UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE FILOSOFIA E CIÊNCIAS HUMANAS
DEPARTAMENTO DE CIÊNCIA POLÍTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA POLÍTICA
DOUTORADO EM CIÊNCIA POLÍTICA
ÁREA DE CONCENTRAÇÃO: RELAÇÕES INTERNACIONAIS

GILLS VILAR LOPES

RELAÇÕES INTERNACIONAIS CIBERNÉTICAS (CiberRI): UMA DEFESA ACADÊMICA A PARTIR DOS ESTUDOS DE SEGURANÇA INTERNACIONAL

RECIFE
2016

GILLS VILAR LOPES

RELAÇÕES INTERNACIONAIS CIBERNÉTICAS (CiberRI): UMA DEFESA ACADÊMICA A PARTIR DOS ESTUDOS DE SEGURANÇA INTERNACIONAL

Tese de Doutorado apresentada como requisito obrigatório para a obtenção do título de Doutor 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
2016

Catalogação na fonte
Bibliotecária Maria Janeide Pereira da Silva, CRB4-1262

L864r Lopes, Gills Vilar.
Relações internacionais cibernéticas (CiberRI) : uma defesa acadêmica a partir dos estudos de segurança internacional / Gills Vilar Lopes. – 2016.
165 f. : il. ; 30 cm.

Orientador : Prof. Dr. Marcelo de Almeida Medeiros.
Tese (doutorado) - Universidade Federal de Pernambuco, CFCH. Programa de Pós-graduação em Ciência Política, 2016.
Inclui Referências, apêndices e anexos.

1. Ciência Política. 2. Relações internacionais. 3. Ciberespaço. 4. Segurança internacional. 5. CiberRI. 6. Cibernética. I. Medeiros, Marcelo de Almeida (Orientador). II. Título.

320 CDD (22. ed.) UFPE (BCFCH2017-008)

Universidade Federal de Pernambuco
Centro de Filosofia e Ciências Humanas
Departamento de Ciência Política
Programa de Pós-Graduação em Ciência Política

RELAÇÕES INTERNACIONAIS CIBERNÉTICAS (CiberRI): UMA DEFESA ACADÊMICA A PARTIR DOS ESTUDOS DE SEGURANÇA INTERNACIONAL

Gills Vilar Lopes

Tese aprovada em 28 de dezembro de 2016.

Banca Examinadora:

_____
Prof. Marcelo de Almeida Medeiros, Doutor, Universidade Federal de Pernambuco (Orientador)

_____
Prof. Marcos Aurélio Guedes de Oliveira, Doutor, Universidade Federal de Pernambuco (Examinador interno)

_____
Prof. Ricardo Borges Gama Neto, Doutor, Universidade Federal de Pernambuco (Examinador interno)

_____
Prof. Augusto Wagner Menezes Teixeira Júnior, Doutor, Universidade Federal da Paraíba (Examinador externo)

_____
Prof. Rodrigo Barros de Albuquerque, Doutor, Universidade Federal de Sergipe (Examinador externo)

Ao povo brasileiro, patrocinador final de grande parte das pesquisas que aqui se confluem.

AGRADECIMENTOS

Ao Programa de Pós-Graduação em Ciência Política (PPGCP) da Universidade Federal de Pernambuco (UFPE), pela excelência de seus professores e profissionais, sempre solícitos. Sou grato também à Coordenadora do PPGCP professora Gabriela Tarouco e a toda sua equipe, bem como à professora Eugênia Barza e ao Programa de Pós-Graduação em Direito (PPGD) da Faculdade de Direito do Recife (FDR), por viabilizarem a defesa desta Tese.

À Banca de Qualificação, formada pelos professores Marcos Guedes, Ricardo Borges e Rodrigo Albuquerque, e à Banca Examinadora – acrescida dos professores Augusto Wagner, Andrea Steiner e Scott Tollefson –, por me apontar o bom caminho.

Ao Programa de Apoio ao Ensino e à Pesquisa Científica e Tecnológica em Assuntos Estratégicos de Interesse Nacional (Pró-Estratégia), da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) e da Secretaria de Assuntos Estratégicos da Presidência da República (SAE), pela imprescindível Bolsa de Doutorado.

À *National Defense University* (NDU), do Ministério da Defesa dos Estados Unidos da América, em Washington, nas pessoas dos professores Kevin Newmeyer, Scott Tollefson e Luis Bitencourt, pela oportunidade de estudar o tema de minha Tese em um ambiente tão motivador.

À lista de *e-mails* "Internet e política", pelos *insights* e mensagens afeitos ao tema aqui versado.

Ao Cel R1 Paulo Cesar Leal e à Mj Selma Gonzales, do Exército Brasileiro, em Brasília, pela atenção depositada.

Ao prof. Joanisval Brito Gonçalves, do IGEPP, em Brasília, por ampliar meus conhecimentos em Defesa Nacional e Inteligência de Estado.

Aos jovens Alexandre César C. Leite, Alexandre Fuccille, Antônio Lucena, Bernardo Wahl, Deywisson Ronaldo, Elton Gomes, Fábio Nobre, Giovanni Okado, Igor Acácio, Kaiser Konrad, Marco Túlio Freitas, Paulo Kuhlmann, Peterson Silva e tantos outros que me enviaram textos sobre "cibercoisas" e que torceram por mim, via *e-mail* ou *in loco*.

À Faculdade Damas, em Recife, na pessoa do prof. Thales Castro, por proporcionar minha primeira experiência como docente de nível superior em RI.

Ao Departamento de Relações Internacionais (DRI) da Universidade Federal da Paraíba (UFPB), na pessoa do prof. Henrique Menezes, por acreditar no meu trabalho e deixar eu pôr em prática algumas das ideias contidas nesta Tese.

Ao Instituto Brasileiro de Estudos em Defesa Pandiá Calógeras (IBED), do Ministério da Defesa, nas pessoas dos professores Antônio Jorge Ramalho e Juliano “o cara” Cortinhas.

Aos colegas e organizadores do 11º Programa de Intercâmbio SAL/SAJ (Ministério da Justiça e Casa Civil da Presidência da República), em Brasília, e da III Escola de Governança da Internet (EGI-CGI.Br), em São Paulo, pelas experiências marcantes.

Ao Exército Brasileiro, cujas visitas técnicas à Academia Militar das Agulhas Negras (AMAN), em Resende, à Escola de Comando e Estado-Maior do Exército (ECEME), no Rio de Janeiro, e ao Centro de Defesa Cibernética (CDCiber), em Brasília, foram imprescindíveis para a consecução deste trabalho.

Ao meu Orientador, prof. Marcelo de Almeida Medeiros, eterno mestre, pelos conselhos e oportunidades dados ao longo de toda minha vida pós-graduanda.

Às Lopes da minha vida: Litoka, Rhanoka e Maroka, por cuidarem de mim, sobretudo nos momentos enfermos.

E, finalmente, um especial agradecimento à minha douta esposa, Dalliana Vilar Lopes, por não medir esforços para construirmos nossos sonhos juntos.

Agradeço-lhes!

Só quando se estuda um novo problema [...] e se descobrem verdades que abrem novas e importantes perspectivas é que nasce uma nova "ciência". (WEBER, 2006, p. 37).

RESUMO

Esta Tese tem como objetivo-mor defender a criação de Relações Internacionais Cibernéticas (CiberRI), um subcampo internacionalista cujo objeto de estudo é o impacto do ciberespaço nas relações internacionais. Como marco teórico, elegem-se os Estudos de Segurança Internacional, haja vista o uso de conceitos pertinentes a eles, tais como guerra, segurança e poder cibernéticos. Assim, a revisão de literatura envolve, principalmente, autores clássicos e modernos de Ciências Sociais, Ciência Política e Relações Internacionais (RI), passando, de forma auxiliar, por Ciência da Computação, Ciência da Informação, Direito, Educação e Filosofia da Ciência. O presente trabalho se divide em três partes principais. A primeira delas situa CiberRI em uma posição cientificamente válida, tendo como parâmetro a aparente dicotomia entre ciências humanas/sociais e naturais, sempre interligada pelos estudos políticos e internacionalistas acerca do poder. Estabelecidos os limites e objeto de CiberRI, engendra-se o Modelo 3C, que visa a sistematizar a excessiva fragmentação temática sobre o ciberespaço em RI, cujos pressupostos (Coerência epistemológica, Consistência teórico-metodológica e Coordenação acadêmica) ligam-se, inexoravelmente, aos três elementos metateoréticos em RI (Ontologia, Epistemologia e Metodologia) e a três campos do saber (Doxológico, Epistêmico e Teórico). A segunda seção apresenta a defesa acadêmica propriamente dita de CiberRI, tendo como base o tripé constitucional que rege as universidades brasileiras: ensino, pesquisa e extensão. Nesse ponto, propõem-se mudanças curriculares e exemplifica-se como ocorre a institucionalização desse novo campo de ensino em universidades estrangeiras, apontando caminhos para a brasileira. Ademais, a definição, aqui, de *Era dos Ruídos* ajuda a contextualizar alguns acontecimentos ciberinternacionais, como o Caso Snowden, assaz pesquisado pela comunidade epistêmica de RI. A terceira seção evidencia como CiberRI pode impactar RI. Assim, cria-se e aplica-se o conceito de *Software Power* como uma ferramenta analítica para a política internacional hodierna, ajudando a "atualizar" RI para as idiossincrasias cibernéticas deste século. Em seguida, aplica-se o Modelo 3C à análise dos trabalhos publicados nos anais do Encontro Nacional da Associação Brasileira de Estudos de Defesa (ABED), identificando como eles tratam a questão do ciberespaço. Seus principais achados apontam para um parco diálogo com os elementos metateoréticos de RI, ao passo que o aumento da importância dada ao tema mostra-se estatisticamente significativa. Devido ao desenho de pesquisa e aos objetivos desta Tese, segue-se a estratégia de metodologia mista do *Nested Analysis*, com o uso tanto de métodos qualitativos quanto quantitativos, tais como *software* estatístico, pesquisa bibliográfica e documental, análise de discurso, webometria e a técnica da análise de correspondência simples (Anacor).

Palavras-chave: Ciberespaço. CiberRI. Relações Internacionais Cibernéticas. Segurança Internacional. *Software Power*.

ABSTRACT

This Ph.D. Dissertation aims to defend the creation of International Cyber Relations (CyberIR), an internationalist subfield whose object is the impact of cyberspace in international relations. As a theoretical framework, the International Security Studies subfield is chosen, considering the use of concepts pertinent to it, such as cyber warfare, cyber security and cyber power. Thus, the literature review involves, mainly, classical and modern authors of Social Sciences, Political Science and International Relations (IR), passing, in an auxiliary way, by Computer Science, Information Science, Law, Education and Philosophy of Science. This work is divided into three parts. The first one places CyberIR in a scientifically valid position, having as a parameter the apparent dichotomy between social and natural sciences, always interconnected by political and internationalist studies of power. Once the limits and object of CyberIR have been established, 3C Model is constructed, aiming to systematize the excessive thematic fragmentation on the cyberspace in IR, whose presuppositions (Epistemological Coherence, Theoretical-Methodological Consistency and Academic Coordination) are inexorably linked to both the three metatheoretical IR elements (Ontology, Epistemology and Methodology) and fields of knowledge (Doxological, Epistemic and Theoretical). The second section presents the proper CyberIR academic defense, based on the constitutional tripod that governs Brazilian universities: teaching, research, and extension. At this point, curricular changes are proposed and the institutionalization of this new field of teaching in foreign universities is exemplified, pointing ways to the Brazilian one. In addition, the Age of Noise definition helps to contextualize some cyberinternational events, such as the Snowden Case, which has been strongly researched by the epistemic community of IR. The third section shows how CyberIR can impact IR. Therefore, the Software Power concept is created and applied as a framework of analyses for the current international politics, thus "updating" IR to the idiosyncrasies of this century. Then, 3C Model is applied to the analysis of the works published in the proceedings of the Brazilian Association of Defense Studies (ABED)'s National Meeting, identifying how they treat the cyber issue; The findings point out to a few dialogues of these with metatheoretical IR elements, while the increase in importance given to the theme shows itself statistically significant. Due to the research design and the objectives of this work, the methodology of Nested Analysis is followed, with the use of both qualitative and quantitative methods, such as statistical software, bibliographical and documentary research, discourse analysis, Webometrics and technique of simple correspondence analysis (Anacor).

Keywords*: Cyberspace. CyberIR. Cyber International Relations. International Security. Software Power.*

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

3C	Coerência epistemológica, consistência teórico-metodológica e coordenação acadêmica
ABED	Associação Brasileira de Estudos de Defesa
ABRI	Associação Brasileira de Relações Internacionais
Anacor	Análise de correspondência simples
ARPANET	*Advanced Research Projects Agency Network*
Art.	Artigo
AT	Área temática
CAPES	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
CCD COE	*Cooperative Cyber Defence Centre of Excellence* (OTAN)
C&T	Ciência e Tecnologia
CF88	Constituição da República Federativa do Brasil de 1988
CIA	*Central Intelligence Agency* (EUA)
CiberRI	Relações Internacionais Cibernéticas
CNPq	Conselho Nacional de Desenvolvimento Científico e Tecnológico
CP	Ciência Política
ECIR	*Explorations in Cyber International Relations*
E.g.	*Exempli gratia* / por exemplo
ENABED	Encontro Nacional da Associação Brasileira de Estudos de Defesa
END	Estratégia Nacional de Defesa
ESI	Estudos de Segurança Internacional
et al.	*Et alii*; e outros
EUA	Estados Unidos da América
FBI	*Federal Bureau of Investigation* (EUA)
I.e.	*Id est*; isto é
IES	Instituição de ensino superior
IGF	Fórum de Governança da Internet (ONU)
Interpol	Organização Internacional de Polícia Criminal
LNA	*Large-N Analysis*
MIT	Instituto de Tecnologia de Massachusetts (EUA)
N.B.	*Nota bene*; note bem
NSA	*National Security Agency* (EUA)
ONU	Organização das Nações Unidas
OTAN	Organização do Tratado do Atlântico Norte
P&D	Pesquisa e Desenvolvimento
PNI	Política Nacional de Inteligência (PNI)
Pró-Estratégia	Programa de Apoio ao Ensino e à Pesquisa Científica e Tecnológica em Assuntos Estratégicos de Interesse Nacional
RI	Relações Internacionais
SAE/PR	Secretaria de Assuntos Estratégicos da Presidência da República
SAM	*Stakeholders*, Ações e Motivos na Segurança Cibernética
SegInfo	Segurança da Informação
SNA	*Small-N Analysis*
St Ciber	Setor Estratégico Cibernético
TIC	Tecnologias de informação e comunicação
UFPE	Universidade Federal de Pernambuco
USCYBERCOM	*U.S. Cyber Command* (EUA)
WWW	*World Wide Web*

LISTA DE SÍMBOLOS

$\cong$	Aproximadamente
$\supset$	contém
e^2	Erro máximo permitido
H_0	Hipótese nula ou de trabalho
H_1	Hipótese alternativa
Σ	Somatório
n	Tamanho da amostra
N	Tamanho da população/universo
σ^2	Nível de confiança
$\chi 2$	Qui-quadrado

SUMÁRIO

INTRODUÇÃO

> Alguns temas foram pesquisados em diferentes disciplinas, e o resultado da interação entre elas tem sido profícuo [para a Ciência Política]. Hoje, uma análise disciplinar [...] explicará *muito menos* do que um exame interdisciplinar. (SOARES, 2005, p. 41, grifo do autor).

Neste raiar de novo século, o ciberespaço já se incorporou à agenda de muitos governos e organizações internacionais, especialmente no que tange à temática da segurança internacional[1], mediante, sobremaneira, aquilo que se chama de Segurança Cibernética. Pode-se dizer o mesmo das mais laureadas instituições de ensino superior (IES) do mundo[2]. Nesse sentido, um novo vocabulário, com suas próprias terminologias, começa a figurar, com frequência crescente, em vários trabalhos acadêmicos de Relações Internacionais (RI) e Ciência Política (CP)[3]. Parte dessa literatura emergente já se refere a alguns Estados – notadamente, Estados Unidos da América (EUA), China e Rússia – como verdadeiras potências cibernéticas (*cyber powers*)[4], capazes de produzir armas cibernéticas (*cyber weapons*) em um contexto de guerra cibernética (*cyber warfare*) e de Defesa Cibernética (*Cyber Defense*), materializando, assim, o que Nye Jr (2011b, *passim*) chama de poder cibernético (*Cyber Power*). Diante desse contexto, indaga-se: por que não pensar também em termos de relações internacionais cibernéticas ou, mesmo, de Relações Internacionais Cibernéticas (CiberRI)?

O presente trabalho lança luz na tese de que, no âmbito específico de RI, os estudos sobre temas relacionados ao ciberespaço já não podem mais ser, simplesmente, rotulados como importantes, relevantes ou interessantes; eles se tornam, sim, imprescindíveis ao próprio aperfeiçoamento dos estudos internacionalistas e do próprio campo de RI, urgindo, assim, a criação de um subcampo científico que busque organizar e sistematizar a produção ciberinternacionalista, bem como apontar caminhos para o seu particular desenvolvimento.

---

[1] Segurança internacional, em minúsculo, refere-se ao objeto homógrafo do subcampo internacionalista Estudos de Segurança Internacional (ESI) ou, simplesmente, Segurança Internacional, em maiúsculo, cujas obras, por assim dizer, canônicas são, em ordem cronológica, Herz (1950), Wolfers (1962) e Jervis (1976), conforme atestam também Buzan, Wæver e Wilde (1998, p. 10-11) e Rudzit (2005, p. 311). Enquanto objeto de estudos, trata-se de uma questão relacional, ou seja, de como as coletividades humanas se relacionam entre si em termos de ameaças e vulnerabilidades, cujo cerne está, firmemente, enraizado nas tradições da política do poder (BUZAN; WÆVER; WILDE, 1998, p. 10, 21, 29).

[2] Para um rol não taxativo de algumas delas, ver subseção 2.3, *infra*.

[3] Apesar de a abreviação RI ser mais corriqueira que a de CP, segue-se aqui o exemplo de Amorim Neto e Santos (2015) e mantém-se esta.

[4] Cf. CZOSSECK, 2013, p. 20; DEMCHAK, 2013, p. 612, 614-617; 2014, p. v, viii; LIAROPOULOS, 2013, p. 139; NASCIMENTO, 2015, p. 72; NEUNECK, 2013, p. 117; OLIVEIRA; LEITE, 2016; SHAHEEN, 2014, p. 86; SINGER; FRIEDMAN, 2014, p. 186.

Como se vê, empregam-se aqui termos que, por um lado, são indispensáveis para a compreensão dos propósitos desta Tese, mas que, por outro, devido aos limites epistemológicos do objetivo de pesquisa, não são aprofundados. À guisa de demonstração, tomem-se como exemplos as seguintes cinco partes do parágrafo anterior: (i) temas relacionados ao ciberespaço; (ii) aperfeiçoamento; (iii) subcampo científico; (iv) busque; e (v) sistematizar.

O primeiro exemplo, *temas* relacionados ao ciberespaço, traz, implicitamente, a observação de que, "[...]nas últimas décadas[...], [há] uma tendência a enfocar a pesquisa [acadêmica] a partir de *temas*[...]" (SOARES, 2005, p. 41, grifo do autor). Portanto, a ênfase deste trabalho não está nas idiossincrasias do ciberespaço em si, mas, sim, em temas transversais, ao mesmo tempo, a ele e a RI.

No segundo exemplo, afirma-se que RI *aperfeiçoa-se*, ao passo que CiberRI *desenvolve-se*. Emprega-se o primeiro verbo no sentido de que é possível diferenciar RI de outros campos do saber e que, portanto, precisa constantemente se aperfeiçoar, ao passo que CiberRI, por existir apenas no mundo normativo, necessita, pois, desenvolver-se. Como se vê, mais adiante, essa diferenciação será importante para a compreensão da hipótese principal.

O terceiro exemplo se refere ao conceito de *subcampo científico*, o qual se liga a dois aspectos ontológicos. O primeiro deles é mais geral e diz respeito à própria definição de campo científico. Já o segundo, mais específico e à luz das diretrizes educacionais brasileiras, reside na distinção entre Área e Campo, a qual é bem mais profunda do que aqui se apresenta[5]. Ora, esta é uma Tese de CP, com área de concentração em RI, e não de Filosofia da Ciência. Porém, faz-se imperioso introduzir alguns elementos desse subcampo da Filosofia – e, mais especificamente da Filosofia da Ciência Social[6] – que demanda clareza e precisão (WALTZ, 2003, p. vii) conceituais, tendo em vista que uma solução filosófica para a delimitação do problema científico pode proporcionar uma resposta à questão de como RI deve proceder como

[5] O cerne dessa discussão no Brasil tem por base a necessária atualização da chamada "Tabela de Áreas de Conhecimento/Avaliação" da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), bem como a padronização das nomenclaturas contidas em Brasil (2014a). Todavia, isso traz à tona o fato de que Brasil (1998, p. 3-4) diferencia "áreas do conhecimento" de "campos de saber" – conceito este inexistente na Tabela supracitada –, a ponto de se poder associar, pelo menos, no caso brasileiro, RI ora a um, ora a outro. Tornando ainda mais complexas as discussões sobre a posição das diversas ciências, há que se mencionar também a existência da mundialmente famosa Classificação Decimal de Dewey (GIL, 1999, p. 81-82) e da Tabela de Áreas do Conhecimento do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq). Enquanto o CNPq se liga diretamente ao Ministério da Ciência, Tecnologia e Inovação (MCTI), cuja tabela em apreço serve, dentre outros, para nortear questões de pesquisa e desenvolvimento (P&D) em ciência e tecnologia (C&T), tais quais bolsas de ensino, pesquisa e extensão universitária, a CAPES se vincula ao Ministério da Educação, e sua tabela serve de parâmetro para avaliar a educações superior nas suas mais diversas áreas. É por causa disso que a presente Tese leva em conta esta última tabela.

[6] A Filosofia da Ciência tem como foco de estudo "[...]o caráter *científico* do conhecimento" (RUDNER, 1969, p. 13, grifo do autor). Já a Filosofia da Ciência Social é uma subdisciplina daquela (*ibid.*, p. 13).

um *campo científico* (JACKSON, 2011, p. 10). Na proposição seminal de Bourdieu (1983c, p. 44), a noção de *campo* deve ser entendida "[...]ao mesmo tempo como campo de forças e campo de lutas que visam transformar esse campo de forças", *i.e.*, um lugar de lutas epistemologicamente concorrenciais (*idem*, 1983b, p. 122). Assim, o que torna um campo científico, na acepção bourdieusiana, é a capacidade de ele funcionar como um universo social no qual se estabelecem leis e teorias científicas comprováveis, testáveis e passíveis de crítica.[7] É diante desse contexto que se defende CiberRI como um sub*campo*, em relação ao campo de RI.[8]

Seguindo, o quarto exemplo traz a ideia de esse subcampo *buscar* organizar e sistematizar a produção ciberinternacionalista. O emprego do verbo buscar – e dos demais que passam essa ideia de apreensão limitada da realidade – resgata uma noção de absorção incompleta/imperfeita/limitada do estado de coisas[9] ciberinternacionalista. Essa limitação se justifica aqui porque, de um lado, "[...]o conhecimento na área cibernética tem crescido exponencialmente e a uma velocidade sem precedentes[...]" (CARVALHO, 2011b, p. 31) e, do outro, "[o] conhecimento científico sempre incide sobre aspectos limitados da realidade, até porque o número de ocorrências[...]" (COHN, 2006a, p. 9), casos (WALLERSTEIN *et al*., 1996, p. 75), fatos (VOEGELIN, 1982, p. 21; WALTZ, 2003, p. ix), estímulos que desencadeiam normas e papéis sociais (BOURDIEU, 1983a, p. 64), universo de elementos das pesquisas sociais (GIL, 1999, p. 99), ações dos indivíduos e exemplos políticos (LIPSON, 1967, p. 25) é infinito.

Finalmente, quando o quinto exemplo remete a essa busca por *sistematizar* a produção ciberinternacionalista, ele está, na verdade, referindo-se aos aspectos de observação, análise e síntese dos fatos e acontecimentos cibernéticos que impactam as RI e/ou as relações internacionais e vice-versa, haja vista que "[...]a pesquisa de *fatos* está intimamente ligada à *sistematização*" (DUVERGER, 1981, p. 32, grifo nosso) e que os fatos são interdependentes das teorias (WALTZ, 2003, p. viii). A sistematização é, nesse prisma, um atributo do conhecimento científico, pois "[...]se preocupa em construir sistemas de ideias *organizadas*

---

[7] Eis aqui, em suma, a grande diferença entre *episteme* e *doxa*, melhor delineada na subseção 1.3, *infra*. Sobre a definição de campos científicos como universos sociais, ver Bourdieu (1983c, p. 44-45).

[8] É também nesse mesmo viés, por exemplo, que: Wallerstein *et al.* (1996, p. 71) epitetam Sociologia Política e Sociologia Econômica como subcampos da Sociologia; Jackson (2013, p. 39) e Sarfati (2011, p. 333) referem-se ao subcampo de Economia Política Internacional em relação a RI; e Silva e Gonçalves (2010, p. 82, 214) referem-se à Geopolítica como subcampo da Geografia Política, bem como à Política Comparada, da CP.

[9] O termo "estado de coisas", deveras empregado neste trabalho, corresponde a seus análogos inglês (*state of affairs*) e alemão (*Zustand*) e possui denotação, essencialmente, descritiva (BOBBIO, 1987, p. 165; RUDNER, 1969, p. 90). Cf. MARX; ENGELS, 2007, p. 38.

racionalmente e em incluir os conhecimentos parciais em totalidades cada vez mais amplas" (GIL, 1999, p. 21, grifo nosso). Como se pretende aprofundar, CiberRI se preocupa não apenas com a sua própria área de estudo, mas também em incorporá-la ao todo internacionalista, político e social que a precede e circunscreve.

São, portanto, em termos como estes – e como o título deste trabalho expressa – que se defende a criação de CiberRI como um subcampo cujo objeto de estudo gira em torno de temas que põem, de um lado, o ciberespaço e, do outro, as relações internacionais ou o próprio campo de RI e seus impactos, sempre tendo como pressupostos os elementos metateoréticos – ontologia, epistemologia e metodologia – de RI[10]. Mas até que ponto RI realmente suporta ou, mesmo, necessita de tal subcampo? E, se necessita, quais seriam, então, seus limites, alcances e objeto? Contextualizar essas perguntas é o *leitmotiv* deste trabalho.

Ao mesmo tempo em que se subsidia a criação de um subcampo de RI, busca-se também evitar tanto "[...]a precipitação [a] que certos autores demonstram em publicar seus trabalhos, a fim de evitar que sejam ultrapassados" (BOURDIEU, 1983b, p. 131-32) quanto a "especialização prematura" que "[...]quase sempre traz consigo a mediocridade intelectual" (MEGALE, 1990, p. 74, 166). O próprio Megale (1990, p. 74), diga-se de passagem, não condena "[...]a especialização, que é fruto do progresso da ciência"; de acordo com o autor, ela "deve vir sempre acompanhada do conhecimento profundo da área ou áreas de saber em que se insere". É nesse viés que a presente Tese se preocupa em situar CiberRI em seu contexto epistemológico mais geral, ou seja, fazendo parte de um todo ainda maior, composto por RI, CP e as próprias ciências sociais. Para tanto, propõe-se situar esse subcampo na panaceia do conhecimento científico, com o intuito de ajudar a "curar RI de sua inveja perene em relação a outros campos científicos, ao destacar o importante trabalho conceitual sobre a 'questão da ciência' que *já feito dentro das próprias ciências sociais*" (JACKSON, 2011, p. 19, grifo do autor, tradução nossa[11]).[12]

---

[10] Esta Tese entende que trazer a discussão de RI em termos metateoréticos – e não "metateóricos" – fortalece o seu próprio *status* de campo científico. Sobre esse assunto em RI, ver Elman e Elman (2003, p. 41), Jackson (2011, *passim*) e Sarfati (2011, p. 20). Sobre o fato de que as ciências sociais, supostamente, não gozam do mesmo prestígio científico que as naturais, ver Gil (1999, p. 21-22).

[11] Texto original: "[...]*to cure IR of its perennial envy of other fields of scholarly inquiry by highlighting the important conceptual work on the matter of science that has already been done within the social sciences themselves*".

[12] Sobre este mesmo ponto que defronta RI em relação à suposta "inveja da Física", ver ELMAN e ELMAN (2003, p. 40).

Ora, RI nasce da CP, que, por sua vez, compreende o núcleo duro das ciências sociais. Por o objeto central da CP ser o poder[13] (DUVERGER, 1981, p. 10, 12, 32; MEGALE, 1990, p. 78, 115; SARTORI, 1981, p. 48), não se pode conceber uma investigação sistemática de RI que não trate desse conceito em uma de suas possíveis dimensões[14], sob o risco quase certo de se engendrar um trabalho, no máximo, internacional, mas não internacionalista[15]. Estas, portanto, são as premissas que orientam a presente Tese.

Exemplos não faltam para demonstrar como temas ligados ao ciberespaço impactam as relações internacionais e, consequentemente, põem desafios ao campo de RI. Elencam-se alguns, nas mais diversas ciências sociais que tangenciam RI, na certeza de que eles são apenas uma parcela mínima de uma lista ainda maior.

No âmbito do Comércio e da Cooperação Internacional, a venda de produtos e serviços ilegais no submundo da Internet traz consigo desafios não só em termos tecnológicos, como também em termos de cooperação interagências, sobretudo, para os órgãos investigativos – tais como ministérios públicos e polícias –, de Inteligência de Estado[16] e, até mesmo, para a Organização Internacional de Polícia Criminal (Interpol), os quais fazem parecer que a luta contra os crimes cibernéticos (*cybercrimes*) está atualmente no mesmo patamar que o combate ao narcotráfico (SOLANA, 2015), a ponto de tal tema parar nas listas de "Procurados" do *Federal Bureau of Investigation* (FBI) (KUCHLER, 2014, p. 1). Nem mesmo a Convenção de Budapeste sobre Crimes Cibernéticos, de 2001, cuja proposta de aplicação na ordem jurídica brasileira gerou fortes rejeições (LOPES; PEREIRA, 2010, p. 8-11), é capaz de trazer ao ciberespaço um mínimo de ordem legal. Esse, aliás, não parece ser o desejo de muitos grupos hacktivistas que militam dentro e o fora do ciberespaço.

---

[13] Poder, "[...]elemento organizador da sociedade[...]" (VOEGELIN, 1982, p. 7), "[...]pode ser causa, consequência ou fim por si só" (VALENTE, 2007, p. 15). Tal conceito é definido de várias formas, tal como "[...]a capacidade de alcançar resultados através da ação planejada" (LIPSON, 1967, p. 103), *i.e.*, "a força acrescida do consentimento" (LIPSON, 1967, p. 109). Autores clássicos de RI como Bull (2002), Carr (2001), Morgenthau (2003) e Wight (2002) transpuseram algumas dessas máximas ao nível internacional com o intuito de investigar sua sustentação teórica e empírica ao longo da história e da política internacional antiga e de suas épocas. Observam-se, ainda, outras definições de CP que atrelam seu objeto principal de estudo ao Estado e/ou à política (LIPSON, 1967, p. 15; MEGALE, 1990, p. 78; WALLERSTEIN *et al.*, 1996, p. 36, 59) e/ou à sociedade (LIPSON, 1967, p. 48; VOEGELIN, 1982, p. 5, 7, 49). Conferir também como Kawamura (1986) atrela tal conceito ao caráter político da tecnologia. Para a definição de poder cibernético, ver Nye Jr (2011b) e subseção 3.1, *infra*.

[14] Tais quais a política (LIPSON, 1967, p. 331-361), militar, econômica, governamental (VOEGELIN, 1982, p. 45), *hard*, *soft*, *smart* e, mais recentemente, cibernética.

[15] Sobre a diferenciação entre internacional e internacionalista, ver subseção 1.1.

[16] Acerca da Atividade de Inteligência, ver Bessa (2014, p. 10, 12, 43), Brasil (2013; 2016), Gonçalves (2008; 2013) e Proença Jr. e Diniz (1998, p. 34-37).

Na esfera diplomática, potências mundiais – notadamente as que participaram o esquema de espionagem cibernética (*cyber espionage*) delatado por Edward Snowden, em 2013 – até hoje respondem aos constrangimentos oriundos da divulgação de documentos sigilosos em *sites* de vazamento, como o WikiLeaks, que se utilizam de criptografia complexa para não deixar rastros. Diga-se de passagem, o Caso Snowden marca a política internacional hodierna, de forma que é possível ouvir suas reverberações na Assembleia Geral da Organização das Nações Unidas (ONU)[17]. A própria arte da diplomacia vem sofrendo transformações neste novo milênio, sendo, até mesmo, chamada por termos como e-Diplomacia, Diplomacia Digital ou Diplomacia da Internet (MALTA; SUÍÇA, [201-]; LOPES; MEDEIROS, 2011, *passim*).

Quanto à Geografia[18], veem-se mapas *online* revelarem, ao público planetário, locais outrora secretos, tais como estruturas estratégicas – ou infraestruturas críticas[19] –, zonas de testes nucleares e de treinamentos militares, fazendo com que governos exijam, das empresas detentoras desses aplicativos e serviços virtuais, a colocação de tarjas ou borrões.

No prisma econômico, têm-se, de um lado, novos conceitos como economia compartilhada e *e-hailing*[20] – como Airbnb e Uber, respectivamente –, que se ancoram na descentralização virtual de serviços e produtos, sem a habitual necessidade de intermediários ou gerentes, e, mesmo, sem a clássica relação empregador-empregado, desafiando, assim, governos, que, a partir de agora, têm de lidar com acontecimentos transnacionais em matérias tradicional e legalmente locais. Do outro lado, há o uso das chamadas moedas digitais ou criptomoedas, cujo principal expoente é o Bitcoin[21], pelo qual se permite questionar premissas do sistema financeiro internacional e da própria Economia Política Internacional, com uma fórmula monetária lastreada não no ouro nem em outra moeda – ou conjunto delas –, mas, sim, em *bytes*, por meio de sua mineração.

---

[17] Cf. Subseção 2.4.3, *infra*, e Organização das Nações Unidas (2013, *passim*).

[18] Para uma discussão sobre se a Geografia é uma ciência social ou não, ver Megale (1990, p. 54-55, 57-58, 73, 79-80, 96-106) e Wallerstein *et al.* (1996, p. 43-48).

[19] Sobre tais estruturas, ver Karas *et al.* (2008, p. 11-12).

[20] Já se fala, também, em Economia Hacker (CNBC, 2016), haja vista que, se o roubo e a venda de informações – pessoais e sigilosas – movimentam o mercado negro bilionário da chamada Internet Profunda, esses valores precisam ser levados em conta pelas economias nacionais.

[21] Bitcoin é uma criptomoeda "[...]trocada de forma anônima, mas que pode ser convertida em dinheiro real, uma vez acessada a conta de um indivíduo" (DILLON; BRUNSMANN, 2015). Usam-na tanto como "[...]protocolo [...]nas funções de banco central (ex: FED, BACEN) quanto de plataforma de pagamentos (ex: Visa, PayPal)" (ALEIXO, 2014). A rede "BBC diz que existem atualmente 15,5 milhões de bitcoins em circulação, cada uma valendo cerca de 392 euros (449 dólares)" (BRITO, 2016). Seu verdadeiro criador ainda permanece desconhecido sob o pseudônimo Satoshi Nakamoto (WEUSECOINS, [201-]), mas fortes indícios recaem sobre o programador australiano Craig Steven Wright (GREENBERG; BRANWEN, 2015), que pode se tornar um dos principais personagens das finanças internacionais nos próximos anos.

Finalmente, no que respeita à segurança internacional, vê-se que, a partir do final dos anos 2000, Estados nacionais modificam sua política externa e de Defesa[22], abarcando o que se conhece por Defesa Cibernética, a qual diz respeito às "[...]relações entre os Estados, como [...]o poder cibernético e [a] guerra cibernética" (PORTELA, 2016, p. 103). Assim, criam-se instituições e doutrinas militares para atuar em um novo domínio, o ciberespaço; desenvolvem-se armas cibernéticas, a fim de satisfazer objetivos nacionais permanentes por meio da atuação conjunta de especialistas em informática – ou, nos dizeres de Clarke e Knake (2015, p. 32-59), guerreiros cibernéticos (*cyber warriors*) – com estratégias clássicas de sabotagem e Inteligência. Recentemente, visualizam-se ataques cibernéticos (*cyber-attacks*) acompanhados por ataques bélicos convencionais. É nesse contexto mais extremado que um *vacum legis* internacional ainda persiste quanto aos chamados crimes de guerra cibernética[23], embora haja esforços importantes no sentido de mitiga-los, como o caso do Manual Tallinn, encabeçado pela Organização do Tratado do Atlântico Norte (OTAN).

Some-se a isso a atuação de indivíduos[24] e grupos não estatais[25] no ciberespaço e ter-se-á um panorama do atual contexto internacional em que se insere CiberRI. Como se vê, há várias possibilidades para a inferência internacionalista, quando se une ciberespaço a relações internacionais e/ou a RI. Todavia, para situar de maneira mais precisa a defesa de CiberRI, esta Tese se foca nos aspectos securitários que envolvem tal união.

Para tanto, utilizam-se pressupostos dos Estudos de Segurança Internacional (ESI), sob a justificativa precípua de este autor ter estudado e trabalhado com os dois mundos que aqui se pretendem correlacionar, quais sejam: ciberespaço e RI, a partir da perspectiva securitária. Trata-se, pois, de *insights* acumulados ao longo de quase uma década, que acabam por culminar com a intuição[26] de se criar um subcampo ciberinternacionalista. Intuição, aqui, diz respeito a

---

[22] Para o caso específico dos países nórdicos, ver Rantapelkonen e Kantola (2013). Para o caso específico da condução da política externa estadunidense atrelada à sua política de Defesa Cibernética, ver Sanger (2012) e Vilar Lopes e Oliveira (2014).

[23] Ou, nas palavras de Portela (2016, p. 101), "atos de guerra no espaço cibernético".

[24] A exemplo de Bradley/Chelsea Manning, Edward Snowden e Julian Assange, responsáveis por grandes vazamentos de informações governamentais secretas e com ampla reverberação na mídia internacional. Cf. BESSA, 2014.

[25] Tais como: hacktivistas mais técnicos como Anonymous e LuzSec ou mais políticos e espalhados, por exemplo, pela América Latina (cf. SORJ; FAUSTO, 2016); *cypherpunks* que deram suporte à Primavera Árabe (ASSANGE *et al*., 2013, p. 5, 22); e, até mesmo, terroristas cibernéticos do *Daesh*/Estado Islâmico (EI) e do Boko Haram. Vale dizer que os estudos sobre a atuação terrorista nas redes sociais têm crescido vertiginosamente nos últimos anos, a exemplo do que faz o grupo de Inteligência SITE ([201-]).

[26] Não confundir intuição com especulação, que, no âmbito científico, tem a ver com Filosofia, e não com CP (SARTORI, 1981, p. 30; WALLERSTEIN *et al*., 1996, p. 23-24, 36). Gil (1999, p. 35) também aponta que, em linguagem popular, é assaz comum identificar especulação com teoria; aqui, logicamente, isso não se sustenta.

"[...]uma condensação de conhecimentos anteriores[, a]ssuntos e experiências diferentes[...]" (CERVO; BERVIAN; DA SILVA, 2010, p. 48). Pode-se dizer que o passo seguinte à intuição é "[...]a antevisão, como substituto da previsão, [que] continua desempenhando um papel extremamente importante entre as atividades do cientista" (RUDNER, 1969, p. 100).

Talvez, essa aproximação estreita possa levantar questionamentos quanto à validade ou ao enviesamento do presente trabalho, uma vez que, "[e]m ciência política, o observador é ao mesmo tempo sujeito e objeto" (DUVERGER, 1962, p. 277). Quanto a isso, reconhece-se que, embora existam juízos de valor na discussão científica (VOEGELIN, 1982, p. 25; WEBER, 2006, p. 15) e que, "[h]oje, a introspecção tem má reputação científica" (DUVERGER, 1962, p. 277), este trabalho leva em conta que "[...]o conhecimento científico se atém aos fatos [e] não está subordinado aos caprichos da subjetividade do cientista" (COHN, 2006a, p. 9), ainda que não pareça "[...]possível excluir inteiramente essa auto-observação" (DUVERGER, 1962, p. 277)[27]. Acredita-se que tal justificativa evidencie a imparcialidade deste intento e as pertinências temática e pragmática que se espera da inferência social, em sentido lato, e dos estudos internacionalistas sobre o ciberespaço, em sentido estrito, os quais ainda são, por falta de analistas internacionais especializados nessa seara, uma esfera quase que exclusiva dos cientistas da computação (NYE JR, 2011a, p. 18; PORTELA, 2016, p. 96).

Tendo em vista que a proposição de um subcampo científico – ainda mais, um que seja internacionalista – não goza de extensa bibliografia[28], emprestam-se algumas ferramentas, estratégias e literatura de outras áreas, tendo sempre como fio condutor a noção de se defender CiberRI com o auxílio de autores clássicos[29] e atuais[30] de Ciências Sociais, CP e RI. Nesse

[27] Essa preocupação com a subjetividade/subjetivismo do pesquisador repousa, em última instância, em discussões metodológicas sobre a questão da "neutralidade científica" e da "objetividade das ciências sociais". Pode-se conferir tal preocupação nos estudos de: ciências sociais, em Bruyne, Herman e Schoutheete (1991, p. 203), Gil (1999, p. 22-23, 39, 45, 50, 52, 110-111), Kawamura (1986, p. 29-30, 34-35), Megale (1990, p. 151, 167-168), Rudner (1969, p.104-125), Wallerstein *et al.* (1996, p. 77-79, 110-111, 114, 128-131) e, principalmente, Weber (2016, p. 559-610); CP, em Cesarini e Hite (2004, p. 6), Sartori (1981, p. 41-43, 193-196) e Voegelin (1982, p. 23-25); RI, em Clarke e Knake (2015, p. 3) e Jackson (2011, p. 126-135); Filosofia da Ciência Social, em Rudner (1969, p. 15); e Web, em Baeza-Yates e Ribeiro-Neto (2013, p. 106).

[28] Quem mais se aproxima disso é Buzan e Hansen (2009; 2012), para com os ESI, embora eles não proponham a criação de um subcampo, e sim a reordenação de um já existente.

[29] Por meio dos clássicos, busca-se autenticar epistemologicamente a *raison d'être* de CiberRI, evitando seus erros de anacronismo. Sobre tal assunto em: Ciências Sociais, ver Albuquerque (2008, p. 120), Cohn (2006c, p. 110) e Megale (1990, p. 17, 36-40, 127-150, 179-200); CP, Lipson (1967, p. 506-511) e Voegelin (1982, p. 18); e RI, Resende (2005, p. 15-17).

[30] Os quais trazem a componente *cibernética* para as discussões internacionalistas. Por se tratar de uma temática recente em RI, faz-se necessário, pois, beber da fonte de outras áreas do conhecimento não ligadas às ciências sociais.

prisma, frisa-se efusivamente que CiberRI analisa temas e fatos afeitos ao espaço cibernético, a partir dos elementos metateoréticos de seus campos-*master*.

Ressalta-se também que se assume aqui uma posição em relação à *independência* de RI em relação à CP, cuja discussão reside, em última instância, no fato de que toda ciência faz "[...]parte de um todo bem maior, [que] tem como ele relações de dependência e de interdependência entre as várias disciplinas deste todo" (MEGALE, 1990, p. 57). Nesse viés, reconhece-se o seguinte silogismo factual: se RI origina-se da CP, e esta faz parte do cerne das ciências sociais modernas (WALLERSTEIN *et al*., 1996, p. 49), então RI também é uma ciência social[31]. Apesar de básica, é a partir dessa premissa que se busca validar a defesa de um subcampo pertencente a uma ciência social que enfatiza aspectos cibernéticos, e não de uma ciência exata que enfatiza aspectos sociais, como o faz, por exemplo, a Cibernética.

Outra questão que merece atenção é o nome que se escolhe para o subcampo ciberinternacionalista. Apesar de os termos "Relações Internacionais Cibernéticas" e "CiberRI" surgirem no Brasil por meio deste autor em 2014, não se confunde tal proposta com seus homógrafos ingleses "*Cyber International Relations*" e "*Cyber-IR*", pois, mesmo que sejam a tradução literal para designar trabalhos e projetos de pesquisas pré e pós-2014, não propõem a sistematização do conhecimento ciberinternacionalista, sob o guarda-chuva de um subcampo científico de RI[32].

Diante dessa contextualização temática e assumindo que (i) "toda investigação nasce de algum problema observado ou sentido, de tal modo que não pode prosseguir a menos que se faça uma seleção da matéria a ser tratada" (CERVO; BERVIAN; DA SILVA, 2010, p. 29), e (ii) que, "[q]uando os conhecimentos disponíveis sobre determinado assunto são insuficientes para a explicação de um fenômeno, surge o *problema*" (GIL, 1999, p. 30, grifo nosso), esta Tese debruça-se sobre o seguinte *problema de pesquisa*: de que maneira a criação de CiberRI impacta o campo de RI?

Como forma de responder à pergunta acima, defende-se a *hipótese principal* de que a criação de CiberRI (*X*), ao oferecer um modelo de sistematização do conhecimento internacionalista sobre o ciberespaço (*w*), potencializa o aperfeiçoamento do próprio campo de RI (*Y*)[33]. Como um dos pontos nevrálgicos de uma Tese de Doutorado é justamente sua hipótese principal, realizam-se algumas considerações sobre a mesma.

---

[31] Cf. MEGALE, 1990, p. 57.

[32] Para mais detalhes dessa diferenciação, ver subseção 2.1, *infra*.

[33] Como lembra Gil (1999, p. 58, grifo do autor), "[n]a pesquisa, a variável independente é indicada pela letra *x* e a dependente pela letra *y*". Conferir também Sartori (1981, p. 235). Alguns metodólogos podem questionar o tipo

Van Evera (1997, p. 10-15) afirma que, para validar, de forma precisa, uma hipótese principal, ela deve aparecer no formato de diagrama de setas, o qual representa as relações entre suas variáveis (BERG, 2001, p. 262). Assim, configura-se o seguinte esquema para a hipótese apresentada acima: $X \rightarrow w \rightarrow Y$, em que:

- *X* é a variável independente "criação de CiberRI", que, neste caso, também se configura como a variável de estudo[34] da hipótese principal;
- *w* é a variável interveniente "modelo de sistematização do conhecimento internacionalista sobre o ciberespaço", a qual se liga à variável independente, mas que não é suficiente para, sozinha, explicar os efeitos de CiberRI em RI; e
- *Y* é a variável dependente "aperfeiçoamento de RI".[35]

A hipótese principal, *supra*, também pode ser disposta, via silogismo hipotético[36], na seguinte forma condicional: se subcampo existir, potencializará o aperfeiçoamento de seu campo-*master*; ora, cria-se CiberRI (*X*); logo, campo de RI é potencialmente aperfeiçoado (*Y*), mediante, dentre outros, a oferta de um modelo de sistematização do conhecimento internacionalista sobre o ciberespaço (*w*). Assim, em razão de sua configuração, a hipótese principal constitui também uma explanação específica[37], e não uma teoria[38], a saber: CiberRI

---

da hipótese principal que aqui se apresenta como sendo o de uma relação causal, embora seu conteúdo explicite um certo viés normativo, e não empírico, tão comum para aquelas. Não se trata, portanto, de uma aberração metodológica, e sim de uma tentativa de amalgamar CP e RI, de um lado, e Filosofia da Ciência Social, de outro, prevalecendo aquelas e seus efeitos sobre esta. Novamente, Gil (1999, p. 59) rememora que "[...]as hipóteses elaboradas nas ciências sociais não são rigorosamente causais; apenas indicam a existência de algum tipo de relação entre as variáveis". Para Sartori (1981, p. 48), essa busca por relações causais nas ciências naturais se chama "determinação causal", já nas sociais, "indeterminação causal"; por certo, a hipótese principal se equipara mais à segunda.

[34] Em CP, a variável de estudo, que pode ser qualquer variável, é aquela cujas causas ou efeitos buscam-se descobrir com a pesquisa (VAN EVERA, 1997, p. 11). No caso da supracitada hipótese principal, o que se busca conhecer são os possíveis efeitos de CiberRI em RI.

[35] A terminologia das variáveis que se utilizam aqui advém de Marconi e Lakatos (2003, p. 138-140).

[36] Sobre tal assunto, ver Cervo, Bervian e Da Silva (2010, p. 47).

[37] Isso se afirma porque a hipótese principal satisfaz os seguintes quatro requisitos: (i) pode ser deduzida de uma teoria geral, que, neste caso, é a de que subcampos científicos, quando bem estruturados, tendem a aperfeiçoar seus campos-pai; (ii) CiberRI pode potencializar o aperfeiçoamento de RI, mas não explica os aperfeiçoamentos que se potencializam sem ou antes de sua criação; (iii) conhece-se a condição antecedente do caso, ou seja, a produção de conhecimentos internacionalistas sobre o ciberespaço, altamente fragmentada e sem intercâmbios acadêmicos; e (iv) os fenômenos intervenientes dessa teoria geral também se observam com a criação de CiberRI, qual seja: a necessidade de sistematização do conhecimento fragmentado para explicar, de forma sistemática, acontecimentos ciberinternacionais. Frisa-se que o dedutivismo do primeiro requisito diz respeito à Filosofia da Ciência e se aplica a campos científicos, e não a fatos sociopolíticos ou acontecimentos internacionalistas. Acerca de explanação específica, consultar Van Evera (1997, p. 40-43).

[38] Embora esta não seja uma Tese de Cientologia ou de Filosofia da Ciência, até que se pode pensar na seguinte *prototeoria*: a excessiva fragmentação temática do conhecimento científico gera a necessidade de novos subcampos, os quais potencializam o aperfeiçoamento de seus campos-*master*. Sobre tal assunto metodológico,

potencializa o aperfeiçoamento de RI. Como a próxima seção busca evidenciar, trata-se, pois, de um processo retroalimentar, e não tautológico.

Aqui, faz-se necessário também ressaltar a problemática questão da dedução nas ciências sociais, tendo em vista que o silogismo acima, por ser um protótipo do raciocínio dedutivo (GIL, 1999, p. 27), implicitamente a emprega. A dedução, enquanto método científico racional que parte do geral e desce para o particular (GIL, 1999, p. 27), pode possuir dois vieses. No primeiro, é a uma técnica de pensamento ou raciocínio (CERVO; BERVIAN; DA SILVA, 2010, p. 29; DUVERGER, 1981, p. 32) assaz usada, por exemplo, pela escolástica antiga (WEBER, 2006, p. 97-98) e pelas ciências naturais para testar leis universais[39], cuja aplicação em ciências sociais, CP e RI é deveras criticada (DUVERGER, 1981, p. 31-32; GIL, 1999, p. 28; JACKSON, 2011, p. 18; VOEGELIN, 1982, p. 20-2; WEBER, 2006, p. 45, 50, 97). No segundo viés, configura-se como uma abordagem típica de desenhos de pesquisa quantitativa (SOUSA; DRIESSNACK; MENDES, 2007), como a que se realiza na subseção 3.2, *infra*. Não se deve, portanto, confundir esse segundo viés de dedução aplicada à ação e ao fato social – na formulação de "leis sociais universais" – com a da lógica metodológica de se testar e refutar hipóteses[40]. Por exemplo, a hipótese principal aqui apresentada diz respeito a um subcampo científico, e não a acontecimentos e fatos propriamente ditos.

Feita essa ressalva, segue-se com a análise pormenorizada da hipótese principal, mediante sua decomposição nas seguintes *hipóteses secundárias*:

i. a criação de CiberRI passa pela oferta de um modelo de sistematização que ajude a corrigir o problema da excessiva fragmentação do conhecimento internacionalista sobre o ciberespaço;
ii. o aperfeiçoamento de RI é traduzido em termos de fomento ao tripé universitário ensino-pesquisa-extensão; e
iii. é possível evidenciar o aperfeiçoamento que CiberRI pode potencializar a RI tanto em casos gerais quanto específicos.

Se se assumir como verdadeira a máxima de que as principais funções de uma hipótese são (i) a generalização da experiência do autor para com o tema, (ii) a ampliação dos dados

---

conferir Van Evera (1997, p. 40). Para um exemplo de silogismo empregado para dar mais cientificidade ao campo de RI, *vide* Jackson (2011, p. 10).

[39] Do tipo "$(x)[fx \supset gx]$", em que, para qualquer *x*, se este contiver *f*, então conterá também *g*. Cf. Rudner (1969, p. 90).

[40] Cf. CERVO; BERVIAN; DA SILVA, 2010, p. 46-47; GIL, 1999, p. 27-28, 30; MEGALE, 1990, p. 66; POPPER, 2008. Certamente, o exemplo mais notório desse primeiro viés é a lógica hipotético-dedutiva (GIL, 1999, p. 29-31), exemplificada pela rejeição à indução, contida na metáfora do cisne negro, de Popper (2008).

empíricos e (iii) a possibilidade de servir de guia à investigação (MARCONI; LAKATOS, 2003, p. 131), então a hipótese principal desta Tese tende a (i) generalizar a experiência acadêmica de seu autor para com o ciberinternacionalismo, (ii) ampliar – e amplificar – os dados sobre esse tema e (iii) ser uma referência para estudos nessa seara.

Diante disso, projeta-se como *objetivo geral* o de defender um subcampo de RI que se volte, de forma sistematizada, aos estudos internacionalistas sobre o ciberespaço. Para tanto, assim como ocorre com a hipótese principal, opta-se também por subdividir o objetivo geral em três *objetivos específicos*, a saber:

- propor um modelo que sistematize a excessiva fragmentação temática dos estudos ciberinternacionalistas;
- definir os limites e potencialidades dos estudos ciberinternacionalistas no ensino, na pesquisa e na extensão de RI; e
- evidenciar como CiberRI pode potencializar o aperfeiçoamento de RI na política internacional, em geral, e no caso brasileiro, no específico.

Tendo em vista que os objetivos específicos, em conjunto, têm o fito de "[...]identificar novos aspectos ou, mesmo, utilizar os conhecimentos adquiridos com a pesquisa, para[...] intervir em determinada realidade em que ocorre o problema" (CERVO; BERVIAN; SILVA, 2010, p. 75), a presente Tese busca intervir diretamente na realidade de RI, ofertando-lhe um novo subcampo.

A *justificativa* para este empreendimento encontra eco em seu próprio marco teórico, os ESI, quando aplicado aos casos concretos. Por exemplo, Demchak (2014, p. vi) frisa que, dentre políticos, militares e acadêmicos, só estes últimos ainda resistem em se adaptar às características dessa nova era, impregnada daquilo que ela chama de conflitos envoltos pelo ciberespaço ou *cybered conflicts* (DEMCHAK, 2013; 2014). Nessa mesma via de pensamento, o ex-Secretário-Geral da OTAN Javier Solana lembra que "responder a ameaças do século XXI com ferramentas do século XX não é uma boa ideia" (SOLANA, 2015, tradução nossa[41]). Esse também não parece ser o melhor caminho para a renovação das ciências sociais, especialmente CP e RI. Nesse viés, Colin S. Gray aponta que, apesar de a literatura técnica e tática sobre o ciberespaço ser abundante, seu tratamento à luz dos ESI é escasso e pobre (LOVELACE JR, 2013, p. iii). Portanto, esta Tese pretende também responder, quantitativa e qualitativamente, aos anseios de outros subcampos internacionalistas, preenchendo tal lacuna, de forma cientificamente sistematizada.

[41] Texto original: "*Responding to twenty-first-century threats with twentieth-century tools is a bad idea*".

Com relação à *metodologia*[42] aplicada a este trabalho, começa-se por sua *técnica de abordagem do método científico*. Tendo em vista que, de um lado, "[o] método de uma ciência *é*, com efeito, o fundamento lógico em que baseia a sua aceitação ou rejeição de hipóteses ou teorias" (RUDNER, 1969, p. 19) e, do outro, a forma com que se sucedem os objetivos específicos, esta Tese se guia pela seguinte lógica: (i) apresentar os limites e objeto de CiberRI; (ii) demonstrar sua viabilidade no ensino, pesquisa e extensão de RI; e (iii) evidenciar seus impactos, em termos qualitativos e quantitativos, gerais e específicos, em RI. A fim de concretizar tal método, escolhem-se as seguintes *técnicas de pesquisa*:

i. *descrição*, para contextualizar os tema, problema de pesquisa, primeira hipótese secundária e primeiro objetivo específico;
ii. *análise*, com vistas a corroborar as segunda e terceira hipóteses secundárias, bem como atingir os segundo e terceiro objetivos específicos, mediante a *coleta de dados* nas mais diversas fontes, tais como as publicações acadêmicas, a própria Web e os jornais[43]; e
iii. *síntese*, consequência direta da análise (CERVO; BERVIAN; DA SILVA, 2010, p. 33), que, neste caso, visa corroborar a hipótese principal e, por fim, atingir o objetivo geral, evidenciando, assim, a perspectiva da "[...]ciência política como de uma ciência de síntese" (DUVERGER, 1981, p. 32).

A coleta de dados mostra-se, portanto, vital para a primeira e a terceira partes desta Tese e exige técnicas apropriadas. Já a análise propriamente dita dos dados é fulcral para as segunda e terceira partes, necessitando, por seu turno, de ferramentas específicas, haja vista que, "além da escolha de seus objetos de estudo, uma disciplina [que se quer ver] estabelecida também é definida pela escolha de métodos de coleta e análise de dados" (AMORIM NETO; SANTOS, 2015, p. 25, tradução nossa[44]).

---

[42] Os conceitos de método e de técnicas de abordagem, pesquisa e coleta de dados são de Cervo, Bervian e Da Silva (2010, p. 25-35, 43-54) e sua diferenciação em relação à metodologia provém de Megale (1990, p. 66-67). Já a nomenclatura "estilo de pesquisa" advém da obra seminal de King, Keohane e Verba (1994, p. 3-7).

[43] Sobre a documentação indireta que se utiliza aqui para pesquisar sobre CiberRI, replica-se o seguinte argumento feito em 1962: "Muitos documentos não têm relação direta com os problemas políticos[...][,] mas são suscetíveis de fornecer indicações ou ainda permitir situar melhor as bases das questões estudadas" (DUVERGER, 1962, p. 95). Após 37 anos, esta parece ser também a linha de raciocínio que Gil (1999, p. 65) segue, ao afirmar que "[e]m muitas situações, não há outra maneira de conhecer os fatos passados senão com base em dados secundários" e atualizados (*ibid*., p. 78) como os jornais (*ibid.*, p. 160, 164). Para uma análise crítica sobre publicações científicas em jornais – e que repousa, em última instância, na distinção entre publicação e publicidade –, ver Bourdieu (1983b, p. 127).

[44] Texto original: "[...]*además de la elección de sus objetos de estudio, una disciplina consolidada se define también por la elección de los métodos de recolección y análisis de datos*".

