyberwars and cybercrimes. In: LEMAN-LANGLOIS, Stéphane (Ed.). **Technocrime**: technology, crime and social control. London, UK: Willan Publishing, 2008. cap. 4, p. 46-65.

GAIO, André M. Reações das instituições militares ao processo de globalização. In: DOUBOR, Ladislau; IANNI, Octavio; RESENDE, Paulo-Edgar A. (Org.). **Desafios da globalização**. Petrópolis: Vozes, 1998. p. 50-59.

GEÓRGIA. **Russian invasion of Georgia: Russian cyberwar on Georgia**. [S.l.]: Government of Georgia, 2008. Disponível em: <http://georgiaupdate.gov.ge/en/doc/10006881/Microsoft%20Word%20-%20CYBERWAR%20short%20version_111008.pdf>. Acesso em: 2 abr. 2012.

GORMAN, Siobhan; BARNES, Julian E. Cyber combat: act of war – Pentagon sets stage for U.S. to respond to computer sabotage with military force. **The Wall Street Journal**, New York, 30 May 2011. Disponível em: <http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html>. Acesso em: 20 dez. 2012.

GUERRA, Eduardo M. **Entrevista para Dissertação de Mestrado (UFPE)** [mensagem pessoal]. Mensagem recebida por <gills@gills.com.br> em 31 maio 2012. O entrevistado é professor de Engenharia da Computação no ITA.

GÜNTHER, Hartmut. Pesquisa qualitativa versus pesquisa quantitativa: esta é a questão? **Psicologia: Teoria e Pesquisa**, maio-ago. 2006, v. 22, n. 2, p. 201-210. Disponível em: <http://www.scielo.br/pdf/ptp/v22n2/a10v22n2.pdf>. Acesso em: 17 nov. 2012.

HAMMES, T. X. Fourth generation warfare evolves, fifth emerges. **Military Review: the professional journal of US Army**, v. 91, n. 3, May-June 2007, p. 14-23. Disponível em: <http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20070630_art006.pdf>. Acesso em: 12 dez. 2012.

HAYDEN, Matt. **Aprenda em 24 horas Redes**. Tradução: Marcos Pinto. Rio de Janeiro: Campus, 1999.

HELD, David; McGREW, Anthony. **Prós e contras da globalização**. Tradução: Vera Ribeiro. Rio de Janeiro: Jorge Zahar Editor, 2001.

HOPKINS, Nick. Stuxnet attack forced Britain to rethink the cyber war. **The Guardian**, Londres, 30 May 2011a, Politics. Disponível em: <http://www.guardian.co.uk/politics/2011/may/ 30/stuxnet-attack-cyber-war-iran>. Acesso em: 28 dez. 2012.

_____. UK developing cyber-weapons programme to counter cyber war threat. **The Guardian**, Londres, 30 May 2011b, Military. Disponível em: <http://www.guardian.co.uk/uk/ 2011/may/30/military-cyberwar-offensive?intcmp=239>. Acesso em: 28 dez. 2012.

IBM SPSS Statistics. Programa de análise quantitativa de dados. Version 21.0.0 for Linux. [S.l]: IBM, 2012. Disponível em: <http://www-01.ibm.com/software/analytics/spss/>. Acesso em: 20 nov. 2012.

INTERNET WORLD STATS. Top 20 countries with highest number of Internet users. Última atualização em: 30 jun. 2012a. Disponível em: <http://www.internetworldstats.com/stats.htm>. Acesso em: 19 jan. 2013.

_____. Top 20 countries with highest number of Internet users. Última atualização em: 30 jun. 2012b. Disponível em: <http://www.internetworldstats.com/top20.htm>. Acesso em: 19 jan. 2013.

IRÃ. Identification of a new targeted cyber-attack. **Iranian Computer Security Incident Response Teams – CSIRT**, 28 May 2012. Disponível em: <http://www.certcc.ir/ index.php?name=news&file=article&sid=1894>. Acesso em: 17 set. 2012.

_____. Iran calls for IAEA to detect Stuxnet agents. **Iranian Student's News Agency**, Tehran, 13 Jun. 2011. Disponível em: <http://old.isna.ir/ISNA/NewsView.aspx?ID=News-1786952&Lang=E>. Acesso em: 23 nov. 2012.

ISO/IEC. **ISO/IEC 27002**: Information technology - Security techniques - Code of practice for information security management. Suíça: International Organization for Standardization / International Electrotechnical Commission, 2005.

KEEGAN, John. **Uma história da guerra**. Tradução: Pedro Soares. São Paulo: Cia das Letras, 2006.

KILIAN JUNIOR, Rudibert. **[GUERRA CIBERNÉTICA] Entrevista** [mensagem pessoal]. Mensagem recebida por <gills@gills.com.br> em 21 maio 2012. O entrevistado é professor de Planejamento Estratégico da Escola de Guerra Naval (EGN).

KING, Gary; KEOHANE, Robert O.; VERBA, Sidney. **Designing social inquiry**: scientific inference in qualitative research. Princeton: Princeton University Press, 1994.

KLEINROCK, Leonard. History of the Internet and its flexible future. **IEEE Wireless Communications**, Feb. 2008, p. 8-18.

_____. **Testimony** [mensagem pessoal]. Mensagem recebida por <gills@gills.com.br> em 20 ago. 2011. O entrevistado é um dos "Pais Fundadores da Internet" e professor do *Computer Science Department* NA *University of California, Los Angeles* – UCLA (EUA).

LANDMAN, Todd. **Issues and methods in Comparative Politics**: an introduction. 3. ed. New York: Routledge, 2005.

LEMAN-LANGLOIS, Stéphane. Afterword: technopolice. In: _____ (Ed.). **Technocrime**: technology, crime and social control. London: Willan Publishing, 2008a. cap. 12, p. 243-246.

_____. Introduction. In: _____ (Ed.). Technocrime, policing and surveillance. Londres: Routledge, 2012. (Routledge Frontiers of Criminal Justice, v. 3).

_____. Introduction: technocrime. In: _____ (Ed.). **Technocrime**: technology, crime and social control. London: Willan Publishing, 2008b. cap. 1, p. 1-13.

LEWIS UNIVERSITY. The History of cyber warfare. 2010. Disponível em: <http://online.lewisu.edu/images/the-history-of-cyber-warfare-infographic.jpg>. Acesso em: 22 dez. 2012.

