RELAÇÕES INTERNACIONAIS CIBERNÉTICAS (CiberRI): O Impacto dos Estudos Estratégicos sobre o Ciberespaço nas Relações Internacionais

Gills Vilar-Lopes
Universidade Federal de Rondônia (UNIR)
gills@unir.br

Área Temática: 17
Política Internacional, Relaciones Internacionales, Política Exterior e Integración Regional: Agencia, estructura, factors exyternos y domésticos en los análisis de Relaciones Internacionales.

Trabajo preparado para su presentación en el 9º Congreso Latinoamericano de Ciencia Política, organizado por la Asociación Latinoamericana de Ciencia Política (ALACIP). Montevideo, 26 al 28 de julio de 2017.

RELAÇÕES INTERNACIONAIS CIBERNÉTICAS (CiberRI): o impacto dos estudos estratégicos sobre o ciberespaço nas Relações Internacionais[1]

Gills Vilar-Lopes[2]

Resumo: Os estudos de Relações Internacionais (RI) sobre o ciberespaço têm ganhado fôlego neste início de século. Observa-se um movimento de institucionalização sobre tal temática nas principais universidades do mundo, sem se esquecer da crescente quantidade de publicações científicas nessa área. Isso se deve, em grande parte, ao aspecto securitário que envolve tal ambiente – Segurança Cibernética –, a ponto de a comunidade epistêmica de RI já falar, até mesmo, em termos como: arma cibernética, defesa cibernética, guerra cibernética, Guerra Fria cibernética, poder cibernético e potências cibernéticas. O achado mais importante aqui – à luz do estilo qualitativo de pesquisa – diz respeito à criação e ao reconhecimento do subcampo de Relações Internacionais Cibernéticas (CiberRI) em RI.
Palavras-chave: Ciberespaço. Estudos Estratégicos. Relações Internacionais. Segurança Internacional.

***Abstract**: International Relations (IR) studies on cyberspace have boosted at the beginning of this century. It is observed an institutionalization on this subject in the world's main universities, without losing sight of growing amount of scientific publications in this area. This is due, in large part, to the security aspect surrounds such an environment - Cyber Security -, so that the IR epistemic community already so-calls even terms such as: cybernetic weapon, cyber defense, cyber warfare, cyber-Cold War, and cyber power(s). The most important finding here - in the light of the qualitative style of research - concerns the creation and recognition of the subfield of Cyber International Relations (CyberIR) in IR.*
***Keywords**: Cyberspace. Strategic Studies. International Relations. International Security.*

***Resumen**: Los estudios de Relaciones Internacionales (RRII) sobre el ciberespacio han ganado aliento a principios de este siglo. Se observa un movimiento de institucionalización sobre tal temática en las principales universidades del mundo, sin olvidar la creciente cantidad de publicaciones científicas en esa área. Esto se debe, en gran parte, al aspecto securitario que implica tal ambiente - Seguridad Cibernética -, hasta el punto de que la comunidad epistémica de RRII ya habla en términos como: arma cibernética, defensa cibernética, guerra cibernética, Guerra Fría cibernética, poder cibernético y potencias cibernéticas. El hallazgo más importante aqui – a la luz del estilo cualitativo de investigación – se refiere a la creación y el reconocimiento del subcampo de Relaciones Internacionales Cibernéticas (CiberRRII) en RRII.*
***Palabras clave**: Ciberespacio. Estudios Estratégicos. Relaciones Internacionales. Seguridad Internacional.*

---

[1] Este trabalho é uma adaptação da subseção 3.1 da Tese de Doutorado em Ciência Política, defendida por este autor junto ao Programa de Pós-Graduação em Ciência Política da Universidade Federal de Pernambuco (PPGCP-UFPE). Cf. VILAR-LOPES, 2016.