A fim de auxiliar a estratégia metodológica e o desenho de pesquisa, utilizam-se *técnicas de coleta de dados* que se baseiam não apenas em aspectos metodológicos de CP e RI[45], mas também em outras áreas, tais como Terminologia[46] e Infometria[47]. Após a coleta dos dados, segue-se o seu julgamento com o auxílio da análise de conteúdo, uma técnica de pesquisa "[...]geralmente usada para uma série ou coleção de revistas científicas[...], de bibliografia sobre um tema ou uma área de conhecimento, de produção de livros ou revistas de determinado período ou de determinada instituição[...]" (MEGALE, 1990, p. 32). A última ferramenta que se utiliza aqui é o *Nested Analysis*, uma estratégia metodológica desenvolvida por Lieberman (2005) e assaz empregada em Política Comparada, que vai além dos debates sobre metodologias qualitativas e quantitativas nas ciências sociais, trazidos sobretudo por King, Keohane e Verba (1994), ao postular a mescla desses dois estilos de pesquisa, e não a sobreposição de um sobre o outro. Acredita-se que a pluralidade e a combinação desses métodos possam auxiliar na defesa da terceira hipótese secundária e do terceiro objetivo específico, haja vista que "[...]nem sempre um único método é suficiente para orientar todos os procedimentos a serem desenvolvidos ao longo da investigação" (GIL, 1999, p. 33).

A fim de facilitar a experiência do leitor, segue-se aqui os exemplos de Barros (2004, p. 23), que, "[p]ara maior fluidez da leitura dos [seus] textos", traduz "as citações em língua estrangeira[...]", colocando a citação original em nota de rodapé. Põem-se também as referências das citações indiretas que ocupam mais de duas linhas em notas de rodapé. As abreviaturas e siglas só figuram na Lista de Abreviaturas e Siglas, *supra*, se, e somente se, aparecerem mais de uma vez no *corpus* desta Tese – ainda que seja em nota de rodapé. Com exceção do acrônimo CiberRI e do já consagrado substantivo ciberespaço, opta-se, ao longo do texto, pelo adjetivo cibernético, após os termos compostos que dizem respeito ao ciberespaço, em vez do prefixo ciber. Pegue-se, por exemplo, a forma "ciberguerra", que, apesar de ser aceita, opta-se por "guerra cibernética", pois é essa a forma que o Ministério da Defesa

[45] O uso de métodos de outras áreas é celebrado por Duverger (1981, p. 33-34) na CP e por Jackson (2011, p. 19-20) nas RI.

[46] Ciência que estuda as linguagens de especialidade e seu vocabulário (BARROS, 2004, p. 21). Para CP, ela é de fundamental importância, pois "[a] linguagem fornece provas esclarecedoras[...], desde que as origens de nossas ideias hão de ser encontradas nas raízes das palavras que as exprimem" (LIPSON, 1967, p. 87). Sartori (1981, *passim*) também dá bastante ênfase no estudo da linguagem para a política e para CP. Como se defende que CiberRI se torne um ramo científico, natural que possua seus próprios termos, ou, como dizem os clausewitzianos, sua própria gramática. Nesse prisma, ver glossários em Guedes Oliveira, Gama Neto e Vilar Lopes (2016, p. 203-210), Lopes (2013, p. 118-120) e Nascimento (2015, p. 150-151).

[47] Ciência que mede informações técnico-científicas por meio da mescla de métodos originários da Biblioteconomia e da Ciência da Informação. Cf. subseção 2.4.2, *infra*.

brasileiro utiliza oficialmente e, também, por ser a tradução literal do título da obra seminal de Clarke e Knake (2012; 2015).

A divisão desta Tese busca ser a mais didática possível e, em certa medida, corresponder às exigências onomatológicas do conhecimento científico de que fala Sartori (1981, p. 190), quais sejam: "em primeiro lugar, a definição e a estabilização (relativa) dos seus conceitos; em segundo lugar, a criação de novos termos, para poder dispor de vocabulário adequadamente preciso e articulado; [e] em terceiro lugar, a adoção de uma sintaxe lógica precisa".

Desse modo, cada uma das três seções principais engloba, respectivamente, uma das três hipóteses secundárias e um dos três objetivos específicos. Na primeira seção, definem-se os conceitos, explanam-se as terminologias que aqui se utilizam, delimita-se o objeto de estudo de CiberRI e propõe-se um modelo para sistematizar o conhecimento internacionalista sobre o ciberespaço. Na segunda seção, atesta-se a pertinência de CiberRI à luz do ensino, da pesquisa e da extensão em RI. E, na última seção, aplica-se CiberRI, mediante a análise do impacto do que se chama aqui de *Software Power* na política internacional e dos trabalhos publicados nos anais do Encontro Nacional da Associação Brasileira de Estudos de Defesa (ABED), o ENABED. Conclui-se com a refutação ou não da hipótese principal, bem como o atingimento ou não do objetivo geral. A Figura 1 apresenta, graficamente, a macrovisão desta Tese.

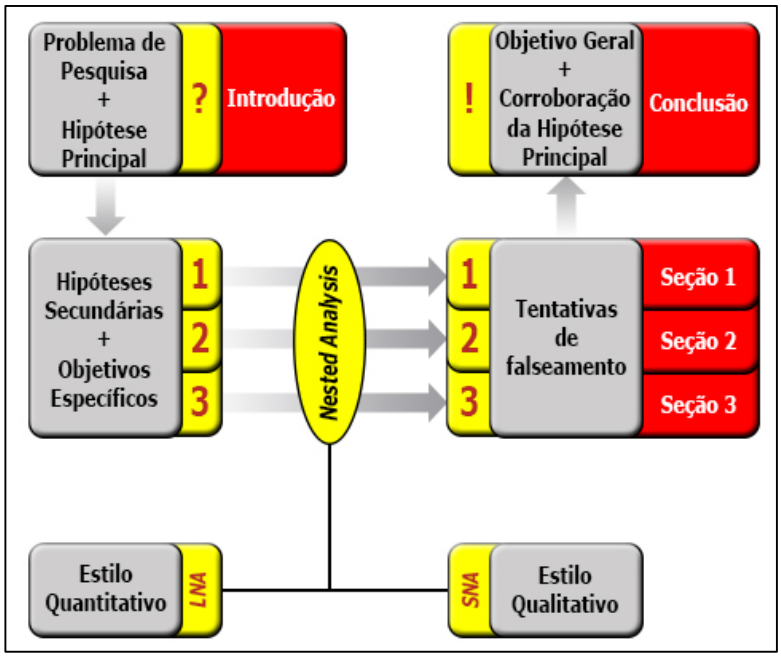

Figura 1 Macrovisão desta Tese
Fonte: Elaboração própria.
Legenda: LNA = *Large-N Analysis*; SNA = *Small-N Analysis*.

1 DAS RELAÇÕES INTERNACIONAIS CIBERNÉTICAS

> As definições só têm valor em [M]atemática ou em [D]ireito, porque elas criam o próprio objeto[...]. Nas ciências de observação, as definições são apenas sínteses provisórias de fatos já conhecidos, que a descoberta de outros fatos recoloca constantemente em foco[...]. (DUVERGER, 1981, p. 9).

Esta primeira seção é essencialmente exploratória. Isso se justifica porque seu tema – as relações internacionais cibernéticas – é deveras genérico, tornando necessários "[...]seu esclarecimento e delimitação, o que exige revisão da literatura[...]", cujo "produto final deste processos passa a ser um problema mais esclarecido, passível de investigação[,] mediante procedimentos mais *sistematizados*" (GIL, 1999, p. 43, grifo nosso). Assim, para situar o tema – o qual constitui, concomitantemente, o próprio objeto de CiberRI –, faz-se mister realizar diferenciações e definições. Mas, como aponta a citação, *supra*, do cientista político[48] francês, questiona-se muito essa busca por definições exaustivas, no âmbito das ciências de observação, como é o caso das ciências sociais (GIL, 1999, p. 34), e, aqui, especificamente de CP e RI. Sintetizar fatos é, portanto, a missão precípua de seus cientistas, e, como não pode deixar de ser, é o que ilumina esta seção, ao mesmo tempo em que busca concretizar o primeiro objetivo específico, qual seja o de propor um modelo que sistematize a fragmentação temática dos estudos internacionalistas sobre o ciberespaço. Assim, projetam-se alguns passos para se concretizar tal intento.

O primeiro deles é definir, em termos metateoréticos, o que é ciberinternacionalismo, à luz do que se conveniou a chamar de ciência. Para isso, tem-se em mente a advertência de que invocar o termo *ciência* – "[...]que é sobretudo uma inquietação ocidental[...]" (MOREIRA, 2015, p. 15) – em trabalhos acadêmicos é também, nos dizeres de Jackson (2011, p. 15), "brincar com fogo", embora esse mesmo autor afirme que "simplesmente remover a pretensão de 'ciência' das discussões de RI é um esforço inútil" (JACKSON, 2011, p. 18, tradução nossa[49]). Assumem-se, pois, os riscos de tal invocação, à medida que se propõe uma espécie de *oximoro científico* para caracterizar o estágio atual de CiberRI, ou seja, conceituá-lo como um subcampo especializado e interdisciplinar por excelência. Isso porque uma definição de subcampo científico leva em conta, de um lado, "[...]as consequências da *especialização* que tende a reduzir, sem cessar, o universo dos concorrentes pela divisão em *subcampos* cada vez mais *estreitamente especificados*" (BOURDIEU, 1983b, p. 144, grifo nosso) e, de outro, a

---

[48] O próprio Duverger (1981, *passim*) prefere "politicólogo" a "politólogo" como tradução alternativa a *political scientist*.

[49] Texto original: "*Simply removing the claim to 'science' from IR discussions is, therefore, probably quite a futile endeavor*".

necessidade, cada vez maior, de "abrir as ciências sociais" (WALLERSTEIN *et al.*, 1996, *passim*) – e, em especial, RI – à permeabilidade de outras ciências, sobretudo as não sociais. Agindo dessa forma, busca-se evitar a crítica de Fragoso Filho (1984, p. 25) de que "[o]s cientistas perderam, em parte, a visão globalizante das ciências, para se embrenharem na ótica estrábica da 'sua' especialidade".

Outro passo para os desígnios desta Tese é delimitar o objeto de estudo de CiberRI. Todavia, diante de termos homógrafos que designam tanto um campo científico quanto seu objeto – tais como História, Redes de Computadores, RI e Segurança Internacional –, confusões entre nomenclaturas são corriqueiras e, em certa medida, até mesmo aceitáveis.[50] Nesse viés, ratifica-se que o objeto das Relações Internacionais Cibernéticas são as próprias relações internacionais cibernéticas, porém aquelas não criam estas, que lhes são *ex-ante*. Contrariamente, no âmbito de ciências não sociais, como Ciência da Computação e Ciência da Informação, o ciberespaço – elemento vital para CiberRI – é também um de seus próprios objetos e é também *ex-post* a eles.

Surge, então, a indagação de como juntar esses dois mundos acadêmicos e aparentemente distantes sob o guarda-chuva de um subcampo internacionalista. Ou, utilizando as estritas palavras de Wallerstein *et al.* (1996, p. 15, 100-101), como unir as "duas culturas" científicas que delimitam, por séculos, as ciências de experimentação e as de observação? Quanto à seara das ciências não sociais, este autor reconhece não ter sugestões; quanto à de RI, propõe a seguinte alternativa.

1.1 Unindo terminologias de "culturas" distintas, porém não tão distantes

Embora não se possa chegar a um consenso sobre o que é ciência (GIL, 1999, p. 20; SARTORI, 1981, p. 158), a "questão da ciência" – conceito vital para a Filosofia da Ciência e, portanto, para a Filosofia da Ciência Social – tem sido abordada pelos estudiosos de relações

[50] Prova disso é a falta de capitulação, em praticamente todo trabalho acadêmico, para designar o objeto principal de um campo, ciência ou Área do Conhecimento quando, na realidade, quer se referir ao próprio campo, ciência ou Área. Retomando os mesmos exemplos, *supra*, têm-se: história, redes de computadores, relações internacionais e segurança internacional. Ver também definições de Jackson (2011, p. 217) e Sarfati (2011, p. 373) para "Relações internacionais" e "relações internacionais". Some-se a esse debate, para complicar ainda mais as querelas terminológicas dos campos e subcampos, o fato de (i) Wallerstein *et al.* (1996, p. 49, grifo nosso) falarem em "[...]uma *área do conhecimento* a que foi dado o nome de '*ciências sociais*'" ou Megale (1990, p. 11, grifo nosso) informar que "o vasto domínio das ciências sociais" compõem-se de "*disciplinas*", e (ii) existir o curso universitário de Ciências Sociais, que ora outorga o título de Cientista Social – que "[...]é o intelectual que se ocupa em produzir novos conhecimentos nas ciências sociais" (MEGALE, 1990, p. 166) –, ora faculta ênfase em Antropologia, Ciência Política ou Sociologia (BRASIL, 2002), que são, por sua vez, Áreas de Avaliação da CAPES. Termina-se aqui tal discussão, sem entrar em outras, ainda mais complexas, como Antropologia Política, Pensamento Político-social e Sociologia Política (cf. MEGALE, 1990, p. 90-91).

internacionais desde a criação de RI, um século atrás (JACKSON, 2011, p. 3, 9, 16, 192). Nesse sentido, torna-se mister realizar uma clara explanação dos critérios que fazem uma dada prática de produção de conhecimento[51] ser reconhecida como *científica* (JACKSON, 2011, p. 11), que, neste caso, diz respeito à produção sistemática do conhecimento sobre o ciberespaço no âmbito de um subcampo internacionalista.

Terminologicamente, observa-se que os textos são o principal *meio de transmissão do conhecimento* (BARROS, 2004, p. 21; LIPSON, 1967, p. 26-27). Apesar de se constituírem em dados pouco estruturados, mal definidos e ambíguos (FREITAS *et al*., 2006, p. 119, 121), eles possuem suas próprias especificidades sintática, semântica, pragmática e, especialmente, "[...]lexical, uma vez que é sobretudo por meio de uma terminologia própria que esse tipo de texto *veicula seus conhecimentos*" (BARROS, 2004, p. 21, grifo nosso).[52] Embora as "[...]questões de terminologia sejam um importante indicador do âmbito da matéria [do que é ciência], [elas] não nos colocam diante dos principais problemas a tratar" (RUDNER, 1969, p. 17). No que tange às questões terminológicas em CiberRI, há dois aspectos por trás das observações acima.

O primeiro aspecto diz respeito ao fato de que, atualmente, "[c]om o advento do computador, foi necessário *codificar o texto em dígitos binários*" (BAEZA-YATES; RIBEIRO-NETO, 2013, p. 190, grifo nosso), abrindo, assim, amplas possibilidades para se produzir, armazenar, coletar e transformar informações em dados brutos (FREITAS *et al.*, 2006, p. 119) no hipertexto, uma nova mídia cuja expressão maior é a Web, criada entre o final dos anos 1980 e início dos 1990 e que roda sobre a Internet. Em outras palavras, pode-se afirmar que "[a] Internet e a Web alteraram a maneira de coletar e de acessar dados textuais de toda natureza" (FREITAS *et al.*, 2006, p. 119), gerando impactos significantes para o progresso da ciência, e, logicamente, para ciências sociais como CP e RI. CiberRI, por seu turno, amplifica – mas não supervaloriza – essa característica.

Essa nova mídia fornece a base para se projetar a Linguagem de Marcação de Hipertexto (HTML) – que, sem dúvidas, é a linguagem *web* mais bem estabelecida (FREITAS *et al.*, 2006, p. 61) – e o Protocolo de Transferência de Hipertexto (HTTP), os quais, juntos, são os responsáveis por originar a World Wide Web (WWW) ou, simplesmente, Web (BAEZA-YATES; RIBEIRO-NETO, 2013, p. 98). Ainda, consoante Baeza-Yates e Ribeiro-Neto (2013,

[51] Como se busca incutir ao longo deste texto, o conceito de conhecimento, aqui, se atrela ao de ciência e vai na mesma direção de Jackson (2011, p. 2, grifo nosso), quando este analisa a busca por explicações racionais nas obras de John Locke e Carl Sagan: "[...]*science as a superior way of gaining and evaluating knowledge*".

[52] Resende (2005, p. 22) parece transpor essa mesma lógica lexical para a Internet.

p. 105, 258), a Web é um hipertexto livre, ou seja, um imenso banco de dados hipertextual que se prolonga ao longo do globo terrestre. Em termos menos políticos, diz-se que a Internet necessita de partes físicas (*hardware*) e lógicas (*software*) para existir e que o ciberespaço é um "[...]conceito que diz respeito à dimensão digital das nossas atividades" (BARRINHA; CARRAPIÇO, 2016, p. 246). Como se percebe, apesar de terem um sentido pareio, ciberespaço e Internet são coisas diferentes (PORTELA, 2016, p. 93).

Definir ciberespaço não é uma tarefa trivial (BETZ; STEVENS, 2011b, p. 36) também em CiberRI, haja vista suas várias interpretações (BEJTLICH, 2013; HOLLIS, 2010, p. 48; NYE JR, 2011b, p. 122). O termo em si não é novo. Seu radical, do grego *kyber*, significa navegar – ou, na expressão mais corriqueira, *to browser* –, daí, por exemplo, a ideia de "navegar na Internet", "navegador *web*" e "*browser* de Internet". Existe também a Cibernética, ciência que estuda os sistemas – geralmente automatizados – e que remonta aos estudos seminais do matemático Norbert Wiener, ainda em meados do século XX. Porém, não se deve confundir ciberespaço com Cibernética (PORTELA, 2016, p. 93), uma vez que, "[a]pesar da relação de sentido que atualmente podemos estabelecer com a Internet, o ciberespaço teve essencialmente origem numa ideia de ficção [científica], cuja denominação foi o produto da imaginação de [William] Gibson[...]" (BARRINHA; CARRAPIÇO, 2016, p. 246). De fato, o escritor estadunidense-canadense Gibson (2014) cunha o termo "ciberespaço" no início dos anos 1980 na obra *Queimando Cromo*[53], mas é com o *Neuromancer*[54] que essa palavra "[...]se popularizou e tornou-se, inclusive, sinônimo de world wide web", isto é, a ideia de ciberespaço como "uma espécie de realidade virtual que reina sobre toda a humanidade" (NOTA..., 2014, p. 16). Portanto, o "Cibernéticas", de CiberRI, advém dessa noção gibsoniana, já incorporada em grande parte da literatura analisada[55], a ponto de Libicki (1996, p. 9, 81-82) se referir à "guerra-Gibson" (*Gibson-warfare*) como uma dimensão virtual da guerra cibernética.

Já o segundo aspecto gira em torno da afirmação de que, "[...]quando um teórico busca compreender uma sociedade política, uma das suas primeiras tarefas, se não a primeira, será

[53] Cf. GIBSON, 2014, p. 354-374.

[54] Cf. GIBSON, 2014, p. 20-325.

[55] Cf. AGUILAR, 2010, p. 29; ARQUILLA; RONFELDT, 1993, p. 163; BEJARANO, 2010, p. 54; BENEDIKT, 1991, p. 1, 12; BETZ; STEVENS, 2011a, p. 9; 2011b, p. 36; CANONGIA; MANDARINO JÚNIOR, 2009, p. 25; CAVELTY, 2008, p. 57; CHOUCRI, 2012, p. 7; DEIBERT, 2012, p. 1; ERIKSSON; GIACOMELLO, 2006, p. 223; HOLLIS, 2010, p. 49, 53; KURBALIJA, 2013, p. 394; LIBICKI, 1996, p. 81; MACHADO, 2014, p. 32-34, 50; MALONE; MALONE, 2013, p. 158; MANDARINO JUNIOR, 2009, p. 61; NASCIMENTO, 2015, p. 15, 29; SINGER; FRIEDMAN, 2014, p. 13; SOMMER, 2007, p. 5; VAISHNAV, CHOUCRI; CLARKE, 2013, p. 19. Quem primeiro transpõe a noção gibsoniana de ciberespaço para descrever o "espaço socioeletrônico global" é John Perry Barlow, cofundador da Electronic Frontier Foundation (EFF) (SOMMER, 2007, p. 5) e autor do famoso manifesto *A Declaração do Ciberespaço* (AGUILAR, 2010, p. 29).

sempre a de *determinar o tipo humano que se expressa na ordem dessa sociedade* concreta" (VOEGELIN, 1982, p. 55, grifo nosso). Diante dessa indicação, adapta-se, aqui, a clássica ideia de animal político (*zoon politikón*) para animal cibernético (*zoon kybernētē*), entendido este como o indivíduo que, não obstante busque viver em sociedade, sente também necessidade de viver – e, às vezes, até mais – no ciberespaço. Embora criticável, é esse o tipo humano do século XXI que caracteriza grande parte das sociedades hodiernas. Essa ideia origina-se a partir da famosa obra *Política*, de Aristóteles[56], a qual se refere, *grosso modo*, ao ser humano enquanto aquele que sente necessidade de viver na *polis*, ou seja, em uma organização político-social com instituições artificiais (LIPSON, 1967, p. 23, 395, 399; MEGALE, 1990, p. 115; SARTORI, 1981, p. 158-160; VOEGELIN, 1982, p. 5, 33, 54). Essa máxima filosófica se transporta às ciências sociais, na medida em que estas passam a estudar a sociedade humana (LIPSON, 1967, p. 46), *i.e.*, "[...]as estruturas sociais que ele [o ser humano] mesmo criou e dentro das quais se move[...]" (WALLERSTEIN, 1996, p. 13). Logo, uma referência com o ciberespaço, enquanto uma dessas estruturas, seria inevitável, não obstante seus aspectos técnicos, muitas vezes, sobressaírem-se aos sociais. É nesse viés que Valente (2007, p. 15) apregoa que "[...]o advento da tecnologia digital, da internet e de recursos como a realidade virtual passou a interferir até mesmo na cognição humana". Por seu turno, Kawamura (1986, p. 96) sustenta que o sistema social faz parte dos seis "grandes sistemas" que se comunicam entre si, quais sejam: social, político, ambiental, econômico, administrativo e estrutural – sendo este formado pelas áreas de transporte, energia, telecomunicações, ciência e tecnologia.[57] Nesse prisma, projeta-se o ciberespaço como uma extensão do *sistema social*, a ponto de, até mesmo, este poder rivalizar com as demais topologias *naturais*[58]. Eis, portanto, o tipo de ser humano e de sociedade que CiberRI busca tocar.

Tais aspectos retomam, por conseguinte, para a discussão ontológica e epistemológica de CiberRI, o debate sobre a noção de um tipo especial, ambíguo (RUDNER, 1969, p. 22) e

---

[56] Segundo Voegelin (1982, p. 17), Aristóteles é um dos fundadores da CP. Porém, para Sartori (1981, p. 157, 176), falar em CP "perene" – isto é, que remonta aos gregos clássicos e, até mesmo, a Maquiavel – é uma futilidade. Para uma crítica à visão aristotélica, ver Hobbes (2005), Lipson (1967, p. 24, 48) e Voegelin (1982, p. 129). E, para uma brevíssima analogia à passagem do *antropo prometeico* para o *cibernantropo*, ver Resende (2005, p. 19), o qual, por seu turno, remete-se à obra de Lefebvre (1980).

[57] Pode-se dizer que o que Kawamura chama de *grandes sistemas*, Buzan, Wæver e Wilde (1998) chamam, com suas nuanças, é claro, de *setores*, no âmbito da teoria da securitização.

[58] Ver, por exemplo, a crescente literatura em ESI que associa o ciberespaço a uma nova topologia ou domínio, aos mesmos moldes da terra, do mar, do ar e, em certa medida, do espaço sideral. Cf. BRASIL, 2012a, p. 24; GRAY, 2013, p. 3, 8-12; NYE JR, 2011a, p. 19. Esta, porém, não é a visão de Raphael Mandarino Junior, que, por muitos anos, dirigiu o Departamento de Segurança da Informação e Comunicações (DSIC) da Presidência da República, o qual afirma não ver "[...]o espaço cibernético como um campo de batalhas" (BRASIL..., 2012).

polissêmico (MEGALE, 1990, p. 41) de conhecimento, o científico. Apesar de haver outras espécies de conhecimento – tais como o senso comum, o vulgar, o dogmático, o religioso, o folclórico e o de opiniões/conselhos/autoridade[59] –, ao conhecimento especificamente científico, fundado por Platão (VOEGELIN, 1982, p. 17), dá-se o nome de *scientia*, termo que significa, puramente, conhecimento (GIL, 1999, p. 20; WALLERSTEIN *et al*., 1996, p. 14). Todavia, Lipson (1967, p. 47), por sua vez, salienta que "[...]a palavra 'ciência' e a expressão 'ciência política' poderão dar origem a confusões, se forem consideradas com rigor demasiado[...]". É nesse sentido que se caracterizou o subcampo de RI como um *oximoro científico*, tendo em vista, também, que "infelizmente, filósofos [da ciência] não têm um consenso sobre o que define um campo de pesquisa como uma 'ciência' ou uma prática de produção de conhecimento como 'científica'" (JACKSON, 2011, p. 26, grifo nosso, tradução nossa[60]).

Sobre a produção de conhecimento no campo de RI, o próprio Jackson (2011, p. 3, grifo nosso, tradução nossa[61]) afirma que "o que está mais em jogo não é uma explicação específica de ciência, e sim *uma vaga e geral sensibilidade*". Com vistas a testar essa sensibilidade científica em RI, cuida-se, a partir de agora, das "duas culturas" que dividiram as áreas do conhecimento, até 1945 (WALLERSTEIN *et al*., 1996, p. 100), entre ciências humanas e naturais, tendo as sociais como suas intermediárias[62]. Essa divisão se mostra relevante para compreender não apenas *o que é* CiberRI, mas também o que *não é* CiberRI, e advém, sobretudo, do fato de que:

> Nas *ciências naturais*, as questões sujeitas a discussão resolvem-se, habitualmente, sem que se recorra às opiniões do objeto de estudo. Em contraste com essa situação, as pessoas[...] estudadas pelos *cientistas sociais* foram entrando cada vez mais na discussão, independentemente de sua opinião ser ou não solicitada pelos estudiosos[...]. (WALLERSTEIN *et al.*, 1996, p. 78, grifo nosso).

---

[59] Cf. GIL, 1999, p. 19-20; KAWAMURA, 1986, p. 19; MEGALE, 1990, p. 42-43, 48. Gil (1999, p. 20-21) chega a incluir, em certa medida, os ensinamentos filosóficos como não científicos, o que, certamente, Sartori (1981, *pasim*) não concorda.

[60] Texto original: "*Unfortunately, philosophers have come to no global consensus about what defines a field of inquiry as a 'science' or a practice of knowledge-production as 'scientific'*".

[61] Texto original: "[...]*what is most often in play is not a specific account of science, but a vague and general sensibility*".

[62] Com as reformulações das ciências sociais, cada vez mais adaptadas ao espírito do seu tempo – e, consequentemente, autoquestionando-se criticamente –, Wallerstein *et al.* (1996, p. 101) sugerem a existência de uma "terceira cultura", a das próprias ciências sociais, as quais, arrisca-se a dizer, alevanta-se juntamente com a crescente importância da Grande Área de Ciências Humanas no Brasil.

Se, por um lado, "[...]o desenvolvimento tecnológico, no sentido da transformação material, fundamentou-se no desenvolvimento das *ciências naturais*", por outro, "o desenvolvimento do 'saber fazer' para a integração do homem à máquina e dos homens entre si, no processo produtivo, teve por base o avanço das *ciências humanas*" (KAWAMURA, 1986, p. 20, grifo nosso). É na ênfase dessas últimas ciências, e não nas primeiras, que, reitera-se, este trabalho se situa, embora, como pode perceber, tratam-se de dois grandes grupos de ciências que se complementam.

Gil (1999, p. 21) afirma que há diversas tentativas de se classificar as várias ciências, porém, dentre a literatura analisa, ele é o que parte do espectro mais amplo de classificação, cujas extremidades alocam duas grandes categorias de ciências, a saber: as formais e as empíricas. Na primeira, alocam-se as ciências que estudam as entidades formais e suas relações, como a Matemática e a Lógica; e, na segunda, os fatos e seus processos, como a CP (SARTORI, 1981, p. 35) e a Economia. Nesse sentido, as ciências tidas como "empíricas" subdividem-se também em duas categorias, quais sejam: as naturais e as sociais. De fato, é uma classificação passível de críticas, porém é um ponto de partida para se alocar CiberRI no difuso espectro das ciências. Para os objetivos desta Tese, modifica-se, suavemente, a classificação de Gil (1999), substituindo as ciências sociais por sua versão mais antiga – e ainda mais ampla –, qual seja: as ciências humanas.

As ciências humanas nascem incialmente como "ciência(s) do homem"[63] (MEGALE, 1990, p. 74, 85; VOEGELIN, 1982, p. 33), em clara contrapartida às que se debruçam sobre os aspectos que estão além do domínio ou do poder humano, ou seja, as "da natureza", amplamente balizadas pela revolucionária física newtoniana. Com o fim da Primeira Guerra Mundial, as diversas disciplinas que se autoproclamam sociais são resumidas a um punhado das que se mantêm até hoje[64] (WALLERSTEIN *et al*., 1996, p. 28, 74). Dessas, a que mais interessa aqui

[63] Para estas, alguns autores (ELMAN; ELMAN, 2003, p. 41; FRAGOSO FILHO, 1984, p. 27; FUNDAÇÃO CALOUSTE GULBENKIAN, 1996, p. 9; LIPSON, 1967, p. 47; MOREIRA, 2015, p. 18, 20; WALLERSTEIN, 1996, p. 19, 22, 52, 75, 10) usam os termos intercambiáveis Humanidades e humanidades; outros, como Sartori (1981, p. 175) e Voegelin (1982, p. 33), mantém "ciências do homem". Megale (1990, p. 52, grifo nosso), por seu turno, divide o conhecimento científico em "[...]ciências exatas, ciências naturais e *ciências do espírito*, abrangendo estas últimas as *ciências humanas e as ciências sociais*", embora, mais adiante, ele mesmo reconheça, como, aliás, também o faz Voegelin (1982, p. 18), que estas não são sinonímias (MEGALE, 1990, p. 53) e que, mais importante para os objetivos desta Tese, aquelas contêm estas (MEGALE, 1990, p. 54-55). Todavia, a presente Tese acompanha, com especial atenção, as sutilezas contidas em Brasil (2012c, p. 23, 28) e mantém o uso de Ciências Humanas e ciências humanas, para fins de posicionar CiberRI no meio desse emaranhado de ciências.

[64] Tais como Antropologia, Ciência Política, Sociologia, Economia e História (MEGALE, 1990, p. 55, 78-83, 86-95, 107-125; WALLERSTEIN *et al*., 1996, p. 30-43, 49). Alguns autores põem Direito e Geografia nesse rol; outros, não. Cf. MEGALE, 1990, p. 54-55, 57-58, 73, 79-80, 96-106; WALLERSTEIN *et al.*, 1996, p. 43-48. Embora esta seja uma discussão secundária – e não "quase inútil" (MEGALE, 1990, p. 58) –, ela serve para

é CP, a qual, a partir de 1945, reivindica "[...]como sua uma herança que já vinha dos gregos[...]" (WALLERSTEIN *et al*., 1996, p. 36), amplia suas preocupações para além das instituições governamentais formais, redefinindo o seu objeto de estudo de maneira a integrar todos os processos sociais com implicações ou intenções políticas (LIPSON, 1967, *passim*; VOEGELIN, 1982, p. 18; WALLERSTEIN *et al*., 1996, p. 71)[65]. Assim, CP se lança como uma ciência social independente das demais, se bem que, como nota Megale (1990, p. 12, 209), a ciência e a realidade sociais são indivisíveis. Décadas depois de sua institucionalização, CP vê o alargamento de seu objeto tocar o ciberespaço, em uma caminhada rumo àquilo que Wallerstein *et al*. (1996, p. 101) chamam de "[...]visão mais não-contraditória dos múltiplos domínios do conhecimento". RI trilha o mesmo caminho.

Evidentemente, "[n]ão existem fronteiras naturais entre os diferentes ramos do saber" (DUVERGER, 1981, p. 10), principalmente no pós-Guerra Fria, quando aumentam as pressões para a integração de arcabouços teórico-metodológicos nas ciências sociais e políticas[66] (BRADY; COLLIER, 2005; LIEBERMAN, 2005). Acrescenta, ainda, Duverger (1981, p. 10, grifo nosso) que:

> Tal como acontece[...] entre os Estados, a classificação das ciências foi estabelecida por questão de comodidade prática (quando não por questão de rivalidades universitárias). [...]*a [C]iência [P]olítica reúne vários domínios*, alguns comuns a outras ciências sociais, enquanto outros lhes são próprios.

A presente Tese busca inserir uma terceira categoria a esses domínios de CP de que fala Duverger e que compreenda também aqueles que não são comuns a outras ciências sociais – ou, simplesmente, "Ciências Não-Sociais" (RUDNER, 1969, p. 88) –, como é o caso, por exemplo, de Ciência da Computação, Redes de Computadores, Segurança da Informação (SegInfo)[67] e Defesa Cibernética. São nessas searas que os estudos sobre a Internet, enquanto

---

demonstrar que os objetos de estudos das ciências sociais não possuem fronteiras intransponíveis, o que se aplica, colateralmente, a CiberRI.

[65] Esta é, certamente, a definição mais socialmente abrangente que se pode atribuir à CP.

[66] Há tempos, prefere-se, pelo menos no Brasil, o termo Ciência Política a Ciências Políticas. Existem diversas explicações para tal uso, no plural, as quais não cabem aqui esmiuçar, mas cujas principais alegações apontam para a existência não de uma, mas de várias ciências políticas – no mesmo sentido em que se defendem, por exemplo, Ciências da Computação, Ciências Sociais, Políticas Públicas e Redes de Computadores. É nessa visão ampliada que se afirma que, por advir da CP, RI é uma das várias ciências políticas; porém, vislumbra-se que CP e RI possuem uma relação parecida com a de Matemática e Álgebra: por mais que sua autonomia aumente, ao ponto de ocorrer uma emancipação total, esta sempre levará consigo o gene paternal daquela. Para uma definição de autonomia, no seio universitário, ver Fragoso Filho (1984, p. 79, 81).

[67] Apesar de a SegInfo não figurar na Tabela das Áreas de Conhecimento de Brasil (2012c), trata-se de um ramo informático e informacional que cuida dos atributos de proteção da informação, quais sejam: disponibilidade, integridade, confiabilidade e autenticidade. No caso brasileiro, a norma que a rege é a ABNT NBR ISO/IEC 27002:2013. No nível estratégico, compete ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR) coordenar tais atividades (BRASIL, 2014a, p. 13), o que é feito, em certa medida e no nível tático, pelo

emanação mais correlata a ciberespaço, desenvolveu-se e aperfeiçoou-se no seio acadêmico. Não se exime, entretanto, a importância, para as ciências sociais, CP e RI, dos estudos sobre tal ambiente, seja como *locus* para relações sociais – e, portanto, políticas, de dominação e de poder –, seja como meio para atingir um fim[68], ainda que seus *outputs* sociais advenham de *inputs* computacionais.

Se, por um lado, "[a] produção científica e técnica no mundo globalizado é abundante e a circulação das informações, rápida" (BARROS, 2004, p. 21), por outro, o ciberespaço propicia a guarda de boa parte dessa informação, seja nos repositórios abertos da Internet indexada, seja na privacidade criptografada da Internet Profunda, todas elas – com seus respectivos protocolos – podendo ser acessadas também pelas redes celulares de telefonia móvel, formando, desse modo, uma completa interação das partes que compõem o todo ciberespacial. Esse ambiente artificial, ao passo que é visto em termos técnicos e práticos que propiciam a produção infinita de informações, também possui vertentes políticas e internacionalistas quando, por exemplo, faculta o acesso e, mais importante, a transmissão de conhecimentos e informações – traduzidos, para o século XXI, em termos de poder (NYE JR, 2011b) – aos mais diversos indivíduos e grupos – estatais, não estatais e, até mesmo, paraestatais –, inclusive aos que, até então, estavam à margem dos grandes centros produtores de saber e poder[69].

Pondo, agora, de forma terminológica, ressalta-se que, pelo fato de o acrograma CiberRI aglutinar o elemento de composição ciber, de um lado, com as iniciais do campo de estudo da ciência – social e política – que estuda as relações internacionais, do outro, torna-se imperativo realizar justificativas conceituais e etimológicas. Elencam-se, abaixo, cinco delas.

Centro de Pesquisas e Desenvolvimento para Segurança das Comunicações (CEPESC) da Agência Brasileira de Inteligência (ABIN) (BRASIL, 2015, p. 19). *Grosso modo*, pode-se dizer que Segurança Cibernética – e no caso brasileiro aquilo que se chama de Segurança da Informação e Comunicação ou SIC (BRASIL, 2014a, p. 19) – advém da SegInfo.

[68] Neste caso, um fim político. Para a inversão da lógica política de que os fins justificam quaisquer meios, e não o contrário – como defende, por exemplo, Lipson (1967, p. 108, 113) –, ver Maquiavel (1996), o pai fundador da CP moderna (BOBBIO, 2007, p. 50). Já para uma análise do ciberespaço à luz do florentino*, vide* Ianni (1999).

[69] Exemplificando para a CP: Meneguello (1998, p. 26, grifo nosso), ao analisar a relação Executivo-Legislativo no pós-abertura política brasileiro, aponta para "[a] perda pelos partidos [políticos] do monopólio da organização e representação traduz[ir] o dilema da representação política na sociedade contemporânea, na qual esses processos emergem redefinidos pela constituição de *um público de massa informado*". Se, já naquele momento, a informação acessível desponta como uma variável interveniente para o novo perfil eleitoral, o que dizer da atualidade, quando eleições presidenciais – como as dos EUA – utilizam-se, sobremaneira, da campanha eleitoral nas mídias sociais *online*? A informação, vital, como não poderia deixar de ser, para a Sociedade da Informação, passa a ser uma *quasi*-variável independente, pois se veem campanhas políticas se adaptarem ao formato – linguagem direta, duração de vídeos, tamanho de textos, uso de tecnologias acessíveis, transparência ativa etc. – e ao próprio ciberespaço, como se o fato de "falar para a Internet" constituísse um dos motes desta nova geração de candidatos a políticos profissionais.

A justificativa inicial diz respeito ao prefixo "ciber" vincular-se às atividades ligadas tanto ao espectro eletromagnético[70] quanto aos computadores (NYE JR, 2011a, p. 19), conectados em redes ou não (BRASIL, 2014a, p. 18). Tal vocábulo advém, como já visto, de ciberespaço (BETZ; STEVENS, 2011b, p. 84), concebido ora como meio (SOLANA, 2015), ora dimensão (ARGENTINA, 2014; BARRINHA; CARRAPIÇO, 2016, p. 246), ora domínio[71]. A revisão da literatura que trata da relação ciberespaço-segurança internacional afirma que esse ambiente – em especial, uma de suas faces, a Internet – é tão complexo, que não lhe faltam epítetos como: metafórico (KARAS *et al.*, 2008, p. 10), onipresente (KREMER; MÜLLER, 2014b, p. 42), multável (BRASIL, 2014a, p. 20), sem limites/localização/fronteiras geofísico-políticas (ARGENTINA, 2014; BRASIL, 2014a, p. 21; GAGNON, 2008, p. 51; SOLANA, 2015; VALENTE, 2007, p. 20), incerto (BRASIL, 2014a, p. 21), com regras próprias (ARGENTINA, 2014; ROJAS ARAVENA, 2001, p. 15), artificial – porque criado pelo ser humano (ARGENTINA, 2015, p. 77; CASTRO, 2016, p. 121; NYE JR, 2011b, p. 124; PORTELA, 2016, p. 94, 106) – e "melhor visto como um 'substrato' cada vez mais universal para todas as sociedades" (DEMCHAK, 2014, p. v, tradução nossa[72]). Em suma, apesar de o conceito de ciberespaço ser polissêmico (NYE JR, 2011b, p. 122), é praticamente uníssono, do ponto de vista internacionalista, concebê-lo enquanto um local em que os "governos têm encontrado dificuldade para aplicar a lei" (SOLANA, 2015, grifo nosso, tradução nossa[73]), tornando-se, assim, um "[...]enorme desafio para o setor de Defesa" (COSTA, 2012, p. 12). Aí mais um motivo para esta Tese focar a questão da segurança internacional para a defesa de CiberRI[74].

---

[70] Existem nuanças conceituais entre espectro eletromagnético e cibernético – e de tantos outros campos, como informático, telemático, telecinético e telecomunicacional – que fogem ao escopo deste trabalho de CP. Uma prova de que isso importa para os fins desta Tese é o fato de Mandarino Junior (2009, p. 48) distinguir Guerra Eletrônica de Guerra Cibernética, em que esta é geralmente definida, em termos menos técnicos e mais político, como o conjunto de "[...]ações de um *[E]stado-nação* para invadir computadores ou redes de *outra nação* com a *intenção* de causar danos ou transtornos" (CLARKE; KNAKE, 2015, p. 10-11, grifo nosso). Atualmente, com o desenvolvimento da chamada Guerra Híbrida, a linha de demarcação entre ambos os espectros se atenua ainda mais.

[71] Cf. ARGENTINA, 2015, p. 77; BRASIL, 2014a, p. 18; ESTADOS UNIDOS DA AMÉRICA, 2010, p. 21; 2012, p. 4; GRAY, 2013, p. 8-32, 37; LIANG; XIANGSUI, 1999, p. 69; LIAROPOULOS, 2013; LOVELACE JR, 2013, p. iii; LYNN III, 2010; REINO UNIDO, 2011; STOLTENBERG, 2016; THE ECONOMIST, 2010, p. 11, 25-28; ZUCCARO, 2011, p. 51. Nesse sentido, *vide* também Touré (2011).

[72] Texto original: "[...]*cyberspace – best viewed as an increasingly universal 'substrate' to all societies*[...]".

[73] Texto original: "[...]*governments have struggled to enforce the rule of law online*".

[74] A ênfase dada aqui à segurança internacional justifica-se também por ser em torno da guerra que "[...]encontra-se não só a origem da [...] disciplina [de RI], como também o cerne das questões que, ainda hoje, afligem os estudiosos das Relações Internacionais" (SARFATI, 2011, p. 14). Para uma diferenciação mais precisa entre Estudos de Defesa e de Segurança, ver, por exemplo, Brasil (2012b, p. 12-15), Lopes (2013, p. 28-29), Proença Jr e Diniz (1998, p. 20), Teixeira Júnior (2011) e Winand e Saint-Pierre (2010). Já no que se refere aos matizes

A segunda justificativa considera as diferentes formas de alocar, cientificamente, RI, tais quais: campo (DEMCHAK, 2014, p. vi; JACKSON, 2011, *passim*) científico-acadêmico (JACKSON, 2011, p. 188; SARFATI, 2011, *passim*) ou de pesquisa (MEDEIROS *et al.*, 2016, *passim*; RESENDE, 2005, p. 17) que é, ao mesmo tempo, uma disciplina (LESSA, 2005, p. 2; LIMA, 2016, p. 9) ou subdisciplina (AMORIM NETO; SANTOS, 2015, p. 30) universitária de origem estadunidense-europeia (ABERYSTWYTH UNIVERSITY, [201-]; MEDEIROS *et al.*, 2016, p. 2; SCHMIDT, 2002, p. 7). Ademais, sua relação pode ser vista ora como independente (SARFATI, 2011, p. 13, 16, 20-21), ora dependente (BUZAN; HANSEN, 2009, p. 256; BRASIL, 2012b, p. 1; VAN EVERA, 1997, p. 89) de CP, "dentro da qual muito dos estudiosos de RI se localizam" (JACKSON, 2011, p. 9, tradução nossa[75]). No último caso, RI se torna uma subárea, como ocorre nos EUA (FERES JR, 2000, p. 97), importante referência para o desenvolvimento e aperfeiçoamento tanto de CP quanto de RI. É nessa associação intrínseca que Amorim Neto e Santos (2015, p. 21) apregoam que RI é um curso que combina com o de CP, cuja separação temática pode se dar "[...]ao volume e ao progresso das pesquisas, bem como à demanda de alunos e ao avanço intelectual de universidades[...]" (MEGALE, 1990, p. 58). Apesar de essa discussão ainda estar em aberto[76], assume-se RI a partir do principal marco referencial para o ensino superior brasileiro que é a Tabela de Áreas de Avaliação da CAPES (BRASIL, 2012c; 2014b, p. 26-27), a qual postula que "Política Internacional" e "Relações Internacionais, Bilaterais e Multilaterais" são Especialidades da Subárea "Ciência Política", para fins da Área de Avaliação "Ciência Política e Relações Internacionais", todas elas englobadas pela Grande Área "Ciências Humanas".[77] Nesse viés, CiberRI jamais deixa de beber da fonte de RI e das demais ciências sociais, especialmente da CP. Afinal, se se pode analisar as interações sociais a partir das relações de poder estabelecidas – à luz, por exemplo, da Sociologia Política ou da Economia Política –, então o ciberespaço reivindica espaço também

conceptuais entre Segurança Cibernética e Defesa Cibernética, consultar Acácio (2015), Acácio e Lopes (2012), Carvalho (2011b), Lopes (2013, p. 30-31), Lopes e Medeiros (2011) e Portela (2016, *passim*).

[75] Texto original: "[...]the discipline of Political Science, within which so much of IR scholarship is located[...]".

[76] Acerca dela no Brasil, Amorim Neto e Santos (2015, p. 27) asseveram que, "*[a]unque la creación de un área [de avaliação] exclusiva de RI siga en la agenda de los internacionalistas [brasileiros] y esté en el horizonte de decisiones relevantes de los comités pertinentes del Ministerio de Educación, el hecho es que liderazgos académicos importantes de RI vienen manteniendo su producción y militancia institucional en el ámbito de la CP, controlando puestos importantes de decisión, tanto en la ABCP [Associação Brasileira de Ciência Política], como en el propio Ministerio*[...]".

[77] Como dito, a Tabela de Áreas do CNPq tem suas diferenças em relação à da CAPES. Por exemplo, naquela, CP engloba "Política Internacional", que, por sua vez, contém "Relações Internacionais, Bilaterais e Multilaterais", o que não ocorre com esta, em que ambos estão na mesma linha hierárquica horizontal.

nas demais ciências sociais, por meio de RI. Na Era da Informação, se informação é poder[78] (BESSA, 2014, p. 104, 128; CHAIA; CHAIA, 2000, p. 5; HERMANY; BOLESINA, 2015, p. 72; VALENTE, 2007, p. 15, 25), o ciberespaço – esse novel espaço de interação social e, portanto, de manifestação para as diversas formas de dominação – projeta-se como uma fonte de exercício e difusão de poder (NYE JR, 2011b, p. 114, 150). Assim, ele se torna também passível de ser estudado sob a ótica de RI, ao mesmo tempo em que ajuda a ampliar o "conhecimento das relações internacionais", que é o grande "desafio da globalização" (LIMA, 2016, p. 9).

A terceira justificativa aponta na direção de este trabalho preferir o termo "acontecimento" a "fenômeno", pois, de acordo com Jean-Baptiste Duroselle[79], apesar de um acontecimento não deixar de ser um fenômeno, sua diferença reside na possibilidade de aquele, ao contrário deste, ser (i) datado e (ii) relacionado diretamente a uma ação humana (DUROSELLE, 2000, p. 19-20).[80] À luz de CiberRI, pode-se exemplificar tal distinção da seguinte maneira: fenômeno é quando um *tsunami* paralisa a usina nuclear japonesa de Fukushima; acontecimento é quando um verme de computador (*worm*), projetado por um Estado-nação, sabota[81] a usina nuclear iraniana de Natanz. Crê-se que tal tipo de analogia também se amolda aos estudos ciberinternacionalistas e, por causa disso, ela é resgatada e utilizada aqui.

A quarta justificativa tem em mente a constatação, ainda que intuitiva, de que as relações internacionais são o foco de estudo de RI (SARFATI, 2011, p. 13). Entretanto, por possuir a mesma grafia, "relações internacionais" e "RI" podem conduzir a más interpretações e análises. Uma alternativa a essa inconveniência seria seguir o exemplo de Waltz (2002) e utilizar "política internacional" como sinônimo de "relações internacionais" (ART; JERVIS, 2013). Contudo, opta-se pela permanência de ambos os termos homógrafos, por entender que relações

---

[78] Frase originariamente citada por Francis Banco, há quase quatro séculos (VALENTE, 2007, p. 15).

[79] Considerado "um dos autores mais influentes da escola francesa de história das relações internacionais" (AVILA, 2000, p. 220).

[80] Sobre essa distinção, que repousa, em última instância, na diferenciação entre os objetos de estudos das ciências naturais e sociais, ver Gil (1999, p. 39), Jackson (2011, p. 11), Lipson (1967, p. 21), Sartori (1981, p. 45-65) e Voegelin (1982, p. 6), bem como a seguinte passagem de Weber (2006, p. 66, grifo nosso): "[o] elemento científico essencial dos *fenômenos* apenas podia ser constituído pelo aspecto 'legal' [de teorias/leis abrangentes], enquanto os '*acontecimentos individuais*' só podiam ser considerados 'tipo'[...]" ideal. Entenda-se o acontecimento ciberinternacionalista, portanto, como um tipo ideal, na acepção weberiana, haja vista que nenhum deles nasceu com tal pretensão. Ainda sobre tipos ideais, ver Rudner (1969, p. 85-97), especialmente a crítica sobre a "ambiguidade crucial" de Weber sobre o caráter lógico dos tipos ideais (*ibid*., p. 86).

[81] Sabotagem, por si só, é intencional, e, pois, proveniente de uma ação humana prévia e dolosamente orquestrada.

internacionais é um termo mais amplo e engloba também a política internacional[82]. Dessa forma, é possível estudar, à luz de CiberRI, os impactos do ciberespaço não apenas na seara da política internacional, como também em outras. Nesse viés, a recíproca é igualmente verdadeira, qual seja: CiberRI encoraja estudos sobre o impacto das relações internacionais no ciberespaço. Um dos mais importantes exemplos disso é o chamado Manual Tallinn (SCHMITT, 2013), espécie de rascunho (*draft*) para uma convenção internacional sobre guerras cibernéticas, resultante da articulação entre especialistas (PIRKER, 2013, p. 190) em Direito, conflitos armados e TIC, sob a tutela do *Cooperative Cyber Defence Centre of Excellence* (CCD COE) da OTAN, com o apoio da Universidade de Cambridge. Tal publicação é certamente o trabalho jurídico mais completo sobre guerra cibernética (YANNAKOGEORGOS, 2014, p. 54) e versa sobre a necessidade de o Direito Internacional[83] regulamentar tal temática entre os Estados (CAVELTY, 2015, p. 91; MEHMETCIK, 2014, p. 131; WEINGÄRTNER, 2013, p. XIII). Resta rememorar que a criação do próprio CCD COE se dá logo após o governo estoniano, cuja capital é Tallinn, sofrer ataques cibernéticos tão impressionantes que praticamente paralisaram suas estruturas estratégicas de TIC, a ponto de a OTAN criar um centro de Defesa Cibernética naquela capital[84].

A quinta e última justificativa conceitual-etimológica toca ainda ao termo ciberinternacionalista – derivação do que é estudado em e a partir de CiberRI. É importante salientar que o adjetivo "internacionalista" possui sentido diferente de "internacional". Este contém aquele e se refere especificamente ao campo epistemológico e científico de RI, uma vez que se vislumbra este em praticamente toda área científica. Entrementes, um estudo internacional, por si só, pode não interessar muito – ou interessar pouco – à comunidade epistêmica de RI[85]. Por exemplo, descrever pormenorizadamente a estrutura da ONU é muito mais profícuo para estudantes de Administração do que de RI; porém, a analisar as "forças

[82] Neste mesmo viés, conferir Duverger (1981, p. 38-39). Certamente, a Tabela CNPq não leva em consideração isso ao alocar RI dentro de Política Internacional.

[83] O ex-Juiz da Corte Internacional de Justiça da ONU Francisco Rezek assim define Direito Internacional: "[s]istema jurídico autônomo, onde se ordenam as relações entre Estados soberanos, o direito internacional público – ou *direito das gentes*, no sentido de direito das nações ou dos povos – repousa sobre o consentimento" (REZEK, 2013, p. 33, grifo do autor). Diferentemente desse ramo do Direito, há o Direito Interno, em que "[...]as normas são hierarquizadas como se inscrevessem, graficamente, numa pirâmide encabeçada pela lei fundamental", que é a Constituição (*ibid.*, p. 24).

[84] Cf. BETZ; STEVENS, 2011a, p. 29-30; CLARKE; KNAKE, 2012, p. 30; 2015, p. 15-19; LIBICKI, 2009, p. 1-3; MEHMETCIK, 2014, p. 130; NYE JR, 2008; 2011b; PAVIA, 2015, p. 266; RUMER, 2007, p. 8; THE ECONOMIST, 2010, p. 58; ZUCCARO, 2011, p. 53-54.

[85] Haas (1992, p. 2-3) conceitua comunidade epistêmica como uma rede formada por especialistas em uma determinada área do conhecimento com autoridade suficiente para reivindicar como politicamente relevante tal conhecimento. Sobre a comunidade epistêmica de RI, ver Sarfati (2011, p. 20-21).

profundas" – nos dizeres da escola francesa de RI – e o contexto internacional que influenciaram a estruturação da ONU – à luz, por exemplo, do *path dependence* – ensinaria mais a estes do que àqueles. Ambos os exemplos não deixam de ser internacionais, pois versam sobre uma organização internacional por excelência; mas o fato de o segundo interessar mais a RI não o torna "mais internacional" que o primeiro nem, mesmo, internacionalista, em sentido estrito, pois só o é se (i) produzido a partir de pressupostos metateoréticos de RI e (ii) aceitos como tal pela comunidade internacionalista. Essa ideia de "comunidade internacionalista" assemelha-se à de "comunidade epistêmica de RI", de Sarfati (2011, p. 20-21), que a compreende como o conjunto de estudos específicos na área de RI, produzidos em nível de graduação ou de pós-graduação. Vale salientar que "internacionalista", aqui, é um adjetivo que se refere à rede de especialistas que produzem – e atestam o conhecimento advindo dessa produção – no campo de RI, e não um substantivo que designa o profissional formado em RI. Desnecessário citar exemplos de trabalhos seminais de RI produzidos por estudiosos formados em outros campos científicos. Vê-se um caso que exemplifica essa preocupação etimológica em Lopes (2013, *passim*), quando ele atrela o termo "ameaça *ciber*existencial" à forma com que militares dramatizam certas ameaças cibernéticas – em detrimento de outras tão ou mais importantes que estas –, a ponto de as considerar ameaças à própria existência do Estado. Nesse ínterim, ele incorpora o elemento de composição "ciber" a um vocábulo – "ameaça existencial" – específico de uma corrente de pensamento internacionalista, a Escola de Copenhague.

Em suma, são nessas distinções conceituais e etimológicas que CiberRI se baseia, apresentando-se enquanto um subcampo científico eminentemente internacionalista, e não meramente internacional. Após essas justificativas, pode-se sintetizar, metaforicamente, CiberRI como uma das várias pontes ou interfaces que ligam duas ciências de culturas aparentemente distantes, que vão desde o nível de conhecimento mais geral/abstrato ao mais particular/concreto, conforme se exemplifica na Figura 2, com o estudo das armas cibernéticas à luz dos ESI.

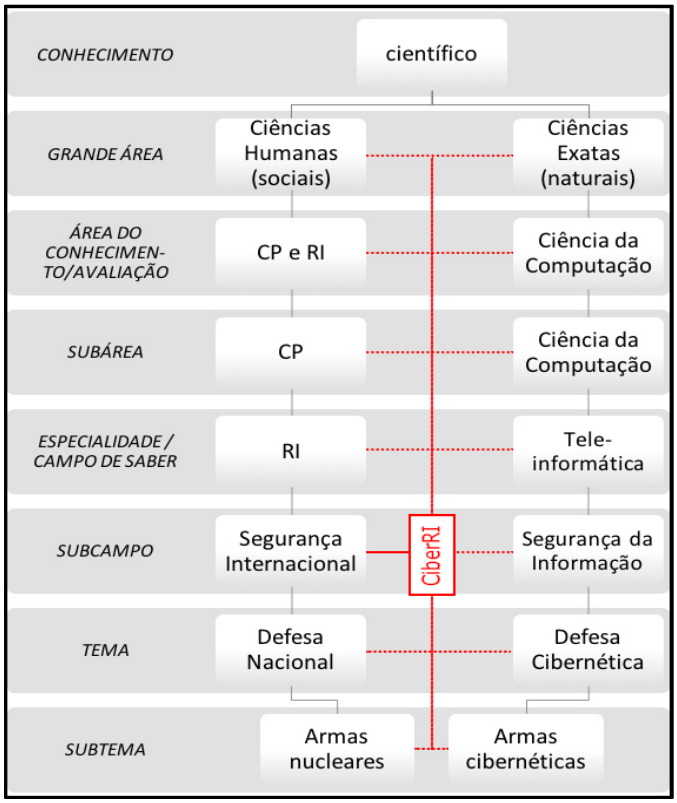

Figura 2 CiberRI e os níveis do conhecimento científico
Fonte: elaboração própria.
Legenda: CP = Ciência Política; RI = Relações Internacionais.
***Nota Bene* (N.B.)**: Brasil (2012c, p. 2) utiliza "Teleinformática", porém é mais corriqueiro "Redes de Computadores", termo, de agora em diante, escolhido.

Assim, é possível sair do nível mais geral do conhecimento e ir até, por exemplo, o da disciplina/campo de RI, e tocar nas idiossincrasias do subcampo de CiberRI, mais especificamente na forma com que ele corrige o problema da excessiva fragmentação temática sobre o ciberespaço em seu campo-*master*, organizando-o[86] e sistematizando-o. Para compreender o modelo que se propõe a corrigir tal problema, faz-se importante situar os elementos metateoréticos que o compõem, na próxima subseção.

1.2 Os elementos metateoréticos em CiberRI: ontologia, epistemologia e metodologia

Não se faz ciência, sem um método científico, ou seja, sem "[...]um conjunto de meios dispostos convenientemente para se chegar a um fim que se deseja" (CRESPO, 2009, p. 2). Ao

[86] O conceito de organização científica aqui pretendido é o mesmo contido na seguinte passagem: "[...]não compete à ciência, meramente, coligir fragmentos desconexos, fortuitos, isolados, de informação; [...]é um ideal da ciência dar uma explicação *organizada* do universo – conjugar, interligar, ajusta, em relação de mútua subordinação, as declarações que consubstanciam o conhecimento adquirido" (RUDNER, 1969, p. 27, grifo do autor). Ver também Rudner (*op. cit.*, p. 72).

traçar um paralelo entre ciência e metodologia em RI, Jackson (2011, p. 26) dispõe de um roteiro formado por três elementos e suas respectivas perguntas-chave, quais sejam:

1. *Ontologia*: como os pesquisadores *conceituam* o que eles estudam?;
2. *Epistemologia*: como os pesquisadores *sabem* o que eles sabem?; e
3. *Metodologia*: como os pesquisadores *selecionam* suas ferramentas?