LOPES, Gills. **A cibersociedade anárquica**: análise do uso das Tecnologias de Informação e Comunicação nos conflitos internacionais do século XXI à luz da Escola Inglesa de Relações Internacionais. 2010. 61 f. Trabalho de Conclusão de Curso (Monografia) – Curso de Relações Internacionais, UEPB, João Pessoa, 2010.

_____. A emergência do tema ciberguerra: contextualizando a criação do Centro de Defesa Cibernética à luz da Estratégia Nacional de Defesa. In: SEMINÁRIO DO LIVRO BRANCO DE DEFESA NACIONAL, 6., 2011, São Paulo. **Concurso de Artigos sobre o Livro Branco de Defesa Nacional**. Brasília: Ministério da Defesa, 2011a. Disponível em: <http://defesa.gov.br/projetosweb/livrobranco/arquivos/apresentacao-trabalhos/artigo-gills-lopes.pdf>. Acesso em: 12 fev. 2012.

_____. Análise sobre o impacto das novas TIC nas estratégias nacionais de defesa e segurança cibernéticas do século XXI. In: Simpósio de Pós-Graduação em RI do Programa "San Tiago Dantas", 3., 2011, São Paulo. **Anais**, 2011b. Disponível em: <http://santiagodantassp.locaweb.com.br/br/simp/ artigos2011/gills_souza.pdf>. Acesso em: 6 out. 2012.

_____. Anonymous, #AntiSec e a questão da liberdade no ciberespaço. **Mundialistas**: opiniões inteligentes em relações internacionais, 22 ago. 2011c. Disponível em: <http://www.mundialistas.com.br/blog/index.php/anonymous-antisec-e-a-luta-pela-liberdade-no-ciberespaco-por-gills-lopes/>. Acesso em: 14 dez. 2012.

_____. Da ciberguerra: idiossincrasias do século XXI e as instituições militares de defesa cibernética de Brasil, Estados Unidos, OTAN e União Europeia. In: ENCONTRO NACIONAL DA ASSOCIAÇÃO BRASILEIRA DE ESTUDOS DE DEFESA, 5., 2011, Fortaleza. **Anais do V ENABED**, 2011d, Fortaleza. Disponível em: <http://abedef.org/encontrosnacionais2/2011-fortaleza>. Acesso em: 17 out. 2012.

_____. Uma Convenção sobre Cyberwars para as Américas? In: Conferencia Sub-Regional del Centro de Estudios Hemisféricos de Defensa (CHDS), 7., 2011e, Santiago do Chile. Disponível em: <http://www.ndu.edu/chds/src_chile/Documents/Posters/PAGE_12_Gills_Lopes_Mac%C3%AAdo_Souza.pdf>. Acesso em: 14 dez. 2012.

_____; AZEVEDO NETO, Francisco A. The anarchical cyber society and freedom 2.0: new challenges to Political Science and International Relations. In: WORLD CONGRESS OF POLITICAL SCIENCE (IPSA), 22., 2012, Madrid. **Panel: Perspectives on International Relations**, 2012. p. 1-23. Disponível em: <http://www.ipsa.org/sites/default/files/ipsa-events/madrid2012/papers/paper-14265-2012-06-15-1514.pdf>. Acesso em: 12 jan. 2013.

LOPES, Gills; MACIEL, João Wandemberg G. A importância das *web-standards* e da *web semântica* para o letramento digital. **Revista Temática**, João Pessoa, ano 6, n. 3, mar. 2010. Não paginado. Disponível em: <http://www.insite.pro.br/2010/Mar%C3%A7o/web-standards_we-sem%C3%A2ntica_wanemberg.pdf>. Acesso em: 20 nov. 2012.

LOPES, Gills; MEDEIROS, Marcelo de Almeida. Da cibersegurança à ciberdefesa Americana: a diplomacia da internet como instrumento de proteção e de integração dos estados da OEA. In: 3° ENCONTRO NACIONAL ABRI 2011, 3., 2011, São Paulo. **Proceedings online...** Associação Brasileira de Relações Internacionais, Instituto de Relações Internacionais - USP, Disponível em: <http://www.proceedings.scielo.br/scielo.php?script=sci_arttext&pid=MSC0000000122011000200017>. Acesso em: 07 jan. 2013.

LOPES, Gills; PEREIRA, Dalliana Vilar. A Convenção de Budapeste e as leis brasileiras. In: SEMINÁRIO CIBERCRIME E COOPERAÇÃO PENAL INTERNACIONAL, 1., 2009, João Pessoa. Disponível em: <http://www.mp.am.gov.br/images/stories/A_convencao_de_Budapeste_e_as_leis_brasileiras.pdf>. Acesso em: 23 dez. 2012.

LOPES, Gills; TEIXEIRA JR, Augusto W. M. O ciberespaço é o novo front: implicações para o pensamento estratégico. **Mundialistas**: opiniões inteligentes em relações internacionais, 26 ago. 2011. Disponível em: <http://www.mundialistas.com.br/blog/index.php/o-ciberespaco-e-o-novo-front-implicacoes-para-o-pensamento-estrategico-por-gills-lopes-e-augusto-teixeira-jr/>. Acesso em: 23 nov. 2012.

LOYOLA, Leandro. General José Carlos dos Santos: "Podemos recrutar hackers". **Revista Época**, São Paulo, n. 687, p. 56-58, 18 jul. 2011.

LUPI, André Lipp P. B. **Soberania, OMC e Mercosul**. São Paulo: Aduaneiras, 2001.

LUPION, Bruno. Exército se arma para defender o espaço cibernético brasileiro. **Estadão.com.br**, São Paulo, 8 jun. 2011. Disponível em: <http://www.estadao.com.br/noticias/nacional,exercito-se-arma-para-defender-o-espaco-cibernetico-brasileiro,729291,0.htm>. Acesso em: 4 ago. 2012.

LYNN III, William J. The Pentagon's Cyberstrategy, one year later: defending against the next cyberattack. **Foreign Affairs**, 28 Sep. 2011. Disponível em:

<http://www.foreignaffairs.com/articles/68305/william-j-lynn-iii/the-pentagons-cyberstrategy-one-year-later>. Acesso em: 4 jan. 2013.

MAHNKEN, Thomas G.; MAIOLO, Joseph A. (Ed.). **Strategic studies**: a reader. London: Routledge, 2008.

MANDARINO JR, Raphael. **Um estudo sobre a segurança e a defesa do espaço cibernético**. Brasília: UnB, 2009. Monografia de Especialização em Ciência da Computação. Disponível em: <http://dsic.planalto.gov.br/documentos/cegsic/monografias_1_turma/raphael_mandarino.pdf >. Acesso em: 5 jan. 2013.

