Agenda de Pesquisa sobre o Espaço Cibernético nas Relações Internacionais

Research Agenda on Cyberspace in International Relations

Rev. Bra. Est. Def. v. 3, nº 1, jan./jun. 2016, p. 91-113
ISSN 2358-3932

LUCAS SOARES PORTELA

INTRODUÇÃO

A percepção sobre um problema ou uma questão das relações internacionais diverge de ator para ator. Encontramos algumas situações que são encaradas como temas de segurança pública e outras vislumbradas como questões de defesa nacional. As Forças Armadas Revolucionárias da Colômbia, por exemplo, são observadas pela Colômbia como uma questão de defesa ao classificá-las como um grupo terrorista, enquanto o Brasil nega esta qualificação.

Da mesma forma que a caracterização de um problema dentro das categorias tradicionais de defesa e segurança pública é complexa, a obscuridade desses dois conceitos aumenta quando tratadas no âmbito do espaço cibernético. Em virtude disso e da securitização desse tema neste século XXI, observamos uma extensão dos assuntos relacionados ao espaço cibernético, que estão além das ciências da computação e outras afins. Assim, nas Relações Internacionais notamos pesquisas de diversos temas sobre o espaço cibernético.

O intuito desse artigo é compreender a evolução quantitativa dos temas da área das Relações Internacionais publicados nos acervos da JSTOR e SciELO. Para tal, consideramos as publicações desde o início do século XXI. Para tal, abordamos os artigos publicados pela JSTOR e SciELO desde o início deste século XXI. Assim, vislumbramos os eixos de pesquisa do espaço cibernético que podem ser explorados dentro das Relações Internacionais.

A metodologia utilizada para tal é cientometria, que é utilizada para examinar o desenvolvimento e as políticas científicas. Esse método pode

Lucas Soares Portela – Mestre em Ciências Militares pela Escola de Comando e Estado-Maior do Exército (ECEME). E-mail: lsportela3@hotmail.com.

ser utilizado para estabelecer comparações entre indicadores de produções cientificas. Para tal levantamento de dados, utilizamos os bancos de dados da JSTOR e SciELO.

Além dos artigos observados nessas bases de dados, autores que discorrem sobre o espaço cibernético foram utilizados para o debate sobre esse ambiente. Dentre eles, podemos citar James Lewis (2009), Martin Libick (2009), Forrest Hare (2010), Daniel Ventre (2011), Ron Deibert (2012) e Peter Knight (2014). Cabe ressaltar que este artigo também utilizou autores das Relações Internacionais, como Joseph Nye (2012) e Fareed Zakaria (2008).

A estrutura utilizada no artigo é composta de três tópicos, além da introdução e das considerações finais. Primeiramente realizamos uma breve revisão sobre o conceito de espaço cibernético; após, dissertamos sobre os aspectos metodológicos utilizados nessa pesquisa. Por último, abordamos o espaço cibernético como objeto das Relações Internacionais, assim como as principais temáticas observadas: configuração, teoria e demais temas; política, relações entre Estados e regulamentação; e segurança cibernética[1] e defesa cibernética.[2]

CONCEITUANDO O ESPAÇO CIBERNÉTICO

Por conter uma dimensão virtual, o espaço cibernético é percebido pelo imaginário de uma sociedade, se assemelhando à Matrix[3] do filme dos irmãos Wachowski. Entretanto, este espaço é composto pela combinação de aspectos informacionais, virtuais e também de estruturas físicas. Richard Clarke (2010) é um dos autores que considera, na conceituação do espaço cibernético, aspectos tangíveis e intangíveis.

Ele conceitua o espaço cibernético como toda a rede de computadores do mundo e todas as coisas conectadas a esses aparelhos ou submetidas aos seus controles. Para esse autor, a adição de aspectos físicos que estão desvinculados da internet ao conceito de espaço cibernético é justificada pelos próprios aspectos informacionais. Por exemplo, encontramos em computadores não conectados na internet informações sobre flutuações de dinheiro, transações de créditos, comércio e até sistemas de controle de geradores e outras estruturas críticas.

Entretanto, cabe ressaltar que, no conceito acima, Clarke (2012) não aborda a figura dos usuários, que são observados na visão de Daniel Ventre (2011) sobre o espaço cibernético. Para esse pesquisador, o espaço cibernético é resultado da soma de três camadas elementares: *hardware*, *software e peopleware*. Essa composição nos permite inferir a definição do espaço cibernético abordada por Daniel Ventre (2011): conjunto de equipamentos físicos (*hardware*), que sustenta uma dimensão virtual com programas, sis-

temas, aplicativos e informações (*software*), cuja manipulação se dá por uma camada cognitiva de usuários (*peopleware*).

Cabe ressaltar que o espaço cibernético não pode ser confundido com a Cibernética, que estuda a organização e relações de controle de sistemas, conforme apontado por Heylighen e Joslyn (2001), ou seja, ela não sinônimo de espaço cibernético. Outra diferenciação necessária é entre o espaço cibernético e a internet. Conforme Clarke (2012), a internet e espaço cibernético não são sinônimos, pois toda a internet faz parte do espaço cibernético, mas nem todo espaço cibernético está conectado na internet.

A invenção do computador começa com a própria Matemática, conforme demonstrado pela obra de Cléuzio Fonseca Filho (2007), intitulada *História da Computação*. Além disso, somente na década de 30 do século passado os primeiros computadores eletromecânicos surgiram, sendo que o primeiro computador eletrônico comercialmente disponível surgiu em 1951 (Fonseca Filho 2007).

Na década de 1960, surgem alguns trabalhos que originaram a internet, e naquele momento já nos encontrávamos na segunda geração de computadores eletrônicos. Nesta mesma geração, uma rede para interconectar os computadores e permitir uma comunicação entre eles estava sendo desenvolvida por um grupo de pesquisadores do Instituto de Tecnologia de Massachusetts, conforme Knight, 2014. De acordo com ele, o conceito de computadores conectados em redes surgiu em 1962, com o trabalho de Joseph Carl Robnett.

Entretanto, a idealização da internet não se limitava à Massachusetts, pois a história da internet tem diversas ramificações. Isso é notado dentro da obra de Knight (2014), pois também aborda a criação da internet dentro do contexto europeu. Ademais, Janet Abbbate (1999) também explica que os padrões que configuram a rede é devido a um número enorme de pessoas, instituições e de diversos projetos na área.

Dentre desses projetos, vale citar aquele desenvolvido pela RAND Corporation. A financiadora dessa pesquisa foi a Força Aérea dos EUA, que precisava garantir uma resiliência durante um ataque nuclear ao território estadunidense, conforme apontado por Knight (2014). Ainda de acordo com ele, essa demanda levou Baran a trabalhar para desenvolver um sistema de comunicação descentralizado, resultando em uma série de artigos em 1964.