[2] Professor Adjunto de Ciência Política do Departamento de Ciências Sociais da Universidade Federal de Rondônia (DCS-UNIR). Doutor em Ciência Política (Relações Internacionais) pela UFPE. *Specialized Course* em *Cybersecurity: Issues in National and International Security* pela *National Defense University* (NDU). Currículo Lattes: http://lattes.cnpq.br/9334674406341967.

Introdução

> "*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[3]).

O subcampo internacionalista de Relações Internacionais Cibernéticas (CiberRI), que aqui se defende, não paira apenas no mundo das ideias; Ele também ganha vida mediante sua aplicação inferencial no empírico. Em outras palavras, teoria e prática se unem, à luz de elementos metateoréticos de Relações Internacionais (RI) – ontologia, epistemologia e metodologia –, para explicar acontecimentos cibernéticos, constituindo, assim, verdadeira práxis ciberinternacionalista[4].

O objetivo geral do presente trabalho é analisa o principal objeto da Ciência Política (CP), o poder, trazido aqui sob a bruma do ciberespaço. Indo além da definição de poder cibernético (*Cyber Power*), de Nye Jr (2011b), já internalizada no vocabulário dos estudos estratégicos sobre o ciberespaço, oferta-se o conceito de *Software Power* como, por que não dizer, uma instituição efetiva[5] da política internacional hodierna. De certa forma, a proposta dessa análise se reveste do mais puro ciberinternacionalismo, engendrando um conceito que só pode existir sob bases, logicamente, ciberinternacionalistas. Falar de CiberRI e não mencionar *Software Power* é o mesmo que versar sobre História das RI e não se referir à Guerra Fria.

Ampara-se metodologicamente no estilo qualitativo de pesquisa, tendo como método norteador a revisão bibliográfica. Como marco teórico, parte-se de pressupostos clássicos de CP/RI, bem de pesquisas mais recentes sobre ciberespaço no âmbito dos Estudos Estratégicos e de Segurança Internacional. Desse modo, o presente *paper* divide-se em quatro seções principais, tendo como cerne a aplicabilidade do conceito de *Software Power* na política internacional.

Poder e sua relação com a segurança 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

---

[3] 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*".

[4] Entendam-se ciberinternacionalista e ciberinternacionalismo enquanto neologismos que se relacionam, inexoravelmente, ao estudo sistemático do ciberespaço a partir de um elemento metateorético de RI.

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

invariavelmente aqueles que, do mesmo modo, designamos como 'intencionais' ou revestidos de uma intenção, de uma finalidade" (RUDNER, 1969, p. 126). Nesse sentido, quando um *software*[6] causa danos a outro *software* ou *hardware* sem que haja, para isso, *intenção*, ou seja, ocorrência de mera falha ou desatualização, não está se falando de *Software Power* nem de Segurança Internacional, mas, sim, de Segurança da Informação aplica à Computação.

Software Power, portanto, enseja uma intenção. Mais precisamente, uma intenção, como não poderia deixar de ser, política. E é a partir, sobretudo, do século XXI, que emerge um novo ambiente, totalmente artificial, em que esse tipo de interação ocorre, qual seja: o ciberespaço, e, especialmente, uma parte importante 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.

O poder, que transmudado às relações entre os Estados, é elemento-chave nos estudos de políticos e internacionalistas. Não é por acaso que Wight (2002), um dos expoentes da chamada Escola Inglesa de RI, constituiu as relações internacionais em termos de política do poder. 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, sobretudo em razão do advento do grupo terrorista *Daesh*.

Como a literatura revisada levanta, a Coreia do Norte invadiu, em 2014, inúmeros *e-mails* da Sony Corporation, expondo dados pessoais de muitos de seus clientes. Em termos econômico-financeiros, isso gerou perdas de valor da multinacional japonesa na National Association of Securities Dealers Automated Quotations (NASDAQ), levando, a efeito dominó, partes de economias nacionais que possuíam ações lastreadas naquela empresa, principalmente nos EUA. Já em termos ciberinternacionalistas, 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

[6] *Grosso modo*, entendido, aqui, como um conjunto de rotinas dispostas em linguagem de programação em um código-fonte computacional.