Uma vez que se defende CiberRI no âmbito acadêmico – e, mais especificamente, universitário –, é porque tal subcampo também pode e deve ser avaliado quanto a esses três elementos, haja vista que o que distingue RI de outros campos científicos é sobretudo a utilização de seus próprios elementos metateoréticos, ou seja, de ontologia, epistemologia e metodologia (SARFATI, 2011, p. 20).

Como dito, não é objetivo desta Tese aprofundar-se em Filosofia da Ciência, porém, pode-se afirmar, *grosso modo*, que a Ontologia diz respeito ao estudo do *ser* e do que existe no mundo (JACKSON, 2011, p. 26), isto é, das características que o tornam tão diferente dos seus pares, de forma que o único exemplar residual seja ele próprio. Esse tipo de pensamento é muito visto nos estudos da Lógica, de origem aristotélica. Em definição mais ampla, Voegelin (1982, p. 6, grifo do autor) chega a afirmar que a Filosofia é "[...]que tem por objeto o *ser*, isto é, a realidade[...]" – para um aprofundamento político quanto a isso, ver Voegelin (1982, p. 31). Já Sartori (1981, p. 30) aponta que "[a] linguagem filosófica[...] não tem finalidade descritiva", o que, pode-se dizer, alimenta os argumentos dos defensores de que o conhecimento filosófico não está contido no científico. Em todo caso, a Ontologia é reconhecida como *o* elemento crucial da ciência (JACKSON, 2011, p. 19).

Já a Epistemologia é um ramo da Filosofia (RUDNER, 1969, p. 13) que trata da delimitação e dos alcances do objeto de estudo e da forma com que o conhecimento sobre ele se organiza e se diferencia dos outros conhecimentos, por meio de pressupostos, arcabouços, premissas e corolários teóricos (BUZAN; HANSEN, 2007, p. 32). De acordo com Gil (1999, p. 23), pode-se dizer que os problemas teóricos, na Epistemologia, são tratados por meio de hipóteses e observações, o que leva, necessariamente, a novos debates – inclusive novas hipóteses e observações – passíveis de conflitos entre os próprios pares; eis aqui uma manifestação do *excesso de falta de consenso* que tanto permeia as ciências sociais como um todo, evidenciado pelas diversas correntes e escolas de pensamento sobre um único tema. Logicamente, para o progresso da ciência, esse excesso nunca é demasiado. Daí que Bourdieu (1983b, p. 124) postula que "[...]os conflitos epistemológicos são sempre, inseparavelmente, conflitos políticos; assim, uma pesquisa sobre o poder no campo científico poderia perfeitamente só comportar questões aparentemente epistemológicas". Embora essa afirmação

bourdieusiana contraria a última de Jackson (2011, p. 19) – ou seja, não entrem em consenso – , como se pretende mostrar, esta Tese vai além das aparências epistemológicas, inserindo CiberRI também nos domínios ontológicos e metodológicos, levando, assim, ao terceiro elemento metateorético.

A Metodologia – longe de ser sinônimo de método (GIL, 1999, p. 26-27; JACKSON, 2011, p. 25; RUDNER, 1969, p. 18-19) – seleciona, à luz de um método teórico, as técnicas e ferramentas para se chegar à veracidade dos fatos (GIL, 1999, p. 26). No que respeita a essa busca, ganha força, nas últimas décadas, a noção de falseabilidade, originária do método hipotético-dedutivo de Popper (2008, *passim*), que defende, à luz da filosofia neopositivista (GIL, 1999, p. 27), que não se pode provar que algo é verdadeiro, mas, sim, que é falso[87]; portanto, a falseabilidade é um pressuposto da ciência, cujo conhecimento tende a ser também falível (GIL, 1999, p. 20-21), para a manutenção do progresso da ciência. Aqui, o cuidado redobrado que internacionalistas, assim como cientistas e filósofos sociais, devem ter é o de investigar os acontecimentos cibernéticos sem a necessidade última de se afirmar uma "verdade" ou "progresso" na pesquisa social (CHERNOFF, p. 120), pois, certamente, aquela nunca será conhecida por completo, enquanto esta será efeitos, e não causa da investigação social. Com CiberRI, não é diferente, tendo em vista que o grande adiantamento de uma ciência pode ser determinado não pelo objeto investigado propriamente dito, mas, sim, pela precisão de seus instrumentos de medida (GIL, 1999, p. 22), ou seja, de seus métodos, a serviço de uma metodologia ainda mais ampla, amparada por uma teoria.

Alguns autores veem na sequência ontologia-epistemologia-metodologia uma ordem a ser respeitada, para se produzir conhecimento científico (JACKSON, 2011, p. 26-28). No caso, a presente Tese segue-a, filtrando os elementos metateoréticos por meio dos ESI. Isso não faz com que o objeto de CiberRI – as relações ciberinternacionalistas – restrinja-se à Segurança Cibernética em nível internacional, mas, sim, que CiberRI amplie e amplifique a temática securitária do ciberespaço. A lógica aqui é sempre a de desconstruir o óbvio e o senso comum para a linguagem científica. Embora pareçam coisas diferentes, as premissas e o objeto continuam os mesmos; o foco é que é redirecionado para algo específico, a segurança internacional. Agindo dessa forma, é possível realizar a observação, a análise e a síntese em

[87] Cf. JACKSON, 2011, p. 1, 12-13; WALTZ, 2003, p. ix. Kuhn (2006), por seu turno, afirma, por meio da observação histórica e do que chama de ciência normal, que tal noção não se sustenta – sobre isso, ver também Buzan e Hansen (2007, p. 42- 44) e Jackson (2011, p. 13-14). Para uma crítica a essa visão de Kuhn, conferir Bourdieu (1983b, *passim*).

CiberRI, a ponto de se examinar também eventos concretos – neste caso, acontecimentos ciberinternacionais – com o auxílio de teorias, *frameworks*[88] e ferramentas metodológicas.

Aqui, segue-se uma linha de raciocínio parecida com a propositura de Figueiredo (2015), porém, enquanto ele advoga em favor do reconhecimento dos Estudos Estratégicos como uma Área de Conhecimento[89] independente da de RI, esta Tese defende a criação de uma subárea, dependente de RI. Os seguintes motivos relevam tal posição: (i) a existência de um objeto de estudo – as relações internacionais cibernéticas – identificável e distinto do de outros campos e subcampos; e (ii) o número razoável e crescente de instituições, pesquisadores e publicações sobre tal temática[90], sobretudo fora do Brasil.

Ao contrário do ser humano, que é o objeto final de estudos das ciências sociais (GIL, 1999, p. 23) – e, consequentemente, de áreas afins a RI, a exemplo de Direito, Economia e História (BRASIL, 2012b, p. 1; LESSA, 2005, *passim*) –, o ciberespaço enseja um diálogo maior com a Grande Área "Ciências Exatas e da Terra", especificamente com a Área de Avaliação "Ciência da Computação". Isso sem perder de vista que CiberRI se enquadra, no caso brasileiro, na Área de Avaliação "Ciência Política e Relações Internacionais". Não obstante "[...]a exposição de ideias novas, aparentemente aberrantes, inevitavelmente desperta[r] resistências" (VOEGELIN, 1982, p. 29), preveem-se algumas resistências e críticas sobre tal proposta interdisciplinar e transcendente aos limites da Grade Área "Ciências Humanas". Sobre elas, antecipam-se duas respostas.

A primeira delas examina se RI, enquanto campo inter e multidisciplinar (LESSA, 2005, p. 2; SARFATI, 2011, p. 20), já não possui subcampos que, de alguma forma, abordam o ciberespaço, tais como Globalização, Direito Internacional e, mesmo, Segurança Internacional. Rebate-se tal argumento, ao apontar que obras já utilizadas nos estudos de outros subcampos internacionalistas também podem – e devem – constituir fontes para o embasamento dos estudos ciberinternacionalistas. Em outras palavras, ao mesmo tempo em que se afirma um conhecimento pré-existente – e, portanto, não sistematizado – à CiberRI, enfatizam-se também características próprias desse subcampo, que se moldam ao contexto ciberespacial.

---

[88] Em suma, *frameworks* subordinam teorias – de médio alcance, em geral – e sugerem normas de procedimento científicos, constituindo-se, muitas vezes, como teorias de grande alcance, a exemplo do Funcionalismo, do Estruturalismo e do Materialismo Histórico (GIL, 1999, p. 36-41). Eles também podem vir sob o nome de quadros de análise ou de referência, como ocorre em Gil (1999, p. 35-36) e Sartori (1981, p. 203). A própria teoria da securitização, da Escola de Copenhague, é, nos termos de seus criadores, um "*new framework for analysis*" (BUZAN, WÆVER; WILDE, 1998).

[89] Tomam-se de Brasil (2012b) os conceitos de Grande Área, Área de Avaliação/Conhecimento, Subárea e Especialidade.

[90] Cf. PORTELA, 2016.

Exemplificando com a área de estudos sobre a globalização: Held e McGrew (2001, p. 11-14) analisam várias definições de globalização, com base nos aspectos material, cognitivo e espaço-temporal. É justamente no último aspecto que os autores afirmam que a revolução telemática nos microssistemas, a cabo desde os anos 1980, desfaz as noções geográficas de fronteira e tempo, bem como a de soberania, questões centrais nos estudos tradicionais de RI (BIERSTEKER, 2002, p. 157; REUS-SMIT; SNIDAL, 2008, p. 12). Trazendo esse terceiro aspecto de Held e McGrew (2001) para os elementos metateoréticos em CiberRI, é possível enfatizar feições negligenciadas pelos supracitados autores[91], ou, mesmo, trazer novos entendimentos para ampliar objetos tradicionais de estudos, como o faz Castells (1999; 2007) para com a Sociologia. Enfim, as possibilidades de amplificar o que, aparentemente, não se mostra relevante em RI são enormes, no que tange ao ciberespaço. Como se vê, CiberRI não expropria nenhum subcampo já existente em RI; mas, sim, se apropria, em determinados casos, de premissas ou dados, gerando novos saberes e atualizando-os ao contexto das relações internacionais do século XXI.

Já a segunda resposta prévia a supostas críticas a CiberRI, como reflexo da primeira, refere-se à possibilidade de os estudos sobre o ciberespaço não serem compatíveis com os elementos metateoréticos de RI. É certo que matemáticos e, principalmente, cientistas da computação monopolizam as discussões acerca do desenvolvimento desse ambiente, durante boa parte da história recente. Mas, com a popularização da Internet nos anos 1990, especialistas de áreas como Ciência da Informação, Marketing e Comunicação reivindicam espaço nesse debate, que permanece atrelado mais às dimensões técnica e estética do que política[92]. É a partir, principalmente, do final dos anos 2000 que a comunidade epistêmica de RI – sobretudo sua ala securitária – debruça-se com maior rigor sobre o ciberespaço. Desde então, produzem-se crescentes estudos nessa seara. Todavia, percebe-se que tal esforço se faz de forma insular e, portanto, longe dos necessários intercâmbios típicos de uma ciência social que prima ser atual e dinâmica. Sistematizar, portanto, parte desse conhecimento em um subcampo potencializa não apenas o aperfeiçoamento do campo de RI, mas o atualiza para o raiar deste novo milênio,

[91] Tal como a capacidade com que pequenos Estados do leste asiático têm em não amarrar seu desenvolvimento a noções tradicionais geográficas ou tecnológicas, sim buscar inserir-se na economia global mediante desenvolvimento de TICs e conectividade, que, embora mais baratas, são também mais pragmáticas (LOPES, 2016). Do outro prisma da questão, repousa a crítica sobre as vantagens que os países desenvolvidos têm da tecnologia (KAWAMURA, 1986, p. 46-47, 67-79, 98-99).

[92] Cf. KRUG, 2000. Para uma transição pendendo para o lado sociológico, ver Castells (2007) e Lévy (1999).

Para uma concepção da tecnologia enquanto questão política, e não simples técnica operativa, ver Kawamura (1986, p. 51).

marcado pelo uso crescente do ciberespaço, e em especial da Internet, nas relações sociais, mundo afora, formando, assim, uma verdadeira sociedade em rede, pós-industrial ou da informação[93].

Para validar o objeto de CiberRI, faz-se imperioso apreender sua substância, a qual "[...]deverá ditar o *método* de seu aprendizado" (LIPSON, 1967, p. 38). Nesse seguimento, a definição do método e, por conseguinte, de sua metodologia é um passo que se demarca após a limitação epistemológica do objeto de estudos. É nesse momento que se torna evidente o fato de que o domínio do trabalho científico não se baseia nas conexões *objetivas* entre as *coisas*[94], mas nas conexões *conceituais* entre os *problemas* (WEBER, 2006, p. 37). Quanto a essa questão do desenvolvimento de métodos, Duverger (1981, p. 34) salienta que nada impede a CP, não obstante o empréstimo repentino de métodos oriundos de outras ciências sociais, desenvolver seus próprios métodos, e que estas, por seu turno, utilizem-nas, pois "[...]essa invenção de novos processos de pesquisas é muito desejável" para o aperfeiçoamento das ciências.

Duverger (1981) deixa de lado uma terceira via metodológica, que diz razão à utilização, por parte das ciências políticas e seus subcampos, de métodos e técnicas empregadas em ciências que não são sociais, como as computacionais, por exemplo. É o que propõe, por exemplo, Lopes (2013, p. 51-99) com seu Espectro de Securitização Militar do Ciberespaço (ESMC), um *framework* de análise que mensura, por meio dos estilos de pesquisa qualitativo e quantitativo, o nível de securitização militar do ciberespaço em determinados tempo e espaço, à luz da teoria da securitização. Outra ferramenta que diz respeito ao elemento metateorético da metodologia em CiberRI é o chamado *Stakeholders*, Ações e Motivos na Segurança Cibernética (SAM), proposto por Kremer e Müller (2014b, p. 41-58), que permite, por meio do estilo qualitativo, enquadrar quem, como e por quais motivos realiza ataques cibernéticos contra alvos civis e militares. Não importa qual estilo de pesquisa se utilize, seja o quantitativo, seja o qualitativo, seja o misto, o importante é testar alguns passos que a literatura especializada sugere, ou seja, experimentar todo tipo de metodologia e métodos, a fim de explicar os acontecimentos e fatos o mais preciso e completo possível. A divisão rígida entre métodos quantitativos e qualitativos cai por terra, sobretudo, por causa dos chamados métodos mistos,

[93] Cf. CASTELLS, 1999. Para uma crítica ao uso enviesado do conceito de Sociedade da Informação, ver Werthein (2000).

[94] Por "coisas" entendam-se, à luz de Weber, "[...]no caso da vida social, os eventos e os objetos correlatos que se oferecem à nossa atenção – não trazem consigo seu significado e só o recebem quando se tornam interessantes – e, por isso, problemáticos – para nós" (COHN, 2006b, p. 37). Talvez, venha daí o termo "estado de coisas", que se amarra tanto aos aspectos práticos quanto teóricos do panorama a ser *descrito* e, por conseguinte, apreendido pelo cientista social, político, internacionalista e ciberinternacionalista.

como sua versão mais extrema, o *Nested Analysis*, aplicado na subseção 3.2, *infra*. Essa distinção metodológica advém de um período que se caracterizou pelo dualismo exacerbado entre ciências naturais e sociais.

Como mencionado, a física newtoniana – e, com efeito, o positivismo –, utilizando-se do método indutivo, constituiu, por um lado, como principal fomentadora metateorética para as explicações sociais até o início do século passado (GIL, 1999, p. 29, 45; KAWAMURA, 1986, p. 23; VOEGELIN, 1982, p. 18-31), e, em certa medida, ainda desperta "[o] interesse apaixonado que os pesquisadores em ciências sociais têm pelas ciências da natureza" (BOURDIEU, 1983b, p. 129). Por outro lado, essa visão começa a perder foco na CP pelo fato de se reconhecer que a realidade social não é estática nem linear (KAWAMURA, 1986, p. 98; FRAGOSO FILHO, 1984, p. 14; WALLERSTEIN *et al*., 1996, p. 92-94), como salientam os pressupostos da ciência newtoniana aplicados aos fenômenos da natureza (GIL, 1999, p. 23; VOEGELIN, 1982, p. 33); pelo contrário, ela se caracteriza pela complexidade de seus elementos e contextos sempre mutáveis.

Esse debate – que, à primeira vista, parece passar longe da discussão de se criar CiberRI – leva ao reconhecimento da existência de dois sistemas que envolvem o ser humano e suas diversas relações, quais sejam: o natural e o social. Como se pretende mostrar aqui, o ciberespaço, entendido também enquanto sistema, traz implicações consideráveis a esses dois sistemas tradicionais. Se "[a]s ciências[...] sociais[...] estudam o homem não como ser vivo, biológico, mas como ser social, como criador de cultura, em quaisquer que sejam os *aspectos* da vida social" (MEGALE, 1990, p. 53, grifo nosso), então é de se esperar que, em algum momento, a Academia abordaria o ciberespaço como um desses aspectos, e, conforme Clarke e Knake (2012; 2015) e Mazanec (2015, p. 219), sob várias definições. Nesse ínterim, o século XXI assiste à ascensão do ciberespaço à categoria de "sistema", não mais de "aspecto", isto é, ele sai da parte e constitui-se, ele próprio, um todo, específico em sua significação, nos dizeres weberianos. Esse terceiro sistema, o cibernético, é um amálgama de características que são coincidentes entre os sistemas natural e social, mas, ao mesmo tempo, diferencia-se por completo deles.

Nesse viés, o ciberespaço é posto como um ambiente nada simples de ser lidado – e, nos casos em que o tomam como topologia, de ser dominado –, assemelhando-se, em muito, às próprias ciências naturais e sociais, as quais "[...]se ocupam de sistemas complexos, ou seja, de sistemas em que os desenvolvimentos futuros resultam de processos temporalmente irreversíveis" (WALLERSTEIN *et al*., 1996, p. 113). Porém, uma grande diferença em relação

a esses dois sistemas tradicionais nasce com o ciberespaço, a saber: sua artificialidade, que lhe é intencionalmente originária.

Ora, a natureza "[...]existe, como nós também existimos, *sem que a tenhamos criado*" (LIPSON, 1967, p. 21, grifo nosso); o sistema social é "[...]o mosaico da sociedade que todos ajudaram a compor, mas que *não foi planejad[o] por ninguém*" (LIPSON, *loc. cit.*, grifo nosso); já o ciberespaço é imaginado e criado pelo ser humano, ainda nos idos do século XX, cujos limites de fronteira e de segurança lhe escaparam à época, haja vista que o contexto de sua criação não permitiu a seus "pais fundadores" pensar em tais questões, pois elas, simplesmente, não eram relevantes ou sequer existiam. Como postula Voegelin (1982, p. 19), "[...]objetos diferentes requerem métodos diferentes"; o mesmo vale para as diferentes "regras de inferências" (KING; KEOHANE; VERBA, 1994, p. 6, 24-27), adotadas nos diferentes tipos de pesquisas empíricas em RI (JACKSON, 2011, p. 18). Todas essas afirmações giram, de uma maneira mais geral, em torno do fato de que "[o]s problemas culturais que fazem mover a humanidade renascem a cada instante e sob um aspecto diferente" (WEBER, 2006, p. 63). Os estudos e acontecimentos internacionalistas sobre ciberespaço renascem neste início de século, provocando uma verdadeira ruptura científica – de que fala Kuhn (2006) – em RI.

Nisso, faz até sentido subdividir os dois primeiros sistemas complexos – naturais e sociais – de acordo com critérios de tempo e espaço, daí a importância da História e da Geografia. Porém, o mesmo não vale para o ciberespaço. O máximo que se pode conjecturar, quanto a isso, são metáforas e analogias. Exemplificando: em História das Relações Internacionais e em Geopolítica, versa-se muito acerca da Guerra Fria; em contrapartida, em CiberRI, pode-se falar em sua correlata digital, a Guerra Fria Cibernética (*Cyber Cold War*), tão empregada em estudos de análise mais técnica, porém com impactos mais políticos – poder-se-ia chamar a isso de securitização cibernética feita por empresas de antivírus, notadamente pela Kaspersky e pela Symantec. É nesses termos que Demchak (2014, p. viii) assevera que tais ferramentas mentais, que capturam processos abstrusos por meio de termos ou imagens simples, como "Westfália Cibernética" (*Cyber Westphalia*) ou *Cyberpolitik*[95], pressupõe uma "infiltração semântica" que altera lentamente a percepção de acadêmicos e abre oportunidades cognitivas para novas teorizações e discussões estratégicas. Uma dessas oportunidades é justamente compreender como esses conceitos são construídos e alocá-los em relação a seu produtor. E isso só ocorre por meio de uma sistematização do conhecimento científico, cujo modelo para os estudos internacionalistas sobre o ciberespaço se apresenta na próxima

[95] Cf. VALENTE, 2007, p. 37-38.

subseção.

1.3 O Modelo 3C de sistematização do subcampo ciberinternacionalista

Como se vê, sobretudo, na subseção 1.1, ciência é, etimologicamente, sinônimo de conhecimento. Gil (1999, p. 20, grifo do autor) vai mais além do que essa afirmação simplória e atesta que "[...]a ciência pode ser caracterizada como uma forma de conhecimento objetivo, racional, *sistemático*, geral, verificável e falível". Portanto, esta subseção propõe um modelo que se volta, de maneira precípua, para o atributo científico da sistematização do conhecimento, no caso, ciberinternacionalista. De acordo com Rudner (1969, p. 47), "[...]os modelos funcionam como recursos heurísticos na ciência" e, como tal, não são passíveis de confirmação e refutação, como as teorias (*ibid*., p. 44-50, 86). O principal problema a ser lidado por tal modelo não é a fragmentação temática, *per se*, mas, sim, as consequências que sua *excessiva* fragmentação traz, fazendo com que a desorganização impere no atual estado de coisas de CiberRI, e, logo, não consiga desenvolvê-lo enquanto subcampo científico.

A despeito de outros campos e subcampos, a fragmentação pode constituir um ponto forte, mas, especificamente para os estudos internacionalistas que envolvem o ciberespaço, ela não o é, pois, *ceteris paribus*, RI deixa de ganhar em termos de aperfeiçoamento, constituindo-se, arrisca-se a dizer, o que na Economia se conhece por *custos de oportunidade*. Dessa forma, propõe-se sua desfragmentação, ou melhor, sua sistematização, por meio de CiberRI. Isso traz novamente à vista a primeira hipótese secundária, no sentido de afirmar que a criação de um subcampo ciberinternacionalista é uma necessidade frente aos atuais desafios que o ciberespaço e seu estudo provocam em RI. Antes, porém, de prosseguir com a apresentação desse modelo que corrige tal problema, é preciso definir os conceitos de fragmentação e sistematização, aos olhos dos objetivos desta Tese.

No âmbito científico, demarcar o que é fragmentação é um ato relativamente maniqueísta, *i.e.*, tanto pode designar algo positivo quanto negativo, dependendo do contexto geral, da situação em específico ou do objeto estudado. Contudo, escolhe-se a conceituação feita por Martins ([200-]), engendrada para avaliar a formulação e a implementação de políticas públicas, mas que sua adaptação diz muito sobre o estado de coisas dos estudos internacionalistas sobre o ciberespaço. Ei-la: "[a] fragmentação é o resultado de um processo descoordenado, inconsistente e incoerente[...]. A[ssim, a] *fragmentação* pode ser atribuída à *falta de coerência, consistência e coordenação*" (MARTINS, [200-], p. 3, grifo nosso).

Ora, se se espera que CiberRI seja reconhecido como um subcampo científico dentro da comunidade epistêmica de RI, então, igualmente, ele tem de trazer contribuições substanciais a

seu campo-*master*. Seguindo essa linha de pensamento, almeja-se que CiberRI forneça um modelo capaz de prover coerência, consistência e coordenação, em termos metateoréticos. Assim, propõe-se o Modelo de Coerência epistemológica, Consistência teórico-metodológica e Coordenação acadêmica (3C) aos estudos internacionalistas sobre o ciberespaço, que, logicamente, pode também ser aplicado a outros campos e subcampos científicos, respeitadas suas devidas adaptações.

Com vistas a corrigir o problema da fragmentação excessiva do objeto de estudos de CiberRI, é preciso dimensioná-lo. Como, então, mensurar essa fragmentação? Em relação a isso, Martins ([200-], p. 4, grifo nosso) também fornece fortes indícios, ao asseverar que:

> *A mensuração da fragmentação é problemática, embora sua qualificação seja possível*. A quantidade [...]de atores envolvidos (pessoas, organizações etc.) e de domínios [...]pode ser bom indicador de complexidade, e, na melhor das hipóteses, indicar potenciais problemas de coordenação[...]. Mas a construção de uma escala de mensuração ou avaliação qualitativa-ordinal da fragmentação deve se apoiar na operacionalização de variáveis que se constituem fatores fragmentadores. [...]*No sentido normativo, atribuir uma condição de problema a uma circunstância de fragmentação equivale a uma aposta na racionalidade, ainda que sujeita a inúmeros constrangimentos*. Nesse sentido, a fragmentação, embora possa ser considerada um padrão recorrente e uma consequência esperada, representa ineficiência.

Em substância, a resposta para a fragmentação temática do ciberespaço em RI se liga inexoravelmente aos alcances de uma integração coordenada, por meio de um prognóstico que leve em conta uma mensuração de sua empiria, consubstanciada, por sua vez, em termos ontológicos, epistemológicos e metodológicos. Em outras palavras, a correção dos problemas oriundos da excessiva fragmentação temática sobre o ciberespaço em RI passa, necessariamente, por um processo retroalimentar de integração e reintegração coordenado e sistematizado do conhecimento já produzido nessa área.

No que concerne à sistematização em si, tal conceito, quando aplicado ao conhecimento científico, associa-se a suas pressuposições (JACKSON, 2011, p. 193). Sobre isso, Wallerstein *et al*. (1996, p. 14, grifo nosso) lembram que as raízes das ciências sociais "[...]mergulham na tentativa[...] de *desenvolver um saber sistemático* e secular *acerca da realidade*, que de algum modo possa ser *empiricamente validado*". Portanto, sistematizar o conhecimento científico – seja social ou político, seja internacionalista ou ciberinternacionalista[96] – pressupõe validar empiricamente dados da realidade social, afinal a ciência pode ser também concebida como "[...]o conjunto de *conhecimentos* obtidos através da *investigação sistemática*, objetiva *e empírica*" (MEGALE, 1990, p. 41, grifo nosso). Logo, esse tipo de investigação compreende

[96] Até mesmo fora da ciência, é possível ver exemplos de sistematização do conhecimento, como aquele levado a cabo pelos adeptos da chamada "teologia da libertação" (SOUSA, 1982, p. 9).

estudos, pesquisas e buscas de dados de forma "[...]criteriosa, metódica, [e] dentro da lógica ou *coerência*" (*ibid*., p. 42, grifo nosso).

Por um lado, se, no século XIX, essa busca pela investigação sistemática da realidade social origina a criação de várias disciplinas especializadas (WALLERSTEIN *et al*., 1996, p. 21), por outro, as últimas décadas do século XX testemunham um movimento inverso. Atualmente, CiberRI resgata um aspecto qualitativo da sistematização proposta séculos atrás, mas não sua propositura oitocentista originalmente contida na demarcação rigorosa de limites para os objetos de pesquisa e suas disciplinas. CiberRI atualiza tal proposta, à luz da multidisciplinaridade e da interdisciplinaridade[97], que são o mote para o aperfeiçoamento científico hodierno, sobretudo para suas IES. Daí, também, o porquê de epitetar CiberRI de *oximoro científico*.

Assim, a sistematização do conhecimento ciberinternacionalista encontra eco nas assertivas de que:

1. A pesquisa científica se baseia em três componentes necessários, quais sejam: sistematização; publicação; e produção de conhecimento sobre o mundo, em que pese o primeiro ser o mais importante deles (JACKSON, 2011, p. 189, 193);
2. "Pesquisar fatos e multiplicar observações, sem comparar nem *sistematizar*, não é um método científico, mas, apenas, empirismo" (DUVERGER, 1962, p. 305, grifo nosso); e
3. "Ao *sistematizarmos* a compreensão do caráter político da tecnologia[,] podemos afirmar que ela contém um elevado potencial de *poder* que se expressa nas *relações sociais*" (KAWAMURA, 1986, p. 45, grifo nosso).

Nesse viés, o ponto de partida para a sistematização temática do ciberespaço em RI – ou seja, sua transmudação de "conhecimento internacionalista sobre o ciberespaço" para "conhecimento ciberinternacionalista" – deve basear-se em um *framework* de análise que seja, ao mesmo tempo, abrangente em seus *inputs* e específico em seus *outputs*. Diante desse prisma, adapta-se o modelo de investigação científica baseado em campos e polos, de Bruyne, Herman e Schoutheete (1991), à lógica do Modelo 3C.

Em resumo, para esses autores, a investigação social pressupõe a imersão do pesquisador em esferas e subesferas que o influenciam na apreensão e compreensão da

[97] Sobre isso, conferir Brasil (2012b), Megale (1967, p. 55, 57-58, 76), Resende (2005, p. 17), Valente (2007, p. 34, 173) e Wallerstein *et al.* (1996, p. 60-62, 71-74, 111). Um dos principais exemplos nas searas multidisciplinar e interdisciplinar em CP são os Estudos de Áreas (*Área Studies*), que florescem durante a Guerra Fria (WALLERSTEIN *et al*., 1996, p. 59-63).

realidade. *Grosso modo*, eles separam os campos entre o da demanda social, o axiológico, o doxológico e o epistêmico; e os polos em epistemológico, teórico, morfológico e técnico (BRUYNE; HERMAN; SCHOUTHEETE, 1991, p. 39-61, 99-130, 157-171, 199-219). Aqui, destacam-se os campos doxológico e epistêmico, bem como o polo teórico, que faz parte do campo epistêmico, mas que, em certo momento, também é elevado à categoria de campo BRUYNE; HERMAN; SCHOUTHEETE, 1991, p. 202).

O mais amplo desses três campos escolhidos é o Doxológico[98]. Esse termo advém do conceito platônico de *doxa* e exprime um conjunto de opiniões não-críticas e não passíveis à discussão (BOURDIEU, 1983b, p. 150; VOEGELIN, 1982, p. 22, 34). Ele corresponde à "realidade de todos os dias", isto é, ao conjunto das ações e conhecimentos em que residem o problema de pesquisa e todas as *informações* acerca dele, carregados daquilo que Weber (2006) chama de *significação*[99], porém sem ainda ser explicitada como tal.

Já o segundo campo é o Epistêmico[100]. As *epistemes* constituem recortes mais amplos da realidade ou do mundo (HAAS, 1992, p. 26-27), em que se busca *apreender* o problema da realidade – *i.e.*, isolar uma parte do seu todo, neste caso, sociopolítico-internacionalista –, procedendo, assim, a uma "ruptura epistemológica", tanto do ponto de vista teórico quanto prático, por meio, dentre outros, da aplicação de *técnicas de coleta* que selecionam e transformam as informações em *dados*. Em suma, este campo busca envolver os limites do conhecimento científico (GIL, 1999, p. 55).

Por fim, o terceiro campo é o Teórico, que reduz a realidade para o formato de hipóteses falseáveis, as quais só serão passíveis de serem refutadas após a análise teórica dos dados – agora, subidos à categoria de *fatos*[101]. Pode-se afirmar que o Campo Teórico leva ainda em consideração a premissa de que "[...]a teoria[,] como explicação de certas experiências[,] só é inteligível para aqueles em que a explicação desperte experiências paralelas como base *empírica* para testar a verdade da teoria" (VOEGELIN, 1982, p. 56, grifo nosso). Essa premissa

---

[98] Sobre linhagens orto*doxa* e hetero*doxa*, ver Bourdieu (1983b, p. 145).

[99] Sobre tal ponto, Weber (2006, p. 95, grifo do autor) assim esclarece: "[t]odos esses sistemas [de pensamento, imprescindíveis para a compreensão dos elementos significativos da realidade] não passam de *tentativas* para conferir uma *ordem ao caos dos fatos* que incluímos no âmbito de *nosso interesse*, e que são realizadas *com base no estado atual de nossos conhecimentos e nas estruturas conceituais* de que dispomos". Lipson (1967, p. 33, grifo nosso) parece beber também da fonte weberiana, ao afirmar que "[...]a história política e os Governos contemporâneos exibem certas estruturas que lhes conferem *significação*. E tais estruturas[...] permitirão que muitos *acontecimentos*, aparentemente *caóticos* e capazes de gerar confusão, *sejam enquadrados nos seus devidos lugares*". Ainda sobre a significação, no âmbito das ciências, ver Rudner (1969, p. 118-119).

[100] Para uma diferenciação entre *doxa* e *episteme*, ver Voegelin (1982, p. 23).

[101] Ainda sobre os fatos, no âmbito da *episteme* sociopolítica-internacionalista, ver Jackson (2011, p. 21), Voegelin (1982, p. 53) e Waltz (2003, p. viii).

da empiria será invocada novamente na terceira e última seção desta Tese. Em suma, ao passo que:

> A *informação* conserva a significação das práticas sociais efetivas, o *dado* deve neutralizar essa significação primeira e transformá-la em significação pertinente para a pesquisa científica. [...]Os *fatos* remetem a enunciados empíricos que descrevem situações observadas[...]. (BRUYNE, HERMAN; SCHOUTHEETE, 1991, p. 203-204, grifo nosso).

Após a exposição desse arcabouço teórico-metodológico, é possível traçar um paralelo entre tal divisão dos campos e a própria esquematização desta Tese, no sentido de apontar que: a Introdução corresponde ao Campo Doxológico; as seções 1 e 2, ao Campo Epistêmico, tendo em vista que elas buscam desagregar os dados mais abrangentes dos estudos internacionalistas sobre o ciberespaço; e a seção 3 corresponde ao Campo Teórico, que reagrupa os dados[102] em informações carregadas de significação, com o intuito de formar um panorama o mais próximo possível do seu estado de coisas.

A Figura 3 apresenta graficamente a visão geral do Modelo 3C de sistematização que se busca aplicar a CiberRI, à luz dos pressupostos científicos e dos arcabouços teórico-metodológicos analisados nesta primeira seção.

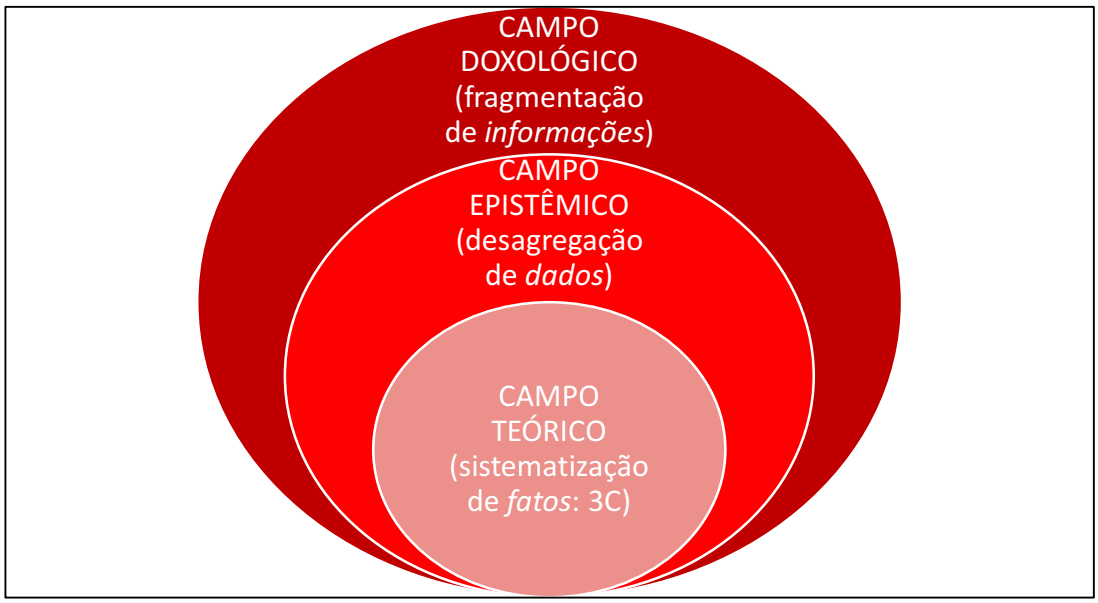

Figura 3 Modelo 3C de sistematização temática do ciberespaço em RI
Fonte: elaboração própria, a partir de Bruyne, Herman e Schoutheete (1991, p. 202) e Martins ([200-]).
Legenda: 3C = Coerência epistemológica, Consistência teórico-metodológica e Coordenação acadêmica.

[102] Eis aqui, portanto, duas características que diferenciam, por exemplo, CP e RI da História: "[...]a necessidade de *segmentar a realidade humana* para poder analisá-la" e "[...]a opção por provas produzidas de forma *sistemática*[...]" (WALLERSTEIN *et al*., 1996, p. 51, grifo nosso).

Nesse viés, a sistematização pressupõe a existência de uma "[...]teoria prévia, que se modifica com o correr da análise. *Observação e sistematização não são duas operações isoladas*[...]. A ideia de ciência é inseparável do emprego associado dessas duas técnicas" (DUVERGER, 1981, p. 32, grifo nosso). Mesmo esta Tese investindo em técnicas complexas, *softwares* de última geração e literatura especializada recente – ou seja, uma busca a mais próxima possível do estado da arte dos estudos internacionalistas sobre o ciberespaço –, a realidade jamais será apreendida por completo, ou, mais especificamente, um acontecimento ciberinternacionalista jamais será descrito de forma exaustiva. Isso se justifica porque, por mais minuciosa que seja a pesquisa ou por mais detalhados que sejam seus resultados (MEGALE, 1990, p. 56), "[...]todo conhecimento reflexivo da realidade infinita realizado pelo espírito humano finito baseia-se no pressuposto tácito de que apenas um *fragmento* limitado dessa realidade poderá constituir de cada vez o *objeto da compreensão científica*" (WEBER, 2006, p. 44, grifo do autor). Este objeto de que fala o pensador alemão não é, aqui, o ciberespaço em si, mas os trabalhos sobre ele, produzidos pela comunidade epistêmica de RI.

Seguindo dessa maneira os passos de Weber (2006, p. 52) sobre a significação cultural como chave motriz para as ciências sociais, bem como os preceitos por traz do Modelo 3C, o ponto-chave desta Tese investiga a *significação cultural* de CiberRI. Isso se liga, umbilicalmente, ao fato de que, se determinada porção de estudiosos de RI tem uma necessidade de conhecer os acontecimentos cibernéticos – necessidade esta comprovada pelo número cada vez maior de pesquisas e estudos sobre o tema (PORTELA, 2016) –, então nada mais lógico do que lhe conferir um *locus* para congregar e agregar tematicamente as pesquisas e os resultados já produzidos sobre o assunto, bem como orientar trabalhos futuros, sob a égide de um subcampo minimamente organizado. Parafraseando Weber (2006, p. 52) e Lipson (1967), o que interessa aqui é analisar a *significação cultural* do *fato histórico* de o ciberespaço constituir, atualmente, um *grande problema*[103] de RI. Essa busca incessante de se enquadrar o impacto do ciberespaço nas relações internacionais como um grande problema de RI se deve, também e em parte, ao que o francês Bourdieu (1983b, p. 125) confabula da seguinte maneira: "[...]a tendência dos pesquisadores a se concentrar nos problemas considerados como os mais

[103] Este é o título da *magnum opus* de Leslie Lipson, que traz cinco grandes problemas – ou questões básicas – da CP, quais sejam: extensão da cidadania; funções do Estado; fonte da autoridade; poder como organizador da autoridade; e limites internos e externos do Estado (LIPSON, 1967, p. 36). Os problemas com que esta Tese mais dialoga são os seguintes: o segundo, principalmente quanto à função primária que atesta ser o Estado o garantidor da segurança dos seus concidadãos; o quarto, especificamente na conceituação do poder político; e o quinto, no que tange às relações internacionais. O fio condutor das cinco teses de Lipson e o Modelo 3C proposto por CiberRI é que ele procura "[...]explicar a natureza da política através do *tratamento sistemático* de seus problemas fundamentais[...]" (LIPSON, 1967, p. 16, grifo nosso).

importantes se explica pelo fato de que uma contribuição ou descoberta concernente a essas questões traz um lucro simbólico[...]". O lucro simbólico de CiberRI, portanto, é ser reconhecido por seus pares como tal, ou seja, como um subcampo internacionalista.

Dessa forma, o viés desta Tese busca se assemelhar aos desígnios do artigo seminal de Hall e Taylor (2003), que buscam sistematizar o conhecimento neoinstitucionalista, mediante a integração de três abordagens – institucionalismo histórico, institucionalismo da escolha racional e institucionalismo sociológico –, as quais são diferentes entre si, mas que guardam características que as aproximam ou distanciam do todo epistêmico de que derivam, *i.e.*, do Institucionalismo. Para tais autores:

> Considerando-se os objetos que elas [as três visões do Neoinstitucionalismo] têm em comum, é paradoxal que essas três escolas de pensamento tenham se desenvolvido de modo independente, ao menos a julgar pela *escassez de referências cruzadas na literatura*. Em consequência, um dos nossos principais cuidados consiste em *nos perguntar o que cada uma delas poderia aprender das outras*. (HALL; TAYLOR, 2003, p. 195, grifo nosso).

Assim, entende-se que grande parte do conhecimento internacionalista já produzido sobre o ciberespaço encontra-se desorganizadamente esparsa e fragmentada sob a bruma de diferentes autores, correntes e instituições. Remontando a Hall e Taylor (2003), a propositura de CiberRI indaga o que cada um deles poderia aprender com e apreender dos demais, e, consequentemente, como RI tiraria melhor proveito dessa sistematização. Uma resposta acadêmica a tal inquietação é vista na próxima seção.

2 UMA DEFESA ACADÊMICA

> Mensagens, representações circulam pela megarrede, sujeitas a múltiplas traduções e interpretações. Desorientam alguns, mas dinamizam novos fluxos acadêmicos. O novo saber flui entre o que vive. (RESENDE, 2005, p. 22).

Como visto, a ciência "[...]investiga problemas que ocorrem na vida real, e esta[...] gera novos valores e [...]padrões de comportamento; daí *a variedade de temas e de aspectos de um único problema* a despertarem a curiosidade e incentivarem o trabalho dos cientistas sociais" (MEGALE, 1990, p. 83, grifo nosso). Nesse sentido, a presente seção analisa justamente como um desses temas científicos, o ciberespaço, torna-se aspecto imprescindível para se compreender um dos grandes problemas de CP e RI na atualidade, que é a questão do poder cibernético e seus desdobramentos internacionais. Com isso, espera-se despertar a curiosidade e, por conseguinte, incentivar trabalhos, sobretudo, de cientistas sociais, políticos e internacionalistas nessa nova seara.

Diante desses desafios, a presente seção se vale de uma ideia que vai ao encontro da máxima de que RI "[...]costuma apresentar resultados promissores, quando enfrentada a partir de um consórcio com áreas acadêmicas *vizinhas*" (BRASIL, 2012b, p. 1, grifo nosso). Posto de forma diferente, defende-se, sob a tutela do que se chama aqui de CiberRI, um consórcio não apenas com outras áreas afins a RI, mas também com outras que dela estão, por assim dizer, distantes, mas que podem apresentar, por mais inesperado que seja, resultados igualmente – ou mais – promissores, conforme se viu na seção anterior.

Até aqui, analisou-se muito d*o que é* CiberRI. Em contrapartida, evidencia-se ser também possível diferenciá-lo, ontológica e epistemologicamente, de outras propostas, conceitos e definições *que não são* CiberRI, e que repousa, em última instância, na produção científica de instituições acadêmicas. Sobre essa diferenciação ontológica de conceitos e descrições, Rudner (1969, p. 105, 124) pondera que ser uma descrição de algo não é, evidentemente, *sê-lo*.

Em linhas gerais, pode-se afirmar, categoricamente, que CiberRI não é *qualquer* estudo, pesquisa ou análise acadêmica que apenas envolva, de um lado, um objeto geralmente estudado em Ciência da Computação ou da Informação e, do outro, em RI. Por exemplo, ao noticiar que os EUA ainda utilizam disquetes para operacionalizar sistemas nucleares sob a antiga – mas não ultrapassada – linguagem de programação COBOL (FORÇAS..., 2016), não se está versando sobre CiberRI, mas, sim, sobre dois objetos de grande interesse, de um lado, para cientistas da computação, por meio dos disquetes e do COBOL, e, de outro, para internacionalistas, especialmente aqueles que se debruçam sobre os impactos dissuasórios e

estratégicos do sistema nuclear estadunidense ou dos acordos – e seus protocolos – de não proliferação nuclear. Portanto, trata-se de um trabalho eminentemente internacional, meramente internacionalista e potencialmente ciberinternacionalista, haja vista que lhe faltam elementos metateoréticos de RI para analisar, por exemplo, os impactos, na política internacional, da manutenção dos disquetes e sua possível falta de segurança, que poderia acarretar o acesso indevido a sistemas de armas de destruição em massa (MAD, do inglês) da maior potência mundial.

Diante da problemática em se garantir critérios mínimos para se qualificar algo como "ciberinternacionalista", CiberRI abarca, em termos epistemológicos, praticamente qualquer tema já abarcado por RI, *desde que* satisfaça a, no mínimo, duas condições, quais sejam: (*i*) pelo menos, uma de suas variáveis de estudo advenha de um tema correlato ao ciberespaço; e (*ii*) aporte-se em um dos três pressupostos metateóréticos de RI, vistos na subseção 1.2, *supra*. Essa relação condicional entre as variáveis e os aspectos metateoréticos, de uma maneira geral, pode ser entendida também a partir daquilo que Weber (2006, p. 32-33) chama de "economicamente relevante" e "economicamente condicionado", ao versar sobre Economia Política. Nesse seguimento, se o mínimo das duas proposições *i* e *ii* for atendido, está-se falando de algo "ciberinternacionalmente condicionado" ou de uma condição suficiente; caso se abarque apenas uma delas, trata-se de algo "ciberinternacionalmente relevante" ou de uma condição necessária.

É nesse sentido que se pode incluir a obra "*Cyberpolitics in international relations*"[104], da egípcia Nazli Choucri, na categoria de "ciberinternacionalmente condicionado". Porém, se, de um lado, ela se enquadra no escopo de CiberRI, do outro, *não é* CiberRI. Na verdade, o que Choucri (2012, *passim*) chama de "política cibernética nas relações internacionais" não é a mesma coisa que esta Tese chama de Relações Internacionais Cibernéticas, haja vista a própria definição de política cibernética dada pela autora, qual seja:

> [...]termo cunhado recentemente para se referir à junção de dois processos ou realidades, quais sejam: interações humanas (*política*), que determinam *quem recebe o que, quando* e *como*; e capacidade de usar um espaço virtual (*ciber*) como nova arena de disputa com suas próprias modalidades e realidades. (CHOUCRI, 2012, p. 4, grifo da autora, tradução nossa[105]).

[104] O livro de Choucri (2012) origina-se do primeiro curso *Cyberpolitics in International Relations*, ofertado pelo projeto *Explorations in Cyber International Relations* (ECIR), entre MIT e Universidade Harvard.

[105] Texto original: "*Cyberpolitics*, a recently coined term, refers to the conjunction of two processes or realities — those pertaining to human interactions (*politics*) surrounding the determination of *who gets what, when*, and *how*, and those enabled by the uses of a virtual space (*cyber*) as a new arena of contention with its own modalities and realities".

Já a portuguesa Joana Maria Gomes Pereira também trata de temas assaz afeitos à CiberRI, em sua Dissertação de Mestrado em RI, institutala "O ciberespaço e a mutação da realidade ou como este novo campo de atuação modifica as relações internacionais". Porém, ela segue uma linha de pensamento que se vê até 2014, em que a comunidade internacionalista foca em temas afeitos ao objeto, e não ao subcampo de CiberRI. Esse trabalho, com efeito, tem o objetivo de perceber, "[...]de forma mais específica, como é que o ciberespaço alterou o entendimento de dois conceitos estruturantes da ordem internacional: soberania e segurança" (PEREIRA, 2013, p. 1).

Igualmente, a coletânea "*Cyberspace and International Relations: theory, prospects and challenges*", editada pelas alemãs Jan-Frederik Kremer e Benedikt Müller, em 2014, traz uma contribuição significativa para os estudos ciberinternacionalistas. Todavia, seu objetivo não é o de criar um subcampo internacionalista sobre o ciberespaço, e sim analisar, teórica e empiricamente, os impactos econômicos, políticos e sociais do diálogo entre ciberespaço e relações internacionais, com o fulcro de evidenciar aquilo que chamam de processo de "ciberização" (*cyberization*) das relações internacionais (KREMER; MÜLLER, 2014a, p. xi).[106]

Na ótica de CiberRI, todos esses trabalhos, produzidos no âmbito da academia, encaixam-se nos dois requisitos básicos para serem considerados "ciberinternacionalistas". Todavia, nenhum deles, assim como os demais analisados nesta Tese, propõem a criação de um subcampo aos moldes do que faz esta Tese. Como se vê, é preciso desagregar os dados, no Campo Epistêmico de RI, para formar uma pintura a mais organizada possível do estado de coisas de CiberRI; somente assim, o conhecimento ciberinternacionalista pode surgir, de forma organizada e sistemática, dando vida a seu próprio subcampo científico.

Agora, relembra-se *o que é* CiberRI. Nos termos do presente trabalho, é um subcampo de RI que trata de temas afeitos ao ciberespaço e que não pode ser abordado por outras ciências[107], da mesma forma com que "[...]o estudo [derivante] da Ciência Política não se enquadra em subárea de qualquer outra disciplina porque apresenta objeto próprio[...], como os estudos sobre [...]poder, [...]Estado, nação, soberania[...]" (DEPARTAMENTO..., [201-]). É

[106] Notar que as autoras utilizam o termo RI para se referir ao objeto, e não ao campo de RI. Quanto àquilo que chamam de "ciberização" das relações internacionais, elas assim definem tal processo: "*'Cyberization' of IR refers to the ongoing penetration of all different fields of activity of international relations by different mediums of the cyberspace on the one hand, and the growing dependence of actors in IR on infrastructure, instruments, and means offered by the cyberspace on the other hand*" (KREMER; MÜLLER, 2014a, p. xi, grifo nosso).

[107] Cf. DUVERGER, 1981, p. 9. Aqui, novamente, resgata-se a definição de Ontologia, posta na subseção 1.2, *supra*.

nesse prisma que não se espera que cientistas da computação estudem, em termos gerais, o exercício do poder ou, em termos específicos, a política internacional no âmbito do ciberespaço[108], mas, sim, que se debrucem, por exemplo, em apontar como as novas TICs impactam – ou possam vir a impactar –, em termos técnicos e tecnológicos, os conflitos internacionais ou o progresso científico das nações – neste caso, podendo, até mesmo, nortear-se pelo inciso IX do Art. 4º da Constituição Federal de 1988 (CF88).[109]

A observação acima igualmente se estende a outras ciências afins a CP/RI, como o Direito[110], cujo objeto de estudo – a lei ou norma jurídica – lhe é, ao contrário do de CP, inerente ao próprio campo. Nesse viés, CiberRI não cria seu objeto característico – como o faz, por exemplo, Redes de Computadores, cujo objeto principal são, como não poderia deixar de ser, as redes de computadores –; ele lhe é *ex-ante*. Mais ainda, por ser interdisciplinar, CiberRI possui um objeto de estudos composto por dois elementos que, separados, são necessários, mas que, juntos, são suficientes para fornecer sua *raison d'être*, quais sejam: o ciberespaço e as relações internacionais. É justamente na junção desses dois elementos que se observa a ideia de CiberRI florescer no seio acadêmico, conforme relata sua brevíssima história.

2.1 Breve histórico de CiberRI

De forma mais genérica, pode-se remontar à ideia de um subcampo ciberinternacionalista a algumas empreitadas acadêmicas que, colateralmente, tocam mais ao objeto de CiberRI do que ao subcampo propriamente dito.

Certamente, dentre todos, o que mais chega perto do que aqui se defende é o projeto estadunidense intitulado *Explorations in Cyber International Relations* (ECIR), patrocinado pelo *U.S. Office of Naval Research* e encabeçado pelo Instituto de Tecnologia de Massachusetts (MIT) e pela Universidade Harvard. Não obstante o "ECIR ser um programa de pesquisa colaborativo e interdisciplinar que busca criar um campo de *relações cibernéticas internacionais* para o século 21" (MIT; UNIVERSIDADE HARVARD, 2013a, grifo nosso,

[108] Nesse mesmo viés crítico, ver Jackson (2011, p. 16).

[109] Cf. BRASIL, 1988, p. 6.

[110] Assim como ocorre com outras ciências, há também divergência quanto a alocar Direito nas ciências sociais (DUVERGER, 1981; MEGALE, 1990; WALLERSTEIN *et al.,* 1996). Todavia, não se pode negar sua relação intrínseca com elas, sobretudo pelo fato de, no Brasil, alguns cursos de Direito chamarem-se, formalmente, "Ciências Jurídicas e Sociais". Diante disso, manteve-se o exemplo dessa ciência aqui; se pertence ou não às ciências sociais, é uma discussão secundárias aos desígnios deste trabalho.

tradução nossa[111]), suas publicações[112] voltam-se, especialmente, para a integração – mediante testagem de teorias e novos procedimentos metodológicos – do ciberespaço à agenda das ciências sociais e jurídicas.

Não se esconde que CiberRI captura seu nome do ECIR (GUEDES DE OLIVEIRA; GAMA NETO; VILAR LOPES, 2016a, p. 31), porém esta Tese dá um passo além – talvez, o passo que faltava àquele projeto –, no sentido de rumar à criação de um subcampo internacionalista, e não à adaptação do campo de RI a outras ciências. Posto de forma diferente, CiberRI buscar constituir "[...]uma espécie de *quase-disciplina*, com os seus programas, revistas, associações e coleções de bibliotecas", como ocorreu, por exemplo, com os estudos sobre Economia Política Internacional, cultura (WALLERSTEIN *et al*., 1996, p. 95, grifo nosso) e Terminologia (BARROS, 2004, p. 21).

Ademais das publicações do projeto ECIR iniciarem em 2009, sobretudo com escritos importantes de Joseph Nye Jr acerca dos conflitos cibernéticos envolvendo a Rússia no final dos anos 2000, podem-se evidenciar algumas contribuições brasileiras que trazem o termo "digitais" no lugar de "cibernéticas", tais como: (i) a apresentação do trabalho "*El régimen internacional de lucha contra los cibercrímenes: la institucionalización de las relaciones internacionales digitales entre los años 1980 y 2000*", de Lopes (2010), na *I Jornada de Estudiantes de Ciencia Política y Relaciones Internacionales*, organizada pela Associação Latino-Americana de Ciência Política (ALACIP), na Argentina, em 2010; e (ii) ao trecho "[...]a Diplomacia da Internet é um conjunto de pressupostos que orienta as *relações internacionais digitais*[...]" do *paper* de Lopes e Medeiros (2011, p. 8, grifo nosso), apresentado e publicado nos anais do Encontro Nacional da Associação Brasileira de Relações Internacionais (ABRI), em 2011.

Se o início dos anos 2000 marca, com os atentados do Onze de Setembro, um momento de inflexão para análises internacionais sobre o ciberespaço como fonte de insegurança (LOPES, 2013), o início dos anos 2010 representa o mesmo para os estudos internacionalistas sobre o ciberespaço, devido, sobretudo, a importantes acontecimentos internacionais, envolvendo ataques cibernéticos e políticas públicas de Segurança e Defesa Cibernética. Um dos grandes destaques fica por conta da tentativa de sabotagem do programa nuclear iraniano, por meio de um *worm* estrangeiro, o Stuxnet. Nesse momento, alguns membros da comunidade

---

[111] Texto original: "*ECIR is a collaborative and interdisciplinary research program that seeks to create a field of international cyber relations for the 21st century*".

[112] Para uma listagem das publicações do ECIR, entre os anos de 2009 e 2013, ver MIT e Universidade Harvard (2013b).

epistêmica de RI se juntam a outros mais afeitos à área computacional para produzir análises sobre o impacto de armas cibernéticas e da guerra cibernética na política internacional. Todavia, muitos desses trabalhos restringem-se a descrever o *worm* e/ou seu *modus operandi*, dando pouca atenção ao contexto geopolítico que envolve o programa nuclear iraniano. Um dos poucos a se ater a esse elo entre ciberespaço e relações internacionais é Sanger (2012), professor de CP/RI na Universidade Harvard, que, ao lado de Joseph S. Nye Jr e Richard A. Clarke, também faz parte de projetos correlatos à temática aqui abordada.

No Brasil, em 2012, a CAPES aprova o projeto "Vigilância nas fronteiras e muros virtuais: um estudo analítico de políticas públicas e sistemas operacionais de proteção às estruturas estratégicas terrestres", encabeçado pelo Programa de Pós-Graduação em Ciência Política da Universidade Federal de Pernambuco (PPGCP-UFPE), para compor o portfólio do Programa de Apoio ao Ensino e à Pesquisa Científica e Tecnológica em Assuntos Estratégicos de Interesse Nacional (Pró-Estratégia)[113], na Área de Concentração "Ciência Política e Relações Internacionais". Esse projeto acaba se tornando um dos primeiros intentos acadêmicos a gerar, de forma interdisciplinar e multi-institucional civil-militar, discussões, eventos e publicações acerca dos impactos técnicos e políticos do ciberespaço no pensamento estratégico brasileiro de Defesa e nos ESI. A partir desse projeto do Pró-Estratégia, surgem novos espaços para se debater o ciberespaço a partir de uma ótica não apenas técnica, mas também estratégica, política e internacionalista. Uma dessas oportunidades é a publicação, em 2014, do primeiro volume da Coleção "Defesa & Fronteiras Virtuais", da Editora da UFPE, intitulado "Segurança e Defesa Cibernética: das fronteiras físicas aos muros virtuais" (MEDEIROS FILHO; FERREIRA NETO; GONZALES, 2014), aglutinando estudiosos e profissionais civis e militares das mais diversas áreas do conhecimento, inclusive de CP e RI.

Como se vê até aqui, é o objeto de CiberRI que está em franco desenvolvimento, não o seu subcampo. A percepção de se criar tal subcampo começa a tomar forma a partir da realização do "I Seminário de Relações Internacionais Cibernéticas (CiberRI)", que ocorre, também em 2014, no Departamento de Relações Internacionais (DRI) da Universidade Federal da Paraíba (UFPB), com o objetivo de discutir as possibilidades de os estudantes e pesquisadores internacionalistas analisarem o ciberespaço a partir de elementos metateoréticos de RI, com ênfase na questão da segurança internacional.