O produto desses trabalhos foi o primeiro protótipo da internet em 1969, chamado *Advanced Research Projects Agency Network* (ArpaNET). Sua composição era de quatro computadores localizados em universidades estadunidenses (Knight, 2014). A partir de então, novas inovações, teorias e conceitos foram incorporados à internet e aos computadores.

Em 1974, os pesquisadores Vint Cerf e Robert Kahn publicaram um artigo criando o TCP/IP (Knight 2014). Essa inovação permitiu a conexão de computadores com tecnologias distintas e que não faziam parte do projeto ArpaNET, ou seja, foi uma abertura daquela rede ao mundo (Knight 2014).

Desta forma, o espaço cibernético não é natural, como por exemplo, os espaços terrestre e aéreo, mas um espaço criado pelo próprio homem. Em virtude disso, esse espaço é distinto dos demais no que tange a interconectividade. Para Ventre (2011), o espaço cibernético transpassa todos os demais, conforme mostrado pela sua figura a seguir:

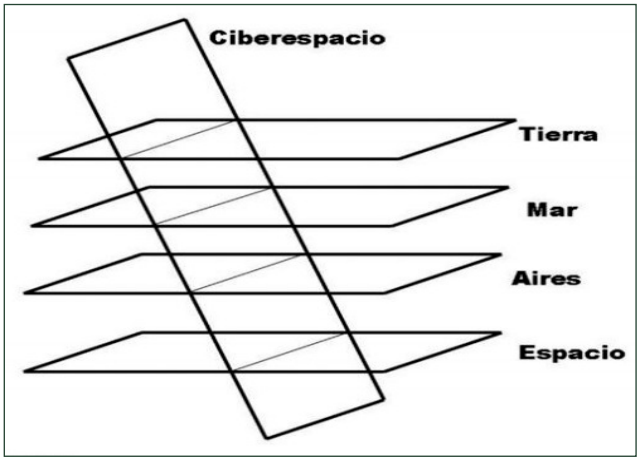

Figura 1 – Relação do Espaço Cibernético com os demais espaços geográficos
Fonte: Ventre (2012, 35).

Por meio desse argumento, Ventre (2011) explica que existem vários pontos de acesso ao espaço cibernético nos demais espaços geográficos. Além disso, de acordo com ele, por meio do espaço cibernético é possível interações entre os outros espaços. Dessa forma, algumas ações em meio virtual podem gerar consequências em meios físicos, como foi no caso do vírus Stuxnet, que colocou uma usina nuclear iraniana em situação crítica no ano de 2010.

ASPECTOS METODOLÓGICOS

O intuito desse artigo, como observado na introdução, é compreender a evolução quantitativa dos temas referentes ao espaço cibernético dentro

das Relações Internacionais. Para tal, abordamos os artigos publicados pela JSTOR e SciELO desde o início deste século XXI. Como tratamos de volume e capacidade de produção, o método de procedimento utilizado foi o cientométrico.

Esse método é utilizado para examinar o desenvolvimento e as políticas científicas, conforme Spinak (1998). Ademais, ele traduz a cientometria em análises quantitativas da economia de ciências e disciplinas. Além, conforme ainda ele, esse método pode ser utilizado para estabelecer comparações entre indicadores de produções científicas.

Ainda sobre a cientometria, podemos defini-lo como o método que mensura o progresso científico em determinada área, composta de avaliação quantitativa e comparações da área em foco, da produtividade e progresso científico (Silva e Bianchi 2001). Esse método é uma derivação da bibliometria, mas não pode confundir-se com esta. Embora ambas observem os mesmos dados, a bibliometria trata e analisa, estatisticamente, os resultados, enquanto a cientometria realiza apenas observações numéricas dos resultados (Silva e Bianchi 2001).

Os indicadores geralmente utilizados pela bibliometria podem ser divididos em quantitativos e qualitativos (Silva e Bianchi 2001). A análise quantitativa é realizada por meio do número de artigos; patentes, número de pessoas da área; e de titulações. Enquanto isso, dos indicadores qualitativos, podemos citar além do próprio texto, as referências e citações utilizadas, coautores e as instituições envolvidas.

A principal limitação da cientometria está na tentativa de comparação entre as publicações e produtividades de áreas científicas distintas (Silva e Bianchi 2001). Isso ocorre porque os hábitos de produção entre elas diferem, o que dificulta a comparação e análises. Independente disso, a cientometria auxilia na compreensão das relações de fenômenos e fatos sobre sua natureza, ocorrência e significado.

A técnica de pesquisa que será utilizada é a documentação indireta. De acordo com Marconi e Lakatos (2003), essa técnica permite reunir materiais que servem de *background* do campo de interesse. Sendo que tal técnica foi realizada por meio de fontes secundárias, ou seja, pelos artigos e livros consultados.

O universo observado é composto por 395 obras publicadas entre 2000 e 2015, sendo artigos e livros, pertencentes aos bancos de dados da JSTOR[4] e SciELO.[5] A amostra foi equivalente ao universo, pois todas as 395 obras foram observadas.[6] Para a seleção desse universo, observamos os artigos dessas bases de dados que tinham em seu título os termos "cyber" e "ciber".

Por sua vez, os artigos foram classificados dentro de três categorias de análise: configuração, teoria e demais temas; política, relações entre

Estados e regulamentação; segurança e defesa. Essas categorias foram formada após análise e agrupamento dos artigos relacionados à área de Relações Internacionais.

A filtragem dos textos ocorreu pela análise dos títulos, resumos e contexto das revistas de cada uma das produções, resultando nas três categorias anteriormente descritas. No caso dos livros encontrados nesses bancos de dados, também foram observados os índices. Quando as obras não dispunham de resumos, também eram consideradas as introduções delas.

Para considerar os artigos que correspondiam a segurança cibernética e a defesa cibernética, utilizamos as definições da União Internacional de Telecomunicação (2016) para o primeiro conceito e a visão francesa junto à Otan (2016) para o segundo. Assim, a segurança cibernética trata de temas relacionados a dimensão da segurança pública. Dessa forma, aborda questões políticas, gestão de riscos, ilícitos, melhores práticas de garantia e tecnologias, usadas para proteger o ambiente cibernético e sua organização, como também os ativos do usuário.

Sobre o zelo desse conceito, encontramos também dispositivos de computação pessoal, infraestrutura, aplicativos, serviços, sistemas de telecomunicações. Além disso, ela também observa as informações transmitidas e/ou armazenadas no espaço cibernético conectado. Cabe ressaltar que o conceito utilizado de segurança cibernética é distinto daquele que engloba a segurança nacional, ou seja, é diferente da segurança cibernética nacional, definida por exemplo, por José Brandão (2011).