FRANCE-PRESSE, 2016). Em outras palavras, um acontecimento cibernético transmuda-se em estopim para disputas econômicas no complexo xadrez da política internacional. Esse exemplo é um dentre vários pelos quais se 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 Estudos Estratégicos, 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 (TI) ocorrem no seio das sociedades. É o que acontece, por exemplo, com a introdução dos seguintes artifícios bélicos: 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 – ou infraestruturas críticas – 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[...].

Não é desconhecido também 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 (2001), passando por 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 segurança –, mas possuem nomes diferentes: no âmbito interno, chama-se Segurança Pública; no externo, Defesa Nacional.[7] No primeiro caso, os órgãos de

[7] Pode-se dizer que Segurança Nacional, palavra tão em voga no período militar brasileiro e receosamente pouco utilizada nos dias atuais, é um meio termo entre ambos os conceitos analisados, pois cuida dos inimigos 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 – nas chamadas ações de garantia da leia e da ordem (GLO), constitucionalmente previstas – e nas Missões de Manutenção de Paz das Nações

investigação dão conta da tarefa; no segundo, 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, empregado, sobretudo, quando a diplomacia não encontra resultados por meio de 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, de 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; PROENÇA 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).

Esta é, em resumo, a noção *mainstream*, sobretudo dos Estudos Estratégicos 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 de CP/RI, que são o território e a soberania. Entrementes, percebe-se que, 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[8]).

***Software Power*: 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 também 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*"

Unidas. Para uma crítica à forma com que certas democracias podem invocar tal termo para se desviar de processos legislativos ordinários, ver Buzan, Wæver e Wilde (1998, p. 29).

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

(KAWAMURA, 1986, p. 35, grifo nosso). Se se assumir a tecnologia a partir dessa espécie de "não neutralidade social" de que falam Kawamura (1986) e Weber (2006), 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 dos Estudos Estratégicos. 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*.

Salienta-se que o presente trabalho opta por criar e manter tal conceito na língua inglesa por dois motivos principais. O primeiro deles diz respeito a uma possível maior aceitação da comunidade epistêmica de RI nacional e estrangeira; já o segundo motivo 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 emprega-se aqui a palavra *software* como um atributo/adjetivo (conceito-fim), e não objeto/substantivo (conceito-meio) do poder, tal como parece fazer Nye Jr (2004; 2011b) com *Soft Power* e *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 indispensável para compreender as mudanças tecnológicas pelas quais passou as sociedades nas 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 das últimas décadas.

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 *worms*, vírus e Cavalos de Troia (*Trojan*), e não em fios, roteadores e processadores. Some-se a isso o uso crescente de ataques distribuídos por negação de serviço ou *Distributed Denial-of-Service attack* (DDoS), que, há pouco tempo, eram apenas ataques por negação de serviço ou *Denial-of-Service attack* (DoS), sem o primeiro "D". Mais do que uma letra, o D de "Distribuído" representa o poder do

software (*power of software*) – no caso, rodando em um computador-mestre – sobre o *hardware*, que, também neste caso, são os computadores-zumbis. O uso de *software* por um *cracker* representa o poder do *software*; já o seu uso por um Estado contra outro, concerne ao *Software Power*. Novamente, ambos os conceitos de *hardware* e *software* estão interligados, mas, diante da observação internacionalista acerca dos acontecimentos cibernéticos mais importantes, privilegia-se, aqui, o segundo.

O conceito de *Software Power* ancora-se em premissas epistêmicas e teóricas de CP/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, grifo nosso).

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, mediante invasão e publicação de mensagens de *e-mail* de um dos candidatos, como, supostamente, aconteceram nas três últimas eleições americanas.