MARIANO, Karina P. Globalização, integração e o estado. **Lua Nova**, n. 71, p. 123-168, 2007.

MARTIN, André C. R. **Congratulação e perguntas** [mensagem pessoal]. Mensagem recebida por <gills@gills.com.br> em 28 set. 2012. O entrevistado é Coordenador do Programa de Pós-Graduação em Geografia Humana da Universidade de São Paulo (USP).

MARX, Garry T. Foreword: Something's happening here and we are there. In: LEMAN-LANGLOIS, Stéphane (Ed.). **Technocrime**: technology, crime and social control. London: Willan Publishing, 2008. p. vii-xix.

MEDEIROS, Assis. **Hackers**: entre a ética e a criminalização. Florianópolis: Visual Books, 2002.

MERCADANTE, Aloísio. As razões do diálogo com os hackers. **Folha de São Paulo**, São Paulo, 11 ago. 2011, p. 3.

MIYAMOTO, Shiguenoli. A segurança e a ordem internacionais no limiar do novo século. In: OLIVEIRA, Odete M. de; DAL RI JÚNIOR, Arno (Org.). **Relações Internacionais**: interdependência e sociedade global. Ijuí/RS: UNIJUÍ, 2003. p. 681-728. (Coleção Direito, Política e Cidadania, v. 10). Texto também publicado em: _____. A segurança e a ordem internacionais no limiar do novo século. Primeira Versão, Campinas, v. 117, IFCH/UNICAMP, jan. 2003.

_____. A segurança internacional no pós-guerra fria. In: DOUBOR, Ladislau; IANNI, Octavio; RESENDE, Paulo-Edgar A. (Org.). **Desafios da globalização**. Petrópolis: Vozes, 1998. p. 276-284.

_____. Os Estudos Estratégicos e a academia brasileira: uma avaliação. Center for Hemispheric Defense Studies – CHDS, May 22-25, 2001, Washington DC. Disponível em: <http://www.obed.ufpa.br/pdfs/miyamoto_s_strategic_studies.pdf >. Acesso em: 2 dez. 2012.

_____. Os estudos geopolíticos no Brasil: uma contribuição para sua avaliação. **Perspectivas**, São Paulo, v. 4, p. 75-92, 1981.

NINIO, Marcelo. A internet é um barril de pólvora. Folha de São Paulo, 29 jul. 2012. Ilustríssima. Disponível em: <http://www1.folha.uol.com.br/ilustrissima/1127046-a-internet-e-um-barril-de-polvora.shtml>. Acesso em: 23 dez. 2012.

NYE, Joseph S. Cyber Insecurity. **Daily News Egypt**, Cambridge, 14 Dec. 2008. Disponível em: <http://belfercenter.ksg.harvard.edu/publication/18727/cyber_insecurity.html>. Acesso em: 24 jul. 2012.

_____. Nuclear lessons for cyber security? **Strategic Studies Quarterly**, v. 5, n. 4, winter 2011a, p. 18-37.

_____. **The future of power**. New York: Public Affairs, 2011b.

OLIVEIRA, Eliézer Rizzo de. O Brasil diante dos desafios internacionais em matéria de segurança e defesa: um enfoque hemisférico. In: ALMEIDA PINTO, J. R. de; ROCHA, A. J. Ramalho da; SILVA, R. Doring Pinho da (Coord.). **O Brasil no cenário internacional de defesa e segurança**. Brasília: Ministério da Defesa, 2004. p. 89-101. (Pensamento brasileiro sobre defesa e segurança, v. 2).

OPPERMANN, Daniel. Virtual attacks and the problem of responsibility: the cases of China and Russia. **Academia**, set. 2009. Disponível em: <http://brasilia.academia.edu/DanielOppermann>. Acesso em: 30 set. 2012.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Instrument for standardized reporting of military expenditures (MILEX). Disponível em: <https://milex.un.org/>. Acesso em: 15 jan. 2013.

PAQUIN, Jonathan. Canadian foreign and security policy: reaching a balance between autonomy and North American harmony in the twenty-first century. *La politique étrangère du Canada*, 15(2), 2009, p. 99-108.

PINHEIRO, Alvaro de S ouza. O conflito de 4ª geração e a evolução da guerra irregular. **PEDECEME On-Line**, n. 16, 3º Quadrim. 2007, p. 16-33. (Coleção Meira Mattos: Revista das Ciências Militares).

PROENÇA JR, Domício. Condicionantes e requisitos para um sistema de inteligência vantajoso para o Brasil. 2009. Disponível em: <https://www.planalto.gov.br/gsi/saei/publicacoes/NTSisInteligenciaFinalPB.pdf>. Acesso em: 2 nov. 2012.

_____; DINIZ, Eugenio. **Política de defesa no Brasil**: uma análise crítica. 1998. Disponível em: <http://www.de9.ime.eb.br/~intec/Domicio/Dia20out2005/Proen%E7a%20Jr%20&%20Diniz%201998%20-%20Pol%EDtica%20de%20Defesa%20no%20Brasil.pdf>. Acesso em: 30 ago. 2012.

POPPER, Karl. **A lógica da pesquisa científica**. Tradução: Leonidas Hegenberg e Octanny S. da Mota. 16. ed. São Paulo: Cutrix, 2008.

RAMIREZ, Jessica. All is not quiet on the digital front. **Newsweek**, 20 Apr. 2010. Technology. Disponível em: <http://www.newsweek.com/2010/04/20/all-is-not-quiet-on-the-digital-dront.html>. Acesso em: 21 dez 2012.

R Core Team. R: A language and environment for statistical computing. Version 2.15.2. Vienna: R Foundation for Statistical Computing, 2012. Disponível em: <http://www.R-project.org/>. Acesso em: 14 dez. 2012.

RODRIGUES, Emanuel dos Reis. **Entrevista** [mensagem pessoal]. Mensagem recebida por <gills@gills.com.br> em 10 jun. 2012. O entrevistado é especialista em segurança da informação, com atuação no Brasil e nos EUA.

RUDZIT, Gunther. O debate teórico em segurança internacional: mudanças frente ao terrorismo? **Civitas**: Revista de Ciências Sociais, Porto Alegre, v. 5, n. 2, jul.-dez. 2005, p. 297-323.