Por outro lado, a definição de defesa cibernética observada é a francesa. De acordo com ela, a defesa cibernética envolve o ato de defender o sistema crítico de informação do espaço cibernético de um Estado. Dessa forma, a definição de segurança e defesa aplicada aqui no espaço cibernético segue as referências estabelecidas por Hobbes (2002) para os conceitos clássicos. A grosso modo, para esse autor, a segurança observa os aspectos legais que regulam uma dada sociedade, enquanto a defesa garante a sobrevivência do Estado.

ESPAÇO CIBERNÉTICO COMO OBJETO CIENTÍFICO

O espaço cibernético não é somente planejado pelo homem, mas também um espaço geográfico que perpassa todos os demais (Ventre 2011). Essa característica é um exemplo da abrangência desse espaço, que se aplica também a outras temáticas, como nas pesquisas científicas. Por isso, pensar no espaço cibernético como objeto exclusivo das ciências da computação é visualizá-lo limitadamente.

No caso desse artigo, pretendemos demonstrar o espaço cibernético dentro das Relações Internacionais. O intuito não é compreender como

o espaço cibernético se tornou um objeto da área, mas como ele é tratado nessa disciplina. Assim, observaremos neste tópico apenas as principais questões sobre o espaço cibernético e algumas vertentes de pesquisas dentro da área das Relações Internacionais.

Os artigos sobre espaço cibernético na área das Relações Internacionais começam a ser desenvolvidos com maior veemência durante o século XXI. Isso é possível de se observar por meio do banco de dados de artigos e livros da JSTOR e SciELO. O gráfico a seguir demonstra essa realidade:

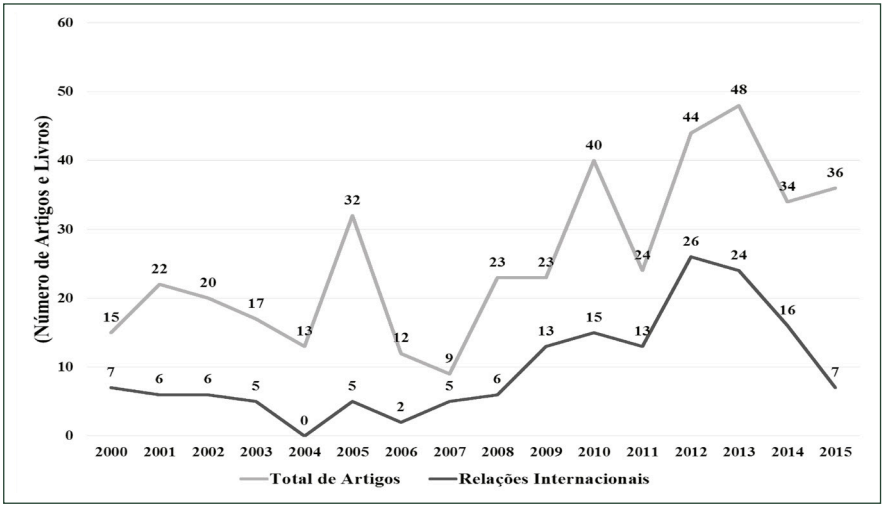

Gráfico 1 – Artigos/Capítulos da JSTOR e SciELO com Ciber/Cyber nos Títulos (2000-2015)
Fonte: Elaboração própria baseada em JSTOR (2016a, 2016b) e SciELO (2016a, 2016b).

Com o Gráfico 1 observamos que o aumento considerável das publicações de 2008 para 2009 pode ser resultado de um processo de securitização. De acordo com Forrest Hare (2010), a securitização do espaço cibernético é percebida em alguns momentos e atos, como na estratégia de defesa cibernética da Estônia, publicada em 2008. Em 2007, a Estônia foi alvo de ataques de *hackers* (O'Connel 2012), influenciando essa estratégia.

Em 2008 também foi percebido o uso do espaço cibernético como uma dimensão da guerra entre Rússia e Geórgia, em que essa sofreu alguns ataques cibernéticos (O'Connel 2012). Face esses incidentes e possíveis ameaças, os Estados Unidos criam o Comando Cibernético em 2009. Um segundo catalizador do aumento de produção pode ser percebido em 2010,

por ocasião das divulgações de documentos do Wikileaks, que revelou os processos informacionais na tomada de decisão dos Estados.

Esses fatos, em especial a manobra estadunidense e as revelações pelo Wikileaks, podem ser considerados os principais catalizadores do aumento das produções científicas observadas, que teve seu auge em 2012 e posterior processo de desecuritização. O processo de securitização do espaço cibernético, de acordo com Ron Deibert (2012), é o principal estimulador dos tomadores de decisões para o desenvolvimento de estratégias de segurança e defesa cibernética.

Ainda sobre os artigos que tratavam das relações internacionais, observamos três grandes áreas de abordagem: configuração, teoria e demais temas; política, relações entre estados e regulamentação; segurança pública e defesa nacional. Os artigos da primeira área observam como o espaço cibernético é formado, suas conceituações e temas afins. A segunda área observa estudos de casos, propostas de regulamentações, consequências delas e questões políticas.

Por sua vez, a última área, observa questões de poder, ataques, segurança e defesa cibernética, crimes cibernéticos e resiliência. Os artigos observados no gráfico anteriormente apresentado podem ser divididos da seguinte forma:

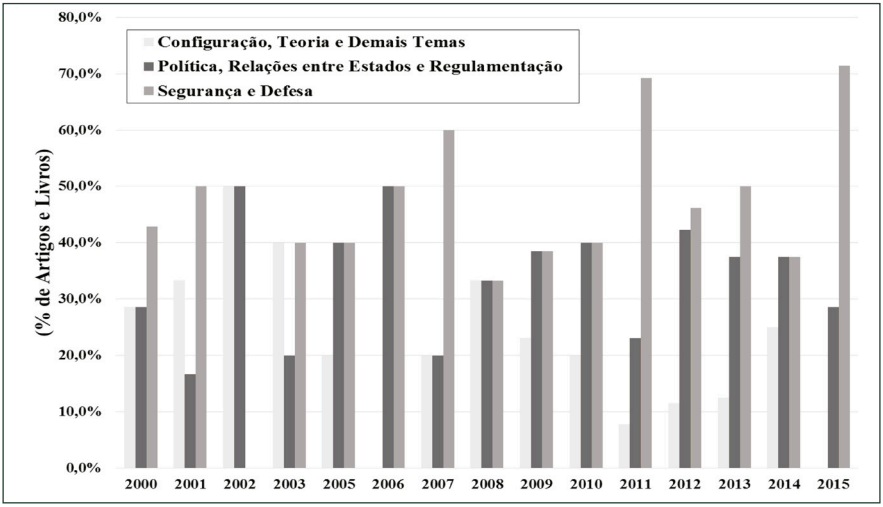

Gráfico 2 – Publicações sobre Espaço Cibernético nas Relações Internacionais (2000-2015)
Fonte: Elaboração própria baseada em JSTOR (2016a, 2016b) e SciELO (2016a, 2016b).