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. O primeiro deles diz respeito a um dos três modelos criados por Bellamy (2001), a partir dos quais a Guerra Centrada em Redes (GCR) pode ocorrer. O autor utiliza essa tipologia para, por exemplo, conjecturar sobre o uso do 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, a definição de *Software Warfare* é bastante limitada a aspectos específicos, com o escopo centrado na Internet e atrelado a combates físicos. Nesse viés, vislumbra-se tal conceito mais em *estratégias* de Defesa do que em *políticas* de Defesa, possibilidade esta

contida na definição de *Software Power*. Em breves palavras: este conceito 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 conta 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 estrategicamente. Veja-se, abaixo, um rápido exemplo de como este *case* 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 no âmbito dos Estudos de Segurança Internacional (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* (CLARKE; KNAKE, 2012; 2015), 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, ele é conhecido, na literatura revisada, 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 objeitvo 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 as de Defesa e de política 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 seção.

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 de *Hard Power* e *Soft Power*[9], volta-se à lógica e às idiossincrasias do ciberespaço.

Como sabido, no sistema internacional anárquico[10], as relações de poder ocorrem em detrimento das capacidades que cada Estado possui – tais quais as 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[11], seja na dimensão de ordem

[9] 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.

[10] 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; JERVIS, 1976, p. 62-63, 67-68, 75-76.

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

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 torna-se 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 si.

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[12], "[u]m dos paradoxos centrais na discussão de questões estratégicas[...]" (PROENÇA JR; DINIZ, 1998, p. 22), cuja expressão-mor é a corrida armamentista[13].

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, quais sejam: 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 seção anterior.

Nye Jr (2011b, p. 123, grifo nosso, tradução nossa[14]) 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 rede mundial de computadores, mas também intranets, tecnologias móveis e comunicações espaciais.

---

[12] 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, sobre isso, Jervis (1976, p. 76).

[13] Daí que a analogia a uma corrida armamentista cibernética está bastante em voga atualmente: troquem-se os exemplos dos porta-aviões pelos das armas cibernéticas.

[14] 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*".

Porém, 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 – refere-se ora a "poder cibernético", na acepção de Nye Jr (2011b, p. 123), ora a "potência cibernética"[15], em sentido bem próximo ao que Kant (2008, p. 28) e Rousseau (2003, p. 122) chamam de "potência", como uma representação juridicamente externa de um Estado frente a outros. Em todo caso, 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[16]), 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 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[17]). Essa visão política nyeiana vai, em certa medida, na mesma linha de raciocínio técnico 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, esse conceito nyeiano preocupa-se, 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

---

[15] 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).

[16] 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*".

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

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 de *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 é a ideia de rejeição de um conceito pelo outro, e sim a sua complementariedade, a ponto de se dizer que *Software Power* pode ser uma espécie de *Cyber Power 2.0*.

O *Software Power* na epistemologia 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 a sorte de conflito internacional, desde o mais brando até o mais bruto.

Dessa forma, o caso estadunidense mostra-se como paradigmático nessa seara, pois é justamente nele que, dentre outros[18], surgem: (i) a primeira rede de computadores, a Advanced Research Projects Agency Network (ARPANET); (ii) a primeira arma cibernética, o Stuxnet; (iii) o primeiro comando militar de Defesa Cibernética, o *U.S. Cyber Command* (USCYBERCOM)[19]; e (iv) o mais ambicioso esquema de espionagem internacional operado por *software* estrategicamente projetado para interceptar informações – sobretudo coleta e análise de meta-dados – no ciberespaço, delatado por Edward Snowden em 2013.

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 (DoD) apregoa que sua:

---

[18] Outras variáveis também podem ser levadas em conta para imputar àquele país a alcunha de pioneiro, 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.

[19] 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*".

> 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[20] e de Inteligência de Estado[21].