_____. Re: **Perguntas para DIssertação** [mensagem eletrônica]. Mensagem recebida por <gills.lopes@ufpe.br> em 13 set. 2012. O entrevistado é professor das Faculdades Integradas Rio Branco (FIRB).

RUMER, Eugene B. Introduction: a cool breezer. **The Adelphi Papers**, v. 47, issue 390, p. 7-11, Routledge, London, 30 Oct. 2007. Disponível em: <http://www.tandfonline.com/doi/full/10.1080/05679320701706880>. Acesso em: 3 fev. 2013. Documento eletrônico acessado por meio da rede corporativa da *Université Laval*.

SAALBACH, K. **Cyber war: methods and practice**. Osnabrück: Universität Osnabrück, 2012. 39 p. Version 4.0 – 25 Mar 2012. Disponível em: <http://www.dirk-koentopp.com/downloads/saalbach-cyberwar-methods-and-practice.pdf>. Acesso em 30 mar. 2012.

SÁ, Nelson de. General detalha implantação do Centro de Defesa Cibernética, novo órgão brasileiro. **Folha de São Paulo**, Brasília, 7 maio 2012, Tec. Disponível em: <http://www1.folha.uol.com.br/tec/1085498-general-detalha-implantacao-do-centro-de-defesa-cibernetica-novo-orgao-brasileiro.shtml>. Acesso em: 4 out. 2012.

SAINT-PIERRE, Héctor L. La Defensa en la Política Exterior del Brasil: el Consejo Suramericano y la Estrategia Nacional de Defensa. Madrid: **Real Instituto Elcano**, 2009. Disponível em: <http://www.realinstitutoelcano.org/wps/wcm/connect/1b12ab804fda364bb164ff8bf7fc5c91/DT50-2009_Saint-Pierre_Defensa_Politica_exterior_Brasil.pdf?MOD=AJPERES&CACHEID=1b12ab804fda364bb164ff8bf7fc5c91>. Acesso em: 16 ago. 2012.

SANGER, David E. **Confront and conceal**: Obama's secret wars and surprising use of American power. New York: Crown: 2012a.

_____. Obama order sped up wave of cyberattacks against Iran. **The New York Times**, New York, 1 Jun. 2012b. World. Disponível em: <http://nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html>. Acesso em: 5 Jun. 2012.

SANTOS, Murilo. Prefácio. In: PROENÇA JR, Domício; DINIZ, Eugenio. **Política de defesa no Brasil**: uma análise crítica. 1998. p. 3-4. Disponível em: <http://www.de9.ime.eb.br/~intec/Domicio/Dia20out2005/Proen%E7a%20Jr%20&%20Diniz

%201998%20-%20Pol%EDtica%20de%20Defesa%20no%20Brasil.pdf>. Acesso em: 30 jul. 2012.

SARAIVA, José Flávio Sombra. Relações Internacionais em tempos de crise: ordem sincrética e novos paradigmas. In: CONFERÊNCIA NACIONAL DE POLÍTICA EXTERNA E POLÍTICA INTERNACIONAL, 6. **Relações internacionais em tempos de crise econômica e Política**. Brasília: Fundação Alexandre Gusmão, 2012. p. 75-91.

SUTHERLAND, Benjamin (Ed.). **Modern warfare, intelligence and deterrence**: the technologies that are transforming them. New Jersey: Wiley, 2012. (The Economist, 104).

TEIXEIRA JR, Augusto W. M. O Conselho de Defesa Sul-americano da UNASUL: criação institucional e cultura estratégica. In: OLIVEIRA, Marcos A. Guedes de (Org.). **Comparando a Defesa Sul-Americana**. Recife: Ed. Universitária da UFPE, 2011. p. 127-147.

THING, Lowell (Ed.). **Dicionário de tecnologia Whatis.com**. Tradução: Bazán Tecnologia e Texto Digital. São Paulo: Futura, 2003.

UNIÃO EUROPEIA. **National cyber security strategies**: setting the course for national efforts to strengthen security in cyberspace. Heraklion: European Network and Information Security Agency (ENISA), 2012.

_____. Parlamento Europeu / Deputados. [201-]. Disponível em: <http://www.europarl.europa.eu/meps/pt/gsasearch.html?query=Piratpartiet>. Acesso em: 12 dez. 2012.

UNIVERSIDADE FEDERAL DE SANTA CATARINA. Tabela 5 Distribuição *t* de *Student*. Última modificação: 9 maio 2011. Disponível em: <http://www.inf.ufsc.br/~verav/TABELAS%20DE%20PROBABILIDADE/Tabela_Dist_t.pdf>. Acesso em: 28 dez. 2011.

UNIVERSITY OF WASHINGTON. Cyberwarfare. 10 Dec. 2010. Disponível em: <http://staff.washington.edu/dittrich/cyberwarfare.html>. Acesso em: 24 out. 2012.

VAZ, Alcides Costa. Relações internacionais em tempos de crise política. In: CONFERÊNCIA NACIONAL DE POLÍTICA EXTERNA E POLÍTICA INTERNACIONAL, 6. **Relações internacionais em tempos de crise econômica e Política**. Brasília: Fundação Alexandre Gusmão, 2012. p. 13-26.

VIOLA, Eduardo Jose. **Globo Universidade**: Relações Internacionais [28 ago. 2010] (26 min). [S.l.]: Rede Globo de Televisão, 2010. Disponível em: <http://globotv.globo.com/rede-globo/globo-universidade/v/relacoes-internacionais/1519643/>. Acesso em: 22 ago. 2012.

VILLA, Rafael D.; REIS, Rossana R. A segurança internacional no pós-Guerra Fria: um balanço da teoria tradicional e das novas agendas de pesquisa. **R. bras. de Informação Bibliográfica em Ciências Sociais (BIB),** São Paulo, n. 62, 2º semest., 2006, p. 19-51.

VILLA, Rafael D.; SANTOS, Norma Breda dos. Buzan, Wæver e a Escola de Copenhague: tensões entre o realismo e a abordagem sociológica nos estudos de segurança internacional.

In: MEDEIROS, Marcelo de A.; COSTA LIMA, Marcos; VILLA, Rafael D.; REIS, Rossana R. (Org.). **Clássicos das relações internacionais**. São Paulo: Hucitec, 2010. cap. 6, p. 117-151.

VIZENTINI, Paulo F. **Manual do candidato**: história mundial contemporânea. Brasília: FUNAG, 2006.