Além de identificar os principais temas que são pesquisados sobre o espaço cibernético nas Relações Internacionais, o Gráfico 2 nos permite compreender sobre quais temas mais se pesquisa. Dessa forma, com exceção de 2002, todos os demais anos focaram nas análises do espaço cibernético, a área de Segurança e Defesa Cibernética. Diante disso, os próximos tópicos desse artigo pretendem compreender um pouco sobre cada uma dessas áreas e posteriormente realizar uma análise mais enfática sobre as pesquisas de Segurança e Defesa Cibernética.

Configuração, teoria e demais temas

De acordo com Ventre (2011), o espaço cibernético é composto por três camadas: *hardware*, *software* e *peopleware*. A primeira camada que configura o espaço cibernético é caracterizada pelos elementos físicos. Enquanto o *hardware* é a camada física do espaço cibernético, a dimensão virtual é constituída pela camada de *software*.

Por sua vez, a categoria *peopleware*, na percepção de Ventre (2011), é a camada cognitiva do espaço cibernético, ou seja, os operadores desse espaço. Assim, embora os usuários estejam englobados na definição de espaço cibernético, eles são diferenciados das outras duas categorias. As relações entre essas camadas, assim como a individualidade de cada uma delas, são focos das pesquisas dentro dessa categoria de pesquisa sobre o espaço cibernético.

A própria internet também é foco considerado dessas abordagens. Podemos citar aqui, por exemplo, o artigo de George Barnett, Bum-Soo Chon e Devan Rosen (2001). Esse artigo observava a relação entre a internet e o espaço cibernético. De acordo com eles, o comércio de telecomunicação, comércio eletrônico, ciências e semelhantes são os componentes mais significativos da estrutura da internet.

Ainda dentro do foco de configurações do espaço cibernético e da internet, encontramos também interesse sobre as redes paralelas ou alternativas desse espaço, como por exemplo, a *Deep Web* e alguns navegadores alternativos de código aberto. A *Deep Web* é definida como uma parte do espaço cibernético que, por algum motivo, não está indexada nas ferramentas de busca, como o Google (Ciancaglini et al. 2015). A indexação consiste em incluir determinados endereços, documentos e materiais nas ferramentas de busca, facilitando o acesso por todos os usuários.

Os principais usuários que recorrem a *Deep Web* são aqueles que buscam garantir seu anonimato na rede. Em virtude disso, de acordo com Ciancaglini et al. (2015), encontramos na *Deep Web* tanto pessoas que querem proteger suas comunicações, como usuários de drogas, assassinos, hackers, jornalistas

em busca de informações privilegiadas entre outros. Essas pessoas buscam termos, assuntos e informações ilegais, que são geralmente bloqueados e também filtrados pelos veículos tradicionais (Ciancaglini et al. 2015).

A configuração do espaço cibernético também é afetada pela economia política da infraestrutura de telecomunicações, provedores de serviços e inclusão digital no mundo. Além dessas, ela também tem uma correlação com as Tecnologias da Informação e Comunicação (TICs). Assim, dentro dessa área de pesquisa também encontramos como tema a influência de novas tecnologias no espaço cibernético, porque elas trazem a necessidade de repensar esse espaço, conforme apontado por Arquilla e Ronfeldt (1997).

As pesquisas que abordam inovação tecnológica e o espaço cibernético discorre também sobre as consequências delas, não somente na configuração, mas também na regulamentação e segurança desse espaço. James Lewis (2009), por exemplo, explica que essa inovação pode ser limitada pelas regulamentações do espaço cibernético. Ainda de acordo com ele, a inovação também pode gerar segurança para o espaço cibernético, devido aos protocolos e capacidades dos novos equipamentos.

Por causa da complexidade dessas relações e do próprio espaço cibernético, outro tema de pesquisas importante são as taxonomias e teorias sobre esse espaço. Conforme apontado por Paulo Zuccaro (2011), os estudos de taxonomias não são determinantes para a política, estratégia e pesquisa, mas nos ajudam a compreender, delimitar posturas e procedimentos sobre o espaço cibernético. Essa necessidade de pesquisa engloba todo o espectro do espaço cibernético, desde economia, segurança e infraestrutura.

Sobre as tentativas de determinar taxonomias, Simmons et al. (2009) explicam que terminologias e conceitos de sucessos têm uma aceitação universal. Ademais, de acordo com o artigo deles, a taxonomia deve respeitar determinados requisitos. O artigo cita, por exemplo, a aceitação, a exclusividade, a compreensão, a inambiguidade, a usualidade, a boa definição e a empregabilidade.

Na tentativa de compreender o espaço cibernético, alguns artigos também tratam da questão teórica do espaço cibernético. Além de artigos sobre o que seria o espaço cibernético, encontramos também teorias sobre governança na era digital e soberania no espaço cibernético. Não querendo nos prolongar, o exemplo que trazemos aqui é o da Teoria do Poder Cibernético, abordado por Joseph Nye (2012).

Política, relações entre Estados e regulamentação

Inicialmente, sabemos que o embate do mundo físico com o ambiente virtual causa também litígios entre soberanias, como possíveis ataques a estru-

turas nucleares e apagões digitais. Em virtude disso, os pesquisadores desta linha tentam clarificar formas de delimitar essas soberanias e evitar novos litígios. Além desse tema, esses pesquisadores também se preocupam com os atos de guerra no espaço cibernético, ou seja, com a guerra cibernética.

De acordo com o Martin Libicki (2009), a guerra cibernética pode surgir de duas origens: deliberadamente ou por meio de crises. Ela surge quando um Estado acredita que pode adquirir vantagens de terceiros com ações dentro do espaço cibernético. Outra forma dela surgir é por meio de crises envolvendo o espaço cibernético, que ao serem escalonadas causam novas crises, resultando em um efeito cascata e desencadeando a guerra cibernética.

Os artigos sobre ela geralmente englobam as duas dimensões de seus objetivos, citados por Libicki (2009): externa e interna. De acordo com ele, a dimensão externa trata das razões para a ciberguerra, enquanto a dimensão interna do gerenciamento e ações operacionais dentro das ciberbatalhas. Além disso, elas também discutem o alcance da guerra cibernética, pois ela apresenta alguns limites, como por exemplo, não poder realizar ocupações territoriais (Libicki 2009).