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 tratam 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 internacional, direcionando suas escolhas políticas na busca por: manter o poder, mediante preservação do *status quo*; aumentar o poder, por meio do imperialismo; ou demonstrar o poder, via diplomacia ou 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[22], 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, apenas por suas próprias capacidades cibernéticas.

Waltz (2002) complementa a ideia de Bull (2002), 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 pode também ser 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 –

---

[20] 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".

[21] Hipótese testada e não refutada, qualitativa e quantitativamente, em Lopes (2013).

[22] 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 das teorias de RI.

nesse ambiente. O exemplo do Stuxnet é novamente posto em cena para exemplificar essa máxima.

A Figura 1 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.

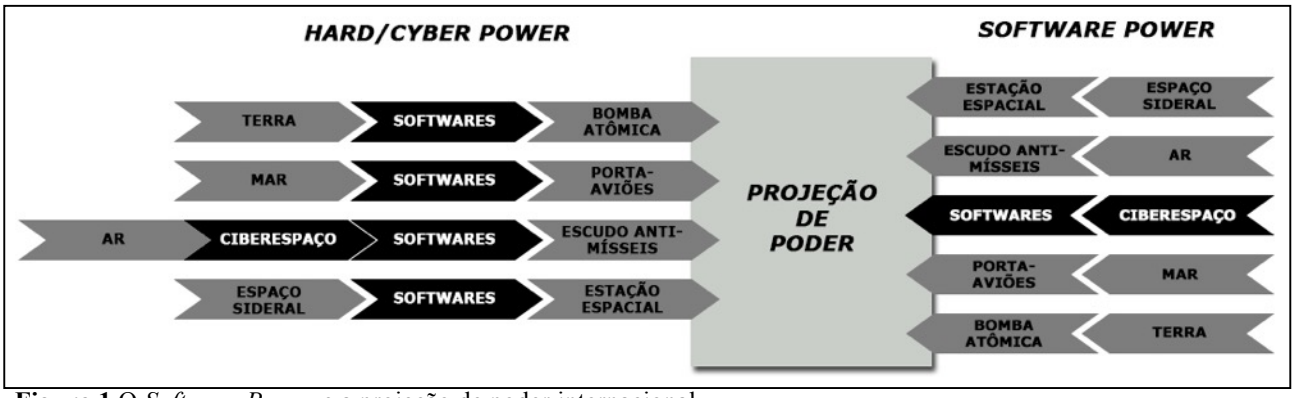

Figura 1 O *Software Power* e a projeção de poder internacional
Fonte: VILAR-LOPES, 2016, p. 107.

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*.

Considerações finais

Atualmente, é verdade que as vias clássicas de demonstração de poder – *hard* e *soft* – 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, pois suas capacidades e projeção de poder no ciberespaço não condizem com o que ocorre na política internacional real; ao contrário, é inversamente proporcional. Eis aí um caso a ser melhor analisado pela comunidade ciberinternacionalista.

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

econômicos – ou seja, em uma concepção *hard* –, mas também por intermédio da "atração"[23] que determinados valores, culturas, instituições e políticas exercem sobre os demais Estados, no que ele chama de *Soft Power*. Porém, utilizam-se essas duas vias para analisar a projeção de poder em ambientes/domínios naturais, ou seja, não criados pelo ser humano e em que a questão do tempo-espaço pode ser controlada. Contudo, 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, 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 essa 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.

Por fim, pode-se dizer que 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 aos Estudos Estratégicos e de Segurança e Defesa Cibernéticas.

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

Referências

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 abr. 2017.

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.

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

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: 8 maio 2017.

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: 2 maio 2017.

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 mar. 2017.

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

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

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

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

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: Bruno S. Guimarães *et al*. Rio de Janeiro: Brasport, 2015.

CLAUSEWITZ, Carl von. **Da guerra**. São Paulo: Tahyu, 2005.