Ainda no mesmo ano de 2014, Vilar Lopes (2014) apresenta o pôster "Relações Internacionais Cibernéticas (CiberRI): uma defesa acadêmica", durante o Encontro Nacional

[113] Parceria entre a CAPES e a extinta Secretaria de Assuntos Estratégicos da Presidência da República (SAE/PR).

da Associação Brasileira de Estudos de Defesa (ABED), em Brasília. É, possivelmente, a primeira vez que a criação de um subcampo ciberinternacionalista é defendida, em termos acadêmicos, ao crivo de parte da comunidade epistêmica de RI.

Finalmente, em 2016, lança-se o terceiro volume[114] da Coleção "Defesa & Fronteiras Virtuais", intitulado "Relações Internacionais Cibernéticas (CiberRI): oportunidades e desafios para os Estudos Estratégicos e de Segurança Internacional" (GUEDES OLIVEIRA; GAMA NETO; VILAR LOPES, 2016b). Destaca-se que essa coletânea reúne cientistas políticos e internacionalistas do Brasil e da Argentina, que analisam, teórica e empiricamente, a inserção do ciberespaço no âmbito dos Estudos Estratégicos, de Defesa e de Segurança Internacional.

Como fica evidente, grande parte da produção do autor desta Tese está ligada diretamente à *ideia de criação do subcampo* ciberinternacionalista, e não apenas à sua *construção*, que é levada a cabo por inúmeros membros e instituições que compõem a comunidade internacionalista. Essa observação traduz-se imperiosa para que não se associe a este trabalho críticas como a que Bourdieu (1983b, p. 130) chama de *ingenuidade da técnica dos "juízes"*, à qual:

> [...]recorre comumente a tradição científica para definir as hierarquias características de um campo determinado[...]. E, ainda, como se suas [as dos 'especialistas internacionais'] análises 'científicas' do estado da ciência pudessem ser outra coisa que não a justificação, cientificamente mascarada, do estado particular da ciência ou das instituições científicas com o qual compactuam.

Esses marcos, logo, são necessários para situar a gênese de CiberRI, a partir do ponto de vista acadêmico, porém não são suficientes para justificar o seu nascimento, consubstanciado, como dito, pela contribuição individual e coletiva de vários estudiosos. O que realmente importa para CiberRI é como a comunidade acadêmica do seu campo-*master* reage – e pode vir a reagir – aos estudos ciberinternacionalistas. E esse é o empreendimento que a próxima subseção busca realizar.

2.2 CiberRI e a universidade

> Um país forte em grande parte se faz com uma academia atuante e dinâmica. (VALENTE, 2007, p. 172).

De nada adianta propor um problema de pesquisa, se nele não estiver contida a sua relevância em termos não só científicos, mas também práticos (GIL, 1999, p. 51). Como visto na subseção 1.1, há vários tipos de conhecimentos espalhados pelo Campo Doxológico e à

[114] O segundo volume, lançado também em 2016, no Ministério da Defesa, intitula-se "Defesa e cooperação interagências", organizado por Marcos Aurélio Guedes de Oliveira e Graciela de Conti Pagliari.

espera de filtragem. Dentre eles, encontra-se o científico, que, transportado para o Campo Epistêmico, abarca uma espécie de conhecimento que se engendra na universidade, a qual é entendida como "[...]um tipo específico de instituição social que faz parte daquilo que se poderia chamar ordem ou sistema educacional[...]" (FRAGOSO FILHO, 1984, p. 13). Cuida-se, portanto, do conhecimento acadêmico[115]. Assim, acredita-se que a universidade é o local por excelência para gestar CiberRI, em termos científicos, cujos resultados são direcionados, em termos práticos, para a sociedade, em seus mais variados setores e domínios. Em outras palavras, "[a] relevância prática do problema [de pesquisa] está nos benefícios que podem decorrer de sua solução" (GIL, 1999, p. 51).

A partir daqui, já é possível elencar algumas vantagens de CiberRI, tais como: desenvolver o pensar sistemático sobre os impactos cibernéticos nas relações internacionais; discutir e analisar, de forma transparente, tais impactos, por meio de um vocabulário específico; apresentar *frameworks* que auxiliem no melhoramento da qualidade das explicações internacionais; e propiciar novas formas para CP e RI tornarem-se mais competitivas e atualizadas neste raiar de novo milênio.

Tendo em vista que "[...]não faz sentido pensar em pesquisa social sem o impulso de um interesse arraigado na sociedade[...]" (COHN, 2006a, p. 11), entende-se ser inútil – do ponto de vista social – versar sobre pesquisa, ensino e extensão de temas correlatos ao ciberespaço, em RI, simplesmente pelo fato de CiberRI ser considerado algo novo. Isso por si só não satisfaz a nenhum produto da ciência. O que se defende aqui é que, em termos sociais, políticos e internacionalistas, tal enfoque traga desafios aos Estados nacionais e à comunidade internacional. Dito de outra forma: largar mão de estudar sistematicamente o ciberespaço em CP ou RI deixa também em aberto questões fundamentais que dizem respeito às sociedades atuais, caracterizadas, dentre outros, pelo alto volume de informações produzido e pela perbeabilidade da interconectividade quase ubíqua que interliga os mundos virtuais e reais cotidianamente.

Por esta ser uma Tese de Doutorado, deve haver, inquestionavelmente, os elementos imprescindíveis da novidade e do pragmatismo tanto para CP quanto para RI. Nesse contexto, busca-se concretizar o segundo objetivo específico proposto na Introdução, *supra*, qual seja: definir os limites e potencialidades dos estudos ciberinternacionalistas no ensino, na pesquisa e na extensão de RI, os quais estão, inexoravelmente, ligados ao aperfeiçoamento desse campo

[115] Como aponta Fragoso Filho (1984, p. 21), a pesquisa aplicada se desenvolve primeiramente no âmbito do conhecimento industrial e de suas revoluções impactantes às sociedades, daí o fato de a ciência ter relações profundas com a tecnologia, como no famoso binômio ciência e tecnologia (C&T).

científico. Logo, sugerem-se adequações curriculares em RI, tanto em nível nacional quanto internacional, a fim de que os estudos sistemáticos nesse subcampo, quando versarem sobre acontecimentos cibernéticos de significação internacionalista, possam amoldar-se às atuais configurações políticas, tecnológicas e internacionais.

Novamente, cabe justificar a escolha pelos ESI, aqui. Cohn (2006, p. 9, grifo do autor) indaga "[...]por que determinados traços da realidade, de preferência a inúmeros outros, têm *significação* para o cientista[...]?". Trazendo essa inquirição para os estudos ciberinternacionalistas sobre o ciberespaço, alguém pode se perguntar por que tal temática interessa mais a este autor do que outros temas tão – ou mais – relevantes de CP ou RI, como, por exemplo, a questão da democracia e sua qualidade em países de grandes contrastes, como o Brasil? A resposta para essa inquirição repousa no fato de que "[...]não podendo conhecer tudo, o cientista concentra a atenção sobre o que lhe foi solicitado ou [o que] é mais viável" e que "[...]apenas *as ideias de valor que dominam o investigador e uma época* podem determinar o *objeto* do estudo e os *limites* desse estudo" (WEBER, 2006, p. 63, grifo nosso). Nesse sentido, afunilam-se os limites do estudo de CiberRI para focar a segurança internacional, pois tanto a experiência do propositor desta Tese quanto a época em que ela é engendrada convergem para reconhecer a pertinência de tais estudos para RI, CP e as ciências sociais como um todo.

Uma vez postos os pressupostos por trás da ideia de CiberRI, é chegado o momento de academicamente defendê-los, tendo como premissa o olhar atento da CF88, que, no *caput* de seu Art. 207, afirma, *in verbis*, que "[a]s *universidades* [...]obedecerão ao princípio de indissociabilidade entre ensino, pesquisa e extensão" (BRASIL, 1988, p. 79). Para cada um desses três componentes da educação superior brasileira é ofertada uma respectiva subseção, *infra*, começando pela "[...]primeira e fundamental função que a universidade vem desempenhando através dos tempos[...]" (FRAGOSO FILHO, 1984, p. 17), que é a de ensinar.

2.3 Ensino de CiberRI

O doutrinador Dallari (1998) apregoa que, para um ramo do Direito existir, são necessários os seguintes três requisitos: (i) ter previsão constitucional; (ii) existir lei versando sobre ele; e (iii) ser ensinado nas faculdades. Logicamente que esses critérios não servem para CP/RI, mas, a partir deles, é possível conjecturar alguns requisitos necessários para CiberRI ganhar vida no campo de RI. Se tais condições existissem, certamente uma delas seria a de se ensinar CiberRI nos cursos superiores de RI. Esta é uma das possibilidades que não apenas se vislumbra nesta Tese, como também já ocorre mundo afora, tanto na graduação quanto na pós-graduação.

Muitas das mais prestigiadas IES do mundo que lecionam Ciências Sociais, CP e RI já incorporaram temas afeitos a CiberRI em suas práticas docentes. A maioria dos exemplos listados abaixo advém do exterior, em que pese a institucionalização de tais temas, ainda que fragmentada, ser vista de forma explícita.

O exemplo mais simbólico de todos advém da *Aberystwyth University*, no País de Gales. Foi lá que a primeira disciplina para o estudo das relações internacionais foi criada em 1919 (SARFATI, 2011, p. 13, 23, 88, 373; SCHMIDT, 2002, p. 7). Por isso, o Departamento de Política Internacional dessa IES reagiu assim, quando do lançamento do *Master in International Politics of the Internet*: "a Universidade em que a disciplina de RI começou pela primeira vez tem o prazer de apresentar um novo programa de Mestrado concebido especificamente para explorar o nexo entre Internet e relações internacionais" (ABERYSTWYTH UNIVERSITY, [201-], tradução nossa[116]). Observa-se também que alguns dos eventos acadêmicos dessa universidade galesa giram em torno de temas específicos à CiberRI, tais como Governança da Internet e Segurança Cibernética.

Outro importante exemplo nessa seara, certamente, é a fundação, em 2001, do *Oxford Internet Institute* (OII), da Universidade de Oxford, autoproclamado como "um departamento de ensino e pesquisa multidisciplinar, dedicado à *ciência social da Internet*" (OXFORD UNIVERSITY, [2016], grifo nosso, tradução nossa[117]). Destacam-se, aqui, o seu *MSc in Social Science of the Internet* e o seu *DPhil in Information, Communication and the Social Sciences* (OXFORD UNIVERSITY, [2016]). Especificamente, quanto ao tema desta Tese, sublinham-se os componentes curriculares *Digital Era Government and Politics* e *Social Dynamics of the Internet*.

Também do Reino Unido, o *King's College London* cria o *Department of Digital Humanities*, o qual já se constitui como "[...]um líder internacional na aplicação de tecnologia nas ciências humanas e sociais" (KING'S COLLEGE LONDON, 2016, tradução nossa[118]), o que inclui, *per se*, CP/RI. Seus Bacharelado e Mestrado em Humanidades e Cultura Digitais abarcam alguns dos seguintes componentes curriculares:

- Introdução às Humanidades Digitais;

---

[116] Texto original: "*The University where the discipline of International Politics first began is delighted to introduce a new Masters program designed specifically to explore the nexus of Internet technology and international relations*".

[117] Texto original: "*A multidisciplinary research and teaching department of the University of Oxford, dedicated to the social science of the Internet*".

[118] Texto original: "[...]*is an international leader in the application of technology in the arts and humanities, and in the social sciences*"

- Mapas, Aplicativos e *GeoWeb*: Introdução às Ciências Humanas Espaciais;
- *Crowds and Clouds*: Ecossistemas Digitais;
- Cultura Digital e Protesto Político;
- Política Digital;
- Métodos Digitais I-II;
- Debates Críticos em Cultura Digital;
- Subculturas e Comunidades Digitais no Mundo;
- Rede *Online* e Política das Mídias Sociais;
- *Big Data* e Direito; e
- Arte e Globalização.

Certamente, o módulo do *Department of Digital Humanities* do *King's College London* que mais se aproxima do viés tratado nesta Tese é "Cultura: conflitos, diplomacia e RI", oferecido em nível de Mestrado.

Já na Suíça, o *Center for Security Studies* (CSS) do Instituto Federal de Tecnologia de Zurique (ETHZ), oferta a disciplina *Technology Governance and International Security*, no âmbito do seu *Master in Comparative and International Studies*. O principal objetivo desse componente curricular é "focar como as inovações sociotecnológicas (*ciberespaço*, agentes bioquímicos e robôs) impactam as políticas de segurança e a estratégia militar" (ETHZ, 2016, grifo nosso, tradução nossa[119]). Vale lembrar que a propositora e docente desse componente é Myriam Dunn Cavelty, uma das mais citadas autoras de RI que estuda o ciberespaço em sua vertente securitária.

Some-se a isso o exemplo espanhol da Universidade de Granada, que também incorpora, ao seu *Máster on line en Estudios Estratégicos y Seguridad Internacional*, o componente curricular *Ciberguerra y Gestión Estratégica de la Información* (UNIVERSIDAD DE GRANADA, [2015]).

Em 2013, o *William Perry Center for Hemispheric Defense Studies* (CHDS) da *National Defense University* (NDU), braço acadêmico do Departamento de Defesa dos EUA (DoD), oferta, pela primeira vez, o curso *Cybersecurity: Issues in National and International Security* (CINIS), que analisa a Segurança Cibernética na visão tanto da SegInfo quanto da segurança internacional. Atualmente, o curso, cuja fase presencial ocorre na capital estadunidense, se chama *Cyber Policy Development* (Cyber) e tem como objetivo o de "se adaptar à política de

[119] Texto original: "[...]*focuses on how sociotechnical innovations (cyberspace, chemical and biological agents and robots) impact security politics and military strategy*".

defesa do *Office of the Secretary of Defense for Western Hemisphere Affairs* e aos *Combatant Commands*, especialmente àqueles relacionados ao DoD" (NATIONAL DEFENSE UNIVERSITY, [2016], grifo nosso, tradução nossa[120]).

Desse mesmo viés civil-militar da NDU, parte-se novamente à Europa para encontrar o *Program on Cyber Security Studies* (PCSS), ofertado pelo *George C. Marshall Center European Center for Security Studies*, com sede na Alemanha. O programa do curso é bastante enfático em defender uma análise *não técnica* dos impactos do ciberespaço para a formulação e a tomada de decisão estratégica. Abaixo, são elencados alguns desses temas abordados durante o curso:

- Governança da Internet;
- Construção de capacidade cibernética;
- Privacidade e segurança;
- Combate ao terrorismo e ao crime cibernético;
- Compartilhamento de informação;
- Liberdade na Internet; e
- Proteção cibernética de estruturas estratégicas (EUROPEAN CENTER FOR SECURITY STUDIES, [2016]).

Todos esses exemplos trazem, para o âmbito das ciências sociais, CP e, especialmente, RI, a tentativa de se expandir o diálogo com as ciências exatas e, especialmente, com o ciberespaço, enfocando sua faceta securitária. Mas, certamente, há uma linha demarcatória entre a sugestão de um novo subcampo e a sua incorporação a um todo bem maior, ou seja, à grade curricular de RI. É nesse viés que Megale (1990, p. 13, grifo nosso) afirma que:

> O programa realmente dado de qualquer disciplina varia conforme o horizonte intelectual do professor – sua formação acadêmica, seus estudos e pesquisas posteriores, sua tendência, facilidade e motivação por tais ou quais *temas* e áreas de investigação –, *mas* todo programa deve enquadrar-se nos objetivos próprios da disciplina, e esta, por sua vez, se enquadra no currículo do curso como um todo.

Como se vê, algumas das principais IES do mundo estão preocupadas em analisar os fenômenos da relação ciberespaço-relações internacionais, mas nenhuma delas sugere a criação de um subcampo aos moldes do que faz a presente Tese, ou seja, de um espaço acadêmico que congregue membros da comunidade internacionalista para se debruçar, sistematicamente, sobre o ciberespaço e seus temas correlatos. Após realizar uma vasta revisão de literatura, não se

[120] Texto original: "[...]*response to the defense policy goals of the Office of the Secretary of Defense for Western Hemisphere Affairs and the objectives of the Combatant Commands, particularly those related to DoD efforts*[...]".

encontra nenhum trabalho que vá nessa direção. Pode-se pensar em algumas razões para isso, tal como a excessiva preocupação com a "especialização prematura" de que fala Megale (1990, p. 74, 166), mas o certo é que esta Tese não vislumbra *timing* melhor para isso ocorrer do que o presente momento, quando do crescimento pelo tema nas IES estrangeiras, e, em certa medida, aqui no Brasil, país com inexpressiva capacidade tecnológica. Essa aparente contradição reforça a máxima de que revoluções científicas podem se dar também nos locais menos prováveis.

Nesse sentido, elencam-se abaixo três exemplos ou etapas, em ordem crescente de complexidade, para esse intento, que migram desde a alteração curricular até a mudança curricular[121] de CP/RI:

i. *incorporar tópico(s) de CiberRI a um componente curricular já existente*[122]: por exemplo, em Antropologia Cultural, é possível relacionar os movimentos da chamada Primavera Árabe com o hacktivismo do grupo Anonymous, como o fazem Lopes e Azevedo (2012) ou a mobilização global de manifestantes pelas redes sociais, aos moldes de Soares (2014), em virtude, por exemplo, do Movimento *Occupy*, ou, ainda, a explicação histórico-cultural para a motivação dos ataques virtuais russos e russófilos contra a Estônia em 2007. Outra dimensão possível é compreender, no âmbito do componente curricular Teoria das RI, como as correntes de pensamento internacionalistas oferecem – ou n'ao – arcabouços explicativos para alguns aspectos do ciberespaço – como o fazem Eriksson e Giacomello (2006) e Hansen e Nissenbaum (2009), para com a segurança internacional –, ou mesmo tentar encontrar a posição epistemológica de autores recentes em um espectro das teorias de RI, como ocorre em Acácio (2015), Acácio e Lopes (2012) e Reardon e Choucri (2012). Como o enfoque desta Tese é a seara securitária, busca-se privilegiar os ESI, aplicados ao ciberespaço. Assim, no plano de aula do componente curricular tradicional de Segurança Internacional é possível, por exemplo, analisar o impacto das chamadas armas cibernéticas, como o Stuxnet, contra estruturas estratégicas

[121] Entende-se por alteração e modificação curriculares, respectivamente, os processos que visem a: "[...]*promover ajustes*, tais como: alteração de carga horária, modificação de pré-requisito das disciplinas, *criação ou extinção de disciplinas optativas*[...]" e "[...]*alteração substantiva na estrutura curricular* vigente e que decorra da *verificação de defasagem ou de inadequação da estrutura atual às exigências da formação do estudante*[...]" (BRASIL, 2004, p. 4, grifo nosso).

[122] O Apêndice A, *infra*, apresenta excerto de plano de aula real incorporando CiberRI a um componente curricular de RI já existente.

estatais, ou, ainda, realizar estudos comparativos sobre os investimentos[123] e as políticas nacionais de Segurança e Defesa Cibernéticas de Estados ou regiões[124], ou, mesmo, levantando o arcabouço legal dessa temática em determinado país[125];

ii. *incorporar CiberRI como um componente curricular homônimo na grade curricular do curso*[126]: pode-se fazer isso tanto na graduação quanto na pós-graduação, aos moldes mais gerais de "Introdução a CiberRI" ou "Tópicos Especiais de RI: CiberRI" ou mais específicos como em "Geopolítica do Ciberespaço" ou "Segurança Cibernética Internacional". Nesse novo componente curricular, pode-se fornecer um panorama ou adentrar em temas mais específicos e correlatos às relações internacionais e ao ciberespaço, mas sempre abordados a partir dos pressupostos metateoréticos de RI, tais como: historicidade da rede mundial de computadores[127]; Governança da Internet[128]; crimes cibernéticos, seus impactos econômicos e seu regime internacional de combate[129]; guerra cibernética e Defesa Cibernética[130]; e testes de resiliência de *frameworks* aplicados às relações internacionais[131]; e

iii. *criar linhas de pesquisa, áreas de concentração ou, ainda, cursos de pós-graduação sobre um tema ou, até mesmo, de CiberRI*: neste caso, como se aponta mais acima, já não é mais raro encontrar cursos de Especialização – pós-graduação *lato sensu* – e de Mestrado e Doutorado – pós-graduações *stricto*

---

[123] Para uma visão internacionalista sobre esse assunto, ver Oliveira e Leite (2016); para uma mais técnica, conferir os diversos relatórios de empresas produtoras de antivírus como Kaspersky, McAfee, Microsoft e Symantec, sobretudo da primeira.

[124] *Vide* LOPES, 2013.

[125] Para o caso argentino, conferir Gastaldi e Justribó (2016), para o Português, Castro (2016).

[126] Na forma do Apêndice B, apresenta-se um exemplo de plano de aula para o componente curricular "Introdução às Relações Internacionais Cibernéticas (CiberRI)".

[127] Sobre isso, ver a primeira parte do curso *História da Internet, Tecnologia e Segurança*, ofertado pela Universidade de Michigan, em: https://www.coursera.org/learn/internet-history.

[128] *Vide*, por exemplo, a criação do Fórum da Governança da Internet, no âmbito da ONU, bem como a publicação do diplomata brasileiro Lucero (2011) sobre tal tema. Ademais, o Comitê Gestor da Internet no Brasil (CGI.Br) sedia, anualmente, a Escola de Governança da Internet no Brasil (EGI): http://egi.nic.br.

[129] Há vários relatórios tanto de empresas especializadas em SegInfo quanto de organismos públicos no Brasil – com especial atenção ao Ministério Público e às polícias civil e federal – e no exterior, como a Convenção de Budapeste sobre Crimes Cibernéticos, no âmbito do Conselho da Europa.

[130] Como o realizado na Dissertação de Mestrado em CP/RI de Lopes (2013).

[131] Um exemplo qualitativo desse tipo de teste pode ser encontrado em Lopes e Medeiros (2011, p. 6-10), quando eles engendram, a partir da teoria dos jogos de dois níveis (*two-level game*), uma lógica explicativa aplicável às negociações diplomáticas sobre a Internet, no âmbito da OEA.

> *sensu* – sobre temas que, aparentemente, estão mais próximos da Ciência da Computação, mas que são estudados sob um enfoque das ciências sociais, especialmente de RI.

Enquanto isso não ocorre, de forma organizada, no Brasil, o que se evidencia é um ou outro evento esparso de CP e RI que já incorpora, exógena[132] e endogenamente[133], CiberRI em seu *corpus*. O mesmo vale para chamadas de bolsas de pesquisa e *workshops*[134]. Há que se levar em conta também o número cada vez maior de Monografias de Graduação e de Especialização, Dissertações de Mestrado e Teses de Doutorado que trazem temas correlatos a CiberRI, demonstrando que tanto discente quanto orientador(a) estão em sintonia com os acontecimentos que envolvem o ciberespaço e as relações internacionais. Porém, apesar de esses dados revelarem um crescente interesse, por parte da comunidade internacionalista, no tema em tela, o desenvolvimento sistematizado e organizado de CiberRI continua inexistente na academia brasileira, em termos, sobretudo, de ensino e extensão.

Por fim, ressalta-se o fato de que alguns editais de concurso público para admissão de docentes de RI já levam em conta aspectos ciberinternacionalistas. É o caso, por exemplo, do concurso para Professor Adjunto de RI/Segurança Internacional da Universidade Federal de São Paulo (UNIFESP), cujo primeiro ponto do certame versa, dentre outros, sobre guerra cibernética[135].

Se se considerar como verdadeira a máxima de que "[e]ducar é conduzir, guiar a um fim[...] essencialmente positivo" (FRAGOSO FILHO, 1984, p. 14), então o condutor dessa jornada precisa de ferramentas para evitar e corrigir percalços no meio do caminho e poder, enfim, chegar a seu destino final. O papel da pesquisa acadêmica vai também nessa direção. Certamente, ela, do tripé universitário brasileiro, é a que mais chama a atenção da comunidade

---

[132] Por exemplo, mediante inscrição de trabalhos avulsos de temas de CiberRI em simpósios temáticos (STs), áreas temáticas (ATs) ou grupos de trabalho (GTs). São os casos dos Encontros Nacionais da ABRI, da Associação Nacional de Pós-Graduação e Pesquisa em Ciências Sociais (ANPOCS), da *International Political Science Association* (IPSA), dentre outros. No caso específico da ANPOCS, seu GT "Ciberpolítica" guarda forte relação temática com a comunicação política a partir das novas mídias digitias.

[133] Via chamadas específicas de artigos que tenham relação direta com os temas tratados em CiberRI. São exemplos as ATs do Encontro Nacional da ENABED, o último Encontro Nacional de Estudos Estratégicos (ENEE) que teve como tema central a Segurança Cibernética e o Seminário Brasileiro de Estudos Estratégicos Internacionais (SEBREEI). De todos, no Brasil, o maior expoente nessa temática foi o I Seminário de Relações Internacionais Cibernéticas (CiberRI), em 2014, já mencionado, *supra*. Outro exemplo vem da França, por meio dos dois números seguidos de uma das revistas mais importantes sobre geopolítica do mundo, o Hérodote: http://www.herodote.org/spip.php?rubrique66.

[134] Como o *workshop* "*Cyber Security: Surveillance State and Global Internet Politics*", realizado sob os auspícios do Núcleo de Pesquisa em Relações Internacionais da Universidade de São Paulo (NUPRI-USP), em 2014.

[135] O conteúdo programático do Edital de Abertura desse concurso encontra-se no Anexo A, *infra*.

internacionalista, como se observa a seguir.

2.4 Pesquisa em CiberRI

Pode-se definir *pesquisa* como "[...]o processo formal e *sistemático* de desenvolvimento do método científico" (GIL, 1999, p. 42) e, neste viés, definir também *pesquisa social* como "[...]o processo que, utilizando a metodologia científica, permite a obtenção de novos conhecimentos no campo da realidade social" (GIL, *loc. cit.*, grifo nosso). Parafraseando o autor acima, pode-se também engendrar uma definição científica para a pesquisa ciberinternacionalista como o processo que, mediante metodologia científica, possibilita obter novos conhecimentos ciberinternacionalistas no campo da realidade internacional.

Para fazer valer a definição acima, de forma mais precisa, esta subseção trata da pesquisa em CiberRI, a partir de um olhar mais atento à segurança internacional, embora, como visto, seja possível aplicar CiberRI também a outros tópicos, afinal, como Portela (2016, p. 91, grifo nosso) observa, "[...]nas Relações Internacionais notamos *pesquisas* de diversos temas sobre o espaço cibernético".

Se, de acordo com Silva (2005, p. 323), há três tipos de saberes utilizados na prática docente – experiência, conhecimentos adquiridos no processo de formação e didática –, então busca-se aplicá-los não apenas ao ensino de CiberRI, mas sobretudo à sua pesquisa, pois é nela que a maioria das elucubrações sobre a relação ciberespaço-RI surgem.

CiberRI ganha notoriedade não apenas nas IES, mas também nos chamados "[...]'institutos de estudos avançados' e de outras estruturas desligadas da docência" (WALLERSTEIN *et al*., 1996, p. 108), como os *think tanks*, a exemplo do Instituto Brasileiro de Estudos em Defesa Pandiá Calógeras (IBED), ligado ao Ministério da Defesa. Nas IES, especialmente as estrangeiras, vê-se o crescimento desses estudos pela comunidade epistêmica de RI. Mas só isso não basta, pois o investigador-intelectual é, por vezes, um ser solitário. É preciso, além de produzir, proliferar os conhecimentos internacionalistas sobre o ciberespaço. Logo, não há espaço mais adequado para isso do que a própria Web, por meio da qual é possível medir não apenas a produção – como se faz na subseção 3.2, *infra* –, como também seus impactos, uma vez que ela "[...]oferece a possibilidade de um novo salto tecnológico para a coleta e o tratamento de dados necessários à realização de pesquisas" (FREITAS *et al.*, 2006, p. 16). Assim sendo, procede-se a um investigação tripartite da pesquisa em CiberRI, a partir do Modelo 3C, engendrado na segunda seção desta Tese.

2.4.1 As informações no Campo Doxológico: separando os acontecimentos cibernéticos

De acordo com os metodólogos sociais Bruyne, Herman e Schoutheete (1991, p. 201, grifo nosso), "[a] pesquisa científica se constrói por referência com o mundo dos *acontecimentos*, que são apenas os *efeitos de estados de coisas* presumidos de uma 'realidade' suposta". A partir dessa inquietação metodológica, tem-se observado, que, no que âmbito específico da pesquisa acadêmica de temas afeitos a CiberRI, a esmagadora maioria dos trabalhos dela resultantes se atrela a acontecimentos conectados à seara da segurança internacional.

Como visto na subseção 1.2, *supra*, observação e sistematização ocupam momentos distintos na pesquisa social. Assim, parte-se para a observação propriamente dita dos principais acontecimentos cibernéticos com reflexos nas relações internacionais. Somente após essa observação das informações no Campo Doxológico sobre o ciberespaço é que se pode analisar seus dados no Campo Epistêmico de RI.

Neste ponto, a história importa. Afinal, ao aspirarmos ao conhecimento *significativo na sua especificidade*, está-se, na realidade, aspirando à sua história (LIPSON, 1967, p. 39; WEBER, 2006, p. 53), uma vez que "[a] verdade científica é, ela própria, de natureza histórica" (WALLERSTEIN *et al.*, 1996, p. 87). Logo, esta subseção trata de situar, no tempo e no espaço – ainda que cibernético –, informações sobre os principais acontecimentos que contribuem para atestar o nascimento de uma espécie de História de CiberRI, haja vista que a história "[...]emerge da ordem dos *acontecimentos* que se vão sucedendo no decurso do tempo" (SOUSA, 1982, p. 6, grifo nosso).

Após uma revisão de literatura baseada principalmente em especialistas em SegInfo e segurança internacional, é possível elencar alguns dos principais acontecimentos cibernéticos com relevante impacto internacional, sobretudo na política internacional e na política externa das grandes potências. Nesse viés, constrói-se, sumariamente, uma espécie de cronologia dos acontecimentos cibernéticos com impactos internacionais, conforme se vê no Quadro 1.

Ano	Acontecimento
1969	Criação da *Advanced Research Projects Agency Network* (ARPANET), predecessora da Internet, com apenas três *sites*
1972	ARPANET possui 29 *sites*
1979	ARPANET possui 61 *sites*
1982	*Central Intelligence Agency* (CIA) lança bomba lógica contra gasoduto soviético na Sibéria
1984	ARPANET possui quase 1.000 computadores hospedeiros
1989	*Sir* Tim Berners-Lee cria a World Wide Web no *European Organization for Nuclear Research* (CERN)
1990	*Sir* Tim Berners-Lee desenvolve a HTML e o primeiro *browser*, o WorldWideWeb
1991	Surgimento do primeiro *site* jihadista, o *Islamic Media Center*

1992	Internet possui 1 milhão de usuários
1993	CERN disponibiliza a Web para o mundo
1994	*Sir* Tim Berners-Lee funda o World Wide Web Consortium (W3C), no MIT
1995	Microsoft lança o Windows 95 e o Internet Explorer 1, impulsionando o acesso mundial à Internet
	Criação da linguagem de programação interpretada JavaScript, assaz usada por *crackers*
	6 milhões de computadores ligados à rede mundial
1998	Internet possui cerca de 300 milhões de páginas
	Internet possui cerca de 100 milhões de internautas
	3.000 hackers atacaram a Indonésia
1999	Internet possui mais de 37 milhões de computadores hospedeiros
	"Bolha da Internet" estoura na Nasdaq
2001	Al-Qaeda lança seu primeiro vídeo *online* intitulado *The Destruction of the American Destroyer Cole*
	Lançamento da Wikipédia
	80.000 hackers atacaram os EUA, ao longo do ano
2002	Lançamento do Mozilla Firefox
2003	China, sozinha, possui cerca de 400 milhões de internautas
	161 bilhões de *gigabytes* são criados, ao longo do ano
2004	Lançamento do Orkut
	Lançamento do Facebook
2005	Lançamento do YouTube
2006	Mark Klein revela esforços da *National Security Agency* (NSA) para coletar dados
	Lançamento do Twitter
	Backbone da rede do Pentágono sofre 3 milhões de *scan* por dia, ao longo do ano
	Julian Assange lança o WikiLeaks
2007	Lançamento do Google Street View
	China ataca rede estadunidense formada por 750.000 computadores
	Russos atacam *sites* governamentais da Estônia
	FBI invade casa de Thomas Drake
	China ataca 300 companhias inglesas
2008	Rede militar dos EUA sofre grandes ataques de códigos maliciosos e máquinas zumbis
	Lançamento do Google Chrome
	Sede da campanha presidencial de Barack Obama é hackeada
	Computadores do Pentágono são invadidos por hackers supostamente contratados pela Rússia
	O maior banco da Índia é hackeado por paquistaneses
	National Aeronautics and Space Administration (NASA) descobre *worm* em *notebooks* da Estação Espacial Internacional
	China e/ou Rússia invadem sistemas de *e-mail* com vistas às eleições presidenciais dos EUA
	WikiLeaks revela vídeos de prisões no Tibete
	Rússia ataca sistemas governamentais da Geórgia
	Aproximadamente 285 milhões de registros foram comprometidos no mundo todo
	Três milhões de ataques a apenas uma das 320 redes informatizadas do governo federal brasileiro
	120 nações aproveitam-se da Internet para atividades de espionagem política, militar e econômica
2009	China rouba propriedade intelectual do Google, que muda sua filial para Taiwan
	WikiLeaks publica relatórios do *U.S. Congressional Research Service* (CRS)
	Descoberta da GhostNet, vultosa rede de espionagem chinesa de *e-mails*
	Aproximadamente 900 milhões de registros foram comprometidos no mundo todo
2010	China hackeia contas do Google, na chamada Operação Aurora
	Worm Stuxnet é descoberto, após sabotar centrífugas nucleares do Irã
	Lançamento do Instagram
	Bradley Manning, ex-soldado estadunidense, é preso por vazar informação confidencial
	Grupo hacktivista Anonymous lança operação "Avange Assange" contra sites ocidentais
	WikiLeaks publica documentos fornecidos por Manning
	Crime cibernético causa prejuízo de quase 388 bilhões de dólares no mundo todo
	Hacktivistas violam aproximadamente 100 milhões de dados de usuários no mundo todo
	Interpol emite ordem internacional de prisão contra Assange
2011	WikiLeaks posta informações de clientes de um banco suíço, embrião para o SwissLeaks
	Tunísia hackeia Facebook, durante a chamada Primavera Árabe
	Descoberta do Duqu, primeira variante do Stuxnet

	57% dos especialistas consultados pela McAfee acreditam em uma corrida armamentista cibernética
	36% deles acreditam que segurança cibernética é mais importante que defesa antimíssil
	45% deles acreditam que segurança cibernética é mais importante que segurança fronteiriça
	Brasil registra aproximadamente 400.000 ataques a computadores, ao longo do ano
	EUA e Reino Unido realizam grande exercício conjunto de segurança cibernética
2012	Descoberto Flame, segunda variante do Stuxnet
	Saudi Aramco, maior companhia petrolífera do mundo, é atacada pelo *worm* Shamoon
	Forte ataque cibernético iraniano contra os maiores bancos estadunidenses
2013	*Syrian Electronic Army* hackeia o Twitter
	Snowden revela a espionagem cibernética da NSA
	Syrian Electronic Army hackeia o jornal The New York Times
2014	Rede de computadores da Casa Branca é comprometida
	Rússia desfere guerra cibernética contra Ucrânia por causa da Crimeia
	Coreia do Norte hackeia Sony
2015	Comprometimento do sistema do *U.S. Office of Personnel Management*
2016	Governo dos EUA alega, novamente, interferência russa, via *hacking*, na campanha presidencial

Quadro 1 Cronologia dos principais acontecimentos cibernéticos para RI (1969-2016)
Fonte: Assange *et al.* (2013, p. 159-164); Baker (2010; 2011; 2012); Bessa (2014, p. 40); Bezerra ([2009]); Bronk (2016); Carr (2009, p. 3-4); Costa (2012); Exército... (2012); Geers (2015); Kremer e Müller (2014b); Leman-Langlois (2012, p. 4); Lemieux e Bales (2012, p. 69); Lewis Universisty, ([2009]); Lipton, Sanger e Shane (2016); McAfee (2009; 2012); Nye Jr (2011b, p. 114-115, 122); Portela (2016, p. 93, 97); Singer e Brooking (2015); Valente (2007, p. 67-69); W3C Brasil ([2016]); Wertheim (2001, p. 164-165); e Zero... (2016).

É possível observar, nos acontecimentos cibernéticos listados no Quadro 1, alguns padrões que reverberam internacionalmente. Por exemplo, a própria criação da ARPANET, projeto da primeira rede descentralizada de computadores, do Departamento de Defesa dos EUA, remonta ao período da Guerra Fria, em que pese a necessidade de se criar uma rede sem um servidor central, para o caso de um ataque nuclear (VALENTE, 2007, p. 67-68). Mais recentemente, têm-se as revelações feitas pelo *site* WikiLeaks, cuja persecução para seu fechamento, por parte de autoridades públicas anglo-saxãs, acaba levando seu criador Julian Assange ao asilo político na Embaixada do Equador em Londres. Como efeito colateral deste último episódio, o Estado equatoriano recebe advertências políticas do governo inglês, sendo que uma das últimas reverberações do caso foi a negação de pouso para o avião do presidente boliviano, sob a alegação de ele estar transportando Edward Snowden (MOURA, 2013). Isso tudo sem mencionar o uso de *drones*[136] nos campos de batalha, as consequências diplomáticas das revelações de Snowden (BESSA, 2014; PORTELA, 2016, p. 103) e as inúmeras alegações públicas de que Estados têm invadido o espaço cibernético uns dos outros.

Todos esses acontecimentos, além de tantos outros, lançam luz sobre a importância de eles serem aprofundados também no âmbito das pesquisas acadêmicas de RI, afinal, como já posto, a maioria deles aponta para vários aspectos do poder, como as suas difusão, projeção,

[136] Como observa Duarte (2012, p. 78), *drone* é espécie do gênero veículo aéreo não tripulado (VANT) direcionado para exercícios de alvo. Ver seu uso atrelado às políticas de Defesa e externa estadunidenses em Sanger (2012, p. xiv-xv, 241-270).

manutenção e busca, por parte de entes estatais. Quanto mais tais acontecimentos se afastam do século XX, mais aumenta, qualitativa e quantitativamente, o número de acontecimentos cibernéticos que podem ter desdobramentos nas relações internacionais. Portanto, o século XXI mostra-se como o *momentum* em que membros da comunidade epistêmica de RI começam a se ater, mais efusivamente, sobre os impactos do ciberespaço nas relações internacionais, sobretudo quanto à sua faceta securitária.

No âmbito do desenvolvimento[137] histórico dos acontecimentos e dos trabalhos acadêmicos que ajudam a dar vida à CiberRI, a próxima subseção destaca alguns dos que têm forte correlação com a presente Tese.

2.4.2 Os dados no Campo Epistêmico: a Infometria de CiberRI

No Campo Epistêmico, seguindo o Modelo 3C, "[o] conhecimento armazenado e estagnado não pode exercer uma função dinamizadora da cultura e da civilização sem a pesquisa" (FRAGOSO FILHO, 1984, p. 28). É preciso, pois, triar as informações do Campo Doxológico e transformá-las em dados, aptos a serem manipulados aos olhos dos objetivos de uma pesquisa.

Com auxílio da Infometria, parte-se do pressuposto de que a Internet é um importante meio de comunicação e armazenamento de informação, imprescindível para a consecução de pesquisas acadêmicas. Logo, nada mais plausível que tal ambiente seja palco de estudos (VANTI, 2002, p. 156; 2005, p. 78), especialmente das ciências sociais (THELWALL, 2005, p. 1). Nesse viés, para que se possa mapear os estudos internacionalistas sobre o ciberespaço na subseção 3.2, realiza-se, agora, uma pesquisa superficial para revelar o panorama do atual estado de coisas da pesquisa em temas afeitos a CiberRI nos *sites* acadêmicos e relacionados a CP/RI. Para tanto, aplicam-se, conjuntamente, três técnicas quantitativas da Informetria, a saber: Bibliometria, Cientometria e Webometria[138]. A primeira delas visa, dentre outros,

---

[137] Prefere-se o termo "desenvolvimento" a "evolução", pois este enseja, no âmbito científico, uma ideia de acumulação e de superação de fases, partindo da mais rudimentar à mais refinada. Como se reconhece a fragmentação temática em RI, é certo que não há hierarquias entre os acontecimentos – embora haja, sim, uma evolução das tecnologias que se empregam neles –, e, por isso, o termo desenvolvimento enseja uma ideia de implementação, ainda que desordenada, como se vê, por exemplo, com os estudos ciberinternacionalistas. Possivelmente, as discussões sobre dimensões ou gerações de direitos humanos ou, mesmo, sobre a teoria da modernização travam-se em termos ontológicos semelhantes aos de desenvolvimento *versus* evolução.

[138] *Grosso modo*, a Webometria está contida na Cibermetria, que, por sua vez – e assim como a Cientometria –, faz parte do amplo espectro da Informetria (VANTI, 2002; 2005, p. 80-82). Webometria ou *Webometrics* – também conhecida por *Internetmetrics*, *Internetometrics*, *Netometrics, Web Bibliometry* ou *Webometry* (VANTI, 2005, p. 79) – é uma subárea da Cibermetria ou *Cybermetrics*. Já a Bibliometria compreende "[...]os estudos que analisam a forma como um determinado campo de estudo[...] usa e dissemina informação através de comunicação formais e informais, recorrendo[...] à aplicação de métodos estatísticos para *análise de conteúdo* de[...] meios de difusão

observar tendências acadêmicas de pesquisa, que, aqui, dizem respeito ao campo de RI. Já a segunda técnica "[...]estuda, por meio de indicadores, uma dada disciplina da ciência" (VANTI, 2002, p. 154), que, neste caso, é RI, mas também pode incidir em CP e Ciências Sociais. A derradeira técnica examina toda a Web (VANTI, 2005, p. 80), cuja vantagem é "poder ser processada na mesma velocidade com que os dados entram no sistema" (FREITAS *et al.*, 2006, p. 16-17). Mas o que interessa mesmo aqui são os resultados dos mecanismos de busca, *sites* e páginas virtuais (*web pages*), bem como suas palavras e *links* (THELWALL, 2009, p. 1). Juntas, essas técnicas permitem "identificar as tendências e o *crescimento do conhecimento em uma área*; [...] medir *o crescimento de determinadas áreas* e o *surgimento de novos temas*" (VANTI, 2002, p. 155, grifo nosso), bem como explorar "[...]estudos históricos *sobre* [...]*uma disciplina ou domínio* e a avalia[r] pesquisa por países, instituições ou indivíduos" (VANTI, 2005, p. 79). Portanto, entende-se que, ao "[...]quantificar o crescimento ou [a] perda de importância relativa de um *tema ou matéria*[...]" (VANTI, 2002, p. 157, grifo nosso), pode-se também validar a segunda hipótese secundária e atingir o segundo objetivo específico desta Tese, expostos na Introdução, *supra*. A Figura 4 exibe as divisões internas da Infometria, destacando os limites que se utilizam aqui.

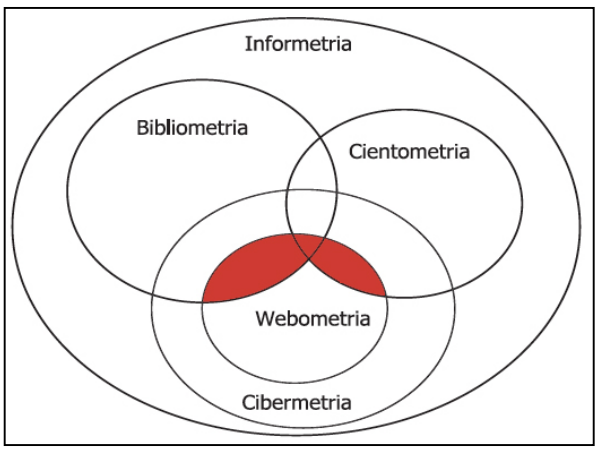

Figura 4 Informetria e seus subcampos
Fonte: VANTI, 2005, p. 81 (com adaptações).

Como se afirma acima, "[a] referência a períodos anteriores, na escala cronológica[,]" contribui "para uma compreensão mais esclarecida dos fatos[...]" (LIPSON, 1967, p. 40) a serem ainda revelados sob a bruma do Campo Doxológico. Assim, busca-se agora justamente

acadêmica" (COUTINHO, 2011, p. 326-327, grifo do autor) e complementa as outras duas técnicas. Cf. PORTELA, 2016, p. 91, 95; THELWALL, 2009, p. 6; VANTI, 2005, p. 82.

coletar dados que auxiliem na produção de tais fatos, por meio dos quais, sustentarão, em termos empíricos, a defesa acadêmica de CiberRI.

Para uma visão global do que o público geral – Campo Doxológico – pesquisa nos trabalhos acadêmicos – Campo Epistêmico –, muitos dos quais resultantes de pesquisas universitárias, focados em temas afeitos a CiberRI, realiza-se uma busca no serviço *online* Google Trends, com o intuito de medir a tendência das pesquisas dos termos "*cyber*" e "ciber" e do tópico "Ciberespaço", restritos à subcategoria "Relações Internacionais", ao longo de 1º de janeiro de 2009 a 31 de outubro de 2016.[139] O Gráfico 1 apresenta os resultados obtidos nessa primeira busca.

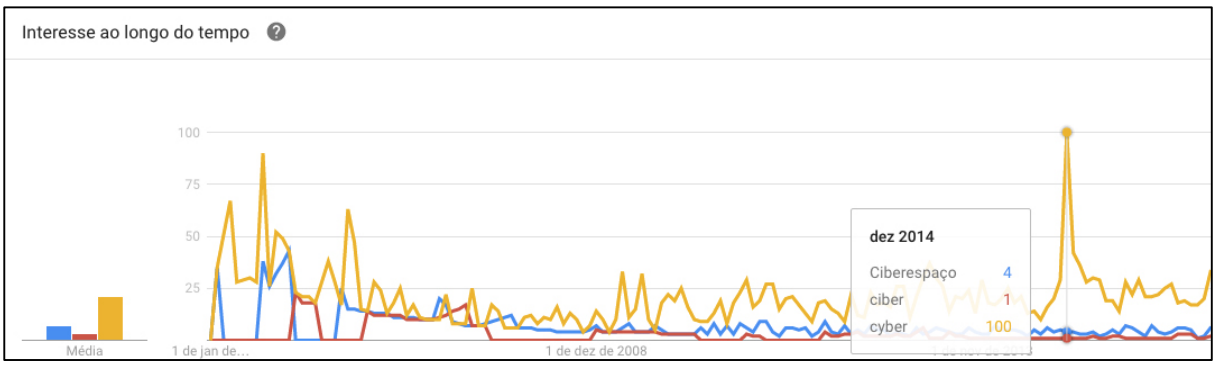

Gráfico 1 Tendências de pesquisas de termos ligados a CiberRI no Google Trends (2004-2016)
Fonte: https://www.google.com.br/trends/explore?cat=521&date=all&q=ciber,cyber, acesso em: 31 out. 2016.

No que tange à comunidade acadêmica de RI, o Gráfico 1 aponta que a busca pelo termo "*cyber*" apresenta muito mais achados que os outros dois concorrentes. Não obstante isso se dever, dentre outras razões, à questão linguística, é possível listar as principais consultas relacionadas às tendências das pesquisas com esse termo mais buscado, conforme se vê no Gráfico 2.

[139] O Google Trends possui o limite temporal inicial de 2004. "Termos de pesquisa" correspondem a palavras específicas; já "tópicos", a termos semelhantes em qualquer língua. Por meio do formulário de pesquisa desse serviço, filtra-se a subcategoria "Relações Internacionais" da categoria "Ciências Sociais", que, por sua vez, faz parte da categoria "Referências", que, neste caso, diz respeito à comunidade científico-acadêmica.

Gráfico 2 Tendências de consultas ao termo "*cyber*" na Referência "RI" (2004-2016)
Fonte: https://google.com.br/trends/explore?date=all&q=cyber,international%20relations, acessado em: 31 out. 2016.

Em relação às tendências de pesquisas nas referências *online* de RI, os tópicos – ou "consultas", no jargão do Google Trends – que mais se destacam são os que se relacionam à temática da Segurança Cibernética, quais sejam: Crime Cibernético (*Cyber Crime*); Guerra Cibernética, em seu sentido lato (*Cyber Warfare*); Terrorismo Cibernético (*Cyber Terrorism*); e o *U.S. Cyber Command* (USCC). Isso se coaduna com a intuição desta Tese em focar a questão da segurança internacional e também com o fato de que "[...]as principais análises sobre a defesa e a segurança cibernética surgem como as principais áreas de pesquisa das Relações Internacionais sobre o espaço cibernético" (PORTELA, 2016, p. 108).

Embora "[...]o processo de pesquisa via Web apresenta pontos fortes e fracos" (FREITAS *et al*., 2006, p. 44), a busca realizada no Google Trens é apenas um dos inúmeros exemplos que se tem disponível para medir o que condiciona os aspectos que envolvem a produção internacionalista sobre o ciberespaço. Geralmente, não se produz um trabalho acadêmico sem que o mesmo esteja atrelado a alguma pesquisa universitária, seja individual, seja institucional. Se se assumir essa premissa como verdadeira, a análise dos Gráficos 1 e 2 não revela muito sobre o *como* e *quem* pesquisa temas afeitos a CiberRI, mas diz muito sobre *o que* se pesquisa, que, neste caso, são temas ligados aos aspectos securitários do ciberespaço. Pelos resultados da busca, é possível afirmar, com alto grau de precisão, que as quatro principais consultas relacionadas ao estudo do ciberespaço em RI têm a ver com Segurança Cibernética e segurança internacional, temas tratados na seção 3, *infra*.

Uma vez traçada uma pintura geral do Campo Epistêmico de RI, é possível conhecer do seu Campo Teórico.

2.4.3 Os fatos no Campo Teórico: a Era dos Ruídos e o Pseudomomento Snowden

Consoante Lipson (1967, p. 15), "[a]preender fatos não é o mesmo que compre[e]nder-lhes a significação. O último aspecto é o mais importante dos dois". Seguindo essa lógica, os dados presentes nos Gráficos 1 e 2 – sobretudo neste último – apenas dizem algo acerca de uma parcela do estado de coisas das pesquisas internacionalistas sobre o ciberespaço, mas não dizem tudo, devido à infinidade do conhecimento científico, da realidade social e da produção intelectual na Web, conforme se discute na subseção 1.1, *supra*.

A transformação dos dados em fatos – neste caso, ciberinternacionalistas – requer sua desagregação dos mesmos, para, mediante análise e síntese, reagrupá-los, de forma que seu substrato, os fatos, possam gerar algum tipo de significação para CiberRI e seu campo-pai.

Como Jackson (2011, p. 17) postula, não há um roteiro para se proclamar RI como uma "ciência", aos moldes de outras áreas já consolidadas como a Física ou a Matemática. O que se tem são critérios dispostos como "científicos", que estão relacionados a certas práticas de produção de conhecimento que, uma vez adotadas, estabelecerão RI como uma ciência, ou seja, como um campo de boa reputação e aceitação no meio científico. Nesse sentido, a aceitação de CiberRI como subcampo de RI liga-se também à qualidade das análises dos dados e dos fatos ciberinternacionalistas, sempre realizadas à luz dos elementos metateoréticos de RI.

Para consubstanciar o que se expõe no parágrafo acima, analisam-se, a partir de agora e de maneira geral, alguns desses fatos, com foco na segurança internacional, à medida que se busca, no específico, evidenciar o estado de coisas atual do Campo Teórico em que CiberRI se insere, epitetado aqui, em termos hobsbawmianos, de *Era dos Ruídos*, palco para um fato ciberinternacionalista em especial, o "psdeudomomento Snowden" brasileiro.[140]

Se já nos anos de 1960, "[a] tarefa de resumir e assimilar [...]acervo de materiais – leis e estatísticas, debates e diretrizes, opiniões e decisões – torna-se cada vez mais difícil" (LIPSON, 1967, p. 27), imagina no século XXI, quando a sociedade é conhecida como a da informação (CASTELLS, 1999; 2007; VALENTE, 2007, p. 19). Inegavelmente, a produção de informações e dados cresce a um ritmo inimaginável tanto em termos de velocidade quanto em tamanho (BAEZA-YATES; RIBEIRO-NETO, 2013, p. 401; CERVO; BERVIAN; DA SILVA, 2010, p. XI), medidos, atual e respectivamente, em *bits* e *bytes*. Em outras palavras, pode-se afirmar que "[...]nunca foi tão simples encontrar uma informação, transmiti-la ou colocar-se em

[140] Note-se que tais análise levam em conta apenas dados qualitativos e interpretação subjetiva. Para uma análise quantitativa e objetiva, ver subseção 3, *infra*.

situação de conhecê-la" (FREITAS *et al.*, 2006, p. 121) e que a Internet possibilitou que a quantidade de informação circulante se tornasse infinita (VALENTE, 2007, p. 25-26). O problema é o que acompanha tais informações, que, no caso aqui, é o ruído estratégico. De forma geral, Freitas *et al*. (2006, p. 121, grifo nosso) dão a seguinte apresentação à problemática que se quer aqui expor:

> [...]é justamente esta facilidade de acesso que gera problemas. De fato, o acesso à informação cria, com a abundância de dados acumulados, uma sobrecarga no momento de necessidades de conhecimento. Onde encontrar tempo para ler tudo? O que se deve ler? Como identificar as informações pertinentes? Como reduzir, selecionar ou produzir conhecimentos úteis à tomada de decisão? *É a abundância de dados que gera problemas, não a falta deles*.

Eis que, diante desse cenário, surge a seguinte indagação: como analisar todo esse mar de informações e conhecimentos que é produzido em largo volume e em escasso tempo? Afinal, informação é matéria-prima farta/abundante nos tempos recentes (VALENTE, 2007, p. 15). Há algumas tentativas como a mineração de *big data*. Mas, especificamente, à luz dos ESI, essa questão se torna ainda mais complexa, haja vista que "[...]nem os mais aguerridos e brilhantes comandantes podem comandar sem informação[...]" (PROENÇA JR; DINIZ, 1998, p. 25). Ademais, os órgãos estratégico-militares têm de lidar com a desinformação e as benesses que o ciberespaço – especialmente a Internet Profunda – acarreta, em termos de sigilo e proteção da informação, dificultando, consequentemente, a autoria e seu rastreio. A questão de como separar o que é estratégico do que é banal no ciberespaço tem se tornado, certamente, uma inquietação a que estrategistas, tomadores de decisão e analistas de Inteligência se deparam diuturnamente[141]; afinal, a informação estratégica tem prazo de validade curto, ainda mais em um ambiente informacional volúvel por excelência.

É nesse viés que a afirmação de que "[n]ossa civilização está mergulhada em papéis até o pescoço, e os que se propõem estudar os problemas que ela encerra correm o risco de ser esmagados ao simples peso da documentação" (LIPSON, 1967, p. 27) continua atual, permitindo apenas trocar "papéis" por "arquivos eletrônicos". É desse dilema entre produção infinita de informação e necessidade inerente de o Estado proteger seus cidadãos – um dos "grandes problemas" que CP encara enquanto ciência social (LIPSON, 1967, p. 83-115) – que surge o que se chama aqui de Era dos Ruídos. Nela, cuja principal característica é interconectividade cibernética, a regra é se perder no emaranhado de dados e informações – convertidos em dígitos binários – e a exceção é encontrar informações estratégicas, longe de

[141] Daí que, nas últimas décadas, emerge a chamada Inteligência de Sinais (*Signal Intelligence* – SIGINT), com o intuito de auxiliar os serviços de Informação na interceptação e decodificação das comunicações eletrônicas e digitais (BESSA, 2014, p. 21).

ruídos, afinal, embora a Web seja uma ferramenta de gestão do processo de pesquisa e difusão dos resultados (FREITAS *et al*, 2006, p. 17), "[...]o que as pessoas buscam é diferente do que publicam na Web" (BAEZA-YATES; RIBEIRO-NETO, 2013, p. 263).

A Era dos Ruídos, como se vê, é um desafio para os estadistas e estrategistas porque, além do hercúleo trabalho para separar a informação realmente pertinente para a tomada de decisão política, tem de manter seus sistemas – sociais e cibernéticos – resilientes a toda sorte de ataque com vistas a, por exemplo, sabotagem, intrusão ou, mesmo, espionagem[142]. Como se observa, a Era dos Ruídos interliga, intimamente, o uso da tecnologia – mais especificamente, das TIC – com a chamada *engenharia social*. Sobre a primeira já se fala muito no presente trabalho, porém, sobre a segunda, ninguém melhor do que um dos hackers mais famosos do mundo, Kevin Mitnick, por uni-las:

> *Engenharia social* usa a influência e a persuasão para enganar as pessoas, manipulando-as ou as convencendo de que o engenheiro social é alguém que na verdade não é. Como resultado, o engenheiro social é capaz de tirar proveito das pessoas para obter informações *com ou sem o uso da tecnologia*. (MITNICK; SIMON, 2002, p. iv, grifo nosso, tradução nossa[143]).

Como se vê, a engenharia social não prescinde da tecnologia para obter informações negadas. Porém, quando ambas se unem para tal intento, potencializam os resultados do intruso. O que dizer, então, da Era da Informação? Mais do que nunca, a tecnologia joga um papel imprescindível para compreender o que é e como se comporta grande parte das sociedades hodiernas, interconectadas mediante o uso das TIC. Diante de tal cenário, a engenharia social ainda continua relevante em casos mais complexos de acesso a informações negadas[144], pois, agora, *dados relevantes para a tomada de decisão estão aí*, armazenados em nuvens, em redes de computadores e, até mesmo, em fontes aberta, à espera de serem analisados.

Certamente, o caso mais conhecido que mescla ciberespaço e espionagem é aquele deflagrado, no ano de 2013, pelo ex-contratado da NSA Edward Snowden. Nesse viés, a presente subseção defende, à luz de CiberRI, a tese de que o Caso Snowden teve tudo para ser o "momento *Sputnik*" brasileiro, no que tange às questões da Segurança e da Defesa

---

[142] Conforme disserta Bessa (2014, p. 13), a "[...]Espionagem, diferentemente do que muita gente pensa, é uma atividade muito antiga. Em todas as épocas e em todos os locais, os generais sempre espionaram seus inimigos para melhor estabelecer as suas estratégias de guerra". Cf. GONÇALVES, 2008; 2013.

[143] Texto original: "*Social engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology*". Conferir, especialmente sobre a junção da engenharia social com a tecnologia, o capítulo 11 de Mitnick e Simon (2002, p. 173-193).

[144] Um interessante uso de combinação entre engenharia social, atividade de Inteligência de Estado e Defesa Cibernética é o de como o Stuxnet foi parar nos sistemas Siemens da usina nuclear iraniana de Natanz. Com certeza, os relatos mais detalhados disso estão em Sanger (2012, p. 188-225, 449-451) e Zero... (2016).