VON CLAUSEWITZ, Carl. **On war**. Tradução: Michael Howard e Peter Paret. Oxford: Oxford University Press, 2007. (Oxford World's Classics). Disponível em: <http://lib.myilibrary.com?ID=114695>. Acesso em: 15 dez. 2012. Documento eletrônico acessado por intermédio da rede corporativa da *Université Laval*.

WALLER, Michael. China revisa a Arte da Guerra. DefesaNet, 1 set. 2000. Geopolítica. Disponível em: <http://www.defesanet.com.br/geopolitica/noticia/1166/China-Revisa-a-Arte-da-Guerra>. Acesso em: 3 jan. 2013.

WIGHT, Martin. **A política do poder**. 2. ed. Tradução: Carlos S. Duarte. Brasília: Editora UnB, 2002. (Clássicos IPRI, 7).

WINAND, Érica; SAINT-PIERRE, Héctor Luis. A fragilidade da condução política da defesa no Brasil. **História**, Franca, v. 29, n. 2, dez. 2010. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0101-90742010000200002>. Acesso em: 6 ago. 2012.

WOODWARD, Alan. **RE: Interview by email for MA's Thesis** [mensagem pessoal]. Mensagem recebida por <gills@gills.com.br> em 8 jun. 2011. O entrevistado é professor do *Department of Computing* na *University of Surrey* (Inglaterra).

GLOSSÁRIO[145]

Ataque de negação de serviço (DoS): Inúmeras tentativas sucessivas para forçar a sobrecarga de um computador – geralmente, um servidor *web* –, fazendo com que seus serviços fiquem inutilizados para usuários e/ou mantenedores.

Ataque distribuído de negação de serviço (DDoS): Tem o mesmo objetivo do ataque DoS, porém um único computador-mestre "escraviza" outros – "zumbis" –, os quais direcionam os ataques. No DDoS, uma única pessoa pode ser responsável por vários ataques.

Bit: é a menor unidade de informação a ser armazenada ou transmitida em meios computacionais, sendo valorada em 0 ou 1 de acordo com a variação da carga elétrica, abaixo ou acima de um nível padrão, respectivamente, em cada um dos capacitores dentro de um dispositivo de armazenamento/transmissão.

Bot: diminutivo de *robot*, é um software implementado para simular ações humanas em outro *software*, repetidas vezes e de maneira padronizada, de maneira similar a como faria um robô físico em relação às ações mecânicas do ser humano.

Botnet: conjunto de *bots* conectados em rede com o propósito de trabalharem de maneira conjunta e distribuída, amplificando o alcance de suas ações.

CERT: sigla para Centro de Estudos para Resposta e Tratamento de Incidentes em Computadores; existem por todo o mundo para tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet.

Código-fonte: é o conjunto de símbolos e instruções inteligíveis por um ser humano, escritos na sintaxe de uma linguagem de programação existente, com o objetivo de resolver, de maneira lógica e ordenada, um determinado problema computacional, sendo a forma original de um programa de computador antes de ser traduzido em linguagem de máquina.

[145] Este elemento pós-textual conta com a colaboração imprescindível de Tiago Freire (SERPRO-PB).

Cracker: geralmente confundido com *hacker*, é o indivíduo que "quebra" códigos-fonte e sistema informáticos de detecção de intrusos, a fim de obter vantagens.

Endereço IP: identificação numérica exclusiva de um equipamento conectado a uma rede de computadores.

Hacker: diz-se de alguém que, geralmente, é autodidata em assuntos ligados à computação e que compartilha seus feitos na própria Internet, a fim de obter satisfação própria.

Hacktivismo: prática de hackear ou invadir sistemas informáticos, alegando motivos políticos e/ou sociais.

Linguagem de alto nível: é como são chamadas as linguagens de programação que possuem um elevado nível de abstração, mais próximo à linguagem humana e mais distante da linguagem de máquina, fazendo com que o programador não precise conhecer características detalhadas de gerenciamento de memória, processadores, registradores etc.

Malware: *software* malicioso projetado para se infiltrar em um sistema de computador alheio de forma ilícita com o intuito de causar danos e/ou roubo de informações.

NTIC: as novas tecnologias de informação e comunicação são TIC ditas "novas", pois baseiam-se nas principais descobertas da revolução dos *microchips*, como possibilidade de acesso e comunicação instantânea de dados.

SCADA: sistema computacional (*software*) que gerencia a infraestrutura física (*hardwares*), em escala industrial.

SQL: acrônimo de *Structured Query Language*, é a linguagem padrão para realizar operações de consulta e escrita em bancos de dados relacionais.

Telemática: mescla das ferramentas de *tele*comunicações com as de infor*mática* para a transmissão de dados a distância.

Worm: *malware* independente e autorreplicante que não necessita de um hospedeiro para executar suas ações.

Vírus: *malware* que possui a característica infectar um programa hospedeiro, de quem necessita para se replicar e se espalhar para outros computadores utilizando-se de diversos meios.

WWW: acrônimo de *World Wide Web*, é um sistema de arquivos de hipermídia (áudio, vídeo, imagem, hipertexto) interligados, executados na Internet e consumidos pelos usuários finais por intermédio de um *software* chamado *browser*.

APÊNDICE A – Esboço do Índice de Politização Orçamentária da Defesa Cibernética (IPoDC)[146]

De forma objetiva, este índice busca falsear a tese de que investimentos das Forças Armadas em áreas relacionadas à defesa cibernética tendem a acompanhar o mesmo ritmo dos outros índices. Ou seja, neste caso, quanto mais um Estado investe em "eletrônicos e comunicações" e, ao mesmo tempo, quanto mais os outros quatro índices se aproximam de seus valores máximos, mais próximos também está o setor militar de politizar o ciberespaço.

A escolha de "eletrônicos e comunicações", aqui, reflete a área correlata mais próxima do tema defesa cibernética, que pode ser encontrada nos relatórios-padrão sobre investimentos militares encaminhados à Organização das Nações Unidas (ONU)[147] (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 2013).

Esses relatórios estão divididos em quatro partes: (i) custos operacionais (*operating costs*); (ii) aquisição e construção (*procurement and construction*); (iii) P&D (*research and development*); e (iv) total. É justamente na terceira parte que figura a variável a ser operacionalizada aqui: eletrônicos e comunicações (*electronics and communications*).

Assim, é possível auferir quanto os três países aqui selecionados investem, por ano, em aquisição e construção de equipamentos e serviços eletrônicos/comunicacionais voltados às suas Forças Armadas.