COVARRUBIAS, Jaime G. La modernización militar. **FASOC**, ano 14, n. 1, p. 3-9, jan.-mar. 1999.

DEMCHAK, Chris C. Foreword. In: KREMER, Jan-Frederik; MÜLLER, Benedikt (Ed.). **Cyberspace and international relations**. Heidelberg: Springer, 2014. p. v-x.

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).

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 mar. 2016.

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

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).

FREITAS, Henrique; JANISSEK-MUNIZ, Raquel; BAULAC, Yves; MOSCAROLA, Jean. **Pesquisa via Web**: reinventando o papel e a ideia de pesquisa. Canoas: Sphinx, 2006.

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.

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.

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 jan. 2017.

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: 7 abr. 2017.

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 mar. 2017.

KAWAMURA, Lili Katsuco. **Tecnologia e política na sociedade**: engenheiros, reivindicação e poder. São Paulo: Ed. Brasiliense, 1986.

LIPSON, Leslie. **Os grandes problemas da Ciência Política**. Tradução de: Thomaz Newlands Neto. Rio de Janeiro: Zahar, 1967. (Biblioteca de ciências sociais).

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.

MAZANEC, Brian M. **The evolution of cyber war**: international norms for emerging-technology weapons. Lincoln, NE: Potomac Books, 2015.

MEGALE, Januário F. **Introdução às ciências sociais**. 2. ed. São Paulo: Atlas, 1990.

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 mar. 2017.

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).

NYE JR, Joseph S. **Soft power**: the means to success in world politics. Nova York: PublicAfffairs, 2004.

_____. **The future of power**. New York: Public Affairs, 2011b. cap. 5.

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.

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: 13 abr. 2017.

PROENÇA JR, Domício; DINIZ, Eugenio. **Política de Defesa no Brasil**: uma análise crítica. Brasília: Humanidade; Editora UnB, 1998.

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: Álvaro Cabral. Rio de Janeiro: Zahar Editores, 1969. (Curso moderno de Filosofia).

SANGER, David E. **Confront and conceal**: Obama's secret wars and surprising use of American power. Nova York: Crown: 2012.

SEGAL, Adam. **Cyber conflict after Stuxnet**: essays from the other bank of the Rubicon. Vienna, VI: CCSA, 2016.

SINGER, Peter W.; FRIEDMAN, Allan. **Cybersecurity and cyberwar**: what everyone needs to know. Oxford: Oxford University Press, 2014.

TUCÍDIDES. **História da Guerra do Peloponeso**. 4. ed. Tradução: Mário da G. Kury. Brasília: Editora UnB, IPRI; São Paulo: IOESP, 2001. (Clássicos IPRI, 2).

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.

VILAR-LOPES, Gills. **Relações Internacionais Cibernéticas (CiberRI)**: uma defesa acadêmica a partir dos Estudos de Segurança Internacional. 2016. Tese (Doutorado em Ciência Política) – Universidade Federal de Pernambuco, Recife, 2016.

VOEGELIN, Eric. **A nova ciência da política.** 2. ed. Tradução de: José Viegas Filho. Brasília: Editora UnB, 1982. (Pensamento político, 12).

WALTZ, Kenneth N. **Teoria das Relações Internacionais**. Tradução: Maria Luísa F. Gayo. Lisboa: Gradiva, 2002. (Trajectos, 50).

WEBER, Max. 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.

WERTHEIM, Margaret. **Uma história do espaço de Dante à Internet**. Tradução: Maria Luiza X. de A. Borges. Rio de Janeiro: Zahar, 2001.

WIGHT, Martin. **A política do poder**. 2. ed. Tradução de: Carlos S. Duarte. Brasília: Editora UnB, 2002. (Clássicos IPRI, 7).

WINAND, Érica; SAINT-PIERRE, Héctor Luis. A fragilidade da condução política da defesa no Brasil. **História**, Franca, v. 29, n. 2, dez. 2010.

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 mar. 2017.