Quando trata das demandas acadêmicas sobre a guerra cibernética, Arquilla e Ronfeldt (1997) elencam três principais abordagens: estudos de caso, exercícios analíticos e atores não estatais. Os estudos de caso são necessários para desenvolver uma perspectiva sobre a guerra cibernética, enquanto os exercícios analíticos permitem ao pesquisador reconhecer os casos próprios dessa guerra (Arquilla e Ronfeldt 1997). Cabe ressaltar ainda que a guerra cibernética tem um envolvimento mais enfático dos atores não estatais, sendo tal fato também objetos de pesquisa, conforme explica Arquilla e Ronfeldt (1997).

Juntamente com a área que trata as questões referentes à soberania, também observamos uma concentração de pesquisas sobre a regulamentação e marcos legais internacionais. As tentativas de regular e organizar esse espaço podem reduzir os litígios e evitar um guerra cibernética, conforme explica Clarke (2012). Ademais, essas pesquisas também observam a relação dessas normas com os interesses dos Estados, pois conforme Oran Young (1982), os regimes internacionais servem aos propósitos de algum ator, geralmente dos centros do mundo.

Entretanto, de acordo com Joseph Nye (2012), não existe uma governança sobre espaço cibernético, e sim um grupo de instituições dispersas que controla esse espaço. Ao realizar essa afirmação, Nye (2012) cita algumas ONGs que controlam esse espaço, como a W3C ou o ICANN. Embora tais instituições sejam organizações não governamentais, elas apresentam laços consideráveis com o território dos Estados Unidos.

A W3C e a ICANN nasceram dentro do projeto da ArpaNET e foram criadas no âmbito do Instituto de Tecnologia de Massachusetts e da Universidade da Califórnia do Sul, respectivamente. Ademais, as sedes dessas instituições estão localizadas em território dos Estados Unidos. Assim, podemos afirmar que ambas as instituições estão sob o domínio estadunidense.

Outro aspecto que devemos considerar sobre as entidades controladoras do espaço cibernético é a natureza delas. De acordo com Ron Deibert (2012), uma parcela significativa do espaço cibernético é de propriedade e operada pelo setor privado. Dessa forma, o espaço cibernético depende diretamente das condições dessas empresas (Deibert 2012).

Isso significa que a criação de um regime internacional sobre espaço cibernético requer a redução do controle sobre essas instituições pelos Estados Unidos. Entretanto, vale lembrar da colocação de Fareed Zakaria (2008), de que as instituições internacionais, criadas inicialmente para evitar conflitos da dimensão das Grandes Guerras Mundiais, também servem de ferramenta para a manutenção do poder dos Estados Unidos. Assim, igualmente como ocorre com o regime internacional do meio ambiente, os Estados Unidos não estão interessados em um regime internacional do espaço cibernético, pois detém as instituições mantenedoras desse ambiente (Portela 2016).

Além de observar o processo de regulamentação do espaço, como também o impacto deste nas políticas dos Estados, essa área também observa as consequências desses acordos e tratados, como também a sua implementação ou revogação. Assim, essa área observa questões tangíveis, como por exemplo, o tipo de cabo utilizado, e também questões intangíveis, como os crimes cibernéticos (Clarke 2012). Isso nos leva a outra categoria de pesquisa sobre o espaço cibernético: segurança e defesa cibernética.

Cabe ressaltar, novamente, que existem diversas abordagens do espaço cibernético como objeto científico. Richard Clarke (2012), por exemplo, explica as pesquisas sobre esse espaço por meio de uma tríade, que abarca os endereços de computadores, as regulamentações adicionais do espaço cibernético e a energia elétrica. Dessa forma, as questões observadas aqui podem ser classificadas nos dois primeiros elementos da tríade, pois são artigos diretamente relacionados ao espaço cibernético.

Para finalizar, podemos dizer, ainda, que as questões que englobam o espaço cibernético dentro das relações internacionais podem ser mais amplas quando considerarmos o terceiro elemento da tríade de Clarke (2012). Isso porque alguns artigos têm impactos sobre os estudos do espaço cibernético, sem nem abordarem esse tema em seus textos. Como exemplo disso, encontramos artigos sobre a energia elétrica dos países, que não abordam em nenhum momento o espaço cibernético, mas têm relação indireta com

este, como é o caso da pesquisa de Jacques Marcovitch (1991), intitulado "Integração Energética na América Latina".

Defesa e Segurança Cibernética

A demanda por pesquisas sobre a segurança e defesa cibernética surge tanto para debatê-las como também para distingui-las, pois elas por vezes se confundem. Sobre essas pesquisas, a área de segurança cibernética trata de temas relacionados a dimensão da segurança pública, como ilícitos e proteção do ambiente cibernético. Enquanto isso, a defesa apresenta questões próprias das relações entre os Estados, como por exemplo, o poder cibernético e guerra cibernética.

Entretanto, devemos recordar que os assuntos de segurança cibernética também são observados dentro das relações internacionais. O exemplo mais evidente foi a proposta da Alemanha e Brasil sobre privacidade da internet na Organização das Nações Unidas (ONU). Essa proposta foi feita à ONU em 2013, pouco tempo após as revelações de Snowden sobre as atividades de espionagem da NSA, e virou resolução em 2014, durante a 69ª Assembleia Geral (O Globo 2014).

Parte dos artigos observados consideravam a defesa e a segurança cibernética em uma mesma pesquisa. Isso pode ser explicado pela complexidade existente em distinguir esses dois conceitos, reflexo da própria dificuldade em definir as variações clássicas de cada um.

Embora haja essa dificuldade, a distinção entre segurança cibernética e defesa cibernética é um exercício necessário para compreender os artigos que tratam dessas duas temáticas. Para tal, cabe nesse momento, abordar os conceitos clássicos de defesa, pois eles servem de parâmetros para compreender suas derivações para o espaço cibernético. De acordo com Bobbio (1994), o conceito de defesa pode ser compreendido conforme uma gama de variações, por isso sua utilização, por vezes, pode induzir-nos ao erro.

Sobre visão militar de defesa, ela não se confirma apenas no momento da agressão, mas anterior a ela. Assim, a defesa não é somente um conceito passivo, mas também um termo ativo, pois ela emprega recursos para dissuadir possíveis agressões e ameaças. Em virtude disso, o conceito de defesa na visão de Clausewitz (1982) é diferenciado em tempos de paz e em tempos de guerra.

Dessa forma, durante o período de paz, Clausewitz (1982) explica que a defesa consiste em esperar e preparar formas de aparar um possível ataque. Por outro lado, em tempos de guerra, ela também consiste em prever a utilização de atos ofensivos. Para compreender qual postura defensiva um Estado deve adotar, ele deve conhecer os seus inimigos e quando eles irão atacar.