Tabela 30 – Investimentos militares em eletrônicos e comunicações nos EUA, Brasil e Canadá (2000-2011)

ANO FISCAL [a)]	EUA (em U$ milhões)	BRASIL (R$ milhares)	CANADÁ (C$ milhões)
2000	--	-- [d)]	409,5
2001	--	-- [e)]	475,7
2002	-- [b)]	-- [d)]	-- [e)]
2003	-- [b)]	-- [d)]	954,2
2004	-- [b)]	0,00	883,9
2005	-- [b)]	0,00	1.044,5
2006	-- [b)]	0,00	629,6
2007	-- [b)]	8.197,00	529,3
2008	-- [b)]	13.629,26	-- [e)]
2009	-- [b)]	23.911,71	579,6
2010	-- [b)]	73.064,72	715,4
2011	-- [c)]	--	661,7
TOTAL	--	**118.802,69**	**6.883,4**

Fonte: Elaboração própria, a partir de Organização das Nações Unidas (2013).
Legenda:
-- Nulo (não informado).

[146] Como já mencionado na Subseção 3.2, o presente Apêndice é uma forma de demonstrar como os dados orçamentários sobre defesa cibernética ainda são deveras escassos.
[147] São os mesmos encaminhados à OEA, diga-se de passagem.

a) O ano fiscal no Canadá começa e termina no meio de cada ano.
b) Valores de *electronics and communications* foram alocados na categoria *other*, juntamente com uma série de outras variáveis, impossibilitando, assim, mensurar quanto é, *de facto*, o investimento em eletrônicos e comunicações deste país.
c) Por reformulação do formulário-padrão, no referido ano, a categoria *electronics and communications* desaparece.
d) Investimentos em *procurement and construction* não são detalhados. Logo, não se sabe quanto em *electronics and communications* é investido.
e) País não disponibiliza formulário no referido ano

Nota: Como o IPoDC é descartado neste trabalho, não se realiza a conversão dos valores para uma única moeda de referência que levasse em conta os índices inflacionários dos períodos analisados.

APÊNDICE B – Comandos para as buscas no Google

Sabe-se que o buscador do Google:

i. limita o número de termos numa mesma pesquisa;
ii. dependendo do grande número de termos numa só pesquisa, ele começa a abranger palavras derivadas dos termos pesquisados; e
iii. não diferencia espaço (“ ”) de hífen (“-”);[148]

Somando-se isso ao fato de que uma quantidade significativa de termos é selecionada (67), divide-se a busca completa em quatro minibuscas, conforme os quatro blocos de código abaixo:

```
site:URL "arma cibernética" OR "armas cibernéticas" OR "arme cybernétique" OR "armes cybernétiques" OR "arsenal cybernétique" OR "ataque cibernético" OR "ataques cibernéticos" OR "attaque cibernétique" OR "attaques cibernétiques" OR "ciber arsenal" OR "ciber defesa" OR "ciberataque" OR "ciberataques"

site:URL "ciberdefesa" OR "ciberespaço" OR "ciberguerra" OR "ciberguerras" OR "cyber arme" OR "cyber armes" OR "cyber arsenal" OR "cyber arsenal" OR "cyber attack" OR "cyber attacks" OR "cyber attaque" OR "cyber attaques" OR "cyber defence" OR "cyber defense" OR "cyber défense" OR "cyber guerre" OR "cyber guerres" OR "cyber war" OR "cyber warfare" OR "cyber wars" OR "cyber weapon" OR "cyber weapons" OR "cyberarme" OR "cyberarmes"

site:URL "cyberarsenal" OR "cyberataque" OR "cyberataques" OR "cyberattack" OR "cyberattacks" OR "cyberdefence" OR "cyberdefense" OR "cyberdéfense" OR "cyberespaço" OR "cyberguerra" OR "cyberguerras" OR "cyberguerre" OR "cyberguerres" OR "cybernetic war" OR "cybernetic warfare" OR "cybernetic wars" OR "cyberspace"

site:URL "cyberwar" OR "cyberwarfare" OR "cyberwars" OR "cyberweapon" OR "cyberweapons" OR "defence cybernetic" OR "défense cybernétique" OR "defesa cibernética" OR "espaço cibernético" OR "guerra cibernética" OR "guerras cibernéticas" OR "guerre cybernétique" OR "guerres cybernétiques" OR "stuxnet"
```

Onde **URL** é:

1. .mil.br, caso variável é *BRA_.mil.br*;
2. .exercito.gov.br, caso *BRA_.exercito.gov.br*;
3. .defesa.gov.br, caso *BRA_.defesa.gov.br*;
4. .forces.ca, caso *CAN_.forces.ca*;
5. .forces.gc.ca, caso *CAN_.forces.gc.ca*;
6. .defense.gov, caso *EUA_.defense.gov*; e
7. .mil, caso *EUA_.mil*.

[148] Assim, os resultados de “*cyber-security*” ou “*cyber security*” são os mesmos. Como se trata de uma busca com termos exatos, o plural das palavras são levados em conta. Embora “ciberataque” esteja contido em “ciberataques”, o resultado da busca por cada um dos termos é diferente.

Observações:

- como o campo “última atualização”, da Busca Avançada do Google traz apenas cinco opções-padrão – em qualquer data, nas últimas 24 horas, na última semana, no último mês e no último ano –, para escolher os anos específicos, tem-se que fazê-lo manualmente, por meio da página de resultados da busca do Google: Ferramentas de pesquisa → Em qualquer data → Intervalo personalizado.
- Outra alternativa para filtrar os resultados das buscas por região é utilizar os parâmetros “site:.br” e “site:.ca” para os casos brasileiro e canadense, respectivamente. Pelo fato de os EUA terem certos privilégios quanto aos nomes de domínios, o uso de “site:.us” não abrange os principais domínios governamentais (.gov) e militares (.mil) daquele Estado/região.