Cibernéticas no País, mas não o foi, dando, em seu lugar, uma versão estrategicamente frustrada, a que se dá, aqui, o nome de "pseudomomento Snowden" brasileiro.

Há duas definições embutidas nessa ideia. A primeira é uma referência ao chamado "momento *Sputnik*" estadunidense. A outra se liga ao fato de que o Caso Snowden, de um lado, *desperta* uma espécie na cultura estratégico-militar brasileira em relação às questões de Segurança Cibernética, mas, de outro, não passa de um *momentum* efêmero. Como se demonstra com o elemento de composição "pseudo", entende-se que esse caso podia ser o "momento *Sputnik*" brasileiro para a tal cultura de Segurança Cibernética, mas acabou interrompido por questões de várias ordens, desde político-econômico-orçamentárias até estratégico-tático-operacional.

Para entendê-lo, é necessário assumir que a Era Espacial se inaugura com o lançamento e a operacionalização orbital do Sputnik I, o primeiro satélite artificial, lançado pela extinta União das Repúblicas Socialistas Soviética (URSS), em 1957 (AGÊNCIA ESPACIAL BRASILEIRA, 2012, p. 8). O impacto desse acontecimento no transcorrer da história contemporânea é de tamanha importância estratégica, sobretudo, para os EUA, originando algo tão revolucionário para a P&D em C&T, que fica conhecido, lá, como "momento *Sputnik*". Essa introspecção estadunidense lança, à época, um olhar crítico em relação a *todo* o seu sistema educacional, a fim de que a geração *Baby Boomer* superasse o *gap* científico-tecnológico em relação aos soviéticos (CHACRA, 2011). Desde então, o espaço sideral começa a ser estrategicamente pensado em paralelo às dimensões e topologias tradicionais, atrelando-o ao temor de que os mesmos foguetes[145] que lançaram o Sputnik I carregassem também ogivas nucleares. Logo, era necessário criar mecanismos de defesa contra tal ameaça. Essa realidade de incerteza e superação tecnológica constante se torna o cotidiano dos estrategistas dos dois blocos antagônicos no período da Cortina de Ferro. Já no século XXI, a incerteza gerada pela Guerra Fria Cibernética, atrelada à dependência e às defasagens bélicas e tecnológicas entre os Estados, torna a concepção de uma cultura de Segurança Cibernética imprescindível para o próprio conceito de desenvolvimento nacional, conforme se apregoa em documentos norteadores da Defesa brasileira.

"Momento *Sputnik*" trata-se, portanto, de uma verdadeira revolução cultural, com vistas a um objetivo maior, de longo prazo e explícito, de projeto de nação, galgado na educação como premissa para o desenvolvimento tecnológico. Nunca se viu algo parecido no Brasil; no máximo, têm-se intenções de se atrelar desenvolvimento nacional ao desenvolvimento do

[145] No Brasil, são conhecidos por veículos lançadores de satélites (VLS).

chamado Setor Estratégico Cibernético (St Ciber), expostas na END (BRASIL, 2012a, *passim*) e no Livro Branco de Defesa Nacional (LBDN). Nesse seguimento, esperava-se que o Caso Snowden fosse o estopim para o tal "momento *Sputnik*" do Brasil, em relação ao Setor Estratégico Cibernético. Logicamente que não se esperava a mesma tonalidade com que os EUA deram ao *seu* "momento *Sputnik*", porém, as medidas – políticas, tecnológicas, econômicas, estratégicas e militares – tomadas pelo governo brasileiro mostraram-se paliativas, e não paradigmáticas; "conformacionárias" – por falta de adjetivo melhor –, e não revolucionárias. Finalmente, as sucessivas crises político-econômicas dos anos 2014-2016, bem como a falta de investimentos *sistemáticos* nessa seara, minaram completamente tal perspectiva. É a esse estado de coisas que se chama de "pseudomomento Snowden", que aconteceu no Brasil, mas, provavelmente, ocorreu também em outros países em desenvolvimento. A pujança da vontade estratégica novamente se depara com a relutância da vontade política.

Outro exemplo disso é a não aprovação da, agora aprovada, Política Nacional de Inteligência (PNI) e sua negligenciada atenção depositada à espionagem cibernética, anos antes mesmo de Snowden surgir na política internacional. O Projeto de Lei que cria a PNI já previa o nascimento de e o investimento em cultura e tecnologia de Segurança Cibernética, sobretudo para evitar o que, anos depois, ocorreu de fato: tomadores de decisão do Alto Escalão brasileiro tornaram-se alvo de espionagem cibernética. O Projeto da PNI continuou engavetado pela Presidência da República até meados de 2016, e, por ironia do destino, a Presidente da República foi um dos principais alvos do esquema de espionagem cibernética internacional, encabeçado pelos chamados *Five Eyes*[146] e delatado por Snowden (BESSA, 2014, *passim*).

Novamente, esperava-se que, com as revelações de que interceptaram as ligações telefônicas da Chefe de Estado, houvesse também mudanças em todos os níveis da "segurança institucional cibernética" no Brasil, desde o nível político-estratégico até o tático-operacional. Essa percepção advinha do fato de que "[...]a imposição da mudança é fator tão constante como os próprios problemas" (LIPSON, 1967, p. 34). Todavia, não foi o que se sucedeu no Brasil. Pelo contrário, deu-se lugar a uma impotência diante dos constrangimentos trazidos pela Era dos Ruídos. Pior dos que os ruídos, que interferem na transmissão da mensagem, é a frustração de não poder ter uma resposta à altura para eliminá-los.

[146] O "*Five Eyes*" ou "Cinco Olhos" é formado por um grupo de cinco países anglófonos composto por Austrália, Canadá, EUA, Inglaterra e Nova Zelândia que compartilha informações obtidas pelo programa de coleta de dados *PRISM*, também revelado por Snowden em 2013 (BESSA, 2014, p. 74, 85). A metáfora dos cinco olhos, em vez de 10 – um par para cada país antropomorfizado –, é assaz pertinente a esse caso, pois faz alusão à forma natural com que as pessoas *espionam*, por exemplo, através da fechadura, isto é, mantendo *apenas um olho aberto*.

O Caso Snowden apenas ilustra como alguns países, tais quais EUA e Inglaterra, estão se adaptando à realidade cibernética em termos estratégicos. Se, "[...]nos primeiros tempos, [...]a obrigação de proteger o grupo [societal] foi cometida aos homens fisicamente aptos[...]" (LIPSON, 1967, p. 89), parece que, hoje, a segurança repousa sobretudo na mente de homens aptos a separar o conteúdo que verdadeiramente importa dos seus ruídos. Portanto, um estudo sistemático sobre essa nova realidade, à luz de teorias e tentativas explicativas oriundas da comunidade epistêmica de RI, tende a impulsionar um subcampo internacionalista, sobretudo em seu Campo Teórico.

Como se vê nesta subseção, a pesquisa acadêmica em temas afeitos a CiberRI são, de longe, as, atualmente, mais se concentram esforços internacionalistas para compreender o ciberespaço. Por conseguinte, é onde, igualmente, não só universidades, mas também governos, têm investido recursos, com o intuito de compreender os principais acontecimentos cibernéticos e seus impactos nas relações exteriores e internacionais. Não obstante essa supervalorização da pesquisa em CiberRI – que, aliás, é um reflexo do que ocorre, nas últimas décadas, no seio universitário como um todo (FRAGOSO FILHO, 1984, p. 24-28) –, há outra possibilidade de inserir os estudos ciberinternacionalistas na defesa acadêmica, qual seja: a extensão.

2.5 Extensão em CiberRI

Embora não haja "[...]ainda uma definição precisa e universalmente aceita do que seja a extensão universitária" (FRAGOSO FILHO, 1984, p. 32), ela pode ser entendida como "[a] prática académica [*sic*] que interliga a universidade, nas suas atividades de ensino e de pesquisa com as demandas da maioria da população[...]" (O PLANO..., [200-]).

Como também lembra Fragoso Filho (1984, p. 29-30), o termo "extensão universitária" surge na América Latina, a partir dos anos 1960, com o intuito de levar a universidade a participar dos problemas da comunidade em que está inserida. Essa relação intrínseca entre extensão universitária e resolução de problemas locais é, logicamente, importante, sobretudo em um país como o Brasil, que possui desigualdades assaz acentuadas. Porém, tal relação não é rígida, afinal, além dos problemas *endógenos* à comunidade local em que se situa um *campus* universitário, núcleo avançado ou polo[147], há também problemas *exógenos* que produzem efeitos colaterais na localidade. O local e o internacional, em muitos casos, se confundem.

[147] Ver diferenciação entre os três em Brasil (2009, p. 13).

Como se afirma, *supra*, CiberRI não toca apenas a temas atinentes a questões que envolvem guerra[148] e paz[149]; é possível sair, sem traumas epistemológicos, da segurança internacional e tocar temas mais próximos ao cidadão comum, a exemplo de aplicativos móveis. Por exemplo, no caso brasileiro, a regulamentação ou a proibição do Uber está na pauta dos municípios, que, por força do inciso I do Art. 30 da CF88, têm a competência de "legislar sobre assuntos de interesse local" (BRASIL, 1988, p. 26), embora, no âmbito federal, o Conselho Administrativo de Defesa Econômica (CADE) já se posicione no sentido de demonstrar que o Uber "[...]ao contrário de absorver uma parcela relevante das corridas feitas por táxis, na verdade, conquistou majoritariamente novos clientes, que não utilizavam serviços de táxi" (ESTEVES, 2015, p. 8). Eis aí um exemplo de tema de estudo, à luz da Política Comparada e Internacional, das relações intergovernamentais brasileiras com outros países. Um projeto de extensão, nesse sentido, iria mais além do que um projeto de pesquisa acadêmica – neste caso, sobre os impactos urbanos, legais e econômicos do uso do Uber no tecido viário –; ele levaria os resultados da pesquisa à crítica social.

Nesse mesmo viés, CiberRI tem muito a oferecer à extensão universitária. Em termos mais práticos, uma IES que se situa na capital federal pode propor um projeto de extensão que discuta com a sociedade aspectos políticos da Atividade de Inteligência no ciberespaço. Alguns temas a serem levantados podem tocar questões como o papel do Legislativo Federal no controle externo de tal atividade, bem como tentar compreender como esse controle se atina também ao ciberespaço.

É possível também discutir com a sociedade, em termos gerais e/ou comparativos, a Governança da Internet, aos moldes de cursos que, embora não sejam "de extensão universitária", têm essa preocupação de incutir uma cultura local sobre tal temática. São

---

[148] Embora polissêmico, pode-se compreender o conceito de guerra, aqui, como "[...]o uso da violência com o objetivo de restaurar uma ordem equilibrada, quer pelo reordenamento das relações sociais a fim de expressar adequadamente a nova relação entre as forças existenciais" (VOEGELIN, 1982, p. 124). Para uma acepção clausewitziana de guerra, ver Duarte (2012, p. 31) e Proença Jr e Diniz (1998, p. 51); para uma copenhaguense, *vide* Buzan, Wæver e Wilde (1998, p. 26); para uma realista, cf. Maquiavel (1996, p. 31); para uma marxista, ver Hobsbawm (2007, p. 398); para sua relação intrínseca com RI, observar Sarfati (2011, p. 14); para uma acepção dos clássicos políticos, ver Kart (2008, p. 8) e Rousseau (2003, p. 136); para sua relação com a diplomacia, *vide* Almeida (2005, p. 12). Acerca das chamadas guerras de quarta geração (G4G), ver: Duarte (2012, p. 10, 22, 24, 27). Para o caso específico das guerras cibernéticas, por exemplo, o termo "violência" assume um sentido mais amplo, que abarca não a mera coerção física, e sim a sobreposição de uma vontade sobre a de outra pessoa (BERLIN, 1969, p. 3) ou Estado, que, no âmbito do *Software Power*, tem mais a ver com a execução de rotinas não pré-estabelecidas de programas de computadores. Em todo o caso, vale lembrar que "[o]s Estados disputam poder, mesmo não estando em guerra" (VALENTE, 2007, p. 60).

[149] Assim como o conceito de guerra, o de paz também encontra em Voegelin (1982, p. 124, grifo nosso) espaço, a saber: "[...]ordem *temporária* de relações sociais que expresse adequadamente o equilíbrio das forças existenciais".

exemplos a *South School on Internet Governance* (SSIG), do *Centro de Capacitación en Alta Tecnología*, da Argentina, e os cursos intensivo e jurídico da Escola de Governança da Internet no Brasil (EGI), promovidos pelo Comitê Gestor da Internet no Brasil (CGI.br), na cidade de São Paulo.

Em termos de CiberRI – e, até mesmo de RI –, pouco se vê acerca dessa prática que engloba os resultados da pesquisa em temas afeitos a CiberRI, de um lado, e a interação com alunos extensionistas, do outro, tendo a sociedade como público-alvo.

Possivelmente, CiberRI pode se desenvolver, em termos extensionistas, de outras maneiras. Uma delas é seguir o exemplo do Decanato de Extensão da Universidade de Brasília (UnB), que, já nos anos 1970, oferecia cursos a distância, por meio de livretos e apostilas, sobre temas introdutórios a CP e RI. Atualmente, cursos dessa natureza são mais do que bem-vindos a CiberRI, tornando-se uma tarefa menos árdua nos dias atuais, sobretudo com o auxílio da própria Internet, haja vista que a criação e o gerenciamento de cursos *online* tornarem-se uma prática constante de grandes IES, a exemplo dos cursos *online* ofertados pela *Harvard Extension School*[150] ou pelo consórcio de universidades que compõem o Coursera[151] e o edX[152]. Tudo isso sem contar com a facilidade de se construir cursos completos virtuais por meio de plataformas pedagógicas baseadas em *software* livre como o Moodle[153].

Por falar no Coursera, há um curso que toca em alguns temas bastante pertinentes a CiberRI, intitulado "História da Internet, Tecnologia e Segurança"[154], desenvolvido pela Universidade de Michigan e ministrado pelo professor Charles Severance. Apesar de este curso inserir-se na categoria Ciência da Computação, suas quatro primeiras aulas versam, em inglês, sobre a história da Internet e podem servir de base para a introdução de um curso, por exemplo, sobre "História das CiberRI" ou "História da Internet e seus impactos nas relações internacionais". Eis, abaixo, a tradução para o título de cada uma dessas aulas:

1. O surgimento da computação eletrônica;
2. A primeira Internet: NSFNet;
3. A Web se torna fácil de usar; e
4. Comercialização e crescimento.

---

[150] https://www.extension.harvard.edu/open-learning-initiative.

[151] https://pt.coursera.org.

[152] https://www.edx.org.

[153] https://moodle.org.

[154] https://pt.coursera.org/learn/internet-history.

É nesse rol de exemplos análogos à extensão universitária que se pode incluir o trabalho pioneiro do alemão Daniel Oppermann em ofertar, ainda em 2010, o curso *online* "Função da Internet no ambiente da Política Internacional", que tinha 20 horas de carga horária, dentro do Projeto Política Internacional Online (PPI Online).[155]

Ora, se se diz que RI possui uma grade multidisciplinar, a Internet é multimídia[156] por excelência. Por meio dela, pode-se enriquecer a experiência dos usuários – alunos e comunidade – por meio das possibilidades de se usar não apenas textos, mas também mapas, imagens – estáticas e interativas –, áudios e vídeos, aproveitando o fato de que, há muito, "[o] mundo da Web e das aplicações multimídia está em constante evolução" (FREITAS *et al.*, 2006, p. 70). Some-se a isso a criação de objetos virtuais de aprendizagem (OVAs)[157] voltados especificamente para CP, RI e CiberRI, que é algo que não se vê com frequência, especialmente no Brasil.

Estudiosos e pesquisadores de RI podem seguir os exemplos de CP, Geopolítica e História e, assim como eles – que fabricam, de forma interativa e animada, mapas e teorias dos jogos –, produzir seus próprios OVAs. Especificamente na área de Segurança Cibernética, têm-se algumas ferramentas mais técnicas, porém que propiciam inferências internacionalistas e que podem servir também de subsídio para a proposição de um curso extensionistas. Vejam-se alguns exemplos a seguir:

- *Real-Time Web Monitor*[158], construído pela empresa de Internet estadunidense Akamai, tem o objetivo de monitorar as principais regiões que sofrem com ataques cibernéticos. Em termos ciberinternacionalistas, pode-se propor, por exemplo, uma breve correspondência entre teoria e prática, no sentido de comparar se as regiões mais problemáticas em termos de segurança – no bojo do que Buzan e Wæver (2003) chamam de Complexo Regional de Segurança (CRS) – também são as mais problemáticas em termos cibernéticos;
- *Targeted Cyberattacks Logbook*[159], produzido pela Kaspersky Lab, traz um

[155] http://politica-internacional.org.

[156] De acordo com Baeza-Yates e Ribeiro-Neto (2013, p. 191), "[m]ultimídia é um termo normalmente utilizado para designar aplicações que manipulam diferentes tipos de dados digitais originários de tipos distintos de mídia. Os tipos mais comuns de mídia em aplicações multimídia são texto, som, imagem e vídeo (que é uma sequência animada de imagens)".

[157] OVAs podem ser definidos como "[...]*any digital resource that can be reused to support learning*" (WILEY, 2000, p. 7).

[158] https://www.akamai.com/us/en/solutions/intelligent-platform/visualizing-akamai/real-time-web-monitor.jsp.

[159] https://apt.securelist.com.

impressionante banco de dados interativo e animado sobre os principais *malwares* e seus diversos reflexos. Peque-se o exemplo do Stuxnet e ter-se-á bastante literatura para refutar ou não o que diz o Logbook proposto; e

- CIBERAMEAÇA - Mapa em Tempo Real[160]: esta feramenta, também desenvolvida pela Kaspersky Lab, é certamente a mais complexa, em termos visuais, para se analisar os ataques cibernéticos em escala mundial. Um de seus diferenciais é vir traduzida para o português. Provavelmente, é o *framework* mais impactante para os estudos de Segurança Cibernética a nível mundial e pode servir de introdução para cursos extensionistas ou como força de aplicar conhecimentos adquiridos da literatura especializada.

Não restam dúvidas de que, no âmbito da extensão universitária, um dos cursos mais relevantes para os objetivos desta Tese é o "Atividade de Inteligência no Brasil e Segurança Internacional"[161], com carga horária de 32 horas, lecionado pelos professores Bernardo Wahl G. de Araújo Jorge e Peterson Ferreira da Silva[162]. Esse curso foi ofertado, em 2016, pela Fundação Escola de Sociologia e Política de São Paulo (FESPSP), ligada à Universidade de São Paulo (USP). Dentre seus oito tópicos, um deles se destina a um tema assaz afeito à CiberRI, qual seja: "Segurança Cibernética: o debate sobre espionagem e privacidade pós-Snowden".

Como se buscou mostrar nesta segunda seção, uma defesa acadêmica de CiberRI perpassa pelo tripé constitucional da universidade brasileira. Em todas essas dimensões acadêmicas, pode-se vislumbrar a imprescindibilidade desse subcampo para RI. Nesse viés, acredita-se que a presente seção atinge o segundo objetivo específico desta Tese, que é o de definir os limites e as potencialidades dos estudos ciberinternacionalistas no ensino, na pesquisa e na extensão de RI.

Parte-se, agora, para desvendar, em termos teórico-metodológicos, como CiberRI impacta e pode vir a impactar o aperfeiçoamento de seu campo-pai.

---

[160] https://cybermap.kaspersky.com. Um tutorial para utilizar tal ferramenta está disponível em: https://www.youtube.com/watch?v=vuOLiu3wFQ0.

[161] http://www.fespsp.org.br/curso/106/atividade_de_inteligencia_no_brasil_e_seguranca_internacional.

[162] Vale notar que ambos os professores têm graduação e pós-graduação em RI.

3 PARTINDO DOS ESTUDOS DE SEGURANÇA INTERNACIONAL

> "*Cyberizar*" o pensamento dos acadêmicos de RI requer trabalhos publicados que os desafiem a pensar além dos conflitos interestatais do passado, além das teorias do jogo ou do poder[...]. (DEMCHAK, 2014, p. vi, grifo nosso, tradução nossa[163]).

O subcampo internacionalista de CiberRI que aqui se defende não paira apenas no campo das ideias – não obstante o considerável número de exemplos por meio dos quais este trabalho buscou consubstanciar seus conceitos e definições. Ele também ganha vida mediante sua aplicação inferencial no mundo empírico, a partir do Campo Teórico. Em outras palavras, teoria e prática se unem, à luz de elementos metateoréticos internacionalistas, para explicar acontecimentos cibernéticos, constituindo-se assim em uma verdadeira práxis ciberinternacionalista.

Se as duas primeiras seções focaram aspectos mais conceptuais, esta derradeira seção tem a dupla missão de analisar duas dimensões empíricas de CiberRI. A primeira delas diz respeito ao principal objeto de CP, o poder, trazido aqui sob a bruma do ciberespaço. Indo além da definição de poder cibernético, já internalizada no vocabulário dos estudos internacionalistas sobre o ciberespaço, oferta-se o conceito de *Software Power* como, por que não dizer, uma instituição efetiva[164] da política internacional hodierna. De certa forma, essa primeira dimensão se reveste do mais puro ciberinternacionalismo, engendrando um conceito que só pode existir sob as bases de CiberRI, fundadas na primeira seção, *infra*. Falar de CiberRI e não mencionar *Software Power* é o mesmo que versar sobre História das RI e não mencionar as duas guerras mundiais.

Já a segunda dimensão desta seção busca apresentar em que ponto se encontram os estudos ciberinternacionalistas no Brasil, com o intuito de consolidar, ainda mais, a defesa acadêmica de CiberRI, pois se entende que a forma mais precisa de mensurar a reação da comunidade epistêmica de RI aos temas afeitos a CiberRI é por meio da análise de sua produção científica.

Essas duas dimensões, uma mais geral e outra mais específica, juntas, trazem à tona o terceiro objetivo específico desta Tese, qual seja o de evidenciar como CiberRI pode

---

[163] Texto original: "*Cyberizing the thinking of international relations scholars requires published works that challenge them to think beyond state-state conflicts of the past, beyond game or power theories that rest largely on isolating events from the new reality of a host of interrelated and ever more deeply integrated substate systems*".

[164] De acordo com Bull (2002, p. 4), as verdadeiras instituições efetivas que moldam a sociedade internacional são o equilíbrio do poder, o Direito Internacional, a diplomacia, o papel das grandes potências e à guerra.

potencializar o aperfeiçoamento de RI, em assuntos de política internacional, no geral, e do caso brasileiro, no específico.

3.1 *Software Power* e sua aplicabilidade na política internacional

O poder se desenvolve a partir das relações sociais, objeto de investigação das ciências sociais (MEGALE, 1990, p. 53). Os acontecimentos a que se chamam de *sociais* "[...]são quase invariavelmente aqueles que, do mesmo modo, designamos como 'intencionais' ou revestidos de uma intenção, de uma finalidade" (RUDNER, 1969, p. 126). Nesse sentido, quando qualquer *software – grosso modo*, entendido aqui como um conjunto de rotinas dispostas em linguagem de programação em um código-fonte computacional – causa danos a outro *software* sem que haja, para isso, *intenção*, ou seja, pela ocorrência de mera falha ou desatualização, não está se falando sobre *Software Power*. Este sim enseja uma intenção, mais precisamente, uma intenção política.

A partir, sobretudo, do século XXI, testemunha-se a emergência de um novo ambiente, totalmente artificial, em que esse tipo de interação ocorre, o ciberespaço, especialmente, uma parte dele, a Internet. Principalmente com o fim da Guerra Fria, o ciberespaço configura-se não apenas como um *locus* social para a interação de indivíduos, mas também para a atuação estratégica de Estados. Ele se torna, nesse último viés, um espaço para, dentre outros, a projeção de poder. Como afirma Valente (2007, p. 15-16), "[...]os Estados não devem estar perdendo a oportunidade de usar esses novos tempos de informação num trabalho de conquista, manutenção ou ampliação de poder". Essa lógica retroalimentar materializa a máxima de que não existe vácuo de poder nas relações internacionais, muito menos no âmbito do ciberespaço.

3.1.1 Poder e sua relação com a segurança internacional

O poder, que transmudado às relações entre os Estados, é elemento-chave nos estudos de CP e RI. Não é por mero acaso que Martin Wight, um dos expoentes da chamada Escola Inglesa de RI, constituiu as relações internacionais em termos de política do poder (WIGHT, 2002). De acordo com Lipson (1967, p. 33), "[o] poder se manifesta de vários modos, desde a presença desapercebida, o respeito e [a] obediência normal até [mesmo] o temor e o terror". Daí, por exemplo, CiberRI também abarcar questões atinentes ao chamado Terrorismo Cibernético, tema tão em voga e deveras estudado e pesquisado atualmente pela comunidade epistêmica de RI[165], sobretudo em razão do advento do grupo terrorista Daesh.

[165] Ver Gráfico 2, *supra*.

Como se observa no Quadro 1, *supra*, a Coreia do Norte hackeia inúmeros *e-mails* da Sony Corporation, expondo dados pessoais de muitos de seus clientes, no ano de 2014. Em termos de Economia Política Internacional, isso gerou perdas de valor da multinacional japonesa na NASDAQ, levando, a efeito dominó, partes de economias que possuíam ações lastreadas naquela empresa, principalmente os EUA. Já em termos de CiberRI, vê-se que aquilo que se inicia no ciberespaço tem consequências fora dele, a saber: imediatamente, o então presidente estadunidense "[...]Barack Obama responde[...] com sanções econômicas contra Pyongyang" (AGENCE FRANCE-PRESSE, 2016). Em outras palavras, um acontecimento cibernético se transmuda em estopim para disputas econômicas no complexo xadrez da política internacional. Esse exemplo é um dentre vários pelos quais a literatura analisada busca demonstrar a interseção entre o que se convém chamar de geopolítica do ciberespaço, uma junção entre a geopolítica das relações internacionais e a do espaço cibernético (BREMMER; GORDON, 2011; BRONK, 2016; ISHII, 2016).

No âmbito dos ESI, a seguinte máxima é bastante conhecida: "[...]as armas e os equipamentos podem mudar, mas os princípios da estratégia permanecem constantes" (LIPSON, 1967, p. 33). Isso quer dizer que a necessidade de se pensar estrategicamente sobrepõe o uso automático de armas, cada vez mais poderosas em sua intenção de causar destruição. Como Nye Jr (2011b, p. 114) apregoa, não é a primeira vez na história que mudanças paradigmáticas na tecnologia da informação ocorrem no seio das sociedades. É o que acontece com a introdução dos cavalos nas guerras tribais, da pólvora entre os povos orientais, das armas de fogo nas guerras interestatais na Era das Revoluções, do avião na Primeira Guerra Mundial, da bomba atômica na Segunda Guerra e, mais recentemente, das chamadas armas cibernéticas em seu intento de danificar estruturas estratégicas nacionais. É nesse mesmo viés que, novamente, Lipson (1967, p. 33, grifo nosso) apregoa que:

> [...]haverá sempre problemas idênticos de moral, treinamento, disciplina[...], bem como o de *aplicar o devido grau de força no lugar certo e no momento preciso*.[...] o que hoje tende cada vez mais a impressionar é a *permanente necessidade de nos ajustarmos, individual e coletivamente, às invenções da tecnologia*, à inovação social[...].

Também não é desconhecido que, dentre as diversas funções do chamado Estado Moderno, sobressai-se a de promover a segurança de seus súditos ou concidadãos. Acerca disso, não falta literatura que ajude a corroborar tal tese, desde o ateniense Tucídides, passando pelos autores clássicos da política – ocidental – e das relações internacionais e chegando ao século XXI, com discussões sobre as chamadas "novas ameaças".

Se a finalidade precípua do Estado é prover segurança, ele necessita, por conseguinte, de meios para tal. É aí que entra a questão da Defesa. Dependendo do âmbito, os meios têm a mesma função – garantir a segurança –, mas possuem nomes diferentes: no âmbito interno, chama-se Segurança Pública; no externo, Defesa Nacional.[166] No primeiro caso, os órgãos de investigação dão conta da tarefa; no outro caso, as Forças Armadas dão o seu tom. Utiliza-se aqui o segundo caso, ou seja, analisa-se um tipo especial de poder, o militar, que é o braço armado do político, utilizado, sobretudo, quando a Diplomacia não encontra resultados por meio de seus tratados, acordos e encontros.

Segurança e proteção compõem, portanto, lados de uma mesma moeda: para serem alcançadas, é imprescindível que se faça o uso da força, ou, na melhor das hipóteses, sua dissuasão, *i.e.*, a capacidade concreta e intencional de projetar poder, para inibir tentativas de uma outra potência agressora ir de encontro aos interesses de um Estado (COVARRUBIAS, 1999, p. 5; PROEÇA JR; DINIZ, 1998, p. 26). Dessa forma, ao afirmar que "[...]o fato de ter que empregar a força, busca o Estado, inevitavelmente, possuir-lhe o monopólio", Lipson (1967, p. 98) faz uma clara referência à máxima de Weber (1967, p. 56) sobre o monopólio estatal do uso legítimo da força física/violência em um dado território. Logo, "[a] lógica da coerção impõe o monopólio" da força (LIPSON, 1967, p. 100).

Em resumo, esta é a noção *mainstream*, sobretudo dos Estudos de Defesa e de Segurança Internacional, na qual se assentam os conceitos de Defesa Nacional e de Segurança Internacional e que deriva, sobremaneira, de dois elementos-chave tanto para CP quanto para RI, que são o território e a soberania. Entrementes, no século XXI, tais conceitos são postos à prova não pelo crescimento da ideia de ciberespaço e da Internet em si, mas por seu uso estratégico-militar nesse ambiente. Dessa maneira, não é incorreto afirmar que "o ciberespaço tem recentemente emergido como uma preocupação de segurança estratégica" (MAZANEC, 2015, p. 219, tradução nossa[167]).

---

[166] Pode-se dizer que Segurança Nacional, palavra tão em voga no período militar brasileiro e receosamente pouco usada nos dias atuais, é um meio termo entre ambos os conceitos analisados, pois cuida do inimigo interno e externo com praticamente o mesmo aparato coercitivo. Certamente, é esta a origem de grande parte dos debates sobre o uso das forças armadas em missões de Segurança Pública, Brasil adentro e nas Missões de Manutenção de Paz das Nações Unidas. Para uma crítica à forma com que certas democracias podem invocar tal termo para desviar-se de processos legislativos ordinários, ver Buzan, Wæver e Wilde (1998, p. 29).

[167] Texto original: "*The cyberspace* [...]*has only recently emerged as a strategic security concern*".

3.1.2 Quando o poder toca o ciberespaço

A junção entre essa segurança estratégica e o ciberespaço é o que se pode chamar de Segurança Cibernética. Primordial para a compreensão de tal conceito é a noção do papel que a tecnologia joga nas capacidades bélicas dos Estados. Todavia, a questão tecnológica é uma condição necessária, mas não suficiente, para explicar os acontecimentos ciberinternacionais. A tecnologia pode ser definida como a junção de "[...]valores, normas, procedimentos e crenças, basead[a] no pensamento matemático, incorporado nos objetos materiais e na prática social, [assim,] é preciso especificá-la enquanto *manifestação cultural*" (KAWAMURA, 1986, p. 35, grifo nosso). Se se assumir a tecnologia a partir dessa espécie de não neutralidade social de que fala Kawamura e Weber, por exemplo, não se deve estranhar o fato de Buzan e Hansen (2009, p. 53) postularem que o estudo das novas tecnologias direciona muitos dos temas de ESI. Daí, acredita-se, advém a necessidade de avaliar o impacto tecnológico das ameaças, vulnerabilidades e estabilidades/instabilidades estratégicas. O ciberespaço não foge à risca dessa observação, constituindo-se ora como meio, ora fim, ora nível de análise cuja unidade básica é o *software*. É na junção dessas três percepções que se concentra o conceito de *Software Power*.

Opta-se por criar e manter tal conceito na língua inglesa por dois motivos principais. O primeiro diz respeito a uma possível maior aceitação internacional; já o segundo aponta para o fato de sua tradução literal não agradar a língua portuguesa, a saber: "poder computacional-programático" ou "poder que advém do programa de computador". Não se trata, porém, de "poder do *software*" ou "poder do programa de computador", pois se emprega aqui a palavra *software* como um atributo/adjetivo (conceito-fim), e não objeto/substantivo (conceito-meio) do poder, tal como parece que faz Nye Jr (2004; 2011b) com *Cyber Power*. Até mesmo "Poder de *Software*" soa estranho aos desígnios aqui perseguidos, haja vista que enfatiza "*Software*", e não "Poder", elemento imprescritível em CP/RI.

Alguém pode indagar onde fica o papel do *hardware* nesse conceito. Logicamente, que o *hardware* é uma parte imprescindível para compreender as mudanças tecnológicas das últimas décadas. Basta mencionar o uso quase ubíquo dos *smartphones* nas grandes e médias cidades do mundo ou, mesmo, o uso de *drones* cada vez menores nos campos de batalha. Porém, entende-se que o papel do *hardware* é secundário na política internacional hodierna, haja vista que as principais questões que lhe diziam respeito – miniaturização e microprocessamento – foram praticamente resolvidas no desenrolar dos anos 1980 e 1990. O que se vê, hoje, é um papel muito mais pujante do *software* sobre o *hardware* – daí, por exemplo, o preço dos celulares terem caído, em detrimento do aumento da oferta de *apps*, serviços e arquivos

multimídia *online* –, a ponto de quando se versa, em RI, sobre "armas cibernéticas", pensa-se em *software* malicioso (*malware*) como *worm*, vírus e Cavalo de Troia, e não em cabos, fios e processadores. Some-se a isso o uso crescente de ataques distribuídos por negação de serviço ou *Distributed Denial-of-Service attack* (DDoS), que, antigamente, eram apenas ataques por negação de serviço ou *Denial-of-Service attack* (DoS), sem o "D". Mais do que uma letra, o D de "Distribuído" representa o poder do *software* (*power of software*) – no caso, rodando em um computador-*master* – sobre o *hardware*, que, também neste caso, são os computadores-*zumbies*. O uso de *software* por um *cracker* representa o poder do *software*; já o seu uso por um Estado contra outro, representa o *Software Power*. Novamente, ambos os conceitos de *hardware* e *software* estão interligados, mas, diante da observação internacionalista sobre os acontecimentos cibernéticos mais importantes, privilegia-se, aqui, o segundo.

Como já dito, os conceitos que esta Tese engendra alinham-se ao Modelo 3C, proposto na subseção 1.3, *supra*. Com o *Software Power* não é diferente; ele se ancora em premissas dos Campos Epistêmico e Teórico de RI, como aquela que afirma que:

> [...]os princípios [da CP] devem ser retomados através de um trabalho de teorização que tenha origem na situação histórica concreta do seu próprio tempo e leve em conta a amplitude global do conhecimento empírico desse tempo. (VOEGELIN, 1982, p. 18).

É nessa direção que se pensa o *Software Power* como uma atualização de conceitos-chave na análise internacionalista – como são os casos de poder e política internacional – para o seu próprio tempo, o século XXI, e com base no conhecimento empírico que se tem desse tempo, *i.e.*, do conhecimento ciberinternacionalista.

Pode-se definir, enfim, *Software Power* como a capacidade político-estratégica de que dispõem Estados para intervir na política internacional ou externa de outro Estado via utilização de *software*. Assumindo-o como tal, não apenas a guerra cibernética pode ser enquadrada nesse conceito, como também as tentativas de um Estado burlar a corrida presidencial estadunidense mediante a invasão e publicação de mensagens de *e-mail* de um dos candidatos, como, supostamente, aconteceu nas três últimas eleições americanas.

Agora, assim como ocorreu com CiberRI, é preciso, pois, diferenciar tal conceito de outros dois que lhe parecem sinônimos, mas que não o são, quais sejam: *Software Warfare* e *Cyber Power* ou poder cibernético[168]. O primeiro diz respeito a um dos três modelos criados por Bellamy (2001), a partir dos quais a Guerra Centrada em Redes (GCR) pode ocorrer. O

[168] Ao contrário do que vinha sendo feito, esta seção prefere utilizar o termo *Cyber Power* a poder cibernético, com vistas a evidenciar a diferenciação entre este e *Software Power*.

autor utiliza essa tipologia para, por exemplo, conjecturar sobre como usar o ciberespaço nas guerras hodiernas. Nesse sentido, *Software Warfare* ou "guerra de *softwares*" constitui:

> [...]um combate travado no campo de fluxo de dados computacionais, através de manipulação de códigos-fonte, acesso à dependência de *softwares* via Internet, com o objetivo de atingir as capacidades inimigas, neutralizando-as e, assim, alcançando uma supremacia no combate físico. (PERON, 2016, p. 122, grifo do autor).

Como se vê, o conceito de *Software Warfare* é bastante limitado a aspectos específicos, com o escopo centrado na Internet e atrelado a combates físicos. Nesse viés, vislumbra-se o *Software Warfare* mais em estratégias de Defesa do que em políticas de Defesa, possibilidade esta contida na definição de *Software Power*. Em breves palavras: este contém aquele, *i.e.*, aquele é uma dimensão deste.

Como já se versou até aqui, ao realizar uma análise tendo como parâmetro CiberRI, o cientista deve ter cuidado para não cair na tentação de analisar *o acontecimento pelo acontecimento*. Em outras palavras, deve-se levar em consideração não apenas os dois requisitos básicos de CiberRI[169], mas também os elementos metateoréticos de RI. Por exemplo, pegue-se o paradigmático caso envolvendo o *worm* Stuxnet, em que a esmagadora maioria da literatura revisada apenas descreve o que ele é e faz, mas se esquece de analisá-lo à luz de RI. Veja-se, abaixo, um rápido exemplo de como o caso do Stuxnet pode ser contextualizado à luz do *Software Power*.

Com os atentados do 11 de setembro de 2001, um nicho sobre as ameaças assimétricas baseadas em redes terroristas e que se utilizam das novas TIC, como a Internet, começa a se formar nos ESI (BUZAN; HANSEN, 2009). A partir daí, os desafios transnacionais ensejados pelo ciberespaço se aguçam, surgindo algumas formas de contorná-los. É justamente no final desse debate, já no século XXI, que o tema da guerra cibernética ressurge vigorosamente com a obra mais importante dessa área desde Arquilla e Ronfeldt (1993; 1997), qual seja: *Cyber War*, escrita pelo ex-Assessor da Casa Branca, Richard A. Clarke, e do *Fellow* do *Council on Foreign Relations*, Robert A. Knake.

A descoberta do Stuxnet, em 2010 (IRÃ, 2011; ZERO..., 2016), causa grandes estragos no programa nuclear iraniano, uma vez que tal *malware* fora projetado, por potências estrangeiras desconhecidas, para controlar e inutilizar as centrífugas Siemens de enriquecimento de urânio daquele país (PORTELA, 2016, p. 94). Pelo fato de o Stuxnet ter sido programado para realizar essa tarefa bem específica, tendo como alvo uma estrutura estratégica,

---

[169] Cf. *caput* da segunda seção, *supra*.

ele é conhecido, na literatura especializada, como a primeira arma cibernética projetada para as guerras do século XXI (BROAD; MARKOFF; SANGER, 2011; FALLIERE *et al.*, 2011; GAMA NETO; VILAR LOPES, 2014; HOPKINS, 2011; IRÃ, 2010; 2011; MELE, 2013; ZERO..., 2016), representando, dessa forma, um marco para os conflitos internacionais de última geração (SEGAL, 2016).

Como se vê, se o Stuxnet é considerado uma – e, até agora, "a" – arma cibernética, é porque ele está envolto em um contexto maior de guerra cibernética e de política externa, que, por ser uma "guerra", também só é assim qualificada se houver um propósito político por trás. Veja-se o que afirma, por exemplo, Voegelin (1982, p. 124) sobre este último aspecto:

> Se existe algum propósito na guerra, deve ser o de restaurar o equilíbrio de forças, e não o de agravar a perturbação; deve ser o de reduzir o excesso de força perturbador, e não a destruição da força a ponto de criar um novo vácuo de poder gerador de desequilíbrio.

Logo, se se engendra o Stuxnet para sabotar, e não destruir, o programa nuclear iraniano, é porque seu(s) criador(es) tinha(m) por objetivo restaurar um equilíbrio de forças – neste caso, nuclear –, e não criar um novo vácuo de poder, mediante, por exemplo, o uso de bombardeios aéreos à usina nuclear alvo do *worm*.

Como se busca brevemente defender, se a análise do Stuxnet não traz algum desses elementos metateoréticos de RI – no caso, Análise de Política Externa, Geopolítica e História das RI, por exemplo –, está-se, na realidade, diante de um ensaio descritivo, e não de uma análise internacional, e, aí, o campo de RI deixa de se atualizar e aperfeiçoar com tal acontecimento. O ambiente da análise pode até migrar para o ciberespaço, mas as premissas internacionalistas continuam as mesmas. Mais do que qualquer outro exemplo, o Stuxnet materializa o conceito de *Software Power*, e não apenas do *Software Warfare*, pois diz questão a políticas públicas nacionais, tais como a de Defesa e externa de uma potência em relação a outra.

Quanto ao conceito de Cyber Power, sua diferenciação enseja uma discussão mais profunda, que diz respeito à própria noção de projeção de poder, como se observa na próxima subseção.

3.1.3 Uma terceira via de projeção internacional de poder?

O conceito de *Software Power* faz engendrar uma terceira via de projeção de poder no sistema internacional que, ao lado dos *Hard Power* e *Soft Power*[170], volta-se à lógica e às idiossincrasias do ciberespaço.

Como sabido, no sistema internacional anárquico[171], as relações de poder ocorrem em detrimento das capacidades que cada Estado possui – tais quais militares, diplomáticas, econômicas, tecnológicas e geoestratégicas –, bem como da habilidade de formar e manter alianças entre si. Para uns, essa anarquia internacional é consequência direta da incapacidade de os Estados-nação em não conseguir mais prover segurança[172], seja na dimensão de ordem interna, seja na de proteção externa, já que ela, a anarquia, lhes impõe limites à formação de uma paz duradoura (LIPSON, 1967, p. 434-439, 456), ou, nas palavras de clássicos da política, de uma paz perpétua. Nesse sentido, a projeção de poder se torna uma forma de dissuasão no cenário internacional, *i.e.*, constitui um *modus operandi* internacional que o Estado encontra para – assim como seus cidadãos, no âmbito interno – sobreviver no ambiente anárquico que paira sobre as relações internacionais.

A dissuasão internacional pode ocorrer de forma quantitativa ou qualitativa. Por exemplo, de um lado, ao demonstrar a *possibilidade de uso* – fator qualitativo – de um porta-aviões, um Estado A projeta mais poder do que um Estado B, que não possui tal capacidade; de outro lado, o fato de um Estado A possuir 10 porta-aviões – fator quantitativo – projeta, internacionalmente, mais poder do que um Estado B que detém apenas um único exemplar, sem mesmo demonstrar a possibilidade de usá-los. Não é à toa que essa lógica dá origem ao Dilema de Segurança[173], "[u]m dos paradoxos centrais na discussão de questões estratégicas[...]"

---

[170] Não se considera o *Smart Power* nem o *Cyber Power* como vias de projeção de poder *stricto sensu*, pois o primeiro é a mera junção das vias *hard* e *soft* do poder, e o segundo analisa a difusão do poder transvertido de informação, não sua projeção, envolta em um contexto dissuasório. Cf. NYE JR, 2011b, p. 114, 150).

[171] O sentido de anarquia aqui é o mesmo daquele consagrado por Bull (2002, p. 57), qual seja: "[...]ausência de governo ou de regras". Transpondo-se ao plano internacional, refere-se à inexistência de uma instituição supranacional que dite os rumos de todos os Estados, ou seja, que faça nascer um governo ou ordem mundial, conforme atesta o subtítulo da obra-mor de Hedley Bull. Cf. HERZ, 1950, p. 157, 173; JERVINS, 1976, p. 62-63, 67-68, 75-76.

[172] Uma crítica a essa posição encontra-se no próprio Bull (2002, p. 317).

[173] Herz (1950, p. 157, grifo nosso) define assim tal dilema, a partir do nível social: *"[g]roups or individuals living in such a constellation must be, and usually are, concerned about their security from being attacked, subjected, dominated, or annihilated by other groups and individuals. Striving to attain security from such attack, they are driven to acquire more and more power in order to escape the impact of the power of others. This, in turn, renders the others more insecure and compels them to prepare for the worst. Since none can ever feel entirely secure in such a world of competing units, power competition ensues, and the vicious circle of security and power accumulation is on*". Ver também Jervins (1976, p. 76).

(PROENÇA JR; DINIZ, 1998, p. 22), cuja expressão-mor é a corrida armamentista[174].

Há um arcabouço teórico, de cunho neoliberal institucionalista, bastante empregado pela comunidade epistêmica de RI, que afirma que a projeção e a obtenção de poder manifestam-se por duas vias: a de forma bruta, mediante o uso de mecanismos militares e econômicos de *Hard Power*; e a de forma branda, pelo *Soft Power* da diplomacia, da influência cultural e de outros meios não brutos. Entrementes, o final do século XX vê surgir o amálgama entre esses dois tipos de poder, o *Smart Power*. E, como já abordado, o século XXI se torna palco para o surgimento do *Cyber Power*, já visto, rasamente, na subseção anterior.

Nye Jr (2011b, p. 123, grifo nosso, tradução nossa[175]) assim define *Cyber Power*:

> [...]conjunto de recursos relacionados a criação, controle e comunicação da informação eletrônica e computacional – infraestrutura, redes, *softwares* e habilidades humanas, incluindo não apenas a Internet de computadores em rede, mas também Intranets, tecnologias móveis e comunicações espaciais.

Porém, adverte-se, novamente, como ocorre no início da seção 2, *supra*, que a má compreensão das terminologias estrangeiras pode pôr uma análise internacionalista a perder. Explica-se: "*Cyber Power*" – às vezes, grafado com ou sem hífen, tendo seus termos juntos ou separados e em maiúsculo ou minúsculo – se refere ora a "poder cibernético", na acepção de Nye Jr (2011b, p. 123), ora a "potência cibernética"[176], em sentido bem próximo ao que Kant (2008, p. 28) e Rousseau (2003, p. 122) chamam de "potência", como uma representação externa de um Estado frente a outros. Em todo caso, não se tira de mente que o fato de que tal conceito "[...]é polissêmico e no ambiente das Relações Internacionais pode se referir a diferentes capacidades do Estado, como a militar, a econômica, a cultural, a política, a diplomática e outras" (WINAND; SAINT-PIERRE, 2010, p. 21).

De acordo com Betz e Stevens (2011b, p. 43, grifo nosso, tradução nossa[177]), este tipo de poder "[...]é parte de uma linhagem terminológica que inclui 'poder aéreo' e 'poder naval' para descrever as operações de poder coercitivo nacional, principalmente militar, em *topologias específicas*". Portanto, *Cyber Power* é o poder que se manifesta no ciberespaço, em vez de se constituir em uma nova ou diferente forma de poder (*ibid*., p. 44). Porém, isso contraria o

---

[174] Daí que a analogia a uma corrida armamentista cibernética está bastante em voga atualmente: troquem-se os exemplos dos porta-aviões e, em seu lugar, acrescentem-se os das armas cibernéticas.

[175] Texto original: "[...]*a set of ressources that relate to the creation, control, and communication of electronic and computer-based information – infraestructure, networks, softwares, human skills. This includes not only the Internet of networked computer, but also Intranets, cellular technologies, and space-based communications*".

[176] Neste caso, tal termo pode aparecer também no plural. Essa peculiaridade ocorre também com o uso de "*cyber powers*" no sentido de "capacidades cibernéticas" (Cf. SINGER; FRIEDMAN, 2014, p. 144).

[177] Texto original: "[...]*cyber-power is part of a terminological lineage that includes 'airpower' and 'seapower' to describe the operations of national, principally military, coercive power in particular environmental domains*".

próprio criador do conceito, quando este afirma que "uma nova revolução da informação está *mudando a natureza do poder* e aumentado sua difusão" (NYE JR, 2011b, p. 114, grifo nosso, tradução nossa[178]). A visão política de Nye Jr vai, em certa medida, na mesma linha técnica de raciocínio de Freitas *et al.* (2006, p. 133), quando estes afirmam que "[...]a Web oportuniza uma forma de coleta e de disseminação das informações nunca antes possível de ser realizada".

Os dois últimos conceitos analisados, especialmente o de *Cyber Power*, não conseguem, arrisca-se a dizer, exprimir, com maior grau de acurácia, o elo intrínseco entre o ciberespaço e a projeção/obtenção de poder na política internacional, muito mais concernente às relações internacionais do que a difusão de poder. Portanto, o conceito nyeiano se preocupa, de forma precípua, em explicar (i) como o poder, travestido de informação, é difundido no ambiente cibernético – especialmente na Internet – e, por conseguinte, (ii) como isso se torna um desafio para o Estado-nação. Posto de outra forma, para Nye Jr (2011b, p. 114, 150), *Cyber Power* trata o ciberespaço como um meio para se chegar a um fim, que é a difusão de poder, mas deixa brechas quanto a se inferir sobre esse mesmo espaço como um fim em si mesmo, tal como o viés realista faz com a terra, o mar, o ar e, em certa medida, o espaço sideral. Nesse sentido, expressões como "dominar o espaço" ou "controlar o espaço aéreo" fazem parte da dimensão estratégica de uma política de Defesa, ao passo que "invadir por terra" ou "dominar pelos mares" encontram-se na dimensão tático-operacional. Assim, a definição *Software Power* enseja expressões do tipo "dominar o ciberespaço"; já *Cyber Power*, "dominar pelo ciberespaço".

Embora a noção de *cyber* englobe a de *software*, as diferenças entre ambos os conceitos, mais do que semânticas, são sintáticas. Em todo o caso, o que se deve prevalecer aqui não a ideia de rejeição de um pelo outro, e sim a sua complementariedade, a ponto de se dizer que *Software Power* pode ser uma espécie de "*Cyber Power* 2.0".

3.1.4 O Software Power nos Campos Epistêmico e Teórico de RI

Vários Estados têm seguido o exemplo pioneiro dos EUA na área de Defesa Cibernética e estão acelerando o processo de fabricação de armas cibernéticas (GAMA NETO; VILAR LOPES, 2014), fomentando aquilo que a literatura especializada chama de Guerra Fria Cibernética (FERREIRA NETO; VILAR LOPES, 2016). Como alguns impactos cibernéticos reverberam na política internacional e vice-versa, a tensão e a instabilidade dessa nova modalidade de corrida armamentista tendem a gerar toda sorte de conflito internacional, desde

[178] Texto original: "*[...]a new information revolution is changing the nature of power and increasing the diffusion*".

o mais brando até o mais bruto, nos dizeres de Joseph Nye Jr.

Dessa forma, o caso estadunidense se mostra como paradigmático nessa seara, pois é justamente nele que, dentre outros[179], surgem: (i) a primeira rede de computadores, a ARPANET; (ii) a primeira arma cibernética, o Stuxnet; (iii) o primeiro comando militar de Defesa Cibernética, o *U.S. Cyber Command* (USCYBERCOM)[180]; e (iv) o mais ambicioso esquema de espionagem internacional operado por *software* estrategicamente projetado para interceptação de informações – sobretudo coleta e análise de meta-dados – no ciberespaço.

Não faltam exemplos de que as capacidades cibernéticas e a projeção de poder são levadas a sério naquele país. Prova disso é a justificativa das prioridades do seu orçamento militar, cujo Departamento de Defesa apregoa o que se segue:

> Nossa capacidade de *projetar poder* é um componente-chave de nossa orientação estratégica. Protegemos importantes capacidades, tais como o novo bombardeiro, a atualização da bomba de pequeno diâmetro, os porta-aviões, a modernização dos nossos soldados e as *capacidades cibernéticas*. Nós também protegemos *capacidades que nos permitam projetar poder em ambientes negados*. (ESTADOS UNIDOS DA AMÉRICA, 2014, p. 9, grifo nosso, tradução nossa).

Mais que isso, o *leading case* estadunidense é prova viva de que o ciberespaço se transforma em um domínio estratégico para ações militares[181] e de Inteligência de Estado[182]. Assim, o estudo do *Software Power*, no âmbito mais geral de CiberRI, proporciona ao internacionalista, dentre outros, a possibilidade de: investigar os nexos da relação ciberespaço-projeção de poder internacional; pensar a projeção de poder no século XXI para além dos conceitos tradicionais do *mainstream* internacionalista; e robustecer a literatura, principalmente, no que diz respeito a Segurança e Defesa Cibernéticas.

Trazendo de volta as noções de Campo Epistêmico e CampoTeórico, do Modelo 3C, pode-se afirmar que o conceito que aqui se engendra também vem acompanhado de ampla base metateorética de CP e RI, por meio de autores que trataram a questão do poder nas relações internacionais de forma sistematizada. Citam-se alguns. O primeiro deles é Morgenthau (2003), para quem os governantes dos Estados agem de forma racional e amoral na política

---

[179] Outras variáveis também podem ser levadas em conta, tais como: maior investimento em Segurança e Defesa Cibernéticas; primeira doutrina militar específica para a atuação no ciberespaço; e alto grau de securitização militar do ciberespaço.

[180] De acordo com Sanger (2012, p. 191, grifo nosso), o "*US Cyber Command is based at Fort Meade, Maryland, so that the Defense Department's operations are alongside those of the NSA. Gen. Keith B. Alexander, who* [à época] *is the director of the NSA, is also the commander of what the Pentagon calls USCYBERCOM*".

[181] Consoante Proença Jr e Diniz (1998, p. 50), "[a]s ações militares são, como deveria ser óbvio, a razão de ser da existência de forças armadas". Duarte (2012, p. 35) as chama de "estado das práticas".

[182] Hipótese testada e comprovada, qualitativa e quantitativamente, em Lopes (2013).

internacional, direcionando suas escolhas políticas na busca por: manter o poder, por meio da preservação do *status quo*; aumentar o poder, por meio do imperialismo; ou demonstrar o poder, por meios diplomáticos ou de projeção de força – ou projeção de capacidades, nos dizeres de Clausewitz (2005). É este último aspecto que mais interessa ao conceito de *Software Power*.

De Bull (2002), obtém-se o conceito de sociedade anárquica, subsídio para uma analogia entre o sistema internacional de Estados e o ambiente cibernético, pois ambos não possuem um Leviatã[183], nos dizeres hobbesianos, que dite as regras de conduta entre seus agentes, o que implica conviver sob a influência de muitos constrangimentos internacionais. Esse vácuo de poder supranacional e cibernético gera incentivos para os Estados usarem o *Software Power* sem ressentimentos morais ou legais, sendo limitados, tecnicamente falando, por suas próprias capacidades cibernéticas.

Waltz (2002) complementa a ideia gerada por Bull, no sentido de apresentar um modelo cujo nível de análise está centrado exclusivamente na esfera internacional, ou seja, no próprio sistema internacional anárquico ou em sua estrutura – daí o nome da vertente realista desta corrente se chamar "Realismo Estrutural". Essa ideia waltziana é pertinente aos propósitos do *Software Power*, pois sua essência busca inferir que o caráter anárquico do ciberespaço, e não seus atores, é que limita as ações estatais – especialmente, as militares – nesse ambiente. O exemplo do Stuxnet é novamente posto em cena para exemplificar essa máxima.

Atualmente, é bem verdade que as vias clássicas de demonstração de poder ainda continuam a ter influência na política internacional, tais como: submarinos nucleares, porta-aviões e capacidade de influenciar o sistema financeiro internacional. Todavia, as recentes operações estratégico-militares no ciberespaço suscitam a ideia de que atores estatais utilizam tal ambiente como uma nova alternativa para o pressuposto realista-morgenthauniano da demonstração de poder. A Coreia do Norte é um exemplo bastante comum na literatura especializada[184], pois suas capacidades e projeção de poder no ciberespaço não condizem com o que ocorre na política internacional real: é inversamente proporcional. Eis aí um caso a ser melhor analisado pela comunidade ciberinternacionalista.

Complementando essa ideia, retoma-se o próprio Nye Jr (2004; 2011b), o qual apregoa que, durante o século XX, o poder não é mais compreendido apenas em termos militares e

---

[183] Ao evocar Hobbes (2005), Voegelin (1982, p. 8, 112-117, 129-133) define o Leviatã como o corpo político ao qual o ser humano se subordina por completo. A analogia internacional, com a falta dessa figura, é, com certeza, uma das principais ideias-força de RI.

[184] Cf. CAVELTY, 2008, p. 110; 2015, 84; CHOUCRI, 2012, p. 234; CLARKE; KNAKE, 2015, p. 22-30; LEWIS, 2013, p. 17-18; NAZARIO, 2009, p. 174; RANTAPELKONEN; KANTOLA, 2013, p. 33; RID, 2012, p. 28; SINGER; FRIEDMAN, 2014, p. 151; p. 17-18; STOHL, 2014, p. 92-93, 98.

econômicos – ou seja, em uma concepção *hard* –, mas também por intermédio da "atração"[185] que determinados valores, culturas, instituições e políticas exercem sobre os demais Estados, no que ele chama de *Soft Power*. Mas se utilizam tanto uma quanto outra via para analisar a projeção de poder em ambientes/domínios não criados pelo ser humano e em que a questão do tempo-espaço pode ser controlada. Porém, o ambiente cibernético é corriqueiramente visto como um potencial ambiente/domínio que constrange o Estado também em termos ontológicos, pois basta lembrar que o território, um dos pilares da Teoria Geral do Estado (DALLARI, 1998), inexiste em tal ambiente (WERTHEIM, 2001), ou melhor, suas partes (*hadware*) estão fisicamente localizadas, mas o todo cibernético é territorialmente desconhecido.

Esta última assertiva se coaduna com a ideia por trás do *ranking* de guerra cibernética, proposto por Clarke e Knake (2015, p. 122), acerca da capacidade que um Estado possui para "guerrear" no ciberespaço. De acordo com esses autores, quanto mais um Estado, como os EUA, depende de sistemas baseados em TIC, mais ciberneticamente vulnerável ele está. Novamente, refutar ou não esa tese para outros Estados mostra-se desafiador para os estudos ciberinternacionalistas.

Associando esses pressupostos teóricos ao teor empírico das políticas públicas nacionais de Inteligência e de Defesa, observa-se que algumas doutrinas e ações estratégicas no ciberespaço impregnam-se de ambos os vieses – *hard* e *soft* –, mas que necessitam de algo a mais para serem compreendidas sob o espírito do tempo atual, que é caracterizado pelo uso constante e incessante do ciberespaço nas relações sociais e de poder. É justamente aqui que o *Software Power* se insere nos estudos de RI, ou seja, como o poder capaz de projetar força sem as preocupações clássicas do tempo-espaço, sem o condicionante da territorialidade, mas permeado pelo constrangimento da anarquia internacional do ciberespaço.

A Figura 5 mostra como o *Software Power* modifica o nível de análise internacionalista em relação ao *software*, fazendo-o passar de um meio objetivando um fim, nos quatro domínios tradicionais, para um fim em si mesmo, originando, por sua vez, um novo domínio para a projeção do poder e, portanto, para a análise política e internacionalista.