A necessidade de reconhecimento constitui o primeiro desafio para a compreensão desses conceitos no espaço cibernético. Isso porque se trata de um espaço em que o disfarce e o anonimato são evidentes. Em virtude disso, no espaço cibernético, um Estado deve se portar como em constante estado de guerra.

Cabe ressaltar que embora o sistema internacional provoque tensões permanentes entre atores, a manutenção de forças armadas por um Estado não o qualifica como em guerra, pois isso depende de um reconhecimento formal de seu soberano, no que entendemos como o conceito de Hugo Grócio (2004), "Direito de Guerra". Durante a II Guerra Mundial, por exemplo, a Inglaterra somente se declarou em situação de guerra após Hitler ter reconquistado a maioria dos territórios que haviam sido perdidos pela Alemanha na guerra anterior. Até então, para o ministro inglês, Neville Chamberlain, não existia uma segunda guerra na Europa, mas apenas a restituição de territórios por Hitler.

Assim, se observamos como os exércitos dos países se comportam, perceberemos diferenças entre as suas administrações quando eles reconhecem que participam de uma guerra e quando estão em período considerado de paz. Ademais, nos chamados períodos de paz, as forças armadas dos países mantém os alistamentos, treinamentos, compra de armamento, entre outros. Em contrapartida, em tempos de guerra, elas são mais agressivas, pois pretendem não somente repelir o ataque, mas também aniquilar o atacante, com ações mais ofensivas e diretas.

Seguindo esta lógica e compreendendo que os ataques cibernéticos[7] utilizados no espaço cibernético são frutos de informações, a defesa cibernética depende também de gestão de dados (Gama Neto e Lopes 2014). Assim, o conceito de defesa cibernética é abordado por Paulo Sérgio de Melo Carvalho (2011) da seguinte forma:

Defesa Cibernética – Conjunto de ações defensivas, exploratórias e ofensivas, no contexto de um planejamento militar, realizadas no espaço cibernético, com as finalidades de proteger os nossos sistemas de informação, obter dados para a produção de conhecimento de inteligência e causar prejuízos aos sistemas de informação do oponente. No contexto do preparo e emprego operacional, tais ações caracterizam a Guerra Cibernética (Carvalho 2011, 18).

Por meio dessa citação, entendemos que a defesa tem uma relação direta com a guerra, os interesses nacionais, garantia da sobrevivência e da soberania.

Outra definição que discutiremos aqui, por exemplo, é aquela dada por Myriam Cavelty (2012). Quando ela trata da definição de segurança e defesa cibernética, nos explica que ela pode ser enquadrada em três abordagens distintas: técnica, crimes-espionagem e defesa militar/civil. Cada

uma dessas abordagens apresenta atores, referenciais e ameaças distintas, conforme o quadro a seguir:

QUADRO 1 – Alternativas de discursos para segurança cibernética

	Técnica	**Crimes-Espionagem**	**Defesa militar/civil**
Atores principais	Especialistas em computadores e indústrias de antivírus	Aplicação da lei e comunidade de inteligência	Especialistas em segurança nacional, militares, defesa civil e segurança interna
Principal objeto de referência	Computadores e redes de computadores	Rede privada e pública	Rede das forças armadas e infraestrutura crítica
Principais ameaças	Malwares, hackers e interrupções de rede	Ameaças persistentes avançadas, crimes cibernéticos, mercenários cibernético, Estados (inteligências estrangeiras)	Ataques a infraestruturas críticas, terrorismo cibernético e Estados (comandos cibernéticos)

Fonte: Elaboração própria baseada em Cavelty (2012).

Essa mesma autora explica que modos de enquadramento de ameaças e riscos cibernéticos podem, com certos limites, ser uma questão de escolha. Da mesma forma, a definição de segurança cibernética pode ser observada conforme o objetivo de pesquisa. Cabe ressaltar, entretanto, que as abordagens não se anulam, mas no caso das Relações Internacionais, a definição que mais se relaciona é a terceira, defesa militar/civil.

Essa abordagem engloba tanto as definições de segurança cibernética, quanto de defesa cibernética. A segurança cibernética é definida quando os atores principais são a defesa civil e a segurança interna, cuja referência são as infraestruturas críticas e as ameaças/ataques a esta. Por sua vez, a defesa cibernética tem relação com os especialistas em segurança nacional e militares, com referência na rede das forças armadas e terrorismo cibernético e ataque ao Estado.

Cabe ressaltar que algumas estratégias, como a *Comprehensive National Cybersecurity Initiative*, de Barack Obama, abordam a guerra cibernética no âmbito da segurança cibernética. Tal abordagem pode dificultar a diferenciação entre segurança cibernética e defesa cibernética, mas cabe observar que isso é fruto de um processo de militarização de temas. De acordo com Mary O'Connell (2012), os Estados Unidos tem militarizado os temas de segurança cibernética, de forma que aborda as questões dela com recursos e ações militares.

Mediante tais colocações, se retornarmos aos artigos observados na coleta de dados da JSTOR e da SciELO e separar aqueles referentes à Defesa Cibernética e os de Segurança Cibernética, obteremos a seguinte tabela:

TABELA 1 – Publicações de Segurança e Defesa Cibernética na JSTOR e SciELO (2000-2015)

	2000	**2001**	**2002**	**2003**	**2004**	**2005**	**2006**	**2007**	**Total**
Defesa Cibernética	1	1	0	1	0	1	1	1	6
Segurança Cibernética	2	2	0	1	0	1	0	2	8
	2008	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**Total**
Defesa Cibernética	1	2	4	3	8	5	4	4	31
Segurança Cibernética	1	3	2	6	4	7	2	1	26
Artigos de Defesa Cibernética: 37				Artigos de Segurança Cibernética: 34					

Fonte: Elaboração própria baseada em JSTOR (2016a, 2016b) e SciELO (2016a, 2016b).

Mediante a Tabela 1, percebemos que há um equilíbrio relativo sobre a produção em Defesa Cibernética e em Segurança Cibernética entre os anos de 2000 e 2015. Ademais, embora a produção de Defesa Cibernética tenha superado a de Segurança Cibernética apenas nos anos de 2010, 2012, 2014 e 2015, no total encontramos mais artigos de defesa do que de segurança cibernética. Cabe ressaltar, ainda, que alguns dos artigos consultados podem ser englobados em ambas as categorias, sendo contabilizados em ambas.

CONSIDERAÇÕES FINAIS

Quando comparado com os demais espaços geográficos, a primeira particularidade do espaço cibernético que devemos ressaltar é a relação dele com os seres humanos. Ele não foi somente criado pelo ser humano, mas explorado desde seu início. Ademais, esse espaço perpassa por todos os demais espaços geográficos.