APÊNDICE C – Resultado completo das buscas nos sítios virtuais

Tabela 31 – Resultados das buscas nos sítios virtuais de EUA, Brasil, Canadá e no mundo (2000-2012)

(continua)

ANO	*EUA_.mil*	*EUA_.defense.gov*	*EUA_MIL*	*EUA_NAC*	*BRA_.mil.br*	*BRA_.exercito.gov.br*	*BRA_.defesa.gov.br*	*BRA_MIL*
2000	2.119	3.065	5.184	76.604	0	0	0	0
2001	2.906	3.729	6.635	99.225	2	0	0	2
2002	1.232	1.035	2.267	40.157	0	0	0	0
2003	931	705	1.636	28.193	1	0	0	1
2004	1.079	1.085	2.164	37.870	2	0	0	2
2005	1.604	1.348	2.952	56.154	1	0	1	2
2006	2.292	1.432	3.724	79.287	4	0	1	5
2007	2.468	2.319	4.787	108.186	5	0	1	6
2008	4.310	2.970	7.280	197.970	13	0	3	16
2009	5.267	3.216	8.483	314.220	29	0	6	35
2010	7.754	3.453	11.207	889.590	48	3	2	53
2011	11.225	5.271	16.496	1.448.930	132	53	11	196
2012	12.353	4.876	17.229	2.292.900	210	168	76	454
Σ	**55.540**	**34.504**	**90.044**	**5.669.286**	**447**	**224**	**101**	**772**

(continuação)

ANO	*BRA_NAC*	*CAN_.forces.ca*	*CAN_.forces.gc.ca*	*CAN_MIL*	*CAN_NAC*	*TOTAL_MIL*	*TOTAL_NAC*	*TOTAL_MUNDO*
2000	3.778	0	0	0	5.438	5.184	85.820	121.445
2001	4.159	0	0	3	7.549	6.640	110.933	161.375
2002	1.153	2	6	8	3.601	2.275	44.911	69.920
2003	142	1	2	3	2.293	1.640	30.628	49.999
2004	325	1	1	2	2.848	2.168	41.043	67.407
2005	343	0	4	4	3.777	2.958	60.274	100.313
2006	686	0	3	3	4.844	3.732	84.817	140.950
2007	1.008	1	2	3	6.015	4.796	115.209	205.470
2008	1.677	0	3	3	10.751	7.299	210.398	373.270
2009	3.351	0	2	2	14.742	8.520	332.313	1.063.600
2010	4.878	0	66	66	24.563	11.326	919.031	1.432.300
2011	78.180	4	207	211	55.120	16.903	1.582.230	3.150.900
2012	93.610	0	187	187	84.703	17.870	2.471.213	5.687.000
Σ	**193.290**	**9**	**486**	**495**	**226.244**	**91.311**	**6.088.820**	**12.623.949**

Fonte: Elaboração própria.

APÊNDICE D – Estatísticas referentes ao IPvDC

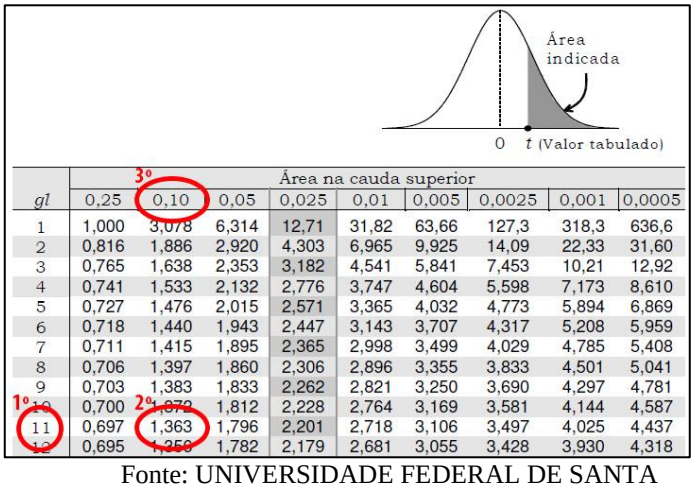
Com a informação dos testes *t* de cada um dos casos, parte-se para o último passo que é realizar a *probabilidade de significância* (P) deles. Como n = 12, o *gl* = 11 graus de liberdade[149].

Utilizando-se a Tabela da Distribuição *t* de *Student* – Tabela 35 –, projeta-se uma coordenada cartesiana, onde X representa o valor do *g1* (11) e Y leva em conta o valor mais próximo do *t* encontrado para o índice auferido em cada um dos casos, que é 1,363 para os casos estadunidense e brasileiro. Portanto, 1,363 está na coluna *0,10* da variável *Área na cauda superior*, que, em outras palavras, corresponde ao P.

Assim, a *probabilidade de significância* (P) para a presente amostra é de aproximadamente 0,10, que é o valor exato do nível de significância assumido, ou seja, tem-se que $\alpha = 0{,}10 = 10\%$.

Portanto, pode-se concluir, com 90% de certeza, que, a partir dos dados analisados, há evidência estatisticamente suficiente de que a hipótese nula (H_0) é *falsa* para os casos estadunidense e brasileiro. Em outras palavras, assume-se a hipótese alternativa (H_1) como verdadeira, *i.e.*, há, *de facto*, um aumento real do interesse militar virtual detectado entre as duas mensurações (D) referentes aos 13 primeiros anos do século XXI, para cada um desses Estados.

Tabela 32 – Distribuição *t* de *Student*



	Área na cauda superior								
gl	0,25	0,10	0,05	0,025	0,01	0,005	0,0025	0,001	0,0005
1	1,000	3,078	6,314	12,71	31,82	63,66	127,3	318,3	636,6
2	0,816	1,886	2,920	4,303	6,965	9,925	14,09	22,33	31,60
3	0,765	1,638	2,353	3,182	4,541	5,841	7,453	10,21	12,92
4	0,741	1,533	2,132	2,776	3,747	4,604	5,598	7,173	8,610
5	0,727	1,476	2,015	2,571	3,365	4,032	4,773	5,894	6,869
6	0,718	1,440	1,943	2,447	3,143	3,707	4,317	5,208	5,959
7	0,711	1,415	1,895	2,365	2,998	3,499	4,029	4,785	5,408
8	0,706	1,397	1,860	2,306	2,896	3,355	3,833	4,501	5,041
9	0,703	1,383	1,833	2,262	2,821	3,250	3,690	4,297	4,781
10	0,700	1,372	1,812	2,228	2,764	3,169	3,581	4,144	4,587
11	0,697	1,363	1,796	2,201	2,718	3,106	3,497	4,025	4,437
12	0,695	1,356	1,782	2,179	2,681	3,055	3,428	3,930	4,318

Fonte: UNIVERSIDADE FEDERAL DE SANTA CATARINA, 2011 (com adaptações).

[149] *Grosso modo*, a utilização do *gl* se explica pelo fato de se utilizar a diferença do interesse militar *entre* os anos, e não *dos* anos.