[185] Daí que Nye Jr (2004) se refere a *Soft Power* também por meio desses termos.

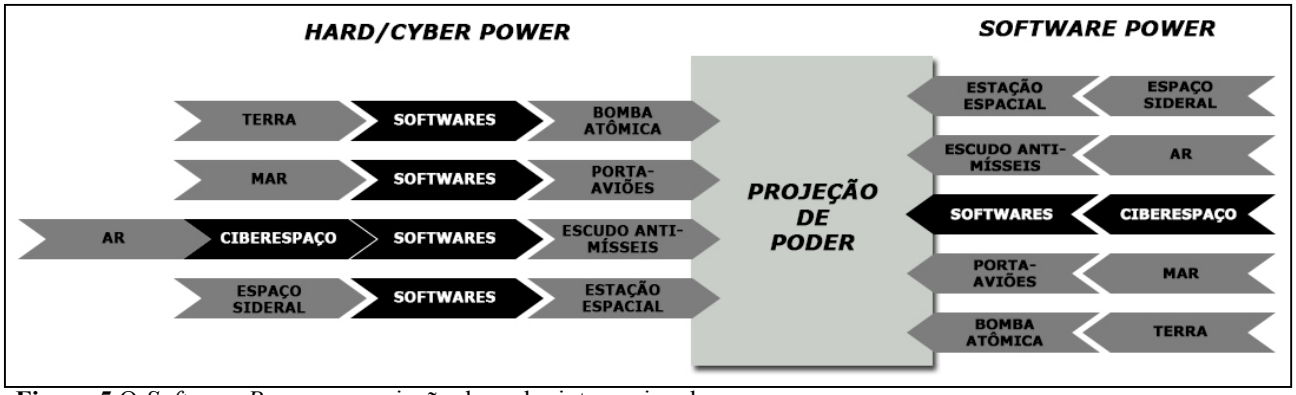

Figura 5 O *Software Power* e a projeção de poder internacional
Fonte: Elaboração própria.

Como se buscou mostrar nesta subseção, CiberRI busca se constituir em bases não apenas teóricas, mas também empíricas. No meio-termo entre esses dois mundos, está o conceito de *Software Power*. Se para a política internacional, os estudos ciberinternacionalistas mostram-se promissores para o aperfeiçoamente de RI, é possível investigar, a partir de agora, como, especificamente, a comunidade epistêmica de RI no Brasil reage a esse estado de coisas. É o que sebusca realizar na próxima subseção.

3.2 Um panorama ciberinternacionalista do Brasil

Como dito, esta última subseção objetiva projetar o estado de coisas de parte do conhecimento ciberinternacionalista já produzido no Brasil. Isso se justifica, dentre outros, pela:

> Existência de uma necessidade profunda de que cientistas políticos e acadêmicos de RI identifiquem, descrevam e expliquem os desenvolvimentos, perspectivas e desafios emergentes do ciberespaço, de forma não só teórica, mas também empiricamente precisa. (KREMER; MÜLLER, 2014, p. xi, tradução nossa[186]).

Ademais, parafraseando Kawamura (1986, p. 14)[187], alerta-se que a principal preocupação desta subseção não é com a *mera quantificação* e análise espacial da observação de CiberRI, e sim com o *avanço* qualitativo da postura dos estudiosos brasileiros de RI que se debruçam sobre a questão do ciberespaço.

---

[186] Texto original: "[...]*there is profound need for political scientists and scholars of IR to identify, describe, and explain these developments, prospects, and emerging challenges theoretically and empirically in an accurate manner*".

[187] Assim trata, *in verbis*, Kawamura (1986, p. 14, grifo da autora): "Nossa preocupação não consiste na quantificação nem na análise da distribuição espacial da ocorrência do objeto de estudo, mas[,] sim[,] na compreensão do *avanço* qualitativo da postura do engenheiro quanto à questão tecnológica no país".

Por se tratar de um tema deveras amplo, delimita-se a abrangência desta pesquisa para temas ciberinternacionalistas afeitos aos assuntos de maior procura e produção acadêmica, conforme comprovam as análises do Campo Epistêmico[188], ou seja, Segurança Cibernética atrelada à segurança internacional.

3.2.1 Introito ao caso brasileiro

Por falar em Epistemologia, tem-se em mente que o principal *locus* que, atualmente, mais congrega estudiosos em matéria de Defesa e de segurança internacional no Brasil encontra-se, esparsamente, no conjunto de anais do Encontro Nacional da ABED[189] (ENABED), acessíveis por meio de seu *site* oficial[190].

A escolha da ABED, e não de outras associações nacionais que possuem áreas temáticas (ATs) atinentes a temas de CiberRI – tais como Associação Nacional de Pós-Graduação e Pesquisa em Ciências Sociais (Anpocs), Associação Brasileira de Ciência Política (ABCP) e ABRI – justifica-se, sobretudo, por questões técnicas e de logística de pesquisa. Exemplificando: apesar de a ABRI possuir uma AT de "Segurança Internacional", os anais do seu encontro nacional de 2015, por exemplo, não estavam mais acessíveis[191] no momento da feitura desta Tese, bem como os de 2011, cujo *site* oficial está fora do ar[192]. Em todo caso, com uma rápida pesquisa *online* no domínio-raiz dos *sites* oficiais dessas três associações nacionais que congregam partes da comunidade espistêmica de RI, é possível constatar a baixa resposta aos termos de busca "ciber" e "*cyber*".[193] Daí o fato de se manter apenas a ABED, cujos anais do seu encontro anual – que, desde 2016, passa a ser bianual – encontram-se disponíveis.

No Brasil, a emergência de pesquisas e publicações internacionalistas sobre o ciberespaço ganha força sobretudo com as versões mais recentes da Política Nacional de Defesa (PND) e da END, que redirecionam grande parte da atenção militar para o fortalecimento do St

---

[188] Cf. subseção 2.4.2, *supra*.

[189] A ABED é uma sociedade acadêmica sem fins lucrativos que congrega estudiosos, civis e militares, das áreas de Defesa e Segurança.

[190] Disponível em http://www.abedef.org/. Vale lembrar que a ABED também edita a Revista Brasileira de Estudos de Defesa (RBED), a qual já conta com dois trabalhos – Vilar Lopes e Oliveira (2014) e Portela (2016) – pertinentes a CiberRI, em suas quatro primeiras publicações, disponíveis em: http://seer.ufrgs.br/index.php/rbed.

[191] http://www.encontronacional2015.abri.org.br/site/anaiscomplementares?AREA=18%20.

[192] http://ena2011.abri.org.br/.

[193] Exemplo de logaritmo para busca: "ciber OR cyber site:abri.org.br"; "ciber OR cyber site:cienciapolitica.org.br"; e "ciber OR cyber site:anpocs.com". Nesses três casos, há que se triar o que é publicado nos respectivos anais e o que é de outros tipos de publicações, tais como revistas e boletins.

Ciber (BRASIL, 2012), com a atuação do Centro de Defesa Cibernética do Exército[194] (CDCiber) – o qual se encontra em vias de se tornar o Comando de Defesa Cibernética do Ministério da Defesa. Mais recentemente, em 2013, o tema volta a se fortalecer com as revelações de Snowden[195], com um foco no papel do controle e da vigilância do Estado sobre o cidadão. Já em 2014, com a aprovação, pelo governo federal, do Marco Civil da Internet[196], estabelecendo princípios, garantias, direitos e deveres para o uso da Internet no País, uma pequena parte da comunidade epistêmica de RI contribui com análises descritivas sobre o tema, haja vista o caráter pioneiro de tal marco legal dificultar uma abordagem mais comparativa com um grande número de observações, por exemplo. Em 2016, alguns trabalhos internacionalistas se propõem a, brevemente, discorrer sobre os futuros impactos da tardia aprovação, também pela Presidência da República, da PNI, a qual já previa – como dito na subseção 2.4.3, *supra* –, antes mesmo de Snowden virar celebridade internacional, uma maior atenção à Segurança Cibernética no âmbito do Sistema Brasileiro de Inteligência (Sisbin) (VILAR LOPES, 2016; WAHL; SILVA, 2016).

Como se vê, o panorama brasileiro aponta para uma ênfase maior nas chamadas novas ameaças à segurança internacional, envoltas, por seu turno, em áreas não correlatadas a RI. Uma delas é a Segurança Cibernética, que transmigra aos Estudos de Defesa e de Segurança Internacional, ao se assimilar, de forma mais geral, ao fato de que "[...]a proposta da *defesa da tecnologia nacional* parte do pressuposto de que o enfrentamento da questão tecnológica se identifica com a defesa da soberania nacional[...]" (KAWAMURA, 1986, p. 101). Esse enfoque internacionalista sobre as TIC põe em questionamento, por exemplo, algumas explicações tradicionais que orbitam as teorias de RI e as análises de política internacional, como é o caso dos próprios conceitos de território e soberania[197], como brevemente já frisado.

Esse conceito, consagrado na expressão "[a] soberania é o poder absoluto e perpétuo de uma República[...]" de Bodin (2011, p. 195), o inventor teórico do Estado moderno (MEGALE, 1990, p. 116), atrela-se, tradicionalmente, à defesa territorial de um Estado-nação (LIPSON, 1967, p. 210, 394) e ao não reconhecimento de poder político superior aos seus próprios limites territoriais (LIPSON, 1967, p. 431, 434). Eis, agora, essas máximas aplicadas ao caso brasileiro,

---

[194] Nada impede, todavia, que outras Armas também atuem estrategicamente no St Ciber, especialmente no âmbito da Defesa Cibernética, como é o caso da Força Aérea Brasileira (FAB), que realizou seu I Seminário de Defesa Cibernética do Comando da Aeronáutica, em dezembro de 2016 (FORÇA..., 2016).

[195] Cf. subseção 2.4.3, *supra*.

[196] O Marco Civil da Internet corresponde à Lei federal nº 12.965, de 23 de abril de 2014.

[197] Cf. BARRINHA; CARRAPIÇO, 2016; BREMMER; GORDON, 2011; BRONK, 2016; FERREIRA NETO; VILAR LOPES, 2016; HERODOTE, 2014; ISHII, 2016; LOPES, 2016; MOREIRA, 2015, p. 17.

com fulcro no Art. 1º, inciso I, de sua CF88: "[a] interferência externa é uma *ameaça* frontal ao princípio constitucional da *soberania*" (BRASIL, 1988, p. 6, grifo nosso). É este também o mesmo sentido que adverte a Doutrina Militar de Defesa Cibernética (DMDC) brasileira, ao afirmar que: "[o] Brasil, como *nação soberana*, necessita possuir *capacidade* para *se contrapor às ameaças externas*, de modo compatível com sua própria dimensão e suas *aspirações político-estratégicas no cenário internacional*" (BRASIL, 2014a, p. 13, grifo nosso).

As diversas facetas da globalização e da revolução das TIC fazem com que as ameaças cibernéticas (*cyber threats*) e o próprio ciberespaço sejam objeto de estudo da comunidade epistêmica de RI, não só no Brasil, como também fora dele, com fulcro no questionamento a postulados geopolíticos e, mesmo, do próprio campo de RI. É nesse prisma investigativo que a presente seção se debruça sobre a produção ciberinternacionalista brasileira.

3.2.3 Aspectos metodológicos

De acordo com Freitas *et al.* (2006, p. 58), o sucesso para "[...]uma boa pesquisa[...] é[...] possuir a habilidade de gerar uma pesquisa adequada e um tanto quanto segura, metodologicamente". Nesse viés, a presente subseção busca esmiuçar a metodologia por trás da pesquisa a que se pretende submeter os trabalhos publicados nos anais do ENABED nos anos em que ele foi realizado, ou seja, entre 2007 e 2016.

O desenho desta pesquisa segue, em grande medida, a lógica do *método hipotético-dedutivo*, de Popper (2008, *passim*), cujo esquema pode ser resumido, de acordo com Gil (1999, p. 30), da seguinte maneira: problema → conjecturas → dedução de consequências observadas → tentativa de falseamento → corroboração. Logo, cada um dessas etapas são seguidas, desde o levantamento do problema de pesquisa até a corroboração ou não das conjecturas – ou hipóteses nula (H_0) e alternativa (H_1), conforme se vê também na próxima subseção.

Para lograr êxito na busca de dados pelo Campo Epistêmico em CiberRI do Modelo 3C, e como já alertado na Introdução, opta-se, aqui, por um diálogo maior entre os estilos qualitativo e quantitativo de pesquisa e análise, levando-se em conta a proposta de Lieberman (2005), intitulada *Nested Analysis*. Justifica-se, brevemente, tal opção metodológica por três razões principais.

A primeira delas acredita ser preciso ir além do chamado "debate KKV", iniciado a partir da obra seminal "*Designing social inquiry*", de Gary King, Robert Keohane e Sidney Verba, em 1994. Embora seja um marco para os estudos metodológicos em ciências sociais – especialmente em CP – (BRADY; COLLIER; SEAWRIGHT, 2004, p. 5-6), tal obra opta por manter a separação entre os estilos quantitativo e qualitativo de pesquisa. Mais que isso, King,

Keohane e Verba (1994, *passim*), conquanto propunham, inicialmente, uma aproximação entre esses dois estilos de pesquisa, também enfatizam o fato de a estatística oferecer certas "lições" aos adeptos dos métodos qualitativos, sendo estes últimos, o verdadeiro calcanhar da CP no Brasil (SOARES, 2005). Logo, ao colocar o método quantitativo em uma posição privilegiada, os autores não produzem um diálogo metodológico, mas sim um duplo monólogo, com maior preponderância do estilo quantitativo, não possibilitando, assim, uma integração, *de facto*, entre os métodos de pesquisa.

A segunda razão para se escolher uma estratégia de metodologia mista remete-se a outra obra importante para o assunto aqui tratado, intitulada "*Rethinking social inquiry*", editada por Henry Brady e David Collier, em 2004. O objetivo geral desse livro é repensar a contribuição das alternativas propostas, uma década atrás, por King, Keohane e Verba (1994) – sobretudo o que Brady, Collier e Seawright (2004, p. xviii, 3-5) chamam de métodos quantitativos *mainstream*. Assim, eles ofertam possibilidades para um "debate *pós*-KKV" que incluem uma maior valorização da análise de estudos de caso ou *Small-N Analysis* (SNA), em detrimento das sugestões de King e seus colaboradores, em favorecer a análise de amostras[198] com muitas observações ou *Large-N Analysis* (LNA), que propiciariam melhores inferências causais. Porém, ao tentar desconstruir o argumento dos autores de "*Designing social inquiry*", Brady e Collier (2004) também isolam os dois estilos em esferas independentes. Portanto, para os desígnios desta Tesa, tal abordagem metodológica não serve, pois os dados quantitativos oriundos do Campo Epistêmico têm de caminhar estreitamente com as informações, qualitativas em sua maioria. Isso leva diretamente à última razão.

A terceira razão diz respeito à proposta de Lieberman (2005) chamada *Nested Analysis*. Em resumo, tal estratégia analítica parte do pressuposto de que é possível sim a existência mútua entre os dois estilos de pesquisa e de análise, ou seja, a existência simbiótica entre esses dois estilos metodológicos que tanta discussão engendra nas mais diversas ciências. Como visto, King, Keohane e Verba (1994), de um lado, e Brady e Collier (2004), do outro, defendem, à sua maneira, que tanto o estilo quantitativo quanto o qualitativo conduzem para os mesmos fins, mas mediante o uso de ferramentas diferentes. O que Lieberman (2005) propõe é uma estratégia de análise que não leve à divisão dos dois estilos. Em outras palavras, ele afirma que LNA e SNA possuem seus problemas inerentes, mas que, se utilizadas em conjunto, podem

[198] Em Estatística, ramo da Matemática Aplicada (CRESPO, 2009, p. 1, 3), *amostra* é um subconjunto finito dos elementos que compõem o universo ou *população*, que, por sua vez, é um conjunto de elementos que possuem uma ou mais características em comum (CRESPO, 2009, p. 10-11; GIL, 1999, p. 99). O Apêndice D, *infra*, traz um exemplo de como calcular a amostra desejada para inferências causais de uma população finita.

resultar em uma análise ainda mais robusta e virtuosa para a pesquisa. Assim, esse autor propõe um método misto e unificado para a Política Comparada, em que a análise estatística de uma grande amostra, LNA, possa gerar investigações relevantes de um ou mais casos, SNA, contidos – ou seja, "*nested*" – nessa mesma amostra.

Vale frisar que se emprega o *Nested Analysis* sobretudo em estudos de Política Comparada e Internacional, *i.e.*, para comparar países. Todavia, devido a seu alcance analítico – assim como ocorre com os *frameworks* utilizados na subseção 1.3, *supra* –, é possível vislumbrar sua aplicação a objetos de pesquisa bem diferentes dos da proposta original; neste caso, a trabalhos acadêmicos de segurança internacional que versem sobre o ciberespaço. A Figura 6 apresenta o escopo dessa estratégia metodológica proposta por Lieberman (2005).

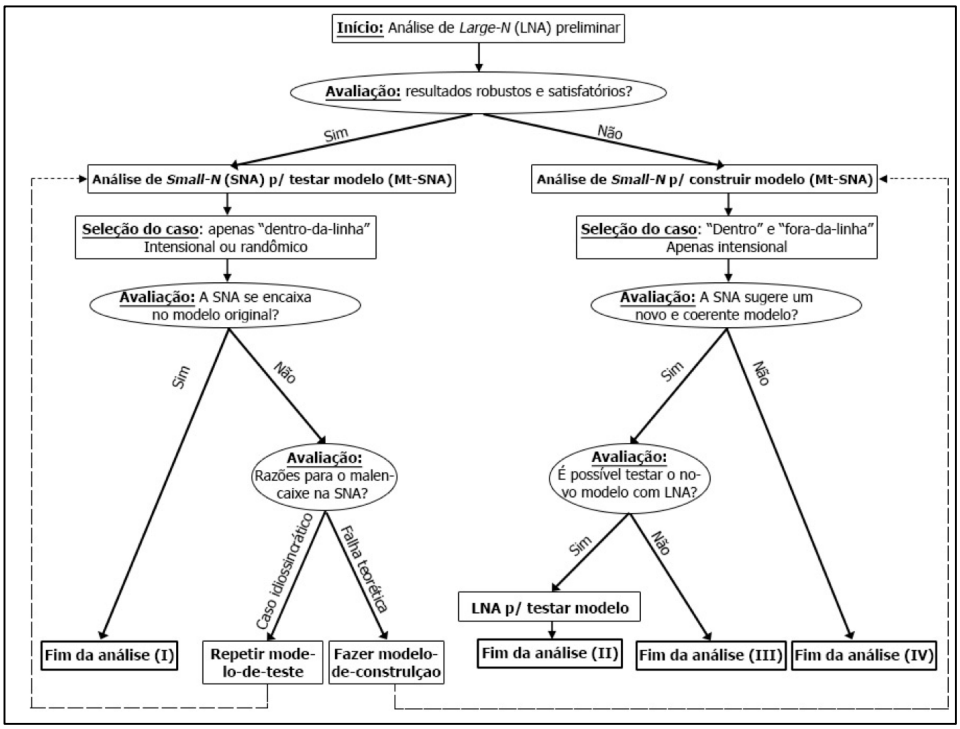

Figura 6 Visão geral do *Nested Analysis*
Fonte: LIEBERMAN, 2005, p. 437, tradução nossa.
Legenda: LNA = *Large-N Analysis*; SNA = *Small-N Analysis*.

Assim, busca-se, ainda que de forma limitada, pintar um grande quadro – não mais doxológico, e sim epistêmico[199] – do estado de coisas que envolve os estudos ciberinternacionalistas no Brasil. Em termos metodológicos, o que se busca evidenciar é o fato de que pesquisar *online* pressupõe praticamente a mesma lógica de fazê-lo de forma tradicional, tendo em vista que envolve "[...]as fases de preparação do terreno, publicação ou aplicação da

[199] Para o mesmo objetivo, só que no Campo Teórico, conferir Acácio (2016) e Acácio e Lopes (2012).

pesquisa, tratamento dos dados e divulgação dos resultados" (FREITAS *et al.*, 2006, p. 47), fases estas vistas na próxima seção e atreladas, como dito, à lógica hipotética-dedutiva.

3.2.3 O que os anais do ENABED dizem sobre o ciberespaço?

Como dito, a proposta de *Nested Analysis* pressupõe, *a priori*, uma larga base de dados para a fase de LNA, imprescindível para, *a posteriori*, seleção e estudo de caso[200] na SNA. Nesse viés, escolhe-se como local de pesquisa uma parte significativa do ciberespaço, a Internet. Tal escolha leva em conta que o processo tradicional de pesquisa tende a ser limitado por fatores como alto custo e tempo demasiadamente prolongado, o que não acontece, em grande parte, quando se usa tecnologias Web (FREITAS *et al*. p. 2006, 16, 57).

Assim, realiza-se, primeiramente, uma busca pelos termos "ciber" e "*cyber*" nos anais do ENABED publicados de 2007 a 2014 e em 2016, com o intuito de criar um banco de dados cuja amostra (*n*) é composta por todos os trabalhos já publicados nos anais do ENABED que versem, em algum grau, sobre o ciberespaço[201]. O Gráfico 3 apresenta os dados resultantes dessa pesquisa.

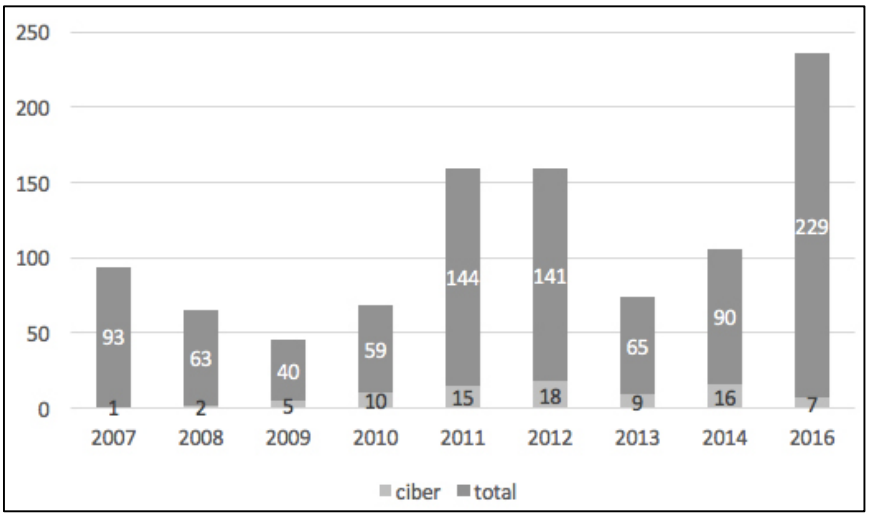

Gráfico 3 Publicações dos anais do ENABED com termos "ciber" e "*cyber*" (2007-2016)
Fonte: Elaboração própria.
Fonte dos dados: http://abedef.org/conteudo/view?ID_CONTEUDO=62; http://www.enabed2016.abedef.org/conteudo/view?ID_CONTEUDO=162.
N.B.: a) Os anais de 2012 são os únicos publicados em sistema acadêmico de indexação: http://seer.ufrgs.br/index.php/rbed/issue/view/2380/showToc.
b) Descartam-se os trabalhos que trazem os termos "cyber" ou "ciber" apenas em suas referências bibliográficas.

[200] Para uma visão geral dos estudos de casos, ver Gil (1999, p. 72-74).

[201] O salto entre os anos de 2014 e 2016 é porque, partir daquele ano, o ENABED passa a ser realizado bianualmente.

Como se observa no Gráfico 3, se se juntar os trabalhos que trazem o termo "ciber" ou "*cyber*" nos três primeiros anos do ENABED, sequer chegam ao valor obtido no quarto ano. De 2010 a 2014, o número de trabalhos aumenta consideravelmente, com uma queda absoluta em 2013. Porém, deve-se levar em conta que, em termos relativos, a quantidade de trabalhos que trazem algum termo relacionado ao ciberespaço no ano de 2013 é de 12% em relação ao número total de publicações, ou seja, a tendência relativa de trabalhos com "ciber" ou "*cyber*" é mantida em torno de 10% entre 2009 e 2014. A nona edição do Encontro, em 2016, é a primeira no formato bianual; talvez isso explique o significativo aumento da quantidade de trabalhos publicados ser a maior de toda a série temporal, 236, o que não explica, entretanto, o fato de a tendência relativa do número de trabalhos que trazem um termo cibernético em seu *corpus* regredir a marcos da segunda edição.

Analisando atentamente esta última observação, levanta-se o seguinte problema: qual a tendência que os trabalhos publicados nos enais do ENABED seguem em relação à importância dada ao ciberespaço? Para descobrir sua resposta, procede-se com o *Nested Analysis*.

Primeiramente, percebe-se que, ao longo das nove edições do ENABED, foram publicados 1.007 trabalhos, daí que o universo ou população desta pesquisa é $N = 1.007$. Desses, 83 trabalhos ($n = 83$), ou seja, aproximadamente 8% do total, trazem alguma informação sobre o ciberespaço. O Apêndice C, *infra*, traz a lista completa desses 83 trabalhos analisados, os quais formam a base do banco de dados que aqui se utiliza para operacionalizar suas variáveis[202].

Feito esse primeiro contato com o que parte da comunidade internacionalista brasileira, de vertente mais securitária, publica sobre o ciberespaço, é possível ascender esses dados do Campo Epistêmico a informações no Campo Teórico de RI.

Como o *Nested Analysis* postula, após examinar os dados mais gerais, torna-se possível evidenciar alguns *cases* que merecem um pouco mais de atenção, por parte do pesquisador. Essa atenção é posta, aqui, mediante uma análise mais profunda e à luz dos elementos metateoréticos vistos na subseção 1.2, *supra*.

Nesse sentido, cada um dos 83 trabalhos, publicados nos anais do ENABED e que chamaram atenção para os objetivos desta pesquisa, é analisado de forma minuciosa e subjetiva,

[202] De acordo com Gil (1999, p. 57), "[o] termo *variável* é dos mais empregados na linguagem das ciências sociais" e designa "[...]qualquer coisa que pode ser classificada em duas ou mais categorias". Cf. CRESPO, 2009, p. 8-9.

com o fito de descobrir o grau de importância que cada um deles dá à questão cibernética. Para isso, cria-se a variável "Grau de importância dada ao ciberespaço".

Como se atesta pelo Gráfico 3, *supra*, trabalhou-se até agora com dados quantitativos. Porém, devido à especificidade que se quer dar à pesquisa ora em tela – qual seja focar um tema em específico, o ciberespaço, à luz de trabalhos sobre segurança internacional no Brasil –, é natural que os dados quantitativos, por si só, não consigam exprimir tal especificidade. Tendo em vista que, se comparados aos dados quantitativos, os "[...]qualitativos são também mais complexos em termos de produção e análise" (FREITAS *et al.*, p. 119). Por causa disso, cria-se uma variável categórica no banco de dados etiquetada "cib_importancia", a qual comporta apenas três valores em relação ao grau de importância dada ao ciberespaço, quais sejam:

1. *nenhuma*: atesta que, embora o trabalho cite um dos dois termos da busca, as informações trazidas são irrelevantes para se compreender os impactos do ciberespaço nas relações internacionais e, mais especificamente, na segurança internacional;
2. *pouca*: este valor atesta que o trabalho traz, em poucas linhas, informações pertinentes a temas de CiberRI, mas que, apesar disso, não chegam a ser desenvolvidas ou aprofundadas em, pelo menos, um parágrafo; e
3. *muita*: atesta que o grau de importância dada à temática securitária do ciberespaço é bastante elevado, no que diz respeito ao trabalho trazer mais de um parágrafo sobre a temática ora em tela, ou mesmo, em sua versão mais extremada, girar, ele próprio, em torno de temas atinentes à questão do ciberespaço.

Antemão, entenda-se, aqui, "irrelevante" com relação aos objetivos da pesquisa. Certamente, o trabalho que se enquadra nessa categoria traz um termo cibernético como ideia secundária, em algum momento do texto, ou como exemplo para uma explicação mais importante que a própria inserção do(s) termo(s). Nesse viés, o trabalho cujo valor na variável que atesta o grau de importância for igual a "nenhuma" se enquadra no mesmo patamar que aqueles que não trazem nenhum dos dois termos em seu corpo textual. Em outras palavras, ele não serve nem para confirmam nem para não refutar a terceira hipótese secundária, haja vista que seus objetivos, enquanto trabalho científico, eram outros que não diziam respeito ao ciberespaço.

A análise que determina o grau de importância que um artigo publicado nos anais do ENABED dá ao ciberespaço é, com certeza, a parte mais importante deste momento da pesquisa, caracterizada por ser uma LSA. Todavia, ela é também a menos visível de todas, pois

praticamente nenhum *software* seria capaz de correlacionar os elementos metateoréticos em CiberRI e o que parte da comunidade epistêmica de RI no Brasil produz. Portanto, tal análise concentra-se na profunda leitura dos artigos, sua relação com os temas atinentes a CiberRI e sua comparação aos demais trabalhos. Feito isso, pode-se prosseguir com a análise dos casos, que vão se afunilando cada vez mais.

Dos 83 trabalhos já triados do universo de 1.007, chega-se à constatação de que 70% deles, ou seja, 58, apenas citam, *en passant*, um ou outro termo da busca, em seu corpo, sem lhe fornecer, portanto, ênfase ou característica securitária. Logo, habilita-se o restante dos trabalhos, *i.e.*, 25, para se aprofundar nas próximas inferências.

Aqui, faz-se necessária outra observação em relação ao *Nested Analysis*. Uma vez realizada a análise quantitativa – neste caso, utilizando-se eminentemente da estatística descritiva[203] – na fase de LNA, realizou-se a análise qualitativa de 8% desses trabalhos na fase de SNA, por meio da revisão documental e bibliográfica e à luz dos ESI. Note-se que os temas que envolvem tais revisões são os mesmos dos que esta Tese lida, como um todo, ou seja, o elo entre ciberespaço e relações internacionais. Seguindo essa lógica, como a presente subseção consubstancia a Tese, e não o contrário, assume-se que tais revisões já foram feitas, ao longo das demais seções e subseções. Assim, não há que se levantar ou explicitar novamente os arcabouços teóricos ou os elementos metateoréticos de RI – os quais só puderam ser conhecidos após uma análise essencialmente qualitativa –, aqui, para correlacioná-los aos trabalhos publicados nos anais do ENABED, pois a SNA que se sucede nesta subseção já leva, implicitamente, em conta tais revisões.

Caso a ressalta acima não fosse feita, neste ponto da análise dos anais do ENABED no Campo Teórico, certamente poder-se-ia levantar a questão de que as premissas do *Nested Analysis* não haviam sido respeitadas, haja vista que, a partir de agora, volta-se a usar métodos quantitativos, mais robustos que os do LNA, é verdade, para testar a correlação entre as variáveis do banco de dados criados. Em outras palavras, tratam-se dos mesmos casos estudados – SNA –, só que auxiliados por métodos quantitativos. Vale lembrar também que os valores da

[203] O método estatístico "[...]fundamenta-se na teoria estatística da probabilidade e constitui importante auxílio para a investigação em ciências sociais" (GIL, 1999, p. 35). Há dois tipos de Estatística, quais sejam: a Indutiva ou Inferencial e a Descritiva (CRESPO, 2006, p. 3). A partir da primeira, tão utilizada nas ciências naturais e, em certa medida, na Economia, é possível propagar os resultados da amostra (*n*) para a população (N). Porém, na estatística descritiva, como seu nome já diz, apenas se descrevem características de *n*, sem que se possa migrar os resultados para *N*. Mais que isso, a inclusão de novos dados em *n*, faz com que, necessariamente, uma nova análise deva ser realizada, pois modificam-se parâmetros imprescindíveis para a pesquisa, tais como o grau de liberdade e o desvio padrão. Daí, também, se justifica o uso aqui de técnicas multivariadas exploratórias – como a Ancor –, ao invés de modelos de regressão. Para o uso da estatística inferencial, o Apêndice D, *infra*, oferece uma fórmula para o cálculo da amostra da população dos anais do ENABED.

variável "cib_importancia" são em relação às *informações* passadas pelos próprios trabalhos, no Campo Teórico, e não aos *dados* meramente colhidos no Campo Epistêmico.

Prosseguindo, pode-se constatar que os dados contidos na variável que mede o grau de importância dada ao ciberespaço são do tipo categórico. Isso leva a uma possibilidade de inferência estatística por meio da associação não só entre essa variável e suas categorias, mas também em relação aos anos em que os trabalhos foram publicados.

Conforme apregoam Freitas *et al*. (2006, p. 29, grifo nosso), "[a] Web é somente um meio: a interpretação de tarefas depende, de fato, da flexibilidade de *softwares* disponíveis[...] e da habilidade dos atores em utilizá-los na busca de soluções *Web*". Levando isso em consideração e o fato de que "[o] processamento por computador é muito útil quando se trabalha com um grande volume de dados, como no caso de levantamentos que envolvem *amostras numerosas*" (GIL, 1999, p. 172, grifo nosso), parte-se, agora, para a *análise de correspondência simples* (Anacor) entre as variáveis do bando de dados. Tal análise é, na realidade, uma *técnica exploratória* bivariada que possibilita, dentre outros, estudar a relação estatisticamente significante[204] de interdependência entre duas variáveis categóricas (FÁVERO; BELFIORE, 2015, p. 177-180), como é o caso em tela.

Além de "cib_importania", a outra variável categórica que se cria é "edicao", que, para o caso particular desta subseção, é assumida como a edição do ENABED, e não como o ano propriamente dito em que o ENABED ocorreu – se não fosse assim, seria mais frutífero, do ponto de vista estatístico, realizar uma análise de série temporal. Nesse viés, a variável "edicao" tem apenas nove categorias – que vai de "enabed2007" a "enabed2016", com a exclusão de "enabed2015". Assim, ao examinar, por exemplo, mapas perceptuais ou diagramas de dispersão – como o mapa simétrico –, gerados a partir da Anacor, será possível perceber se há uma tendência dos trabalhos publicados nos anais do ENABED a dar mais importância à temática cibernética em segurança internacional ou não.

Eis, portanto, a finalização da fase de aplicação da pesquisa, dando, agora, prosseguimento à fase de *análise dos dados*, que pode ser realizada tanto *online* quanto via *software* (FREITAS *et al.*, 2006, p. 53). Segue-se a última opção, mediante uso do *software* estatístico STATA®.

---

[204] A um nível de 5% ou a "[...]um resíduo padronizado ajustado [em cada célula] com valor positivo superior a 1,96[...]" (FÁVERO; BELFIORE, 2015, p. 184). Quanto ao erro máximo permitido nas pesquisas sociais, Gil (1999, p. 106) lembra que usualmente se trabalha com uma estimativa de erro entre 3% e 5%; daí se utilizar a margem máxima neste trabalho.

Por meio do banco de dados, disponível *online* para replicabilidade[205], é possível gerar uma Tabela 1, de dimensão 3x9, que alocará as frequências absolutas observada para cada par "Edição do ENABED" X "Grau de importância dada ao ciberespaço".

Tabela 1 Frequências absolutas para os pares "ENABED" e "Importância dada ao ciberespaço"

Importância / Edição	Nenhuma	Pouca	Muita	Σ
ENABED2007	1	0	0	**1**
ENABED2008	4	0	0	**4**
ENABED2009	3	0	0	**3**
ENABED2010	10	0	0	**10**
ENABED2011	12	0	3	**15**
ENABED2012	12	3	3	**18**
ENABED2013	5	1	3	**9**
ENABED2014	11	4	1	**16**
ENABED2016	0	1	6	**7**
Σ	**58**	**9**	**16**	**N = 83**

Fonte: Elaboração própria.

Consonante apregoa Gil (1999, P. 172), depois de tabular os dados, uma análise estatística deve proceder à análise, a qual se desenvolve em dois níveis, quais sejam: a descrição dos dados e sua avaliação. É o que se persegue de agora em diante.

Como se vê, por meio da Tabela 1, há bem mais trabalhos que, embora possuam o termo "ciber" e/ou "*cyber*", não dão nenhuma importância para sua relação securitária com o ciberespaço. No outro prisma, é possível visualizar que, por um lado, os anais do ENABED 2016 tenham menos trabalhos publicados com esses termos em relação às últimas cinco edições do encontro, por outro, eles são, de longe, os que mais publicaram trabalhos com alto grau de importância ao ciberespaço. Todavia, a análise que se faz dessa tabela de contingência é apenas univariada, isto é, "[...]leva em consideração a distribuição de frequências para cada variável isoladamente, sem uma análise de classificação cruzada" (FÁVERO; BELFIORE, 2015, p. 193). Para conhecer as relações de interdependência entre elas, é necessário proceder com a análise bivariada.

Para tanto, a hipótese a ser testada e corroborada aqui é a de que, com o passar dos anos, o grau de importância dada ao tema do ciberespaço aumenta, embora, como já se projete, o número de trabalhos sobre o ciberespaço tenha caído no último ano analisado. É preciso, pois, testar, obrigatoriamente, as seguintes hipóteses:

- H_0: a associação entre as variáveis "cib_importancia" e "ano" é aleatória; e

[205] O banco de dados utilizado nesta Tese encontra-se disponível, em formato .dta, do STATA®, no seguinte repositório público: https://github.com/gillsvilarlopes/tese-ppgcp-ufpe.

- H_1: a associação entre essas duas variáveis não é aleatória.

Caso H_1 não seja refutada[206], pode-se concluir que, em termos estatísticos, há uma tendência significativa entre as duas variáveis, no sentido de apontar para uma importância crescente dada ao ciberespaço no seio de parte da comunidade epistêmica de RI brasileira.

Como "[...]há muitas possibilidades de testar hipóteses[...]" (GIL, 1999, p. 65), opta-se, como mencionado, pela Anacor. A fim de avaliar a significância estatística entre as duas variáveis, utiliza-se o a função "chi2" do STATA® – esse termo corresponde à distribuição $\chi 2$ ou qui-quadrado –, cujo *output* gerado para o comando "tab2 edicao cib_importancia, chi2" é: "Pearson chi2(16) = 36.8141 Pr = 0.002".

Grosso modo, esse resultado é assaz pertinente para os objetivos desta subseção porque, por meio dele, pode-se afirmar, ao nível de 5% de significância[207] – ou, em outros termos, 95% de certeza – e a 16 graus de liberdade[208], que há sim uma associação estatisticamente significante entre as duas variáveis testadas, e não aleatória.

O fato de ter gerado 16 graus de liberdade é também significativo, pois quanto mais distante de N=83 – assumindo-se, assim, a preferência de $\chi 2 > N$, ou seja, $\chi 2 > 83$ –, mais fortes são os indícios de que não se pode refutar H_1.

O próximo passo, agora, é compreender a relação de dependência entre cada par de categorias, mediante o uso da *análise dos resíduos padronizados ajustados*[209]. De forma mais específica, essa análise permite revelar "[...]os padrões característicos de cada categoria de uma variável segundo o excesso ou a falta de ocorrências de sua combinação com cada categoria da outra variável" (FÁVERO; BELFIORE, 2015, p. 182). Relembrando: as categorias da variável "edicao" são "enabed2009" até "enabed2016"; e as da "cib_importancia" são "nenhuma", "pouca" e "muita". A Figura 7 apresenta o *output* gerado *software*, mediante o comando "tabchi edicao cib_importancia , a".[210]

---

[206] De acordo com Gil (1999, p. 180), "[a] hipótese nula é construída com o objetivo de ser rejeitada". Aqui, se vislumbra na prática o que diz, circunstancialmente, na Introdução e na subseção 1.3, a saber: a ciência moderna tende a preferir não refutar hipóteses, ao invés de confirmá-las.

[207] Afirma-se isso porque o valor de "Pr" – ou seja, Prob. $\chi 2_{calc}$ – deu menor que 0.05 (5%).

[208] O $\chi 2$ é, no caso, 16. Para uma análise algébrica do teste $\chi 2$ e da análise de resíduos, ver Fávero e Belfiore (2015, p. 180-184). Para uma explicação mais geral sobre esse teste, ver Gil (1999, p. 181-182). O cálculo desses testes pode ser realizado manualmente ou por meio de *software* ou, ainda, *online*, a exemplo da página http://www.socscistatistics.com/pvalues/chidistribution.aspx.

[209] Também conhecidos como *resíduos padronizados* ou *resíduos padronizados ajustados*.

[210] Para poder rodar o comando "tabchi" no STATA®, é necessário instalar o seu *plug-in*, conforme os passos de Fávero e Belfiore (2015, p. 247).

```
. tabchi edicao cib_importancia , a

          observed frequency
          expected frequency
          adjusted residual

──────────┬──────────────────────────────────
Ano da    │ Grau de importância dada
edição do │      ao ciberespaço
ENABED    │   muita  nenhuma    pouca
──────────┼──────────────────────────────────
enabed2007│      0        1        0
          │  0.193    0.699    0.108
          │ -0.492    0.661   -0.351
          │
enabed2008│      0        2        0
          │  0.386    1.398    0.217
          │ -0.700    0.940   -0.499
          │
enabed2009│      0        5        0
          │  0.964    3.494    0.542
          │ -1.127    1.514   -0.804
          │
enabed2010│      0       10        0
          │  1.928    6.988    1.084
          │ -1.648    2.214   -1.176
          │
enabed2011│      3       12        0
          │  2.892   10.482    1.627
          │  0.078    0.944   -1.492
          │
enabed2012│      3       12        3
          │  3.470   12.578    1.952
          │ -0.317   -0.336    0.898
          │
enabed2013│      3        5        1
          │  1.735    6.289    0.976
          │  1.132   -0.992    0.027
          │
enabed2014│      1       11        4
          │  3.084   11.181    1.735
          │ -1.470   -0.110    2.027
          │
enabed2016│      6        0        1
          │  1.349    4.892    0.759
          │  4.657   -4.211    0.306
──────────┴──────────────────────────────────

22 cells with expected frequency < 5
9 cells with expected frequency < 1

          Pearson chi2(16) =  36.8141   Pr = 0.002
 likelihood-ratio chi2(16) =  40.5145   Pr = 0.001
```

Figura 7 Análise dos resíduos padronizados ajustados das variáveis do banco de dados
Fonte: Elaboração própria (a partir do STATA®).

Ao examinar a Figura 7, deve-se procurar, para cada par de categorias, o valor positivo maior que e mais próximo de 1,96. Assim, pode-se visualizar, de pronto, relações de dependência entre alguns pares de categoria, tais quais enabed2009-nenhuma e enabed2014-muita, tornando mais concreta a intuição que origina a hipótese alternativa.

Uma vez confirmado que há tais relações, é possível, enfim, proceder com a Anacor propriamente dita, permitindo, assim, que se conheçam as *coordenadas (scores) das categorias*[211]. É a partir delas que se construirá o mapa perceptual para as duas variáveis. A Figura 8 apresenta o conjunto de tabelas gerado pelo *software*, após a inserção do comando "ca edicao cib_importancia".

```
. ca edicao cib_importancia

Correspondence analysis                         Number of obs     =        83
                                                Pearson chi2(16)  =     36.81
                                                Prob > chi2       =    0.0022
                                                Total inertia     =    0.4435
    9 active rows                               Number of dim.    =         2
    3 active columns                            Expl. inertia (%) =    100.00

                  |  singular    principal                            cumul
        Dimension |    value      inertia        chi2    percent    percent
    --------------+-------------------------------------------------------
            dim 1 |  .5933137    .3520211       29.22      79.37      79.37
            dim 2 |  .3025274    .0915228        7.60      20.63     100.00
    --------------+-------------------------------------------------------
            total |              .4435439       36.81        100

Statistics for row and column categories in symmetric normalization

                   |         overall        |        dimension_1      |        dimension_2
        Categories |  mass  quality  %inert |  coord   sqcorr  contrib |  coord   sqcorr  contrib
    ---------------+------------------------+-------------------------+-------------------------
    edicao         |                        |                         |
       enabed2007  | 0.012   1.000    0.012 |  0.780    0.837    0.012 |  0.481    0.163    0.009
       enabed2008  | 0.024   1.000    0.023 |  0.780    0.837    0.025 |  0.481    0.163    0.018
       enabed2009  | 0.060   1.000    0.059 |  0.780    0.837    0.062 |  0.481    0.163    0.046
       enabed2010  | 0.120   1.000    0.117 |  0.780    0.837    0.124 |  0.481    0.163    0.092
       enabed2011  | 0.181   1.000    0.050 |  0.119    0.068    0.004 |  0.616    0.932    0.227
       enabed2012  | 0.217   1.000    0.018 |  0.010    0.001    0.000 | -0.346    0.999    0.086
       enabed2013  | 0.108   1.000    0.032 | -0.468    0.985    0.040 |  0.080    0.015    0.002
       enabed2014  | 0.193   1.000    0.119 |  0.244    0.129    0.019 | -0.886    0.871    0.501
       enabed2016  | 0.084   1.000    0.570 | -2.241    0.993    0.714 |  0.255    0.007    0.018
    ---------------+------------------------+-------------------------+-------------------------
    cib_import~a   |                        |                         |
            muita  | 0.193   1.000    0.595 | -1.498    0.973    0.729 |  0.350    0.027    0.078
          nenhuma  | 0.699   1.000    0.210 |  0.463    0.952    0.252 |  0.146    0.048    0.049
            pouca  | 0.108   1.000    0.195 | -0.319    0.076    0.019 | -1.561    0.924    0.873
    ----------------------------------------------------------------------------------------------
```

Figura 8 Anacor das variáveis do banco de dados
Fonte: Elaboração própria (a partir do STATA®).

Examina-se o complexo resultado da Anacor, para as variáveis "edicao" e "cib_importancia", em três partes. Primeiramente, a parte superior direita apresenta informações gerais da análise a que se submeteram os 83 trabalhos, em que: o nível de significância é de 0,02% (0.0022); há duas dimensões modeladas; e o resultado da inércia total é de 0.4433 – este dado é imprescindível para explorar as duas dimensões e poder gerar os

[211] Para a definição algébrica dessas coordenadas, ver também Fávero e Belfiore (2015, p. 187-191).

gráficos, pois a inércia principal total é diretamente proporcional à associação entre as variáveis/categorias no mapa a ser construído.

A segunda parte da Anacor expõe duas dimensões, em termos macros. Sempre a primeira dimensão apresenta valores maximizados em relação à segunda (FÁVERO; BELFIORE, 2015, p. 204-205). Pelo que mostra a Figura 8, *infra*, a primeira dimensão tem um poder de quase 80% (79.37) e a segunda tem pouco mais de 20% (20.63) em explicar a inércia principal total.[212]

A última parte a ser analisada toca à representatividade dos pares das duas variáveis. Aqui, o que mais importa são as categorias dispostas na primeira coluna e sua associação às colunas das duas dimensões, pois elas formarão as coordenadas a serem levadas em conta na construção dos gráficos. Por exemplo, para a variável "edicao", a categoria "enabed2016" é a mais representativa no que tange à composição inercial da primeira dimensão, ou seja, tem 71,4% (0.714); já, para a variável "cib_importancia", a categoria "pouca" tem 87,3% (0.873) na segunda dimensão.

Tendo em vista as informações repassadas pela Figura 8, é possível, enfim, criar o *gráfico de projeção das coordenadas nas dimensões*, por meio do comando "caprojection", cujo *output* é mostrado no Gráfico 4.

[212] Esses dois valores são obtidos pela divisão de sua respectiva inércia principal pela total. Tome-se o exemplo da primeira dimensão: 0.3520211 ÷ 0.4435439 = 0,7937 = 79,37%.

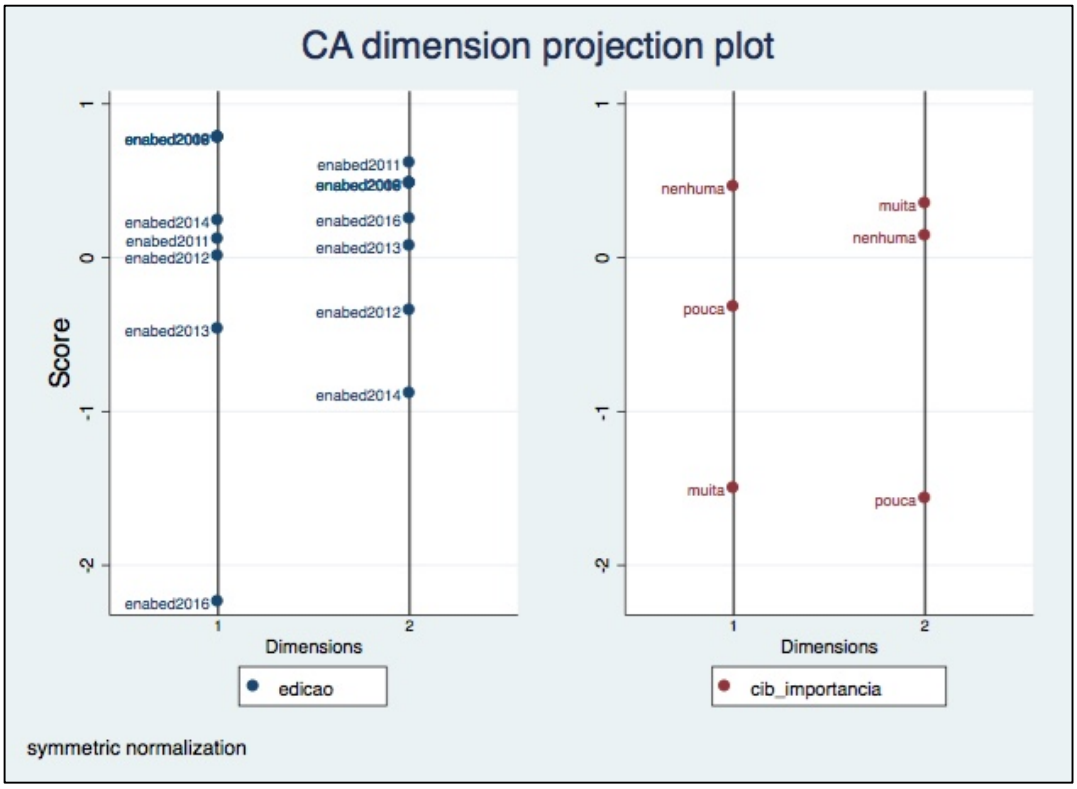

Gráfico 4 Projeção das coordenadas nas dimensões
Fonte: Elaboração própria (a partir do STATA®).

Como se vê no Gráfico 4, a Dimensão 1 é a que maximiza os valores; daí, por exemplo, as categorias das duas variáveis aparecem de forma decrescentemente ordenada nela, tanto em azul para a variável "edicao" quanto em vermelhor para "cib_importancia". Outra observação relevante é que, com exceção da categoria "enabed2016", todas as demais categorias encontram-se bem afastadas do ponto de origem, que é abaixo de -2. Certamente, essa discrepância do "enabed2016" aparecerá no *mapa perceptual*, cuja projeção, no Gráfico 5, se dá mediante o comando "cabiplot, origin".

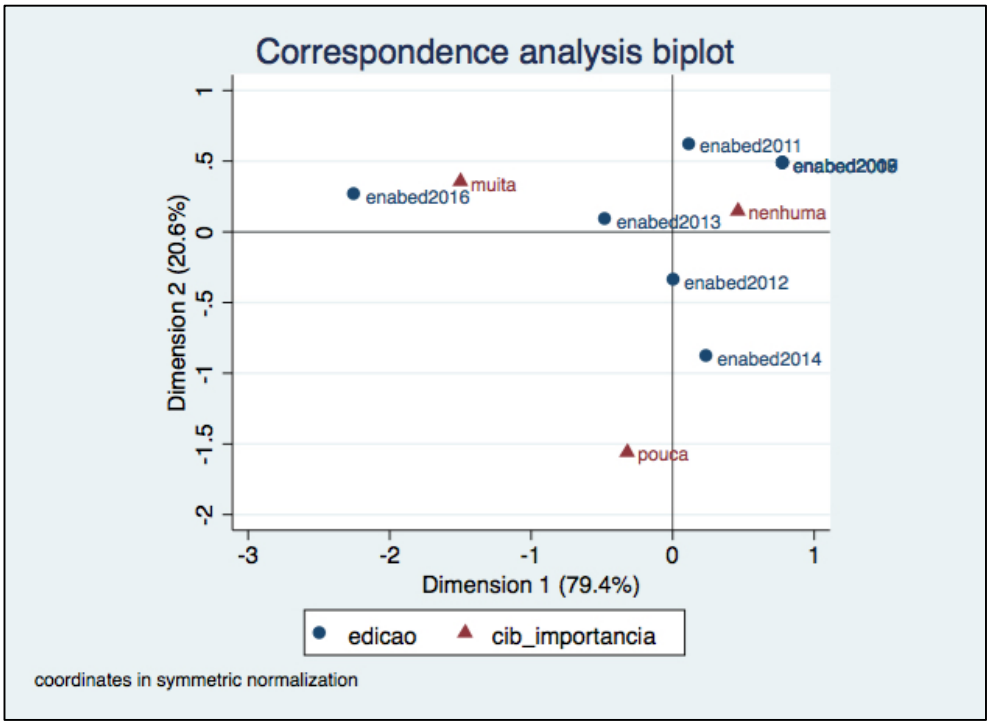

Gráfico 5 Mapa perceptual (*biplot*) da relação entre as categorias do banco de dados
Fonte: Elaboração própria (a partir do STATA®).

Como previsto, a categoria "enabed2016" se destaca no *mapa conceptual*[213] do Gráfico 5. Certamente, o que mais chama a atenção são os dois *outliers*, quais sejam: "enabed2016" e "muita", bem como a praticamente interposição dos "enabed2007" a "enabed2009" associados à categoria de "nenhuma" importância. Se as informações obtidas nas Figuras 7 e 8 e no Gráfico 4 já apontavam para uma provável não refutação de H_1, o Gráfico 5 apenas atesta o fato de que, com o passar dos anos, o grau de importância dada ao ciberespaço aumenta, por parte dos trabalhos publicados nos anais do ENABED.

Se, de um lado, o conceito de *Software Power* exacerba os elementos metateoréticos da Ontologia e da Epistemologia em CiberRI, a análise dos trabalhos publicados nos anais do ENABED faz o mesmo com a questão da Metodologia.

Um passo complementar a esta pesquisa seria examinar como esses trabalhos que tratam do ciberespaço utilizam os elementos metateoréticos acima para compreender o ciberespaço. Sobre isso, Acácio (2016) e Acácio e Vilar Lopes (2012) dão um indício: falta, principalmente, o elemento epistemológico da teoria para vincular, de uma maneira ainda mais consistente, a

[213] Esse mapa é do tipo simétrico, também conhecido como *biplot*, pois as linhas e as colunas representativas das categorias das variáveis possuem a mesma escala (FÁVERO; BELFIORE, p. 191).

relação ciberespaço-relações internacionais e as próprias RI, para se privilegiar, cada vez mais, a análise e a síntese, tanto cobrada por alguns autores de CP e de RI.[214]

Vale também relembrar que a amostra (*n*) dos trabalhos aqui analisados é apenas, como em toda amostra, um "[s]ubconjunto do universo ou da população, por meio do qual se estabelecem ou se estimam as características desse universo ou população" (GIL, 1999, p. 100), ou seja, $n \neq N$, o que implica dizer que as explicações oriundas da análise da amostra aqui submetida a teste não podem ser generalizadas para o restante dos elementos contidos em *N* e não abarcados por *n*. O Apêndice D, *infra*, fornece um caminho para se tentar prever uma tendência, mas que aqui, repete-se, não objeto de análise.

Resgata-se, da Introdução, o terceiro objetivo específico desta Tese, que é o de evidenciar como CiberRI pode potencializar o aperfeiçoamento de RI na política internacional, em geral, e no caso brasileiro, no específico. Para o primeiro caso, a presente seção ofertou o *Software Power*; para o segundo, a análise dos anais do ENABED. Aquele faz com que CiberRI desenvolva-se enquanto subcampo internacionalista, o qual não surge do nada e *sem* nada para oferecer a seu campo-pai, quer dizer, traz consigo arcabouços teórico-epistemológicos que enxergam a política internacional como ela realmente é: envolta em uma era de *bits* e *bytes* a serem triados dos ruídos. Já, para o caso brasileiro, a análise mostra que, embora haja uma tendência crescente de se dar mais importância ao tema do ciberespaço nos Estudos de Defesa e de Segurança Internacional, no Brasil, essa produção necessita ser mais representativa em seu universo. Essas análises, entende-se, não só geram aperfeiçoamentos ao campo de RI, como também lhe fornece respostas, mais macros, a perguntas que sequer lhe eram feitas.

[214] Sobre tal discussão no âmbito de CP, ver Voegelin (1982, p. 56); e de RI, *vide* Jackson (2011, p. 193) e Resende (2005, p. 16).

CONCLUSÃO

> Umas das lições dos recentes progressos conceptuais e científicos é que o comportamento de máquinas adaptativas inorgânicas de uma variedade de tipos revelou-se de um profundo interesse para os investigadores[...] sociais[...]. (RUDNER, 1969, p. 16-17).
>
> Parece-nos ingênuo, portanto, crer que um fenômeno tão abrangente [como é a Revolução da Informação] ainda não se tenha refletido nas Relações Internacionais que, *a priori*, são relações sociais. Refletiu, e muito. (VALENTE, 2007, p. 21, grifo nosso).

Consoante Gil (1999, p. 51), "[m]uitas vezes a escolha de um problema é determinada não por sua relevância, mas pela oportunidade que oferecem determinadas instituições". O problema de pesquisa desta Tese se encaixa tanto na relevância quanto da oportunidade institucional, pois ele vai além do modismo que o tema atualmente enseja em muitas áreas do conhecimento, cujos resultados de pesquisas – muitos dos quais, deva-se frisar, são financiados por dinheiro público, mediante agências de fomento – não são continuados, em sua maioria; são, portanto, pontuais. Assim, entende-se que esta Tese é, de um lado, a combinação e a cominação de quase uma década – praticamente financiada pelo Poder Público – de análises sobre a relação ciberespaço-relações internacionais e, do outro, um pontapé para estudos sistematizados sobre a relação ciberespaço-RI. Portanto, nada mais lógico do que enfatizar a defesa de CiberRI na academia, sobretudo a brasileira.

Em seu importante esforço de apontar a emergência de uma agenda de pesquisa sobre o ciberespaço em RI, Portela (2016, p. 96-97) enfatiza que seu objetivo, ali, "[...]não é compreender como o espaço cibernético se tornou um objeto da área, mas como ele é tratado nessa disciplina". Como se vê, a presente Tese se volta para ambos os objetivos de que fala o autor e vai mais além: oferta um *locus* específico para congregar parte da comunidade epistêmica de RI que estuda o ciberespaço.