Surgido na segunda metade do século passado, o espaço cibernético intriga pesquisadores de diversas áreas, principalmente por causa do seu ineditismo e seu caráter abstrato. Prova disso foi a sua própria criação, resultado de diversas pesquisas acadêmicas, artigos e produções científicas. Além disso, ele não é objeto de apenas algumas áreas acadêmicas, mas perpassa por todas elas, desde as ciências da computação até as ciências sociais.

O impacto da produção científica sobre espaço cibernético nas Relações Internacionais começa a ser notado com maior veemência no início do século XXI. Entretanto, esse aumento não é exclusivo dessa área, pois os

dados coletados demonstraram um aumento diretamente proporcional das produções das Relações Internacionais em comparação com o valor total de artigos e livros sobre o espaço cibernético.

As produções observadas sobre espaço cibernético se concentravam em três grandes conjuntos: configuração, teoria e demais temas; política, relações entre estados e regulamentação; segurança pública e defesa nacional. Assim, as pesquisas observadas sobre o espaço cibernético nas Relações Internacionais podem ser resumidas pelo seguinte quadro:

QUADRO 1 – Pesquisa sobre Espaço Cibernético nas Relações Internacionais

Área de Concentração		**Alguns Temas Abordados**
1	Configuração, teoria e demais temas	- Organização e delimitação de limites - Entrave entre um espaço em período feudal e um mundo globalizado - Influência de novas TICs nas relações internacionais
2	Política, relações entre Estados e regulamentação	- Organização jurídica do espaço cibernético e suas denotações e consequências - Entraves entre soberanias do espaço cibernético - Presença de Estado no espaço cibernético - Privacidade e liberdade do indivíduo
3	Segurança e defesa	- Litígios e crimes cibernéticos - Vulnerabilidades - Resiliência da rede - Ciberguerra - Espionagem e invasão

Fonte: Elaboração própria baseada em JSTOR (2016a, 2016b) e SciELO (2016a, 2016b).

Dessas áreas de concentração, a última teve um número elevado de produções. Assim, dos artigos observados, os que tratavam da segurança e defesa cibernética ganham maior evidência, reflexo de um espaço cibernético propício a crimes e conflitos entre Estados. Esse aumento também é reflexo da securitização desses temas em algumas ocasiões, como em 2008 e 2009, face a guerra Rússia-Geórgia e criação do Comando Cibernético pelos Estados Unidos.

Ademais, quando tratados como temas separados, a segurança cibernética e a defesa cibernética apresentam um número semelhante de produções no século XXI. Entretanto, parte considerável das produções abordou as duas temáticas no mesmo texto, que é reflexo da dificuldade em perceber separadamente a segurança pública e a defesa nacional dentro do espaço cibernético. Ao tentar realizar essa distinção, esse artigo compreende

que a defesa cibernética tem uma relação direta com a guerra, defesa dos interesses nacionais, garantia da sobrevivência e da soberania. Por sua vez, a segurança cibernética está relacionada com todos os litígios que podem ameaçar o ambiente cibernético de um Estado.

Finalmente, a complexidade das camadas do espaço cibernético permite aos pesquisadores da área das Relações Internacionais tratarem de uma vasta gama de temas. Além disso, as principais análises sobre a defesa e a segurança cibernética surgem como as principais áreas de pesquisa das Relações Internacionais sobre o espaço cibernético. Entretanto, essas produções são condicionadas pela securitização e desecuritização dessas duas temáticas.

REFERÊNCIAS

Abbate, J. 1999. *Inventing the Internet*. Cambridge: MIT Press.

Arquilla, J., Ronfeldt, D. 1997. *Cyberwar is Coming*. National Security Research Division. Estados Unidos: RAND Corporation.

Barnett, G., Chon, B.-S., Rosen, D. 2001. *The Structure of the Internet Flows in Cyberspace*. Networks and Communication Studies, 15 (1-2). França: Netcom.

Bobbio, N. 1994. *Dicionário de política*. 6. ed. Brasília: Editora Universidade de Brasília.

Brandão, J. E. M. de S. 2011. Uso de redes sociotécnicas para a segurança cibernética nacional. In: Barros, O. S. R. (Org.). *Desafios estratégicos para segurança e defesa cibernética*. Brasília: Secretária de Assunto Estratégicos da Presidência da República

Cavelty, M. D. 2012. *The militarisation of Cyberspace:* why less may be better. 4th International Conference on Cyber Conflict. Estonia: Nato.

Carvalho, P. S. M. de 2011. Conferência de Abertura: o setor cibernético nas forças armadas brasileira. In: Barros, O. S. R. (Org.). *Desafios estratégicos para segurança e defesa cibernética*. Brasília: Secretária de Assunto Estratégicos da Presidência da República.

Ciancaglini, V., Balduzzi, M., Mcardle, R., Goncharov, M. 2013. *Deepweb and Cybercrime:* It's Not All About TOR. Trend Micro Research Paper. Tóquio: TrendMicro.

Clarke, R. A. 2012. *Cyber War:* the next threat to national security and what to do about it. New York: HarperCollins Publishers.

Clausewitz, C. V. 1982. *On War*. Reino Unido: Penguin Books Limited.

Deibert, R. 2012. *Distributed Security as Cyber Strategy:* Outlining a Comprehensive Approach for Canada in Cyberspace. Canada: Canadian Defence & Affairs Institute.

Fernandes, J. P. T. 2012. A ciberguerra como uma nova dimensão dos conflitos do século XXI. *Revista Relações Internacionais*, 33.

Fonseca Filho, C. 2007. *História da Computação:* O caminho do Pensamento e da Tecnologia. Porto Alegre: EDIPUCRS.

Gama Neto, R. B., Lopes, G. V. 2014. Armas Cibernéticas e Segurança Internacional. In: Medeiros Filho, O., Ferreira Neto, W. B., Gonzales, S. L. de M. (Org.). *Segurança e Defesa Cibernética:* da fronteira física aos muros virtuais. Coleção I - Defesa e Fronteiras Cibernética Pernambuco: Editora UFPE.

Grotius, H. 2004. *O Direito da Guerra e da Paz*. Ijuí: UNIJUÍ.

Hare, F. 2010. *The Cyber Threat to National Security:* Why can't we agree. Conference on Cyber Conflict. Estonia: CCDCOE.

Hobbes, T. 2002. *Leviatã*: ou a matéria, forma e poder de um Estado eclesiástico e civil. São Paulo: Martin Claret.

Jstor. 2016a. Search: Ciber. *Banco de dados de Revistas Científicas*. Nova York: Ithaca Harbors. Disponível em: <http://www.jstor.org/action/doAdvancedSearch?c6=AND&sd=&q5=&isbn=&f0=ti&q6=&q2=&f4=all&group=none&q3=&q1=&c2=AND&c4=AND&la=&ed=&f6=all&q4=&f3=all&f2=all&pt=&acc=off&f5=all&q0=ciber&c3=AND&c1=AND&c5=AND&f1=all>. Acesso em: 18 jan. 2016.