Tabela 33 – Estatísticas referentes ao IPvDC

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	n/	INTERVALO	EUA				BRASIL				CANADÁ			
2	gl		anterior	posterior	TOTAL	∑D2	anterior	posterior	TOTAL	∑D2	anterior	posterior	TOTAL	∑D2
3	1	2000-2001	5.184	6.635	1.451	2.105.401	-	2	2	4	-	3	3	9
4	2	2001-2002	6.635	2.267	(4.368)	19.079.424	2	-	(2)	4	3	8	5	25
5	3	2002-2003	2.267	1.636	(631)	398.161	-	1	1	1	8	3	(5)	25
6	4	2003-2004	1.636	2.164	528	278.784	1	2	1	1	3	2	(1)	1
7	5	2004-2005	2.164	2.952	788	620.944	2	2	-	-	2	4	2	4
8	6	2005-2006	2.952	3.724	772	595.984	2	5	3	9	4	3	(1)	1
9	7	2006-2007	3.724	4.787	1.063	1.129.969	5	6	1	1	3	3	-	-
10	8	2007-2008	4.787	7.280	2.493	6.215.049	6	16	10	100	3	3	-	-
11	9	2008-2009	7.280	8.483	1.203	1.447.209	16	35	19	361	3	2	(1)	1
12	10	2009-2010	8.483	11.207	2.724	7.420.176	35	53	18	324	2	66	64	4.096
13	11	2010-2011	11.207	16.496	5.289	27.973.521	53	196	143	20.449	66	211	145	21.025
14	12	2011-2012	16.496	17.229	733	537.289	196	454	258	66.564	211	187	(24)	576
15		∑D	72.815	84.860	12.045	67.801.911	318	772	454	87.818	308	495	187	25.763
17		MÉDIA (D-linha)			1.003,75				37,83				15,58	
19		(D-linha)2			1.007.514,06				1.431,36				242,84	
21		SD =			2250,49				80,14				45,58	
23		t =			1,55				1,64				1,18	
24														
25		P =			0,10	aprovado			0,10	aprovado			0,25	rejeitado

Fonte: Elaboração própria.

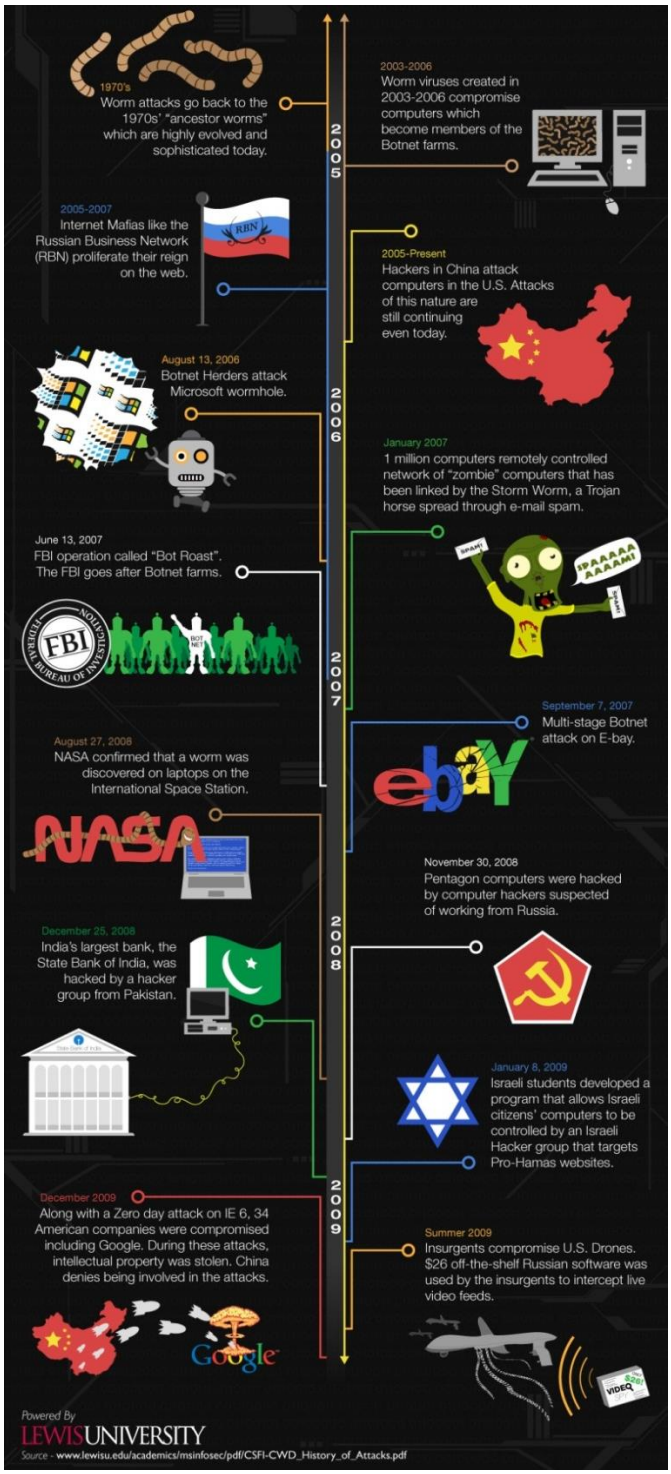
APÊNDICE E – Exemplo de GPL de saída de comando para o Gráfico 11

Código gerador de gráfico, a partir de IBM SPSS Statistics (2012):

```
GGRAPH
  /GRAPHDATASET NAME="graphdataset" VARIABLES=ipvdc ipddc pais MISSING=LISTWISE
REPORTMISSING=NO
  /GRAPHSPEC SOURCE=INLINE.
BEGIN GPL
  SOURCE: s=userSource(id("graphdataset"))
  DATA: ipvdc=col(source(s), name("ipvdc"), unit.category())
  DATA: ipddc=col(source(s), name("ipddc"), unit.category())
  DATA: pais=col(source(s), name("pais"), unit.category())
  GUIDE: axis(dim(1), label("IPvDC"))
  GUIDE: axis(dim(2), label("IPdDC"))
  ELEMENT: point(position(ipvdc*ipddc), label(pais))
END GPL.
```

ANEXO A – Histórico da *cyber warfare* na política internacional (1970-2009)

Esquema 7 – Histórico da *cyber warfare* na política internacional (1970-2009)



Fonte: LEWIS UNIVERSITY, 2010, com adaptações.

Nota: O verme Stuxnet, caso mais emblemático até então, somente é revelado em 2010 (CLARKE; KNAKE, 2012, p. 291; IRÃ, 2011; LOPES, 2011a; SANGER, 2012a, p. ix; SUTHERLAND, 2012, p. 166).