Como se postulou, três qualidades fazem com que um conhecimento se torne científico: que ele seja sistemático, público e voltado à produção de conhecimento do mundo (JACKSON, 2011, p. 195), sendo a principal delas a primeira. Assim, chega-se a esta seção conclusiva na certeza de que esta Tese buscou mostrar como, dentro das ciências sociais, da CP e da RI, o subcampo internacionalista de CiberRI explica seu objeto de estudo, qual seja as relações internacionais cibernéticas, especificamente, ao: (i) propor um modelo para sistematizar o que já foi produzido nessa temática e ajudar a direcionar as próximas produções, (ii) buscar ser o mais transparente possível em suas ambições e limitações, tornando as críticas tão presentes quanto os exemplos, e (iii) produzir não apenas conhecimento sobre o mundo, como, outrossim, produzr ao mundo um novo conhecimento, o ciberinternacionalista.

Do mesmo modo que acontece com RI, CiberRI também é academicamente pluralista e interdisciplinar. Como se vê ao longo do texto, para se explicar os acontecimentos internacionais, RI assume pressupostos ontológicos, epistemológicos e metodológicos próprios ou de outras ciências sociais; quando não encontra sustentação explanatória, vale-se até mesmo de certas ciências exatas, como a Estatística. Todavia, no século XXI, percebe-se que, até mesmo com o enfoque em métodos estatísticos, o campo de RI – sobretudo o ensinado e praticado *no* Brasil – encontra lacunas em descrever ou explicar acontecimentos internacionais que se relacionam com o ciberespaço. Nesse sentido, o ensino de RI – sobretudo o praticado *fora do* Brasil – tem buscado, cada vez mais, aportes nas Ciências Exatas mais recentes, como a Ciência da Computação e a interdisciplinar Ciência da Informação, com especial destaque para os subcampos de Redes de Computadores e a área de SegInfo. Porém, apesar de o ciberespaço nascer da Linguística, é por intermédio das ciências que cuidam da interação automatizada homem-máquina que ele se materializa.

CiberRI não trata, pois, simplesmente de transfundir acriticamente conceitos computacionais e informacionais para RI; tal proposta procura, como se defende na seção introdutória, a realização de um diálogo mais próximo entre dois conjuntos de ciências distintas, prevalecendo, logicamente, os pressupostos de CP/RI sobre os das demais. Assim, CiberRI enfatiza um conceito imprescindível para o entendimento do estado de coisas das relações internacionais hodiernas, qual seja: a informação, bem como seus meios de acesso e propagação, o ciberespaço, sobretudo a Internet e a Web.

Teoricamente, como Nye Jr (2011b) aponta em seu conceito de poder cibernético, a informação se torna um dos ativos mais importantes para a Sociedade da Informação. Historicamente, o atual momento caracteriza-se por aquilo que aqui se chama de Era dos Ruídos, ou seja, uma era em que "[...]é, sobretudo, a abundância de informação que cria obstáculos, pois o custo de análise é, nestes casos, diretamente proporcional ao volume de dados" (FREITAS *et al.*, 2006, p. 122). Empiricamente, como o caso Snowden especialmente demonstra, um único indivíduo – e não mais agências estatais e governamentais – pode deter e difundir informações altamente estratégicas para a segurança do Estado e da sociedade[215]. Já quanto à atuação descentralizada e que se utiliza das benesses da Terceira Revolução Industrial – ou Revolução da Informação –, Castells (1999) a nomeia de Sociedade em Redes. A ideia de articulação estatal em rede para combater crimes transnacionais constitui-se rara ocasião em

[215] Quando se fala em "segurança do Estado e da sociedade" remete-se, na verdade, ao dispositivo constitucional mais relevante para o serviço brasileiro de Inteligência de Estado, a saber: o Art. 5º, XXXIII, da CF88.

que RI dialoga com Ciência da Computação e, sobretudo, da Informação, a fim de, juntas, descrever e analisar acontecimentos cibernéticos com impactos para as seguranças nacional e internacional. Todavia, sem uma inferência mais específica sobre o ciberespaço, à luz do "social", entende-se que a análise internacionalista fica prejudicada, assemelhando-se, dessa forma, mais a um ensaio descritivo dos acontecimentos internacionais do que a uma análise propriamente internacionalista. É por esses motivos que se justifica, aqui, a criação de CiberRI.

Em última análise, prevê-se que CiberRI saia do papel e alcance a "institucionalização da investigação" de que falam Wallerstein *et al*. (1996, p. 50, 74), por meio de novos programas e departamentos nas universidades, associações acadêmicas e revistas especializadas. Isso já ocorre nas principais IES do mundo, falta, porém, ocorrer também no Brasil. Eis aqui um paradoxo: é justamente onde tais estudos ainda não engrenaram que a presente proposta emerge. Um paradoxo acadêmico para um objeto de estudo tão paradoxo como o ciberespaço, que faz juntar duas "culturas" científicas distintas, porém não tão distantes.

Se a primeira seção anuncia os pressupostos que regem CiberRI, a segunda busca demonstrar que eles são compatíveis com o tripé que rege a educação superior, pelo menos, no Brasil. Assim, não restam dúvidas de que sua implantação no seio universitário já é realidade nas principais IES do mundo. Indo mais além, pode-se dizer que essa é uma tendência mundial, *a matter of time*, nos dizeres dos próprios proponentes não só do *ciber* quanto das *RI*.

Observa-se que poucas IES civis, no Brasil, têm denotado importância à temática ciberinternacionalista, destacando-se os militares – como a Academia Militar das Agulhas Negras (AMAN) e a Escola de Comando e Estado-Maior do Exército (ECEME) – e poucos estudantes de CP, Estudos Estratégicos e RI, espalhados por este país de proporções continentais. Já se vê Monografias de Graduação e de Especialização, Dissertações de Mestrado e, agora, Tese de Doutorado sobre temas atinentes a CiberRI.

Nesse sentido, para que CiberRI saia do papel e ganhe a prática didática, é preciso proceder a algumas alterações de cunho pedagógico-curricular. Não se defende aqui que se deva seguir, de supetão, os exemplos estrangeiros e criar instituições específicas para o trato ciberinternacionalista. Isso, se possível fosse, poria em prática o mimetismo tão criticado pelos intelectuais brasileiros e brasilianistas, ao longo dos tempos. Entretanto, é preciso partir de algum lugar. Talvez, isso se explique pelo fato de a universidade brasileira, como "[q]ualquer universidade concreta[,] sintetiza as múltiplas determinações de um desenvolvimento da comunidade nacional onde tem origem" (FRAGOSO FILHO, 1984, p. 14), ou seja, que o grau não tão alto de desenvolvimento tecnológico nacional pode ser sentido em várias instâncias da sociedade brasileira, o que inclui, *per se*, as suas universidades. Se o País não investe em C&T

– de onde provém o ciberespaço e a Internet –, fica difícil de falar também em P&D nessa seara; consequentemente, a curiosidade – mola propulsora para as revoluções culturais e tecnológicas – nessas e em outras áreas, como as ciências sociais, CP e RI, tende a diminuir. Longe de ser uma visão aquiescente de uma condição intransponível de subdesenvolvimento ou, mesmo, de defender uma lógica *standardizada* na formação docente (MACEDO, 2015, *passim*), esta é uma constatação factual que leva em conta, de um lado, os cortes, cada vez maiores, em P&D e C&T no Brasil e, do outro, o aumento do fascínio que o ciberespaço desperta nas ciências sociais e políticas alhures. Daí a importância, aqui, de enaltecer os parcos projetos de fomento que visam contornar essa situação no País.

Ora, se se absorver tal ideia deinstitucionalização do conhecimento ciberinternacionalista como a forma mais extremada de se deixar de tratar um tema só porque ele é "importante" ou "relevante", mas, sim, porque é "imprescindível" para um determinado campo científico, então tem-se a materialização da tese lançada logo no primeiro parágrafo deste trabalho. Isso fornece alguns indícios favoráveis para a validação da hipótese principal.

Comparado ao ensino e à extensão, a pesquisa universitária é a que mais se desenvolve dentre os produtores de conhecimento ciberinternacionalista, tanto no Brasil quanto no estrangeiro. Isso se deve, em grande parte, à atual ênfase dada à pesquisa, em detrimento do ensino. Como ocorre no todo universitário, as poucas pesquisas e publicações em CiberRI sofrem do que Fragoso Filho (1984, p. 25) chama de "[...]caráter fragmentário, de inciativa pessoal dos pesquisadores, confinada aos limites de uma disciplina, sem se fundamentar numa visão mais ampla". Nesse prisma, a *coordenação acadêmica*, contida no Modelo 3C, tem por meta ajudar a aprimorar esse caráter, no sentido de construir um subcampo internacionalista organizado, a ponto de se tornar alvo de bolsas, editais de agências de fomento, incentivo à institucionalização, diálogo interdepartamental, tema de dossiês de revistas e eventos acadêmicos, reportagens de jornais etc.

Longe de ser um subcampo fechado em si mesmo, CiberRI alimenta a pretensão de fazer com que os resultados de suas pesquisas sejam também apreciados pelos tomadores de decisão estratégica e política, ainda que, inicialmente, figurem apenas em considerandos que justifiquem a necessidade de se conhecer este mundo, em constante transformação informacional.

Buscou também, aqui, analisar casos impactantes da política internacional, que têm relação intrínseca com o ciberespaço, como o Edward Snowden traz, acerca da espionagem cibernética feita, de forma sistemática, por nações estrangeiras no Brasil e em outros países.

Mais do que contar a história, CiberRI vai mais além e a situa em um campo, teórico, bem maior.

A terceira e última seção formula e aplica um conceito, uma ideia-força ciberinternacionalista, para ser pensado de forma mais estratégica e politicamente ampla que o altamente aceito *Cyber Power*. Trata-se do *Software Power*, que surge como uma alternativa explanatória para a análise internacionalista sobre a projeção e a obtenção de poder no século XXI. Em suma, esse novo arcabouço conceptual visa a explicar como potências criam programas e sistemas de computadores (*software*) voltados especificamente para projetar e/ou obter poder estatal, interferindo, dessa forma, na ordem internacional.

Ademais, atesta-se a afirmação de Portela (2016, p. 106) de que "[o] impacto da produção científica sobre [o] espaço cibernético nas Relações Internacionais começa a ser notado com maior veemência no início do século XXI". Nesse sentido, a última subseção da terceira seção buscou mensurar até que ponto estudiosos brasileiros de Defesa e de Segurança Internacional dão importância ao ciberespaço e seus desafios na segurança internacional. Para tanto, desenhou-se uma pesquisa pautada na estratégia metodológica do *Nested Analysis*, que defende o uso amalgâmico de métodos quantitativos e qualitativos, como mais uma prova de que CiberRI vem para agregar e congregar na Academia, e não para separar por meio de sua aparente especialização. Essa tarefa foi realizada mediante tanto LNA quanto SNA nos trabalhos publicados nos anais do ENABED. De todos os 1.007 textos publicados, 83 citam algum aspecto cibernético. Por fim, descobriu-se que, pelo menos em termos estatísticos, observa-se uma tendência, limitada à amostra, é verdade, que corresponde a 8% da população analisada, de poucos trabalhos trazerem muita importância ao tema em apreço, nos últimos anos.

De maneira geral, buscou-se demonstrar que a Era dos Ruídos não é uma espécie de *fim da história* para o Estado, haja vista que "[o] mundo mudou e está mudando cada vez mais rápido. E o Estado está mudando com ele, contrariando aqueles que pregam seu envelhecimento e a atual inadequação diante de um mundo tão dinâmico" (VALENTE, 2007, p. 17).

De forma efusiva, a presente Tese enfatiza o papel metodológico das novas tecnologias em amparar a defesa de CiberRI, sobretudo como se vê na busca por dados no Campo Epistêmico e na salvaguarda da pesquisa dos anais do ENABED. Todavia, elas "[...]não devem ser vistas como um significado para substituição de capacidades metodológicas, mas[,] sim[,] como ferramentas para *assistir* a esse processo", ou seja, enquanto elemento metateorético em RI, a ênfase na metodologia só é incentivada em CiberRI quando ela estiver largamente amparada em uma teoria de pesquisa igualmente internacionalista. Isso nada mais é do que se

evidenciar a inexorabilidade relação entre os três elementos metateoréticos, postos a serviço da pesquisa ciberinternacionalista.

Conforme apregoa Megale (1990, p. 42, grifo do autor), "[...]para se chegar ao *status* de ciência, o conhecimento deve passar por etapas entre as quais a verificação ou confirmação dos resultados". Nesse sentido, entende-se que não só a hipótese principal desta Tese foi testada, como também o foram suas partes decompostas – conjecturas ou hipóteses secundárias –, em cada uma das três seções principais, a ponto de ela não ser refutada[216]. Logo, chega-se à conclusão de que o objetivo geral desta Tese – defender, academicamente, a criação de um subcampo em RI que se volte, de forma precípua, aos estudos sistematizados da relação ciberespaço-relações internacionais-RI – foi alcançado, haja vista que tanto sua teoria quanto sua empiria foram esboçados e postos à prova para a realidade social, política e internacional deste início de século, marcada pelo uso cada vez maior do ciberespaço, especialmente da Internet, seja para a paz, seja para a guerra, temas indissociáveis para o contínuo aperfeiçoamento de CP/RI.

Como definido inicialmente, este trabalho, seminal em sua essência[217], busca ser um estopim para futuras pesquisas sobre a relação de poder, no âmbito das relações internacionais, que emana do – e para – o ciberespaço, pois, como postula Voegelin (1982, p. 29), "[a] ciência não é conquista individual desde ou daquele estudioso: é um esforço de cooperação. O trabalho efetivo só é possível se inserido numa tradição de cultura intelectual". Eis, aqui, portanto, a nossa contribuição.

---

[216] Note-se que o fato de a hipótese se mostrar válida quer dizer que ela passou satisfatoriamente por todos os testes a que foi submetida, porém não se pode afirmar, com 100% de certeza, que ela foi definitivamente confirmada. Isso faz parte não só do método hipotético-dedutivo, mas também do caráter progressista e crítico da ciência. Daí que CiberRI, assim como os demais subcampos científicos, tem de se desenvolver, e que RI, *idem* aos campos científicos, se aperfeiçoar.

[217] Amorim Neto e Santos (2015, p. 29, grifo nosso) definem estudos seminais como o conjunto de "[...]*artículos o libros que abren un campo de investigación o marcan el comienzo de un período de creciente incidencia en un tema particular. Estos dan origen a otros estudios que, frecuentemente, les deben sus hipótesis e ideas'".*

REFERÊNCIAS

ABERYSTWYTH UNIVERSITY. New Masters in International Politics of the Internet. [201-]. Disponível em: <https://www.aber.ac.uk/en/interpol/research/research-centres-and-institutes/ccrc/news/> Acesso em: 14 set. 2016.

ACÁCIO, Igor D. P. Segurança internacional no século XXI: o que as teorias internacionalistas têm a dizer sobre o ciberespaço?. In: GUEDES DE OLIVEIRA, Marcos A.; GAMA NETO, Ricardo B.; VILAR LOPES, Gills (Org.). **Relações Internacionais Cibernéticas (CiberRI)**: oportunidades e desafios para os Estudos Estratégicos e de Segurança Internacional. Recife: Ed. UFPE, 2016. p. 35-58. (Defesa & Fronteiras Virtuais, 3).

_____; 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**. Caxambu: ANPOCS, 2012. Disponível em: <http://www.anpocs.org/portal/index.php?option=com_docman&task=doc_details&gid=8169&Itemid=76>. Acesso em: 6 dez. 2015.

AGENCE FRANCE-PRESSE – AFP. EUA promete resposta 'proporcional' à ciberataque russo. **IstoÉ**, 11 out. 2016. Mundo. [*online*]. Disponível em: <http://istoe.com.br/eua-promete-resposta-proporcional-a-ciberataque-russo/>. Acesso em: 12 out. 2016.

AGÊNCIA ESPACIAL BRASILEIRA – AEB. **Programa Nacional de Atividades Espaciais**: 2012-2021. Brasília: Ministério da Ciência, Tecnologia e Inovação, 2012. Disponível em: <http://www.aeb.gov.br/wp-content/uploads/2013/01/PNAE-Portugues.pdf>. Acesso em: 16 nov. 2016.

AGUILAR, Luis J. Introducción: estado del arte de la Ciberseguridad. In: INSTITUTO ESPAÑOL DE ESTUDIOS ESTRATÉGICOS. **Ciberseguridad**: retos y amenazas a la seguridad nacional en el ciberespacio. Madrid: Ministerio de Defensa, 2010. p. 12-46. (Cuadernos de estrategia, 149).

ALBUQUERQUE, J. A. Guilhon. Montesquieu: sociedade e poder. In: WEFFORT, Francisco C. (Org.). **Os clássicos da política**. 15. ed. 1. imp. São Paulo: Ática, 2008. v. 1. cap. 5.

ALEIXO, Gabriel. Bitcoin: o que uma moeda digital tem nos ensinado. **Instituto de Tecnologia e Sociedade do Rio**, Rio de Janeiro, 11 jun. 2014. Disponível em: <https://feed.itsrio.org/bitcoin-o-que-uma-moeda-digital-tem-nos-ensinado-76bf0b518f6d>. Acesso em: 12 out. 2016.

ALMEIDA, Paulo Roberto de. **O Brasil e o processo de formação de blocos econômicos**: conceito e história, com aplicação aos casos do Mercosul e da Alca. 2005. Disponível em: <http://www.pralmeida.org/05DocsPRA/1091BrBlocosEconomicos.pdf>. Acesso em: 23 out. 2016.

AMORIM NETO, Octavio; SANTOS, Fabiano. La ciencia política en Brasil en la última década: la nacionalización y la lenta superación del parroquialismo. **Revista de Ciência Política**, Santiago, v. 35, n. 1, p. 19-31, 2015.

ARAÚJO JÚNIOR, Antonio H. de. O método experimental. In: HEGENBERG, L.; ARAÚJO JÚNIOR, A. H. de; HEGENBERG, F. E. N. (Org.). **Métodos de pesquisa**: de Sócrates a Marx e Popper. São Paulo: Atlas, 2012. cap. 20, p. 161-171.

ARGENTINA. Ministerio de Defensa. **Decreto 2645/2014**. Directiva de Política de Defensa Nacional. Buenos Aires: InfoLEG, 2014. Disponível em: <http://www.infoleg.gov.ar/infolegInternet/anexos/240000-244999/240966/norma.htm>. Acesso em: 7 jun. 2016.

_____. Ministerio de Defensa. **Libro Blanco de Defensa**. Buenos Aires: Ministerio de Defensa, 2015. Disponível em: <http://www.libroblanco.mindef.gov.ar/files/livro-branco-de-defesa-2015-web.pdf>. Acesso em: 7 mar. 2016.

ARQUILLA, John; RONFELDT, David. (Ed.). **Athena's Camp**: preparing for conflict in the information age. Santa Monica, CA: RAND Corporation, 1997. cap. 2, p. 23-60.

_____. Cyberwar is coming!, **Comparative Strategy**, v. 12, n. 2, p. 141-165, 1993.

ART, Robert; JERVIS, Robert. Kenneth Waltz and his legacy. **Foreign Affairs**, 22 maio 2013. Disponível em: <https://www.foreignaffairs.com/articles/united-states/2013-05-22/kenneth-waltz-and-his-legacy>. Acesso em: 6 jun. 2016.

ASSANGE, Julian; APPELBAUM, Jacob; MÜLLER-MAGUHN, Andy; ZIMMERMANN, Jérémie. **Cypherpunks**: liberdade e o futuro da Internet. Tradução de: Cristina Yamagami. São Paulo: Boitempo, 2013.

AVILA, Carlos Federico Domínguez. Resenha: DUROSELLE, Jean-Baptiste. Todo império perecerá. **Revista Brasileira de Política Internacional**, Brasília, v. 43, n. 2, p. 220-222, jul.-dez. 2000. Disponível em: <http://www.scielo.br/pdf/rbpi/v43n2/v43n2a18.pdf>. Acesso em: 5 jun. 2016.

BAEZA-YATES, Ricardo; RIBEIRO-NETO, Berthier. **Recuperação de informação**: conceitos e tecnologia das máquinas de busca. 2. ed. Porto Alegre: Bookman, 2013.

BAKER, Wade H. B *et al.* **2009 data breach investigations report**. [S.l.]: Verizon Business RISK Team, 2010. Disponível em: <http://www.verizonenterprise.com/resources/security/reports/2009_databreach_rp.pdf>. Acesso em: 23 nov. 2016.

_____. **2010 data breach investigations report**. [S.l.]: Verizon Business RISK Team; U.S. Secret Service, 2011. Disponível em: <http://www.verizonenterprise.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf>. Acesso em: 23 nov. 2016.

_____. **2012 data breach investigations report**. [S.l.]: Verizon Business RISK Team; U.S. Secret Service; Dutch High Tech Crime Unit, 2012. Disponível em: <http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf>. Acesso em: 23 nov. 2016.

BARRINHA, André; CARRAPIÇO, Helena. Cibersegurança. In: DUQUE, Raquel; NOIVO, Diogo; SILVA, Teresa de A. (Coord.). **Segurança contemporânea**. Lisboa: Pactor, 2016. cap. 16, p. 245-262.

BARROS, Lídia A. **Curso básico de Terminologia**. São Paulo: EdUSP, 2004.

BEJARANO, Maria José C. Alcance y ámbito de la seguridad nacional en el ciberespacio. In: INSTITUTO ESPAÑOL DE ESTUDIOS ESTRATÉGICOS. **Ciberseguridad**: retos y amenazas a la seguridad nacional en el ciberespacio. Madrid: Ministerio de Defensa, 2010. cap. 1, p. 48-82. (Cuadernos de estrategia, 149).

BEJTLICH, Richard. Don't underestimate cyber spies: how virtual espionage can lead to actual destruction. **Foreign Affairs**, 2 maio 2013. Disponível em: <http://www.foreignaffairs.com/articles/139357/richard-bejtlich/dont-underestimate-cyber-spies?cid=nlc-this_week_on_foreignaffairs_co-050913-dont_underestimate_cyber_spies_4-050913>. Acesso em: 19 mar. 2016.

BELLAMY, Christopher. What is information warfare?. In: MATTHEWS, Ron; TREDDENICK, John. **Managing the Revolution in Military Affairs**. Nova York: Palgrave, 2001. p. 56-75.

BENEDIKT, Michael. Introduction to 'Cyberspace: first steps'. In: _____ (Ed.). **Cyberspace**: first steps. Cambridge, MA: MIT Press, 1991. p. 1-25.

BERG, Bruce L. **Qualitative research methods for the social sciences**. 4. ed. Boston: Allyn & Bacon, 2001.

BERLIN, Isaiah. Two concepts of liberty. **Four essays on liberty**. Oxford: Oxford University Press, 1969.

BESSA, Jorge. **O escândalo da espionagem no Brasil**: o caso Snowden. Brasília: Thesaurus, 2014.

BETZ, David J.; STEVENS, Tim. Introduction. **Adelphi Series**, v. 51, n. 424, p. 9-34, 2011a. Dossiê especial "Cyberspace and the State: toward a strategy for cyber-power". Disponível em: <http://www.tandfonline.com/toc/tadl20/51/424?nav=tocList>. Acesso em: 14 maio 2016.

_____. Power and cyberspace. **Adelphi Series**, v. 51, n. 424, p. 35-54, 2011b. Dossiê especial "Cyberspace and the State: toward a strategy for cyber-power". Disponível em: <http://www.tandfonline.com/toc/tadl20/51/424?nav=tocList>. Acesso em: 14 mar. 2016.

BIERSTEKER, T. J. State, sovereignty and territory. In: CARLSNAES, W.; RISSE, T.; SIMMONS, B. A. (Ed.). **Handbook of International Relations**. Londres: SAGE, 2002. p. 157-176.

BOBBIO, Norberto. **Estado, governo, sociedade**; por uma teoria geral da política. Tradução de: Marco Aurélio Nogueira. 14. ed. Rio de Janeiro: Paz e Terra, 1987. (Pensamento Crítico, 69).

BODIN, Jean. **Os seis livros da República**: livro primeiro. Tradução de: José C. O. Morel. São Paulo: Ícone, 2011. (Fundamentos do Direito).

BODNER, M. Russian military launches cybertraining program for youth. **The Moscow Times**, 1 set. 2015. Disponível em: <http://www.themoscowtimes.com/news/article/russian-military-launches-cyber-training-program-for-youth/529210.html>. Acesso em: 24 nov. 2016.

BOURDIEU, Pierre. Esboço de uma teoria da prática. In: ORTIZ, Renato (Org.). **Pierre Bourdieu**. Tradução de: Paula Montero e Alícia Auzmendi. São Paulo: Ática, 1983a. cap. 2, p. 46-81. (Grandes cientistas sociais, 39).

_____. O campo científico. In: ORTIZ, Renato (Org.). **Pierre Bourdieu**. Tradução de: Paula Montero e Alícia Auzmendi. São Paulo: Ática, 1983b. cap. 4, p. 122-155. (Grandes cientistas sociais, 39).

_____. Trabalhos e projetos. In: ORTIZ, Renato (Org.). **Pierre Bourdieu**. Tradução de: Paula Montero e Alícia Auzmendi. São Paulo: Ática, 1983c. cap. 1, p. 38-45. (Grandes cientistas sociais, 39).

BRADY, Henry E.; COLLIER, David (Ed.). **Rethinking social inquiry**: diverse tools, shared standards. New York: Rowman & Littlefield Publishers, 2004.

BRADY, Henry; COLLIER, David; SEAWRIGHT, Jason. Refocusing the discussion of Methodology. In: BRADY, Henry; COLLIER, David (Ed.). **Rethinking social inquiry**: diverse tools, shared standards. New York: Rowman & Littlefield Publishers, 2004. cap. 1, p. 3-20.

BRASIL. Congresso Nacional. Resolução nº 2, de 2013-CN. Dispõe sobre a Comissão Mista de Controle das Atividades de Inteligência (CCAI). **Diário Oficial [da] República Federativa do Brasil**. Brasília, 2013. Disponível em: <http://www2.camara.leg.br/legin/fed/rescon/2013/resolucao-2-22-novembro-2013-777449-publicacaooriginal-141944-pl.html>. Acesso em: 2 nov. 2016.

_____. Constituição (1988). In: FERNANDES, Marcos A. O. (Org.). **Constituição da República Federativa do Brasil**. 22. ed. São Paulo: Rideel, 2016.

_____. Gabinete de Segurança Institucional. **Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015-2018**: versão 1.0. Brasília: Presidência da República, 2015. Disponível em: <http://dsic.planalto.gov.br/documentos/publicacoes/4_Estrategia_de_SIC.pdf>. Acesso em: 4 set. 2016.

_____. Ministério da Defesa. **Doutrina Militar de Defesa Cibernética**. Brasília: Estado-Maior Conjunto das Forças Armadas, 2014a. Disponível em: <http://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_2014.pdf>. Acesso em: 12 set. 2016.

_____. Ministério da Defesa. **Política Nacional de Defesa (PND) e Estratégia Nacional de Defesa (END)**. Brasília: Ministério da Defesa, 2012a. Disponível em:

<http://www.defesa.gov.br/arquivos/estado_e_defesa/END-PND_Optimized.pdf>. Acesso em: 2 nov. 2016.

_____. Ministério da Educação. **Comunicado nº 003/2012 – Área – Ciência Política e Relações Internacionais**. Considerações sobre multidisciplinaridade e interdisciplinaridade na Área. Brasília: CAPES, 2012b. Disponível em: <http://www.capes.gov.br/images/stories/download/avaliacao/Interdisciplinaridade_Ciencia_Politica.pdf>. Acesso em: 16 jun. 2016.

_____. Ministério da Educação. **Edital Pró-Estratégia 050/2011 - projetos aprovados**. Brasília: CAPES, 2011. Disponível em: <http://www.capes.gov.br/images/stories/download/editais/resultados/Resultado_Edital-050_2011_ProEstrategia.pdf>. Acesso em: 14 nov. 2016.

_____. Ministério da Educação. **Parecer CNE/CES nº 968/98**. Brasília: Conselho Nacional de Educação, 17 dez. 1998. Disponível em: <http://portal.mec.gov.br/cne/arquivos/pdf/1998/pces968_98.pdf>. Acesso em: 12 nov. 2016.

_____. Ministério da Educação. Câmara de Educação Superior do Conselho Nacional de Educação. Resolução CNE/CES 17, de 13 de março de 2002. Estabelece as Diretrizes Curriculares para os cursos de Ciências Sociais - Antropologia, Ciência Política e Sociologia. **Diário Oficial [da] República Federativa do Brasil**, Poder Executivo, Brasília, DF, 9 abr. 2002. Seção 1, n. 67, p. 34. Disponível em: <http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=34&data=09/04/2002>. Acesso em: 12 out. 2016.

_____. Ministério da Educação. Secretaria de Educação Profissional e Tecnológica. Portaria nº 129, de 5 de maio de 2009. Normatiza a atribuição de denominações às diversas estruturas educacionais que integram a Rede Federal de Educação Profissional, Científica e Tecnológica. **Diário Oficial [da] República Federativa do Brasil**, Poder Executivo, Brasília, DF, 6 maio 2009. Seção 1, n. 84, p. 13.

_____. Ministério da Educação. **Tabela de Áreas de Conhecimento**. Brasília: CAPES, 2012c. Disponível em: <http://www.capes.gov.br/images/stories/download/avaliacao/TabelaAreasConhecimento_072012.pdf>. Acesso em: 12 nov. 2016.

_____. Ministério da Educação. **Tabela de Áreas de Conhecimento/Avaliação**. Brasília: CAPES, 2014b. Disponível em: <http://www.capes.gov.br/avaliacao/instrumentos-de-apoio/tabela-de-areas-do-conhecimento-avaliacao>. Acesso em: 12 nov. 2016.

_____. Presidência da República. Decreto nº 8.793, de 29 de junho de 2016. Fixa a Política Nacional de Inteligência. **Diário Oficial [da] República Federativa do Brasil**, Poder Executivo, Brasília, DF, 30 jun. 2016. Seção 1, p. 5-7. Disponível em: <http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=30/06/2016&jornal=1&pagina=5&totalArquivos=112>. Acesso em: 4 ago. 2016.

_____. Universidade Federal do Vale do São Francisco. Anexo da Res. nº 08/2004, de 16.11.2004. Disponível em:

<http://www.univasf.edu.br/acessoainformacao/arquivos/normas_gerais.pdf>. Acesso em: 26 nov. 2016.

BRASIL está entre os menos preparados para ataques de hackers, diz estudo. **BBC Brasil**, Brasília, 31 jan. 2012. [*online*]. Disponível em: <http://www.bbc.com/portuguese/noticias/2012/01/120131_ciberdefesa_pai.shtml>. Acesso em: 27 nov. 2016.

BREMMER, Ian; GORDON, David. The geopolitics of cybersecurity. **Foreign Policy**, 12 jan. 2011. Disponível em: <http://foreignpolicy.com/2011/01/12/the-geopolitics-of-cybersecurity>. Acesso em: 12 maio 2016.

BRITO, Ana. Empresário australiano assume "paternidade" da bitcoin. **Público**, Lisboa, 2 maio 2016. Disponível em: <http://publico.uol.com.br/tecnologia/noticia/empresario-australiano-assume-paternidade-da-bitcoin-1730709>. Acesso em: 2 maio 2016.

BROAD, William J.; MARKOFF, John; SANGER, David E. Israeli test on worm called crucial in Iran nuclear delay. **The New York Times**, 15 January jan. 2011. World. Disponível em: <http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all>. Acesso em: 3 set. 2016.

BRONK, Chris. **Cyber threat**: the rise of Information Geopolitics in U.S. national security. Santa Barbara, CA: Praeger, 2016. Kindle edition. Sem paginação.

BRUYNE, Paul de; HERMAN, Jacques; SCHOUTHEETE, Marc de. **Dinâmica da pesquisa em ciências sociais**: os polos da prática metodológica. 5. ed. Tradução de: Ruth Joffily. Rio de Janeiro: Francisco Alves Editora, 1991.

BULL, Hedley. **A sociedade anárquica**: um estudo da ordem na política mundial. Tradução de: Sergio Bath. Brasília: Editora UnB; IPRI; São Paulo: Imprensa Oficial de São Paulo, 2002. (Clássicos IPRI, 5).

BUZAN, Barry; HANSEN, Lene. **A evolução dos Estudos de Segurança Internacional**. Tradução: Flávio Lira. São Paulo: Ed. Unesp, 2012.

_____. **The evolution of International Security Studies**. Cambridge: Cambridge University Press, 2009.

BUZAN, Barry; WÆVER, Ole. **Regions and powers**: the structure of international security. Cambridge: Cambridge University Press, 2003.

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

CALANDRELI, Stanilaw. A batalha russa no ciberespaço. **Jornal GGN**, 12 abr, 2011. Disponível em: <http://jornalggn.com.br/blog/luisnassif/a-batalha-russa-no-ciberespaco>. Acesso em: 26 nov. 2016.

CANONGIA, Claudia; MANDARINO JUNIOR, Raphael. Segurança cibernética: o desafio da nova Sociedade da Informação. **Parcerias estratégicas**, v. 14, n. 29, p. 21-45, dez. 2009.

CARR, Edward H. **Vinte anos de crise (1919-1939)**: uma introdução ao estudo das relações internacionais. 2. ed. Tradução de: Luiz Alberto F. Machado. Brasília: Ed. UnB/IPRI, 2001. (Clássicos IPRI, 1).

CARR, Jeffrey. **Inside cyber warfare**: mapping the cyber underworld. Cambridge: O'Reilly, 2009.

CARVALHO, Paulo Sérgio M. de. A defesa cibernética e as infraestruturas críticas nacionais. In: CICLO DE ESTUDOS ESTRATÉGICOS. **Anais**. ECEME, Rio de Janeiro, 2011. Disponível em: <http://www.eceme.ensino.eb.br/ciclodeestudosestrategicos/index.php/CEE/XCEE/paper/viewFile/5/7>. Acesso em: 26 nov. 2016.

_____. Conferência de abertura: o Setor Cibernético nas forças armadas brasileiras. In: BARROS, Otávio S. Rêgo; GOMES, Ulisses de M.; FREITAS, Whitney Lacerda de (Org.). **Desafios estratégicos para a Segurança e a Defesa Cibernética**. Brasília: Secretaria de Assuntos Estratégicos da Presidência da República – SAE, 2011. p. 13-34.

CASTELLS, Manuel. **A sociedade em rede**. 2. ed. São Paulo: Paz e Terra, 1999. (A era da informação: economia, sociedade e cultura, 1).

_____. **Fim do milênio**. 4. ed. Tradução de: Klauss Brandini Gerhardt e Roneide Venâncio. São Paulo: Paz e Terra, 2007. (A era da informação: economia, sociedade e cultura, 3).

CASTRO, Nuno Emanuel Teixeira. ***The walking virtually dead***: entre uma *algoritmocracia jus constituendum* e um homem virtual transparente, existe espaço para o direito a uma identidade informacional?. 2016. 136 f. Dissertação (Mestrado em Segurança da Informação e Direito do Ciberespaço) – Universidade de Lisboa; Instituto Superior Técnico, Lisboa, 2016.

CAVELTY, Myriam Dunn. **Cyber-security and threat politics**: US efforts to secure the information age. Londres; Nova York: Routledge, 2008.

_____. The normalization of cyber-international relations. In: THRÄNERT, Oliver; ZAPFE, Martin (Ed.). **Strategic Trends 2015**: key developments in global affairs. Zurique: Center for Security Studies, 2015. cap. 5, p. 81-98.

_____. Cyberwar: concept, status quo and limitations. **CSS Analysis in Security Policy**, n. 71, p. 1-3, 2010.

_____; BRUNNER, E. M. Introduction: information, power and security. In: CAVELTY, M. D.; KRISHNA-HENSEL, V. M. S. F. (Ed.). **Power and security in the information age**. Hampshire: Ashgate, 2007.

CERVO, Amado L.; BERVIAN, Pedro A.; DA SILVA, Roberto. **Metodologia científica**. 6. ed. 5. reimp. São Paulo: Pearson Prentice Hall, 2010.

CESARINI, Paola; HITE, Katherine. Introducing the concept of authoritarian legacies. In: _____ (Ed.). **Auhtoritarian legacies and democracy in Latin America and Southern Cone**. Notre Dame, IN: UNDPress, 2004. p. 1-24.

CHACRA, Gustavo. Obama alerta para "momento Sputinik". **Estadão**, 26 jan. 2011. Disponível em: <http://internacional.estadao.com.br/noticias/geral,obama-alerta-para-momento-sputnik-imp-,671223>. Acesso em: 10 nov. 2016.

CHAIA, Vera; CHAIA, Miguel. **Mídia e Política**. São Paulo: Editora Educ; Neamp, 2000.

CHERNOFF, Fred. Methodological pluralism and the limits of naturalism in the study of Politics. In: LEBOW, Richard Ned; LICHBACH, Mark Irving (Ed.). **Theory and evidence in Comparative Politics and International Relations**. Nova York, NY: Palgrave Macmillan, 2007. cap. 5, p. 107-141. (New visions in security).

CHOUCRI, Nazli. **Cyberpolitics in international relations**. Cambridge, MA: MIT Press, 2012.

CIJIC – CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO. I Conferência Internacional de Lisboa sobre Segurança da Informação e Direito Constitucional e Direito no Ciberespaço. Faculdade de Direito da Universidade de Lisboa, Lisboa, 3 nov. 2016. Disponível em: <http://www.cijic.org/2016/11/03/i-conferencia-internacional-de-lisboa-sobre-seguranca-da-informacao-e-direito-constitucional-do-ciberespaco>. Acesso em: 16 nov. 2016.

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.

_____. **Guerra cibernética**: a próxima ameaça à segurança e o que fazer a respeito. Tradução de: Bruno S. Guimarães *et al*. Rio de Janeiro: Brasport, 2015.

CLAUSEWITZ, Carl von. **Da guerra**. São Paulo: Tahyu, 2005.

CNBC – CONSUMER NEWS AND BUSINESS CHANNEL. The Hacking Economy. [*online*]. 2016. Disponível em: <http://www.cnbc.com/the-hacking-economy>. Acesso em: 16 nov. 2016.

COHN, Gabriel. Apresentação: o sentido da ciência. In: WEBER, M. **A 'objetividade' do conhecimento nas Ciências Sociais**. Tradução de: Gabriel Cohn. São Paulo: Ática, 2006a. p. 7-12. (Ensaios comentados).

_____. Comentários. In: WEBER, M. *A 'objetividade' do conhecimento nas Ciências Sociais*. Tradução de: Gabriel Cohn. São Paulo: Ática, 2006b. p. 13-107. (Ensaios comentados).

_____. Max Weber: pensador da sociedade. In: WEBER, M. **A 'objetividade' do conhecimento nas Ciências Sociais**. Tradução de: Gabriel Cohn. São Paulo: Ática, 2006c. p. 108-112. (Ensaios comentados).

COVARRUBIAS, Jaime G. La modernización militar. **FASOC**, ano 14, n. 1, p. 3-9, jan.-mar. 1999.

COSTA, Camilla. Exército brasileiro prepara sistema de prevenção contra ataques cibernéticos. **BBC Brasil**, São Paulo, 10 fev. 2012. [*online*]. Disponível em: <http://www.bbc.com/portuguese/noticias/2012/02/120208_guerra_cibernetica_cc.shtml>. Acesso em: 24 nov. 2016.

COSTA, Carlos E. B. da. Tendências mundiais e seus reflexos para a Defesa brasileira. **A Defesa Nacional**, ano C, n. 821, p. 4-16, 1. sem. 2013. Disponível em: <http://pt.calameo.com/read/001238206946338f5b22f>. Acesso em: 14 mar. 2016.

COUTINHO, Clara P. **Metodologia de investigação em ciências sociais e humanas**: teoria e prática. Coimbra: Almedina, 2011.

CRESPO, Antônio Arnot. **Estatística fácil**. 19. ed. São Paulo: Saraiva, 2009.

CZOSSECK, Christian. State actors and their proxies in cyberspace. In: ZIOLKOWSKI, Katharina (Ed.). **Peacetime regime for state activities in cyberspace**: International Law, International Relations and Diplomacy. Tallinn: NATO CCD COE Publication, 2013. p. 1-29.

DALLARI, Dalmo de A. **Elementos de teoria geral do Estado**. 2. ed. São Paulo: Saraiva, 1998.

DEIBERT, Ron. **Distributed security as cyber strategy**: outlining a comprehensive approach for Canada in cyberspace. Calgary: Canadian Defence & Foreign Affairs Institute, 2012.

DEMCHAK, Chris C. Economic and political coercion and a rising Cyber Westphalia. In: ZIOLKOWSKI, Katharina (Ed.). **Peacetime regime for state activities in cyberspace**: International Law, International Relations and Diplomacy. Tallinn: NATO CCD COE Publication, 2013. p. 595-620.

_____. Foreword. In: KREMER, Jan-Frederik; MÜLLER, Benedikt (Ed.). **Cyberspace and international relations**. Heidelberg: Springer, 2014. p. v-x.

DEPARTAMENTO DE CIÊNCIAS SOCIAIS DA UNIVERSIDADE FEDERAL DE RONDÔNIA. **Apresentação do Curso de Ciências Sociais**. [*online*]. Porto Velho: UNIR, [201-]. Disponível em: <http://www.cienciassociais.unir.br/?pag=estatica&id=505&titulo=Curso>. Acesso em: 24 nov. 2016.

DILLON, Conor; BRUNSMAN, Jörg. Como funciona o lado obscuro da internet. **Deutsche Welle (DW)**, 3 set. 2015. [*online*]. Disponível em: <http://dw.com/p/1GQGh>. Acesso em: 5 set. 2015.

DUARTE, Érico. **Conduta da guerra na era digital e suas implicações para o Brasil**: uma análise de conceitos, políticas e práticas de defesa. Brasília: IPEA, 2012. (Texto para Discussão, 1760).

DUROSELLE, Jean-Baptiste. **Todo império perecerá**: teoria das relações internacionais. Tradução de: Ane Lize S. de S. Magalhães. Brasília: Editora Unb, 2000.

DUVERGER, Maurice. **Ciência Política**: teoria e método. Tradução de: Heloísa de C. Lima. Rio de Janeiro: Jorge Zahar Editores, 1962. (Biblioteca de Ciências Sociais).

_____. **Ciência Política**: teoria e método. 3. ed. Tradução de: Heloísa de C. Lima. Rio de Janeiro: Jorge Zahar Editores, 1981. (Biblioteca de Ciências Sociais).

ELMAN, Colin; ELMAN, Miriam Fendius. Lessons from Lakatos. In:_____ (Ed.). **Progress in International Relations Theory**: appraising the field. Cambridge, MA: MIT Press, 2003. p. vii-xii. (BCSIA Studies in International Security). cap. 2, p. 21-68.

ERIKSSON, Johan; GIACOMELLO, Giampiero. The information revolution, security, and International Relations: (IR)relevant Theory?. **International Political Science Review**, v. 27 n. 3, p. 221-244, 2006. Disponível em: <https://doi.org/10.1177/0192512106064462>. Acesso em: 3 dez. 2015.

ESTADOS UNIDOS DA AMÉRICA. **Defense budget priorities**. Washington, DC: Department of Defense, 2014. Disponível em: <http://www.defense.gov/news/Defense_Budget_Priorities.pdf>. Acesso em: 3 dez. 2015.

_____. **National Security Strategy**. Washington, DC: The White House, 2010.

_____. **Sustaining U.S. global leadership**: priorities for 21st century Defense. Washington, DC: Department of Defense, 2012.

ESTEVES, Luiz Alberto. **Rivalidade após entrada**: o impacto imediato do aplicativo Uber sobre as corridas de táxi porta-a-porta. Brasília: Conselho Administrativo de Defesa Econômica – CADE, 2015. Disponível em: <http://www.cade.gov.br/noticias/rivalidade-apos-entrada-o-impacto-imediato-do-aplicativo-uber-sobre-as-corridas-de-taxi.pdf>. Acesso em: 13 nov. 2016.

ETHZ – EIDGENÖSSISCHE TECHNISCHE HOCHSCHULE ZÜRICH. Technology Governance and International Security. 2016. Disponível em: <http://www.vvz.ethz.ch/Vorlesungsverzeichnis/lerneinheitPre.do?semkez=2016W&lang=en&ansicht=ALLE&lerneinheitId=110188>. Acesso em: 26 nov. 2016.

EUROPEAN CENTER FOR SECURITY STUDIES. Program on Cyber Security Studies (PCSS). [2016]. Disponível em: <http://www.marshallcenter.org/mcpublicweb/en/nav-main-wwd-res-courses-pcss-en.html>. Acesso em: 14 nov. 2016.

EXÉRCITO Brasileiro investe R$ 5 mi em jogo eletrônico de guerra. **DefesaNet**, Brasília, 5 jan. 2012. [*online*]. Disponível em: <http://www.defesanet.com.br/cyberwar/noticia/4247/Exercito-Brasileiro-investe-R$-5-mi-em-jogo-eletronico-de-guerra>. Acesso em: 23 nov. 2016.

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

FÁVERO, Luiz Paulo; BELFIORE, Patrícia. **Análise de dados**: técnicas multivariadas exploratórias com SPSS® e STATA®. Rio de Janeiro: Elsevier, 2015.

FERES JR; João. Aprendendo com os erros dos outros: o que a história da Ciência Política americana tem para nos contar. **Revista Sociologia e Política**, Curitiba, n. 15, p. 97-110, nov. 2000.

FERREIRA NETO, Walfredo B.; VILAR LOPES, Gills. Por uma teoria da fronteira cibernética. In: GUEDES DE OLIVEIRA, Marcos A.; GAMA NETO, Ricardo B.; VILAR LOPES, Gills (Org.). **Relações Internacionais Cibernéticas**: oportunidades e desafios para os Estudos Estratégicos e de Segurança Internacional. Recife: Ed. UFPE, 2016. p. 59-82. (Defesa & Fronteiras Virtuais, 3).

FIGUEIREDO, Eurico de L. Estudos Estratégicos como área de conhecimento científico. **Revista Brasileira de Estudos de Defesa**, v. 2, n. 2, p. 107-128, jul./dez. 2015.

FORÇA Aérea Brasileira discute Defesa Cibernética em Brasília. **InfoRel**, Brasília, 12 dez. 2016. Agenda. [*online*]. Disponível em: <http://www.inforel.org/noticias/noticia.php?not_id=7089&tipo=2>. Acesso em: 12 dez. 2016.

FORÇAS nucleares norte-americanas ainda usam disquetes. **Público**, Lisboa, 26 maio 2016. Tecnologia. [*online*]. Disponível em: <https://www.publico.pt/tecnologia/noticia/forcas-nucleares-norteamericanas-ainda-usam-disquetes-1733112>. Acesso em: 26 maio 2016.

FRAGOSO FILHO, Carlos. **Universidade e sociedade**. Campina Grande: Edições GRAFSET, 1984. (Tempo universitário, 1).

FREITAS, Henrique; JANISSEK-MUNIZ, Raquel; BAULAC, Yves; MOSCAROLA, Jean. **Pesquisa via Web**: reinventando o papel e a ideia de pesquisa. Canoas: Sphinx, 2006.

FUNDAÇÃO CALOUSTE GULBENKIAN. Preâmbulo. In: WALLERSTEIN, Immanuel *et al*. **Para abrir as ciências sociais**. São Paulo: Cortez, 1996. p. 9-11.

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

GAMA NETO, Ricardo B.; VILAR LOPES, Gills. Armas cibernéticas e segurança internacional. In: MEDEIROS FILHO, Oscar; FERREIRA NETO, Walfredo B.; GONZALES, Selma L. de M. (Org.). **Segurança e Defesa Cibernética: das fronteiras físicas aos muros virtuais**. Recife: Ed. UFPE, 2014. (Defesa & Fronteiras Virtuais, 1). cap. 1, p. 23-45.

GASTALDI, Sol; JUSTRIBÓ, Candela. A estratégias de Segurança e Defesa Cibernéticas na Argentina. In: GUEDES DE OLIVEIRA, Marcos A.; GAMA NETO, Ricardo B.; VILAR LOPES, Gills (Org.). **Relações Internacionais Cibernéticas (CiberRI)**: oportunidades e desafios para os Estudos Estratégicos e de Segurança Internacional. Recife: Ed. UFPE, 2016. (Defesa & Fronteiras Virtuais, 3).

GEERS, Kenneth (Ed.). **Cyber war in perspective**: Russian aggression against Ukraine. Tallinn: NATO CCD COE Publications, 2015.

GIBSON, William. **Neuromancer**. Tradução de: Fábio Fernandes. São Paulo: Aleph, 2014. Edição especial de 30 anos.

GIL, Antonio Carlos. Métodos e técnicas de pesquisa social. 5. ed. 3. tir. São Paulo: Atlas, 1999.

GONÇALVES, Joanisval B. **Atividade de Inteligência e legislação correlata**. 3. ed. Niterói: Impetus, 2013.

_____. ***Sed quis custodiet ipso custodes*? O controle da Atividade de Inteligência em regimes democráticos**: os casos de Brasil e Canadá. 2008. 797 f. Tese (Doutorado em Relações Internacionais) – Instituto de Relações Internacionais da Universidade de Brasília, Brasília, 2008.

GOODIN, R. E.; TILLY, C. **The Oxford Handbook of Contextual Political Analysis**. Oxford: OUP, 2008.

GRAY, Colin S. **Making strategic sense of cyber power**: why the sky is not falling. Carlisle, PA: U.S. Army War College Press, 2013.

GREENBERG, Andy; BRANWEN, Gwern. Bitcoin's creator Satoshi Nakamoto is probably this unknown Australian genius. **Wired**, 8 dez. 2015. Security. [*online*]. Disponível em: <https://www.wired.com/2015/12/bitcoins-creator-satoshi-nakamoto-is-probably-this-unknown-australian-genius>. Acesso em: 11 dez. 2015.

GUEDES DE OLIVEIRA, Marcos. A.; GAMA NETO, Ricardo B.; VILAR LOPES, Gills. Apresentação. In: _____ (Org.). **Relações Internacionais Cibernéticas (CiberRI)**: oportunidades e desafios para os Estudos Estratégicos e de Segurança Internacional. Recife: EDUFPE, 2016a. p. 27-31. (Defesa & fronteiras virtuais, 3).

HAAS, Peter M. Epistemic communities and international policy coordination. **International Organization**, v. 46, n. 1, p. 1-35, Winter 1992.

HALL, Peter A.; TAYLOR, Rosemary C. R. As três versões do neo-institucionalismo. **Lua Nova**, n. 58, p. 193-223, 2003.

HANSEN, Lene; NISSENBAUM, Helen. Digital disaster, cyber security and the Copenhagen School. **International Studies Quarterly**, n. 53, p. 1555-1575, 2009.

HELD, David; McGREW, Anthony. **Prós e contras da globalização**. Tradução de: Vera Ribeiro. Rio de Janeiro: Jorge Zahar Editor, 2001.

HERMANY, Ricardo; BOLESINA, Iuri. Poder local e a Lei de Acesso à Informação nos Executivos municipais do Rio Grande do Sul. **Revista Jurídica da Presidência**, Brasília, v. 17, n. 111, fev./maio 2015, p. 63-85.

HERODOTE: Revue de geógraphie et de geópolitique. Paris: Institut Français de Géopolitique de l'Université Paris 8, n. 152-153, 1-2 sem. 2014. Dossiê *Cyberespace : enjeux géopolitiques*. Disponível em: <http://www.herodote.org/spip.php?rubrique66>. Acesso em: 12 jun. 2016.

HERZ, John H. Idealist internationalism and the security dilemma. **World Politics**, v. 2, n. 2, p. 157-180, jan. 1950.

HOBBES, Thomas. **Leviatã**: ou, matéria, forma e poder de um Estado eclesiástico e civil. Tradução de: Heloísa da Graça Burati. São Paulo: Rideel, 2005.

HOBSBAWM, Eric J. **A era dos impérios**: 1875-1914. 11. ed. Rio de Janeiro: Paz e Terra, 2007.

HOLLIS, David M. USCYBERCOM: the need for a combatant command versus a subunified Command. **Joint Force Quarterly (JFQ)**, NDU Press, Issue 58, p. 48-53, 3d quarter 2010.

HOPKINS, Nick. Stuxnet attack forced Britain to rethink the cyber war. **The Guardian**, Londres, 30 maio 2011, [*online*]. Politics. Disponível em: <http://www.guardian.co.uk/politics/2011/may/30/stuxnet-attack-cyber-war-iran>. Acesso em: 8 jun. 2016.

HURRELL, Andrew. **On global order**: power, values, and the constitution of international society. Nova York: Oxford University Press, 2007.

IANNI, Octávio. O príncipe eletrônico. **Perspectivas**, São Paulo, v. 22, p. 11-29, 1999. Disponível em: <http://seer.fclar.unesp.br/perspectivas/article/viewFile/2079/1701>. Acesso em: 12 nov. 2016.

IRÃ – REPÚBLICA ISLÂMICA DO IRÃ. Cyber attack on Bushehr facility, enemy's propaganda: Iran. **Iranian Student's News Agency**, Tehran, 28 set. 2010. Nota oficial do governo iraniano. Disponível em: <http://old.isna.ir/ISNA/NewsView.aspx?ID=News-1622868&Lang=E>. Acesso em: 30 set. 2014.

_____. Iran calls for IAEA to detect Stuxnet agents. **Iranian Student's News Agency**, Tehran, 13 jun. 2011. Nota oficial do governo iraniano. Disponível em: <http://old.isna.ir/ISNA/NewsView.aspx?ID=News-1786952&Lang=E >. Acesso em: 30 set. 2014.

ISHII, Andre. Geopolitics, the state, and cybersecurity in a globalized world. **Geopolitical Monitor**, 13 mar. 2016. Opinion. Disponível em: <https://www.geopoliticalmonitor.com/geopolitics-the-state-and-cybersecurity-in-a-globalized-world>. Acesso em: 1 abr. 2016.

JACKSON, Patrick T. **The conduct of inquiry in International Relations**: Philosophy of Science and its implications for the study of world politics. Londres; Nova York: Routledge, 2011. (The new international relations).

JERVIS, Robert. **Perception and misperception in international politics**. Princeton: Princeton University Press, 1976.

KANT, Immanuel. **A paz perpétua**: um projecto filosófico. Tradução de: Artur Morão. Covilhã: Lusofonia Press: 2008. Disponível em: <http://www.lusosofia.net/textos/kant_immanuel_paz_perpetua.pdf>. Acesso em: 29 set. 2015.

KARAS, T. H.; MOORE, J. H.; PARROTT, L. K. Metaphors for cyber security. **Sandia Report**: SAND2008-5381. New Mexico, EUA: Sandia National Laboratories, 2008. Disponível em: <http://prod.sandia.gov/techlib/access-control.cgi/2008/085381.pdf>. Acesso em: 21 mar. 2016.

KAWAMURA, Lili Katsuco. **Tecnologia e política na sociedade**: engenheiros, reivindicação e poder. São Paulo: Ed. Brasiliense, 1986.

KEOHANE, Robert O. International institutions: two approaches. **International Studies Quarterly**, v. 32, n. 4, p. 379-396, 1988.

KING, Gary; KEOHANE, Robert O.; VERBA, Sidney. **Designing social inquiry**: scientific inference in qualitative research. Princeton: Princeton University Press, 1994.

KING'S COLLEGE LONDON. Department of Digital Humanities. 2016. Disponível em: <http://www.kcl.ac.uk/artshums/depts/ddh>. Acesso em: 26 nov. 2016.

KREMER, J.; MÜLLER, B. Preface. In: _____ (Ed.). **Cyberspace and international relations**: theory, prospects and challenges. Heidelberg: Springer, 2014a. p. xi-xvii.

_____. SAM: a framework to understand emerging challenges to states in an interconnected world. In: _____ (Ed.). **Cyberspace and international relations**: theory, prospects and challenges. Heidelberg: Springer, 2014b. p. 41-58.

KRUG, Steve. **Don't make me think**: a common sense approach to web usability. Berkeley, CA: New Riders, 2000.

KUCHLER, Hannah. High-profile hacking increases pressure to respond to public fears. **Financial Times Special Report**: Cybersecurity, 6 jun. 2014. Disponível em: <http://im.ft-static.com/content/images/aa751c52-ecc2-11e3-8963-00144feabdc0.pdf>. Acesso em: 17 ago. 2016.

KUHN, Thomas S. **A estrutura das revoluções científicas**. 9. ed. Tradução de: Beatriz Vianna Boeira e Nelson Boeira. São Paulo: Perspectiva, 2006. (Debates, 115).

KURBALIJA, Jovan. E-Diplomacy and Diplomatic Law in the Internet era. In: ZIOLKOWSKI, Katharina (Ed.). **Peacetime regime for state activities in cyberspace**: international law, international relations and diplomacy. Tallinn: NATO CCD COE, 2013. p. 393-424.

LEFEBVRE, Henri. **Hacia el cibernantropo**: una crítica de la tecnocracia. Barcelona: Gedisa, 1980.

LEHMANN, K. E. Unfinished transformation: the three phases of complexity's emergence into international relations and foreign policy. **Cooperation and Conflict**, v. 47, n. 3, p. 404-413, 2012.

LEMAN-LANGLOIS, Stéphane (Ed.). **Technocrime, policing and surveillance**. Londres: Routledge, 2012. (Routledge Frontiers of Criminal Justice, 3).

_____. The local impact of police videosurveillance on the social construction of security. In: _____ (Ed.). **Technocrime**: technology, crime and social control. Londres: Willan Publishing, 2008. cap. 3, p. 27-45.

LEMIEUX, Frédéric; BALES, Brian. Investigating transnational cybercrime: current challenges and emerging initiatives. In: LEMAN-LANGLOIS, Stéphane (Ed.). **Technocrime, policing and surveillance**. Londres: Routledge, 2012. (Routledge Frontiers of Criminal Justice, 3). cap. 5, p. 65-78.

LESSA, Antônio Carlos. Instituições, atores e dinâmicas do ensino e da pesquisa em Relações Internacionais no Brasil: o diálogo entre a história, a ciência política e os novos paradigmas de interpretação (dos anos 90 aos nossos dias). **Revista Brasileira de Política Internacional**, Brasília, v. 48, n. 2, p. 169-184, dez. 2005.

LÉVY, Pierre. **Cibercultura**. Tradução de: Carlos Irineu da Costa. São Paulo: Editora 34, 1999.

LEWIS, James Andrew. Cybersecurity and cyberwarfare: assessment of national doctrine and organization. In: In: UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH – UNIDIR. **The cyber index**: international security trends and realities. Nova York; Genebra: Organização das Nações Unidas, 2013. cap. 1, p. 9-90.

LEWIS UNIVERSITY. The history of cyber warfare. [2009]. Disponível em: <http://online.lewisu.edu/msis/resources/the-history-of-cyber-warfare>. Acesso em: 24 nov. 2016.

LIANG, Qiao; XIANGSUI, Wang. **Unrestricted warfare**. Pequim: PLA Literature and Arts Publishing House, 1999.

LIAROPOULOS, Andrew. Exercising State sovereignty in cyberspace: an international cyber-order under construction? In: INTERNATIONAL CONFERENCE ON INFORMATION WARFARE AND SECURITY, 8., 25-26 mar. 2013, Denver. **Proceedings**... Denver: Regis University, 2013.