_____. 2016b. Search: Cyber. *Banco de dados de Revistas Científicas*. Nova York: Ithaca Harbors. Disponível em: <http://www.jstor.org/action/doAdvancedSearch?Search=&acc=off&f1=all&q6=&la=&c4=AND&c1=AND&ed=&c2=AND&group=none&f4=all&sd=&c6=AND&f3=all&q0=cyber&f2=all&q3=&pt=&c5=AND&f6=all&q2=&q1=&c3=AND&f5=all&isbn=&f0=ti&q5=&q4=>. Acesso em: 18 jan. 2016.

Heylighen, F., Joslyn, C. 2001. Cybernetics and Second-Order Cybernetics. In: Meyers, R. A. (Ed.). *Encyclopedia of Physical Science & Technology*. New York: Academic Press.

Knight, P. T. 2014. *A Internet no Brasil:* Origens, Estratégia, Desenvolvimento e Governança. Indiana: AuthorHouse.

Lewis, J. 2009. *Innovation and Cybersecurity Regulation*. Commentary. Washington: Center for Strategic & International Studies.

Libick, M. 2009. *Cyberdeterrence and cyberwar*. Pittsburgh: Rand Corporation.

Marconi, M. de A., Lakatos, E. M. 2003. *Fundamentos de Metodologia Científica*. 5. ed. São Paulo: Editora Atlas.

Marcovitch, J. 1991. Integração energética na América Latina. *Revista Brasileira de Energia*, 1 (3).

Nye, J. S. 2012. *O futuro do poder*. São Paulo: Benvirá.

O'Connel, M. E. 2012. Cyber Security without Cyber War. *Journal of Conflict & Security Law*, 17 (2): 187-209.

O Globo. Onu aprova resolução proposta por Brasil e Alemanha sobre privacidade on-line. *O Globo*. Rio de Janeiro, 27 nov. 2014. Disponível em: <http://oglobo.globo.com/sociedade/tecnologia/onu-aprova-resolucao-proposta-por-brasil-alemanha-sobre-privacidade-on-line-14678862> Acesso em: 22 ago. 2015.

Otan. 2016. *Cyber Definitions*. Resources. Estonia: CCDCOE. Disponível em: <https://ccdcoe.org/cyber-definitions.html> Acesso em: 13 mar. 2016.

Portela, L. S. 2015. *Movimentos centrais e subjacentes no espaço cibernético do século XXI*. Dissertação de Mestrado em Ciências Militares. ECEME, 2016.

Scielo. 2016a. Pesquisa Artigo: Ciber. *Banco de Dados da Scientific Electronic Library Online*. São Paulo: SciElo. Disponível em: <http://search.scielo.org/?q=ciber&where=ORG>. Acesso em: 15 jan. 2016.

_____. 2016b. Pesquisa Artigo: Cyber. *Banco de Dados da Scientific Electronic Library Online*. São Paulo: SciElo. Disponível em: <http://search.scielo.org/?q=cyber&where=ORG>. Acesso em: 15 jan. 2016.

Silva, J. A. da, Bianchi, M. de L. P. 2001. *Cientometria*: a métrica da ciência. Paidéia, 11 (20).

Simmons, C., Ellis, C., Shiva, S., Dasgupta, D., Wu, Q. 2009. *AVOIDIT*: A Cyber Attack Taxonomy. Department of Computer Science. Tennessee: University of Memphis.

Spinak, E. 1998. Indicadores cienciométricos. *Ciência da Informação*, 27 (2).

Ventre, D. 2011. Ciberguerra**.** In: Academia General Militar. *Seguridad global y potências emergentes em um mundo multipolar*. XIX Curso Internacional de Defensa. Espanha: Universidad Zaragoza.

UIT. 2016. *Definition of cybersecurity*. Study Group 17. Suíça: ONU. Disponível em: <http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx>. Acesso em: 15 mar. 2016.

Young, O. R. 1982. Regime Dynamics: the Rise and Fall of International Regimes. *International Organization*, 36 (2).

Zakaria, F. 2008. *O mundo pós-americano*. São Paulo: Companhia das Letras.

Zuccaro, P. M. 2011. Tendência Global em Segurança e Defesa Cibernética: Reflexões sobre a proteção dos interesses brasileiros no ciberespaço In: Barros, O. S. R. (Org.). *Desafios estratégicos para segurança e defesa cibernética*. Brasília: Secretária de Assunto Estratégicos da Presidência da República.

NOTAS

1. Segurança Cibernética trata de temas relacionados a dimensão da segurança pública, por exemplo, questões políticas, gestão de riscos, ilícitos, melhores práticas de garantia e tecnologias, usadas para proteger o ambiente cibernético e sua organização.
2. De acordo com ela, a defesa cibernética envolve o ato de defender o sistema de informação crítico do espaço cibernético de um Estado.
3. O filme retrata o espaço cibernético como uma dimensão negra com letras verdes flutuando alternadamente de cima para baixo e de baixo para cima.
4. Criado pela Fundação Andrew W. Mellon, a JSTOR é uma biblioteca online de artigos e periódicos acadêmicos. Ela está sediada nos Estados Unidos.
5. Biblioteca eletrônica brasileira criada pela Fundação de Amparo à Pesquisa de São Paulo, em parceria com o Centro Latino-Americano e do Caribe de Informação em Ciências da Saúde.
6. Listagem completa dos artigos observados disponível nos links das referências JSTOR (2016, 2016a) e SciELO (2016, 2016a).
7. De acordo com Martin Libick (2009), o ataque cibernético pode ser caracterizado como a interrupção ou corrupção de um sistema por um Estado.

AGENDA DE PESQUISA SOBRE O ESPAÇO CIBERNÉTICO
NAS RELAÇÕES INTERNACIONAIS

RESUMO

O objetivo deste artigo é vislumbrar as pesquisas sobre espaço cibernético nas Relações Internacionais. A metodologia utilizada para tal é a cientometria, com uso de dados sobre produções científicas na JSTOR e SciELO. Conclui-se que o maior número de produções na área é em defesa e segurança cibernética.

Palavras-chave: Relações Internacionais; Espaço Cibernético; Defesa Cibernética; Segurança Cibernética.

ABSTRACT

This article aims to glimpse the research on cyberspace in the International Relations field. The methodology used for this is the literature review and the collection of data on scientific production in JSTOR and SciElo. We conclude that the largest number of productions in the area is in defense and cyber security.

Keywords: Defense; Cyberdefense; International Relations.

Recebido em: 05/02/2016. Aceito para publicação em: 11/05/2016.