LIBICKI, Martin C. **Cyberdeterrence and cyberwar**. Santa Monica, CA: RAND Corporation, 2009.

_____. **What is information warfare?** 3. reimp. Washington, DC: National Defense University, 1996.

LIEBERMAN, Evan S. Nested Analysis as a mixed-method strategy for comparative research. **The American Political Science Review**, v. 99, n. 3, p. 435-452, ago. 2005. Disponível em: <https://doi.org/10.1017/S0003055405051762>. Acesso em: 16 nov. 2016.

LIMA, Sérgio E. M. Acesso digital e democratização do conhecimento. **Correio Braziliense**, Brasília, p. 17 out. 2016. Opinião, p. 9.

LIPSON, Leslie. **Os grandes problemas da Ciência Política**. Tradução de: Thomaz Newlands Neto. Rio de Janeiro: Zahar, 1967. (Biblioteca de Ciências Sociais).

LIPTON, Eric; SANGER, David E.; SHANE, Scott. The perfect weapon: how Russian cyberpower invaded the U.S. **The New York Times**, 13 dez. 2016. Politics. [online]. Disponível em: <http://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html>. Acesso em: 16 dez. 2016.

LOPES, Gills. El régimen internacional de lucha contra los cibercrímenes: la institucionalización de las relaciones internacionales digitales entre los años 1980 y 2000. In: JORNADA DE ESTUDIANTES DE CIENCIA POLÍTICA Y RELACIONES INTERNACIONALES, 2010, Buenos Aires.

_____. **Reflexos da digitalização da guerra na política internacional do século XXI**: uma análise exploratória da securitização do ciberespaço nos Estados Unidos, Brasil e Canadá. 2013. 133 f. Dissertação (Mestrado em Ciência Política) – Universidade Federal de Pernambuco, Recife, 2013.

LOPES, Gills; 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. **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: 2 jan. 2015.

LOPES, Gills; MEDEIROS, Marcelo de A. Da cibersegurança à ciberdefesa americana: a Diplomacia da Internet como instrumento de proteção e de integração dos Estados da OEA. In: ENCONTRO NACIONAL ABRI 2011, 3., 2011, São Paulo. **Proceedings online**. Associação Brasileira de Relações Internacionais, Instituto de Relações Internacionais – USP, p. 1-15. Disponível em: <http://www.proceedings.scielo.br/pdf/enabri/n3v2/a17.pdf>. Acesso em: 14 fev. 2016.

LOPES, Gills; PEREIRA, Dalliana Vilar. A Convenção de Budapeste e as leis brasileiras. In: SEMINÁRIO CIBERCRIME E COOPERAÇÃO PENAL INTERNACIONAL, 1., 2009, João Pessoa, UFPB. **Doutrina**. Ministério Público do Amazonas, 2010, Manaus, p. 1-15. Disponível em: <http://www.mpam.mp.br/centros-de-apoio-sp-947110907/combate-ao-crime-organizado/doutrina/574-a-convencao-de-budapeste-e-as-leis-brasileiras>. Acesso em: 7 out. 2016.

LOPES, Maurício A. Conectividade redesenha a geografia global. **Correio Braziliense**, Brasília, 15 nov. 2016, p. 11. Opinião.

LOVELACE JR, Douglas C. Foreword. In: GRAY, Colin S. **Making strategic sense of cyber power**: why the sky is not falling. Carlisle, PA: U.S. Army War College Press, 2013. p. iii.

LYNN III, William J. Defending a new domain: the Pentagon's cyberstrategy. **Foreign Affairs**, v. 89, n. 5, set.-out. 2010. Disponível em: <https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain>. Acesso em: 3 nov. 2016.

LUCERO, Everton. **Governança da Internet**: aspectos da formação de um regime global. Brasília: FUNAG, 2011.

MACEDO, Roberto Sidnei. Implicação, autorização e standardização curricular: a formação de professores como re-existência. **Revista e-Curriculum**, São Paulo, v. 13, n. 4, p. 733-750, out./dez. 2015. Disponível em: <http://revistas.pucsp.br/index.php/curriculum/article/view/25261/18787>. Acesso em: 13 out. 2016.

MACHADO, Jussara de Oliveira. **Ciberguerra**: conceitos, doutrinas, estratégias, operações, instituições e o caso dos Estados Unidos. 2014. 139 f. Dissertação (Mestrado em Relações Internacionais) – Programa de Pós-Graduação em Relações Internacionais, Pontifícia Universidade Católica de Minas Gerais, Belo Horizonte, 2014.

MALONE, Eloise F.; MALONE, Michael J. The "wicked problem" of cybersecurity: analysis of United States and Canadian policy response. **Canadian Foreign Policy Journal**, v. 19, n. 2, p. 158-177, ago. 2013. Disponível em: <http://dx.doi.org/10.1080/11926422.2013.805152>. Acesso em: 20 set. 2016.

MANDARINO JUNIOR, Raphael. **Um estudo sobre a segurança e a defesa do espaço cibernético brasileiro**. 2009. 156 f. Monografia (Especialização em Ciência da Computação) – Departamento de Ciência da Computação da Universidade de Brasília (UnB), Brasília 2009.

MARCONI, Maria de A.; LAKATOS, Eva M. **Fundamentos da metodologia científica**. 5. ed. São Paulo: Atlas, 2003.

MARTINS, Humberto F. **Introdução ao governo matricial**: o problema da fragmentação. Brasília: IGEPP, [200-]. Disponível em: <http://igepp.com.br/uploads/ebook/2._introducao_ao_governo_matricial_-_o_problema_da_fragmentacao.pdf>. Acesso em: 22 nov. 2016.

MARX, Karl; ENGELS, Friedrich. **A ideologia alemã**. Tradução de: Rubens E. Nélio, Schneider Luciano e Cavini Martorano. São Paulo: Boitempo, 2007.

MALTA; SUIÇA. E-diplomacy Platform. **Diplo**, [201-]. [*online*]. Disponível em: <https://www.diplomacy.edu/e-diplomacy>. Acesso em: 13 set. 2016.

MAQUIAVEL, Nicolau. **O príncipe** (com as notas de Napoleão Bonaparte). Tradução: J. Cretella Jr e Agnes Cretella. São Paulo: Revista dos Tribunais, 1996.

MAZANEC, Brian M. **The evolution of cyber war**: international norms for emerging-technology weapons. Lincoln, NE: Potomac Books, 2015.

MCAFEE. Cyber Defense Report. 2012. Disponível em: <http://www.mcafee.com/us/about/news/2012/q1/20120130-02.aspx>. Acesso em: 21 nov. 2014.

_____. MCAFEE. Virtual Criminology Report. 2009. Disponível em: <http://img.en25.com/Web/McAfee/VCR_2009_EN_VIRTUAL_CRIMINOLOGY_RPT_NOREG.pdf>. Acesso em: 22 out. 2016.

MEDEIROS, Marcelo de A.; BARNABÉ, Israel; ALBUQUERQUE, Rodrigo; LIMA, Rafael. What does the field of International Relations look like in South America?. **Revista Brasileira de Política Internacional**, n. 59, v. 1, e004, p. 1-31, 2016.

MEDEIROS, Marcelo de A.; VILAR LOPES, Gills. #TerrorismoCibernético ou uso terrorista das redes sociais e seus reflexos na segurança internacional: o caso do Estado Islâmico. In: CASTRO, Thales. (Org.). **Engrenagens e dinâmicas da política internacional**. Curitiba: Ithala, 2016. No prelo.

MEGALE, Januário F. **Introdução às ciências sociai**. 2. ed. São Paulo: Atlas, 1990.

MEHMETCIK, Hakan. A new way of conducting war: cyberwar, is that real?. In: KREMER, Jan-Frederik; MÜLLER, Benedikt (Ed.). **Cyberspace and international relations**. Heidelberg: Springer, 2014. p. 125-139.

MELE, Stefano. **Cyber-weapons**: legal and strategic aspects. 2. ed. Roma: Italian Institute of Strategic Studies, 2013. Disponível em: <http://www.strategicstudies.it/wp-content/uploads/2013/07/Machiavelli-Editions-Cyber-Weapons-Legal-and-Strategic-Aspects-V2.0.pdf>. Acesso em: 10 nov. 2016.

MENEGUELLO, Rachel. **Partidos e governos no Brasil contemporâneo (1985-1997)**. São Paulo: Paz e Terra, 1998.

MIT - MASSACHUSETTS INSTITUTE OF TECHNOLOGY; UNIVERSIDADE HARVARD. About ECIR. 2013a. Disponível em: <http://ecir.mit.edu/index.php/home/working-papers>. Acesso em: 14 nov. 2016.

_____. List of ECIR publications. 2013b. Última atualização: 1 dez. 2013. Disponível em: <http://ecir.mit.edu/images/stories/Images/Conference2014/Folder/ECIR%20PUBLICATIONS%2012_30_2013%20NC.pdf>. Acesso em: 15 nov. 2016.

MITNICK, Kevin; SIMON, William L. **The art of deception**: controlling the human elements of security. Indianapolis: Wiley Publishing, 2002.

MOREIRA, Adriano. Pensar o ensino superior e a ciência. **Revista da Escola de Guerra Naval**, Rio de Janeiro, v. 21, n. 2, p. 15-23, jul.-dez. 2015. Disponível em: <http://www.jmksistemas.com.br/ojs/index.php/revistadaegn/article/view/165/127>. Acesso em: 14 set. 2016.

MOURA, Nayanna Sabiá de. **Ciclo do regionalismo pós-neoliberal da Unasul**: uma análise sobre o bloqueio do espaço aéreo europeu ao avião presidencial de Evo Morales em julho de

2013. 2013. Dissertação (Mestrado em Relações Internacionais) – Universidade Estadual da Paraíba, João Pessoa, 2013.

NASCIMENTO, Fransllyn Sellynghton Silva do. **Multidimensionalidade dos conflitos cibernéticos**. 2015. 151 f. Trabalho de Conclusão de Curso (Graduação) – Departamento de Relações Internacionais, Universidade Federal de Roraima, Boa Vista, 2015.

NATIONAL DEFENSE UNIVERSITY. Cyber Policy Development (Cyber). [2016]. Disponível em: <http://chds.dodlive.mil/programs/courses/cyber-policy-development-cyber/>. Acesso em: 20 nov. 2016.

NAZARIO, Jose. Politically motivated Denial of Service attacks. In: CZOSSECK, Christian; GEERS, Kenneth (Ed.). **The virtual battlefield**: perspectives on cyber warfare. Amsterdam: IOS Press, 2009. p. 163-181. (Cryptology and Information Security, 3).

NEUNECK, Götz. Types of confidence-building measures. In: UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH – UNIDIR. **The cyber index**: international security trends and realities. Nova York; Genebra: Organização das Nações Unidas, 2013. cap. 2, p. 91-132.

NISSENBAUM, Helen. Where Computer security meets national security. **Ethics and Information Technology**, n. 7, p. 61-73, 2005.

NOTA À EDIÇÃO COMEMORATIVA. In: GIBSON, William. **Neuromancer**. Tradução de: Fábio Fernandes. São Paulo: Aleph, 2014. p. 14-17. Edição especial de 30 anos.

NYE JR, Joseph S. Cyber insecurity. **Daily News Egypt**, Cambridge, 14 dez. 2008. Disponível em: <http://belfercenter.ksg.harvard.edu/publication/18727/cyber_insecurity.html>. Acesso em: 13 set. 2016.

_____. Nuclear lessons for cyber security?. **Strategic Studies Quarterly**, v. 5, n. 4, p. 18-37, Winter 2011a. Disponível em: <http://www.au.af.mil/au/ssq/2011/winter/nye.pdf>. Acesso em: 14 nov. 2016.

_____. **Soft power**: the means to success in world politics. Nova York: PublicAfffairs, 2004.

_____. **The future of power**. New York: Public Affairs, 2011b. cap. 5.

OLIVEIRA, Ahmina R. S.; LEITE, Alexandre C. C. A condição da China como potência cibernética. In: GUEDES DE OLIVEIRA, Marcos A.; GAMA NETO, Ricardo B.; VILAR LOPES, Gills (Org.). **Relações Internacionais Cibernéticas (CiberRI)**: oportunidades e desafios para os Estudos Estratégicos e de Segurança Internacional. Recife: Ed. UFPE, 2016. cap. 6. (Defesa & Fronteiras Virtuais, 3).

MORGENTHAU, Hans J. **A política entre as nações**: a luta pelo poder e pela paz. Tradução de: Oswaldo Biato. Brasília: Editora UnB; IPRI; São Paulo: Imprensa Oficial do Estado, 2003. (Clássicos IPRI).

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Statement by H. E. Dilma Rousseff at the opening of the general debate of the 68th session of the UN General Assembly**. Nova York: Assembleia Geral da ONU, 2013. p. 1-6. Disponível em: <http://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf>. Acesso em: 14 nov. 2016.

OXFORD UNIVERSITY. Oxford Internet Institute. [2016]. Disponível em: <http://www.oii.ox.ac.uk>. Acesso em: 26 nov. 2016.

PARK, J.; CHO, M. South Korea blames North Korea for December hack on nuclear operator. **Reuters**, 17 mar. 2015. [*online*]. Disponível em: <http://www.reuters.com/article/2015/03/17/us-nuclear-southkorea-northkorea-idUSKBN0MD0GR20150317>. Acesso em: 24 nov. 2016.

PAVIA, José F. Brazil-NATO: new global security partners? In: SMITH-WINDSOR, Brooke A. (Ed.). **Enduring NATO, rising Brazil**: managing international security in a recalibrating global order. Roma: NATO Defense College, 2015. p. 253-268.

PEREIRA, Joana M. Gomes. **O ciberespaço e a mutação da realidade ou como este novo campo de atuação modifica as relações internacionais**. 2013. 68 f. Dissertação (Mestrado em Relações Internacionais) – Faculdade de Economia da Universidade de Coimbra, Coimbra, 2013. Disponível em: <https://eg.sib.uc.pt/bitstream/10316/24638/1/JoanaPereira_Disserta%3C%A7%3C%A3oMestrado.pdf>. Acesso em: 27 out. 2016.

PERON, Alcides E. dos Reis. Guerra virtual e eliminação da fricção? O uso da cibernética em operações de contrainsurgência pelos EUA. In: GUEDES DE OLIVEIRA, Marcos A.; GAMA NETO, Ricardo B.; VILAR LOPES, Gills (Org.). **Relações Internacionais Cibernéticas (CiberRI)**: oportunidades e desafios para os Estudos Estratégicos e de Segurança Internacional. Recife: Ed. UFPE, 2016. p. 35-58. (Defesa & Fronteiras Virtuais, 3). p. 109-132.

PIRKER, Benedikt. Territorial sovereignty and integrity and the challenges of cyberspace. In: ZIOLKOWSKI, Katharina (Ed.). **Peacetime regime for state activities in cyberspace**: international law, international relations and diplomacy. Tallinn: NATO CCD COE, 2013. p. 189-216.

POLICARPO, Poliana; BRENNAND, Edna. **Cibercrimes na E-democracia**. Belo Horizonte: D'Plácido, 2016.

POPPER, Karl. **A lógica da pesquisa científica**. Tradução de: Leonidas Hegenberg e Octanny S. da Mota. 16. ed. São Paulo: Cutrix, 2008.

PORTELA, Lucas S. Agenda de pesquisa sobre o espaço cibernético nas Relações Internacionais. **Revista Brasileira de Estudos de Defesa**, v. 3, n. 1, p. 91-113, jan./jun. 2016. Disponível em: <http://seer.ufrgs.br/index.php/rbed/article/view/62071>. Acesso em: 24 nov. 2016.

PROENÇA JR, Domício; DINIZ, Eugenio. **Política de Defesa no Brasil**: uma análise crítica. Brasília: Humanidade; Editora UnB, 1998.

RANTAPELKONEN, Jari; KANTOLA, Harry. Insights into cyberspace, cyber security, and cyberwar in the Nordic countries. In: RANTAPELKONEN, Jari; KANTOLA, Mirva. **The fog of Cyber Defence**. Helsinki: Filand's National Defence University, 2013. p. 24-36.

REARDON, Robert; CHOUCRI, Nazli. The role of cyberspace in International Relations: a view of the literature. In: ISA ANNUAL CONVENTION, 1 abr. 2012. Disponível em: <http://ecir.mit.edu/images/stories/Reardon%20and%20Choucri_ISA_2012.pdf>, Acesso em: 3 fev. 2015.

REINO UNIDO. **The UK Cyber Security Strategy**: protecting and promoting the UK in a digital world. Londres: Cabinet Office, nov. 2011. Disponível em: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf>. Acesso em: 3 nov. 2016.

RESENDE, Paulo-Edgar A. As ciências sociais na ótica das relações internacionais. In: BERNARDO, Teresinha; RESENDE, Paulo-Edgard A. (Org.). **Ciências sociais na atualidade**: movimentos. São Paulo: Paulus, 2005. cap. 1, p. 15-22.

REUS-SMIT, C.; Snidal, D. Between utopia and reality. In: _____ (Ed.). **The Oxford handbook of International Relations**. Nova York: Oxford University Press, 2008. p. 3-37.

REZEK, Francisco. **Direito Internacional Público**. 14. ed. rev., aumen. e atual. São Paulo: Saraiva, 2013.

RID, Thomas. Cyber war will not take place. **Journal of Strategic Studies**, v. 35, n. 1, p. 5-32, 2012. Disponível em: <http://dx.doi.org/10.1080/01402390.2011.608939>. Acesso em: 14 set. 2016.

ROJAS ARAVENA, F. Seguridad humana: aportes en la reformulación del concepto de seguridad. **FLACSO**, 2006. Disponível em: <http://www.enlaceacademico.org/uploads/media/Seguridad_Humana-Aportes_en_Reformulacion-Espana.pdf>. Acesso em: 17 mar. 2016.

ROUSSEAU, Jean-Jacques. **Rousseau e as Relações Internacionais**. Tradução de: Sérgio Bath. São Paulo: IOESP; Editora UnB; IPRI, 2003. (Clássicos IPRI).

RUDNER, Richard S. **Filosofia da Ciência Social**. Tradução de: Álvaro Cabral. Rio de Janeiro: Zahar Editores, 1969. (Curso moderno de Filosofia).

RUDZIT, Gunther. O debate teórico em segurança internacional: mudanças frente ao terrorismo?. **Civitas** – Revista de Ciências Sociais, v. 5. n. 2, p. 297-323, jul.-dez. 2005. Disponível em: <http://revistaseletronicas.pucrs.br/ojs/index.php/civitas/article/viewFile/5/1598>. Acesso em: 13 out. 2016.

RUMER, Eugene B. Introduction: a cool breezer. **The Adelphi Papers**, v. 47, issue 390, p. 7-11, Routledge, London, 30 out. 2007. Disponível em: <http://www.tandfonline.com/doi/full/10.1080/05679320701706880>. Acesso em: 13 abr. 2016.

SANGER, David E. **Confront and conceal**: Obama's secret wars and surprising use of American power. Nova York: Crown: 2012.

SARFATI, Gilberto. **Teorias de relações internacionais**. 4. tir. São Paulo: Saraiva, 2011.

SARTORI, Giovanni. **A política**: lógica e método nas ciências sociais. Tradução de: Sérgio Bath. Brasília: Editora UnB, 1981. (Pensamento politico, 36).

SCHMIDT, Brian C. On the history and historiography of International Relations. In: CARLSNAES, Walter; RISSE, Thomas; SIMMONS, Beth (Ed.). **Handbook of International Relations**. 2. ed. Londres: SAGE, 2013. cap. 1, p. 3-28.

SCHMITT, Michael N. (Ed.). **Tallinn manual on the international law applicable to cyber warfare**. Cambridge: Cambridge University Press; OTAN, 2013.

SEGAL, Adam. **Cyber conflict after Stuxnet**: essays from the other bank of the Rubicon. Vienna, VI: CCSA, 2016.

SHAHEEN, Salma. Offense-defense balance in cyber warfare. In: KREMER, Jan-Frederik; MÜLLER, Benedikt (Ed.). **Cyberspace and international relations**. Heidelberg: Springer, 2014. p. 77-97.

SILVA, Guilherme A.; GONÇALVES, Williams. **Dicionário de Relações Internacionais**. 2. ed. rev. e ampl. Barueri, SP: Manole, 2010.

SILVA, Reginaldo de S. As demandas sociais e a formação de professores: desafios à prática docente. In: BERNARDO, Teresinha; RESENDE, Paulo-Edgard A. (Org.). **Ciências sociais na atualidade**: movimentos. São Paulo: Paulus, 2005. cap. 13, p. 323-343.

SINGER, Peter W.; BROOKING, Emerson. Terror on Twitter: how ISIS is taking war to social media – and social media is fighting back. **Popular Science**, Harlan, 11 dez. 2015. Disponível em: <http://www.popsci.com/terror-on-twitter-how-isis-is-taking-war-to-social-media>. Acesso em: 7 jul. 2016.

SINGER, Peter W.; FRIEDMAN, Allan. **Cybersecurity and cyberwar**: what everyone needs to know. Oxford: Oxford University Press, 2014.

SITE Intelligence Group. [201-]. Disponível em: <http://siteintelgroup.com>. Acesso em: 23 out. 2016.

SOARES, Ana Letícia V. Compartilhando a democracia: o papel das mídias sociais no processo de securitização da Primavera Árabe. **Revista de Iniciação Científica em Relações Internacionais**, v. 2, n. 3, 106-117, 2014.

SOARES, Gláucio Ary Dillon. O calcanhar metodológico da Ciência Política no Brasil. **Sociologia, Problemas e Práticas**, n. 48, p. 27-52, maio 2005.

SOLANA, Javier. Cyber war and peace. **Project Syndicate**, 30 Apr. 2014. Disponível em: <http://www.project-syndicate.org/commentary/global-internet-cyber-security-by-javier-solana-2015-04>. Acesso em: 2 maio 2016.

SOMMER, Joseph. Coffee pots and protocols: the role of the cyberlawyer. In: MURRAY, Andrew D. **The regulation of cyberspace**: control in the online environment. Abingdon: Routledge-Cavendish, 2007. cap. 1, p. 3-21.

SORJ, Bernardo; FAUSTO, Sergio. **Political activism in the era of the Internet**. Tradução de: Raymond Maddock. São Paulo: Edições Plataforma Democrática, 2016. Disponível em: <http://www.plataformademocratica.org/Arquivos/Political_activism_in_the_era_of_the_Internet.pdf>. Acesso em: 14 nov. 2016.

SOUSA, João Pedro G. de. Apresentação. In: VOEGELIN, Eric. **A nova ciência da política.** 2. ed. Tradução de: José Viegas Filho. Brasília: Editora UnB, 1982. p. 5-10. (Pensamento político, 12).

SOUSA, Valmi D.; DRIESSNACK, Martha; MENDES, Isabel A. C. Revisão dos desenhos de pesquisa relevantes para Enfermagem. Parte 1: desenhos de pesquisa quantitativa. **Revista Latino-americana de Enfermagem**, v. 15, n. 3, maio-jun. 2007. Disponível em: <http://www.scielo.br/pdf/rlae/v15n3/pt_v15n3a22.pdf>. Acesso em: 13 dez. 2015.

STOHL, Michael. Dr. Strangeweb: or how they stopped worrying and learned to love cyber war. In: CHEN, Thomas M.; JARVINS, Lee; MACDONALD, Stuart (Ed.). **Cyberterrorism**: understanding, assessment, and response. Nova York: Springer, 2014. cap. 5, p. 85-102.

STOLTENBERG, Jens. Press conference. OTAN, 14 jun. 2016. [*online*]. Disponível em: <http://www.nato.int/cps/en/natohq/opinions_132349.htm?selectedLocale=en>. Acesso em: 15 jun. 2016.

TEIXEIRA JÚNIOR, Augusto Wagner M. O Conselho de Defesa Sul-americano da UNASUL. In: GUEDES DE OLIVEIRA, Marcos A. (Org.). **Comparando a Defesa sul-americana**. Recife: Editora UFPE, 2011. p. 127-147.

THE ECONOMIST. Londres, v. 396, n. 8689, 3-9 jul. 2010. 92 p.

THELWALL, Michael. **Introduction to Webometrics**: quantitative web research for the Social Sciences. San Rafael, CA: Morgan & Claypool Publishers, 2009. (Synthesis lectures on information concepts, retrieval, and services, 4).

TOURÉ, Hamadoun. The international response to cyberwar. In: _____ (Ed.). **The quest for cyber peace**. Geneva: International Telecommunication Union – ITU, 2011, p. 86-103.

UNIVERSIDAD DE GRANADA. Máster on line en Estudios Estratégicos y Seguridad Internacional. Disponível em: <http://www.estudiosestrategicos.es/?q=content/programa-acad%3C%A9mico>. Aceso em: 26 nov. 2016.

UNIVERSIDADE FEDERAL DE MINAS GERAIS. **O Plano Nacional de Extensão Universitária**. Belo Horizonte: FORPROEX, [200-]. (Extensão Universitária, 1). Disponível em: <https://www.ufmg.br/proex/renex/documentos/Colecao-Extensao-Universitaria/01-Plano-Nacional-Extensao/Plano-nacional-de-extensao-universitaria-editado.pdf>.

VAISHNAV, Chintan; CHOUCRI, Nazli; CLARK, David. Cyber international relations as an integrated system. **Environment Systems and Decisions**, v. 33, n. 4, p. 561-576, nov. 2013. Disponível em: <https://dspace.mit.edu/handle/1721.1/103775>. Acesso em: 12 set. 2016.

VALENTE, Leonardo. **Política externa na era da informação**: o novo jogo do poder, as novas diplomacias e a mídia como instrumentos de Estado nas relações internacionais. Rio de Janeiro: Revan; UFF, 2007.

VAN EVERA, Stephen. **Guide to methods for students of Political Science**. Ithaca, NY: Cornell University Press, 1997.

VANTI, Nadia A. P. Os links e os estudos webométricos. **Ciência da Informação**, Brasília, v. 34, n. 1, p. 78-88, jan./abr. 2005.

_____. Da bibliometria à webometria: uma exploração conceitual dos mecanismos utilizados para medir o registro da informação e a difusão do conhecimento. **Ciência da Informação**, Brasília, v. 31, n. 2, p. 152-162, maio/ago. 2002.

VILAR LOPES, Gills. **Relações Internacionais Cibernéticas (CiberRI)**: uma defesa acadêmica. In: ENCONTRO NACIONAL DA ASSOCIAÇÃO BRASILEIRA DE ESTUDOS DE DEFESA, 8., 2014, Brasília. Pôster. Disponível em: <https://www.academia.edu/9285057/Rela%3C%A7%3C%B5es_Internacionais_Cibern%3C%A9ticas_CiberRI_uma_defesa_acad%3C%AAmica>. Acesso em: 12 ago. 2016.

_____. A Política Nacional de Inteligência (PNI) e as relações internacionais. **Mundorama**, Brasília, n. 107, jul. 2016. Disponível em: <http://www.mundorama.net/2016/07/07/a-politica-nacional-de-inteligencia-pni-e-as-relacoes-internacionais-por-gills-vilar-lopes/>. Acesso em: 14 out. 2016.

_____; OLIVEIRA, Carolina F. J. Stuxnet e defesa cibernética estadunidense à luz da Análise de Política Externa. **Revista Brasileira de Estudos de Defesa**, ABED, v. 1, n. 1, p. 55-69, 2014. Disponível em: <http://seer.ufrgs.br/index.php/rbed/article/view/39457>. Acesso em: 12 ago. 2016.

VILLA, R.; REIS, R. A segurança internacional no pós-Guerra Fria. **Revista Brasileira de Informação Bibliográfica em Ciências Sociais,** n. 62, p. 19-51, 2006.

VOEGELIN, Eric. **A nova ciência da política.** 2. ed. Tradução de: José Viegas Filho. Brasília: Editora UnB, 1982. (Pensamento político, 12).

W3C BRASIL – World Wide Web Consortium - Escritório Brasil. Linha do tempo da Web. [2016]. Disponível em: <http://www.ceweb.br/linhadotempo>. Acesso em: 23 nov. 2016.

WAHL, Bernardo; SILVA, Peterson. Por que a Política Nacional de Inteligência (PNI) é importante?. **Mundorama**, Brasília, n. 107, jul. 2016. Disponível em: <https://www.mundorama.net/2016/07/18/por-que-a-politica-nacional-de-inteligencia-pni-e-importante-por-bernardo-wahl-e-peterson-silva/>. Acesso em: 14 out. 2016.

WALLERSTEIN, Immanuel *et al*. **Para abrir as ciências sociais**. São Paulo: Cortez, 1996.

WALTZ, Kenneth N. Foreword: thoughts about assaying theories. In: ELMAN, Colin; ELMAN, Miriam F. (Ed.). **Progress in International Relations Theory**: appraising the field. Cambridge, MA: MIT Press, 2003. p. vii-xii. (BCSIA Studies in International Security).

_____. **Teoria das Relações Internacionais**. Tradução de: Maria Luísa F. Gayo. Lisboa: Gradiva, 2002. (Trajectos, 50).

WEBER, Max**. A 'objetividade' do conhecimento nas Ciências Sociais**. Tradução de: Gabriel Cohn. São Paulo: Ática, 2006. (Ensaios comentados).

_____. A política como vocação. In: GERTH, H. H.; WRIGHT MILLS, C. (Org). **Max Weber**. Rio de Janeiro: Livros Técnicos e Científicos, 1967. p. 55-89.

_____. **Metodologia das ciências sociais**. 5. ed. Tradução de: Augustin Wernet. São Paulo: Cortez; Campinas: Editora Unicamp, 2016.

WEINGÄRTNER, Dieter. Foreword. In: ZIOLKOWSKI, Katharina (Ed.). **Peacetime regime for state activities in cyberspace**: international law, international relations and diplomacy. Tallinn: NATO CCD COE, 2013. p. XIII-XIV.

WERTHEIM, Margaret. **Uma história do espaço de Dante à Internet**. Tradução de: Maria Luiza X. de A. Borges. Rio de Janeiro: Zahar, 2001.

WERTHEIN, Jorge. A sociedade da informação e seus desafios. **Ciência da Informação**, Brasília, v. 29, n. 2, p. 71-77, maio/ago. 2000. Disponível em: <http://revista.ibict.br/ciinf/article/view/889/924>. Acesso em: 15 set. 2016.

WEUSECOINS. [201-]. Disponível em: <http://www.weusecoins.com>. Acesso em: 3 ago. 2016.

WIGHT, Martin. **A política do poder**. 2. ed. Tradução de: Carlos S. Duarte. Brasília: Ed. UnB, 2002. (Clássicos IPRI, 7).

WILEY, D. A. Connecting learning objects to instructional design theory: a definition, a metaphor, and a taxonomy. In: _____ (Ed.). **The instructional use of learning objects**: online version. Logan, UT: [s.n.], 2000. Disponível em: <http://www.reusability.org/read/chapters/wiley.doc>. Acesso em: 14 out. 2016.

WINAND, Érica; SAINT-PIERRE, Héctor Luis. A fragilidade da condução política da defesa no Brasil. **História**, Franca, v. 29, n. 2, dez. 2010.

WOLFERS, Arnold. **Discord and collaboration**: essays on international politics. Baltimore: The Johns Hopkins University Press, 1962.

YANNAKOGEORGOS, Panayotis A. Rethinking the threat of cyberterrorism. In: CHEN, Thomas M.; JARVINS, Lee; MACDONALD, Stuart (Ed.). **Cyberterrorism**: understanding, assessment, and response. Nova York: Springer, 2014. cap. 3, p. 43-62.

ZERO days: world war 3.0. Produção de Alex Gibney. [S.l.]: Jigsaw Productions, 2016. 1 vídeo web (116 min), widescreen, color. Documentário sobre o Stuxnet. Disponível em: <http://www.zerodaysfilm.com>. Acesso em: 5 nov. 2016.

ZUCCARO, Paulo M. Tendência global em Segurança e Defesa Cibernética: reflexões sobre a proteção dos interesses brasileiros no ciberespaço. In: BARROS, Otávio S. Rêgo; GOMES, GOMES, Ulisses de M.; FREITAS, Whitney Lacerda de (Org.). **Desafios estratégicos para a Segurança e a Defesa Cibernética**. Brasília: Secretaria de Assuntos Estratégicos da Presidência da República – SAE, 2011. p. 49-77.

Obras de referência[218]

ACADEMIA BRASILEIRA DE LETRAS. Busca no Vocabulário Ortográfico da Língua Portuguesa. [*online*]. Disponível em: <http://www.academia.org.br/nossa-lingua/busca-no-vocabulario>. Acesso em: 20 out. 2016.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 6023: informação e documentação - referências - elaboração. Rio de Janeiro, 2002.

_____. NBR 10520: informação e documentação - citações em documentos - apresentação. Rio de Janeiro, 2002.

_____. NBR 14724: informação e documentação - trabalhos acadêmicos – apresentação. 3. ed. Rio de Janeiro, 2011.

BOBBIO, Norberto; MATTEUCCI, Nicola; PASQUINO, Gianfranco. **Dicionário de política**. 13. ed. Tradução de: Carmen C. Varriale *et al*. Brasília: Editora UnB, 2016. v. 1-2.

BRASIL. Fundação Instituto Brasileiro de Geografia e Estatística. **Normas de apresentação tabular**. 3. ed. Rio de Janeiro: IBGE, 1993. Disponível em: <http://biblioteca.ibge.gov.br/visualizacao/livros/liv23907.pdf>. Acesso em: 14 set. 2016.

GARCIA, Othon M. **Comunicação em prosa moderna**. 27. ed. 2. reimp. Rio de Janeiro: FGV, 2011.

MEGALE, Januário F. Expressões latinas usadas nos clássicos de ciências sociais e em textos acadêmicos. In: _____. **Introdução às ciências sociais**. 2. ed. São Paulo: Atlas, 1990. p. 200-208.

SANTIAGO, Sandra; LIMA, Etiene. **Orientação dirigida aos alunos de graduação e pós-graduação**. Recife: SIB-UFPE, [201-]. Disponível em: <https://www.ufpe.br/sib/images/documentos/orientacao.pdf>. Acesso em: 14 set. 2016.

SOARES, Delfim. Glossário de Sociocibernética. Disponível em: <http://www.compuland.com.br/delfim/gloss.htm>. Acesso em: 11 out. 2016.

[218] O título desta subseção consona com a indicação de Gil (1999, p. 77) e Megale (1990, p. 29).

UNIVERSIDADE DA CALIFÓRNIA EM LOS ANGELES – UCLA. Resources to help you learn and use Stata. Disponível em: <http://www.ats.ucla.edu/stat/stata/>. Acesso em: 14 out. 2016.

APÊNDICE A – Exemplo de plano de aula que incorpora CiberRI

O plano de aula abaixo é uma adaptação de um já aplicado, por este autor enquanto Professor Substituto do Departamento de Relações Internacionais da Universidade Federal da Paraíba (DRI-UFPB), à turma matutina de "Estudos Regionais: Ásia" (60 h/a), no ano letivo 2014.1.

Como a Ementa desse componente curricular, assim como qualquer ementa, é item de repetição obrigatório do Plano Pedagógico do Curso de Bacharelado em RI da UFPB, adequaram-se o Conteúdo Programático e a Bibliografia para CiberRI.

EMENTA
Estudo das relações internacionais dos países asiáticos. O colonialismo e o processo de descolonização. O contexto da Guerra Fria e a busca do desenvolvimento. Análise da situação político-econômica dos Estados independentes. Os processos de integração e as lideranças regionais: China, Índia, Japão. **Conflitos e questões estratégicas. A inserção da Ásia na nova ordem mundial**.

CONTEÚDO PROGRAMÁTICO
• Os estudos sobre a Ásia no Brasil • Aspectos históricos da Ásia: imperialismo e descolonização • Processos de integração regional asiáticos • Relações Internacionais Cibernéticas (CiberRI) na Ásia • Relações Brasil-Ásia • A segurança regional na Ásia • Japão e Coreia do Sul: gigantes econômicos, anões políticos • BRIC: Brasil, Rússia, Índia e China

BIBLIOGRAFIA
[...] CARR, Jeffrey. *Inside cyber warfare*: mapping the cyber underworld. 2. ed. Cambridge, EUA: O'Reilly, 2012. p. 81-83, 246-247. CLARKE, Richard A.; KNAKE, Robert K. *Cyber war*: the next threat to national security and what to do about it. 2. ed. New York: Ecco, 2012. p. 291-296.

[...]

NYE, Joseph S. Cyber Insecurity. *Daily News Egypt*, Cambridge, 14 dez. 2008. Disponível em: <http://belfercenter.ksg.harvard.edu/publication/18727/cyber_insecurity.html>. Acesso em: 8 mar. 2014.

[...]

OPPERMANN, Daniel. Virtual attacks and the problem of responsibility: the cases of China and Russia. *Carta Internacional*, v. 5, n. 2, NUPRI-USP, p. 11-25, dez. 2010. Disponível em: <http://citrus.uspnet.usp.br/nupri/arquivo.php?id=21>. Acesso em: 30 mar. 2014.

CRONOGRAMA LETIVO		
AULA	**DATA**	**TÓPICO / REFERÊNCIA(S)**
[...]	[...]	[...]
04	30 maio (6ª) às 8h	*4 CiberRI na Ásia: Guerra Rússia-Geórgia; casos Stuxnet-Irã e China-Google; e capacidades cibernéticas da Coreia do Norte* *Obrigatórias*: CARR, 2012, p. 81-83, 246-247; CLARKE; KNAKE, 2012, p. 291-296 ; NYE, 2008; OPPERMANN, 2010
[...]	[...]	[...]

Legenda: Disponível em formato PDF. Disponível apenas na xerox. Disponível apenas na Internet.
Fonte: DRI-UFPB.

APÊNDICE B – Exemplo de plano de aula para "Introdução às CiberRI"

TÍTULO
Introdução às Relações Internacionais Cibernéticas (CiberRI)

OBJETIVO
Analisar os impactos do ciberespaço nas relações internacionais do século XXI, bem como respostas do campo de RI.

EMENTA
O estudo das relações internacionais cibernéticas. A pertinência das Teorias de RI para com o ciberespaço. O uso de ferramentas analíticas de RI no ciberespaço. Estudo de casos impactes em CiberRI.

CONTEÚDO PROGRAMÁTICO
• O subcampo de CiberRI • Ciberespaço e RI • Teorias de RI e o ciberespaço • Metodologia em RI e ciberespaço • O Caso Snowden e a espionagem internacional

BIBLIOGRAFIA
O subcampo de CiberRI • GUEDES DE OLIVEIRA, Marcos. A.; GAMA NETO, Ricardo B.; VILAR LOPES, Gills. Apresentação. In: _____ (Org.). **Relações Internacionais Cibernéticas (CiberRI)**: oportunidades e desafios para os Estudos Estratégicos e de Segurança Internacional. Recife: EDUFPE, 2016. p. 27-31. (Defesa & fronteiras virtuais, 3). **Ciberespaço e RI** • CHOUCRI, Nazli. **Cyberpolitics in international relations**. Cambridge, MA: The MIT Press, 2012.

- DEMCHAK, Chris C. Foreword. In: KREMER, Jan-Frederik; MÜLLER, Benedikt (Ed.). **Cyberspace and international relations**. Heidelberg: Springer, 2014. p. v-x.
- KREMER, J.; MÜLLER, B. Preface. In: _____ (Ed.). **Cyberspace and international relations**: theory, prospects and challenges. Heidelberg: Springer, 2014a. p. xi-xvii.
- NYE JR, Joseph S. **The future of power**. New York: Public Affairs, 2011b. cap. 5.
- PEREIRA, Joana M. Gomes. **O ciberespaço e a mutação da realidade ou como este novo campo de atuação modifica as relações internacionais**. 2013. 68 f. Dissertação (Mestrado em Relações Internacionais) – Faculdade de Economia da Universidade de Coimbra, Coimbra, 2013. Disponível em: <https://eg.sib.uc.pt/bitstream/10316/24638/1/JoanaPereira_DissertaçãoMestrado.pdf>. Acesso em: 27 out. 2016.
- PORTELA, Lucas S. Agenda de pesquisa sobre o espaço cibernético nas Relações Internacionais. **Revista Brasileira de Estudos de Defesa**, v. 3, n. 1, p. 91-113, jan./jun. 2016. Disponível em: <http://seer.ufrgs.br/index.php/rbed/article/view/62071>. Acesso em: 24 nov. 2016.
- REARDON, Robert; CHOUCRI, Nazli. **The role of cyberspace in International Relations: a view of the literature**. In: ISA ANNUAL CONVENTION, 1 abr. 2012. Disponível em: <http://ecir.mit.edu/images/stories/Reardon and Choucri_ISA_2012.pdf>, Acesso em: 3 fev. 2015.
- VAISHNAV, Chintan; CHOUCRI, Nazli; CLARK, David. **Cyber international relations as an integrated system**. Environment Systems and Decisions, v. 33, n. 4, p. 561-576, nov. 2013. Disponível em: <http://dx.doi.org/10.1007/s10669-013-9480-3>. Acesso em: 12 set. 2016.

Teorias de RI e ciberespaço

- 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. Caxambu: ANPOCS, 2012. Disponível em: <http://www.anpocs.org/portal/index.php?option=com_docman&task=doc_details&gid=8169&Itemid=76>. Acesso em: 6 dez. 2015.

- ERIKSSON, Johan; GIACOMELLO, Giampiero. The information revolution, security, and International Relations: (IR)relevant Theory?. **International Political Science Review**, v. 27 n. 3, p. 221-244, 2006. Disponível em: <https://doi.org/10.1177/0192512106064462>. Acesso em: 3 dez. 2015.

Metodologia em RI e ciberespaço

- KREMER, J.; MÜLLER, B. SAM: a framework to understand emerging challenges to states in an interconnected world. In: _____ (Ed.). **Cyberspace and international relations**: theory, prospects and challenges. Heidelberg: Springer, 2014. p. 41-58.
- LOPES, Gills. **Reflexos da digitalização da guerra na política internacional do século XXI**: uma análise exploratória da securitização do ciberespaço nos Estados Unidos, Brasil e Canadá. 2013. 133 f. Dissertação (Mestrado em Ciência Política) – Universidade Federal de Pernambuco, Recife, 2013. p. 51-99.

O Caso Snowden e a espionagem internacional

- BESSA, Jorge. **O escândalo da espionagem no Brasil**: o caso Snowden. Brasília: Thesaurus, 2014.
- O DEBATEDOUDO, n. 83, maio 2014. Dossiê "Um ano pós-Snowden". Disponível em: <https://odebatedouro.files.wordpress.com/2014/05/debat84_v1.pdf>. Acesso em: 14 set. 2016.

APÊNDICE C – Trabalhos analisados oriundos dos anais do ENABED

A Tabela 2, *infra*, apresenta os 83 trabalhos selecionados, de um total de 1.007, publicados nos anais do ENABED, entre 2007 e 2016, que trazem o termo "ciber" ou "*cyber*" em seu corpo textual. Note-se não são levados em consideração os que, pelo menos, possuem um dos dois termos *apenas* nas Referências. Isso se deve ao fato de os seu "[...]formato livre e seu caráter polissêmico[...] obriga[re]m o pesquisador a realizar *um trabalho de limpeza de dados antes de qualquer esforço de interpretação*" (FREITAS *et al.*, 2006, p. 121, grifo nosso).

Outro destaque da Tabela 2 é para a variável "Grau de importância dada ao ciberespaço", que busca medir, em termos categóricos, não apenas o espaço dado, no texto, para o ciberespaço, como também a sua relação com que está sendo discutido na Tese ora em apreço, ou seja, temas atinentes a CiberRI.

Esta mesma tabela compreende o banco de dados criado para operacionalizar as variáveis e disponível, nos formatos Excel® e STATA®, no seguinte endereço eletrônico: https://github.com/gillsvilarlopes/tese-ppgcp-ufpe.

Tabela 2 Trabalhos publicados no ENABED que contém "ciber" e "*cyber*" (2007-2016)

ID	Ano	Título do trabalho	Grau de importância dada ao ciberespaço
1	2007	O conceito de Revolução nos Assuntos Militares	nenhuma
2	2008	Medidas adotadas pelo governo brasileiro frente ao Plano Colômbia	nenhuma
3	2008	Defesa Nacional, teorias de guerra e doutrina básica da Força Aérea Brasileira	nenhuma
4	2009	A Estratégia de Defesa brasileira como fomentadora de emprego e renda: a oportunidade de um "PAC da Defesa"	nenhuma
5	2009	Formação dos Oficiais das Forças Armadas no Brasil: Urgente coordenação dos fundamentos e conteúdos pelo Ministério da Defesa	nenhuma
6	2009	Mecanismos unilaterais de cerceamento tecnológico e comercial e regimes que o Brasil não aderiu	nenhuma
7	2009	A Estratégia Nacional de Defesa e a nova ordem internacional	nenhuma
8	2009	O Brasil e a proteção e o controle de bens sensíveis	nenhuma
9	2010	Jogos (outros que não de) guerra	nenhuma
10	2010	Realismo político e novas ameaças: um estudo de caso da *Global War on Terror*	nenhuma
11	2010	O movimento do ensino militar no Comando do Exército	nenhuma
12	2010	Academia da Força Aérea: educação e transformação para atendimento das demandas pós-modernas	nenhuma
13	2010	Base Industrial de Defesa: do cerceamento tecnológico à diplomacia de defesa	nenhuma
14	2010	C&T e Indústria de Defesa: o papel da Engenharia Militar no desenvolvimento nacional autônomo	nenhuma
15	2010	A opção brasileira pelos aviões Rafale franceses, na ótica das restrições de acesso e desenvolvimento de tecnologia	nenhuma

16	2010	A Política Externa Brasileira e o programa nuclear iraniano – Uma análise do Tratado de Não- Proliferação Nuclear e da Estratégia Nacional de Defesa	nenhuma
17	2010	A Integração Regional na América do Sul e a Nova Ordem Mundial: novas questões e desafios	nenhuma
18	2010	A Estratégia Nacional de Defesa e a Unasul: afinidades pouco eletivas	nenhuma
19	2011	A Estratégia Nacional de Defesa, o profissionalismo militar e as relações civis-militares no Brasil	nenhuma
20	2011	Desafios da Inteligência no ciberespaço	muita
21	2011	Das operações de coleta de Inteligência à guerra de informações: securitização do espaço cibernético	muita
22	2011	Ciência e Tecnologia: "política por outros meios"?	nenhuma
23	2011	Avaliação da eficácia e eficiência da base logística de defesa: uma abordagem	nenhuma
24	2011	A DCNS e o programa de submarinos: experiências e perspectivas de setores de defesa brasileiros sobre a transferência de tecnologia estratégica	nenhuma
25	2011	Arcabouço regulatório da base logística de Defesa	nenhuma
26	2011	O papel da integração do Sistema de Ciência, Tecnologia e Inovação de interesse da Defesa com a BID no processo de obtenção da tecnologia militar	nenhuma
27	2011	Da ciberguerra: idiossincrasias do século XXI e as instituições militares de Defesa Cibernética de Brasil, Estados Unidos, Otan e União Europeia	muita
28	2011	Forças de autodefesa do Japão: rumo ao Estado normal?	nenhuma
29	2011	O processo de transformação do Exército Brasileiro: um estudo sobre os reflexos da era do conhecimento	nenhuma
30	2011	Política de Defesa Nacional, Estratégia Nacional de Defesa e Doutrina Militar de Defesa: América do Sul e segurança regional	nenhuma
31	2011	Dissuasão: nova forma de mediar conflitos?	nenhuma
32	2011	Transformações contemporâneas no ensino superior militar	nenhuma
33	2011	Inovação no setor de Defesa e transformação do Exército	nenhuma
34	2012	Geopolítica e território cibernético: teoria de fronteiras, política e estratégia para essa nova dimensão territorial	muita
35	2012	A geopolítica da América do Sul: o papel determinante da Defesa na integração do setor elétrico	pouca
36	2012	O Parlamento e a Política de Defesa Nacional	nenhuma
37	2012	A crise fiscal dos EUA: implicações para a indústria de Defesa brasileira	nenhuma
38	2012	Uma estratégia para o desenvolvimento e a sustentação da base logística de Defesa brasileira	nenhuma
39	2012	A política pública industrial de Defesa brasileira: reflexões sobre o papel da futura carreira civil de analistas do Ministério da Defesa	nenhuma
40	2012	Restrições orçamentárias no Departamento de Defesa e seus impactos sobre a política americana de Segurança	nenhuma
41	2012	Jogos e cenários: simulações em benefício da Defesa	nenhuma
42	2012	Aplicações da Ciência da Informação na Defesa Nacional: possibilidades de cooperação, contribuição e integração entre as áreas	nenhuma
43	2012	As dimensões do campo de batalha e a guerra omnidimensional	pouca
44	2012	Os Estados Unidos da América e o desenvolvimento de uma Estratégia para o Espaço Cibernético	muita
45	2012	Segurança Cibernética na Política de Defesa brasileira: um caso de securitização?	muita
46	2012	O Conceito de Guerrilha e o Debate sobre a Transformação da Guerra	nenhuma
47	2012	Limites e perspectivas da securitização: estudos de caso no contexto sul-americano contemporâneo	pouca
48	2012	Novas ameaças no século XXI: o terrorismo transnacional	nenhuma
49	2012	A Estratégia Nacional de Defesa como oportunidade para o debate público da Atividade de Inteligência	nenhuma
50	2012	Sugestões para a Inteligência de Defesa deste século	nenhuma

51	2012	O terrorismo na América do Sul e a segurança regional comparada	nenhuma
52	2013	Dessecuritização da Amazônia e as fronteiras metafísicas	nenhuma
53	2013	Os Estados Unidos da América e o desenvolvimento de uma Estratégia para o Espaço Cibernético	muita
54	2013	Espectro da Securitização Militar do Ciberespaço (ESMC): uma nova perspectiva sobre a Defesa Cibernética	muita
55	2013	Segurança Internacional e Guerra Cibernética	muita
56	2013	A articulação entre a Defesa e o orçamento: uma moldura teórico-conceitual	nenhuma
57	2013	Segurança e Defesa nos BRICS: é possível uma agenda comum?	pouca
58	2013	Integração do Sistema de Simulação de Combate da Defesa	nenhuma
59	2013	Revisão da Política de Defesa do governo brasileiro à luz do conceito da Base Logística de Defesa	nenhuma
60	2013	O primeiro Curso Avançado de Defesa Sul-Americano (CAD-SUL): reflexões sobre a defesa da Amazônia	nenhuma
61	2014	O poder no ciberespaço: o uso da força através da tecnologia da informação	muita
62	2014	Segurança regional e nexo entre segurança e desenvolvimento: percepção de ameaça nas políticas declaratórias de defesa de África do Sul, Brasil e Índia	nenhuma
63	2014	*Arms acquisition – why is it so difficult?*	pouca
64	2014	Guerra pós-moderna? As operações *targeted killing* da USAF e CIA entre o conceito de *virtuous war* e simulacros	pouca
65	2014	Políticas públicas no setor de Defesa: por uma análise da influência dos estudos sobre o tema para a consolidação da cultura de Defesa	nenhuma
66	2014	Jogos em mobilização nacional	nenhuma
67	2014	Defesa e Segurança; guerra e não-guerra: conceitos teóricos; reflexos práticos	pouca
68	2014	O Programa Espacial Brasileiro: uma oportunidade de fortalecer o poder nacional	nenhuma
69	2014	A ativação de um Comando Conjunto na Amazônia Azul para a defesa proativa do Pré-Sal	nenhuma
70	2014	A geopolítica brasileira e a estratégia chinesa para o Atlântico-Sul: prospecção de cooperação ou de conflito?	nenhuma
71	2014	Potencialidades e contingenciamentos na cooperação entre Brasil e África do Sul para desenvolvimento e produção de produtos e serviços de Defesa	nenhuma
72	2014	A modernização das Forças Armadas brasileiras e a integração com a Base Industrial de Defesa (BID): avaliação dos programas do Exército, Marinha e Aeronáutica	pouca
73	2014	Base Industrial de Defesa (BID) no Brasil: análise da indústria de sistemas espaciais voltados para a Defesa	nenhuma
74	2014	A Responsabilidade do brasil na segurança do Atlântico Sul	nenhuma
75	2014	Cenários para indústria de defesa no Atlântico Sul a partir do benchmarking das grandes organizações brasileiras	nenhuma
76	2014	Estratégias de atuação das Forças Armadas brasileiras em missões de paz no continente africano: uma discussão sobre novas tendências	nenhuma
77	2016	As capacidades espaciais e a Cibersegurança na República da Índia: reflexos para as forças armadas	muita
78	2016	A conduta da guerra na *cyberwarfare*: novo domínio, arma estratégica ou instrumento de força?	muita
79	2016	Análise da Doutrina Militar de Defesa Cibernética a luz do DIH/DICA	muita
80	2016	Alternativas de otimização do Ciclo OODA no ciberespaço aplicadas ao contexto brasileiro	muita
81	2016	Arcabouço político-administrativo do espaço cibernético brasileiro	muita
82	2016	A importância das TICs na logística de Defesa: estudo de caso de caso sobre a Guerra do Golfo (1991)	pouca
83	2016	Guerra cibernética: a fragilidade das comunicações brasileiras e as implicações para a Marinha	muita

Fonte: Elaboração própria.
Fonte dos dados: http://abedef.org/conteudo/view?ID_CONTEUDO=62 e http://www.enabed2016.abedef.org/conteudo/view?ID_CONTEUDO=162.

APÊNDICE D – Cálculo da amostra para a população dos anais do ENABED

Como informado, em nota de rodapé da subseção 3.2.2, apresenta-se, abaixo, a fórmula e o cálculo da amostra (*n*) necessários para se inferir sobre a população ou universo (*N*) dos trabalhos publicados nos anais do ENABED e que versam sobre o ciberespaço. Em outras palavras, busca-se conhecer o número mínimo para, a partir deles, poder fazer com as conclusões das análises de *n* possam ser replicadas a *N*.

Novamente, adverte-se que esta Tese utiliza a Estatística Descritiva, e não a Inferencial ou Indutiva, à qual cabem a fórmula e o cálculo que se seguem.

Primeiramente, tome-se a fórmula geral para se calcular amostras para populações finitas[219], como é o caso dos trabalhos publicados no ENABED, de 2007 a 2016, conforme se apresenta na Equação 1.

Equação 1 Fórmula para o cálculo de amostras para populações finitas

$$n = \frac{\sigma^2 . p \, . q \, . N}{e^2 . (N - 1) + \sigma^2 \, . p \, . q} \qquad (1)$$

Onde:

- n = tamanho da amostra, a ser descoberto;
- σ^2 = nível de confiança, escolhido pelo pesquisador[220], elevado ao quadrado e expresso em número de desvios-padrão = 2;
- p = porcentagem com que o fenômeno acontece, expresso em número natural = 8% = 8; [221]
- q = percentagem complementar (100 – p) = 92;

[219] Para a fórmula do cálculo de amostras para populações infinitas, ver Gil (1999, p. 106-107).

[220] Como já visto implicitamente na subseção 3.2.3 e tendo como base a teoria geral das probabilidades, o nível de confiança de uma amostra está diretamente relacionado com a chamada curva normal ou curva de Gauss; mais especificamente "[...]à área da curva normal definida a partir dos desvios-padrão em relação à sua média" (GIL, 1999, p. 105). Geralmente, nas ciências sociais, trabalha-se com um nível de confiança entre de aproximadamente 95%, o que corresponde a uma área da curva normal que compreende *dois* desvios-padrão – lembrando que desvio-padrão é a raiz quadrada da variância (s). Assim, para o exemplo deste Apêndice, toma-se o valor de 95% da área, o que equivale, para os fins da Equação 1, ao número "2". Para uma explicação mais detalhada da distribuição normal e da curva normal, ver Crespo (2009, p. 139-142).

[221] Como se vê na subseção 3.2.3, dos 1.007 trabalhos analisados, apenas 83 deles, ou seja, aproximadamente 8% satisfazem aos critérios da pesquisa.

- N = tamanho da população = 1007;
- e^2 = erro máximo permitido = 5; [222]

Tendo esses dados em mente, aplicam seus respectivos valores à fórmula geral da Equação 1, por meio da Equação 2.

Equação 2 Cálculo da amostra da população dos trabalhos do ENABED sobre ciberespaço

$$n = \frac{2^2 . 8 . 92 . 1007}{5^2 . (1007 - 1) + 2^2 . 8 . 92} = \frac{2.964.608}{28.094} \cong 105{,}5 \cong 106 \quad (2)$$

Portanto, como se vê na Equação 2, o pesquisador que desejar fazer *inferências* sobre o universo a partir de uma amostra de trabalhos que contenham o termo "ciber" ou "*cyber*" em seu corpo textual e publicados nos anais do ENABED, entre 2007 e 2016, deve pesquisar, no mínimo, 106 trabalhos.

[222] Como se está trabalhando com probabilidades, não se esperam resultados que satisfaçam 100% aos objetivos tanto do pesquisador quanto da amostra em relação à população. Em outras palavras, há sempre um erro de medição a ser levado em conta, em uma relação inversamente proporcional ao tamanho da amostra, ou seja, quanto maior o tamanho da amostra, menor o erro de medição. No caso das pesquisas sociais, estima-se tal erro, geralmente, em 5%; isso quer dizer que, de cada 100 casos, pode-se explicar, satisfatoriamente, no mínimo, 95 deles.

ANEXO A – Pontos para provas de concurso para professor de RI da UNIFESP

UNIVERSIDADE FEDERAL DE SÃO PAULO
CONCURSO PÚBLICO
EDITAL Nº 520, DE 12 DE AGOSTO DE 2016.
ANEXO I
RELAÇÃO DE PONTOS PARA A(S) PROVA(S) Escrita e Didática
ÁREA/SUBÁREA: Relações Internacionais/Segurança Internacional

1. A TEORIA DA GUERRA: DO CONCEITO CLÁSSICO ÀS **GUERRAS** ASSIMÉTRICAS, PREVENTIVAS E **CIBERNÉTICAS**
2. SEGURANÇA MULTIDIMENSIONAL E OS COMPLEXOS REGIONAIS DE SEGURANÇA
3. A ESCOLA DE COPENHAGEN
4. OS NOVOS ESTUDOS: O CONSTRUTIVISMO, O FEMINISMO E OS ESTUDOS DA PAZ
5. INTERVENÇÕES HUMANITÁRIAS E OPERAÇÕES DE PAZ
6. PROLIFERAÇÃO E NÃO PROLIFERAÇÃO: AS ARMAS DE DESTRUIÇÃO EM MASSA
7. O TERRORISMO INTERNACIONAL
8. TEMAS TRANSNACIONAIS: O NARCOTRÁFICO E O CRIME ORGANIZADO
9. A AGENDA NÃO TRADICIONAL: SEGURANÇA HUMANA
10. POLÍTICA DE DEFESA E SEGURANÇA INTERNACIONAL NO BRASIL

Fonte: http://concurso.unifesp.br/editais/edital520-2016.htm (grifo nosso).