UNIVERSIDADE DE BRASÍLIA
INSTITUTO DE RELAÇÕES INTERNACIONAIS
PROGRAMA DE PÓS-GRADUAÇÃO EM RELAÇÕES INTERNACIONAIS

ILANA DANIELLE SOARES SANTOS

CONFLITOS CIBERNÉTICOS:
A ASCENSÃO DO CIBERESPAÇO SEGUNDO A PRODUÇÃO CIENTÍFICA DE RELAÇÕES INTERNACIONAIS INDEXADA NA *WEB OF SCIENCE*

BRASÍLIA
2021

ILANA DANIELLE SOARES SANTOS

Conflitos cibernéticos: A ascensão do ciberespaço segundo a produção científica de Relações Internacionais indexada na *Web of Science*

Dissertação apresentada ao Programa de Pós-Graduação em Relações Internacionais do Instituto de Relações Internacionais da Universidade de Brasília, como requisito parcial para a obtenção do título de Mestre em Relações Internacionais. Linha de pesquisa: Política Internacional Comparada.

Orientadora: Profª Drª Cristina Y. A. Inoue

Brasília, 2021

ILANA DANIELLE SOARES SANTOS

Conflitos Cibernéticos: A ascensão do ciberespaço segundo a produção científica de Relações Internacionais indexada na *Web of Science*

Dissertação apresentada ao Programa de Pós-Graduação em Relações Internacionais do Instituto de Relações Internacionais da Universidade de Brasília, como requisito parcial para a obtenção do título de Mestre em Relações Internacionais. Linha de pesquisa: Política Internacional Comparada

Orientadora: Profª Drª Cristina Y. A. Inoue

BANCA EXAMINADORA

_____

Professora Dra. Cristina Yumie Aoki Inoue
Instituto de Relações Internacionais – UnB
Orientadora

_____

Professor Dr. Antônio Jorge Ramalho da Rocha
Instituto de Relações Internacionais – UnB
Membro

_____

Professor Dr. Robson de Oliveira Albuquerque
Departamento de Engenharia Elétrica – Faculdade de Tecnologia – UnB
Membro

_____

Professora Dra. Maria Helena de Castro Santos
Instituto de Relações Internacionais – UnB
Suplente

Brasília, 2021

Para meus pais.

AGRADECIMENTOS

Agradeço primeiramente a meu marido Erick e a nossos filhos Luísa e Lucas. A Erick agradeço não apenas pelo incentivo, pela compreensão com as ausências necessárias à frequência às aulas e à elaboração desta dissertação, mas também pelos *insights*, pelas inúmeras revisões, por sua habilidade com tabelas que muito me ajudou e sobretudo por ser um marido e pai tão presente, com quem divido tão equilibradamente quanto podemos as atribuições familiares, na prática viabilizando minha participação no mestrado. Muito obrigada, Love.

A Luísa e Lucas agradeço acima de tudo pelos beijinhos. Sem os beijinhos eu jamais teria sido capaz de atravessar essa maratona que tem sido o mestrado. Eles são a minha água. Aliás, são também meu ar. Minha terra. E o meu fogo. Estão ambos avisados que na hipótese de aprovação desta dissertação substituirão "mamãe" por "mestra!" ao que eu responderei "uaalllarr" em prol do humor.

Agradeço, portanto, e imensamente, às mulheres que cuidaram dos meus filhos nos momentos em que eu estava envolvida com o trabalho, os estudos e as palavras. Nominalmente a Maria do Socorro Cardoso Alves, a Vanessa Rejane Fernandes de Oliveira e a Valquíria Fernandes Batista, pelo cuidado e ternura devotados, muitíssimo obrigada.

A meus pais Francineide e João Batista, meu agradecimento fundamental. Sem vocês eu não seria. Cogitei escrever eu "nem sequer" seria, mas que injustiça monumental, porque ser não é pouca coisa, pelo contrário, é tudo. Obrigada pela vida e por me proporcionarem uma tão farta de amor, aquele amor bom que tem carinho, que tem limite, tem incentivo, tem escuta, tem chamada de atenção e tem confiança. Obrigada por suas próprias jornadas, que aventureiras viagens trouxeram uma neta do vovô Chico e da vovó Maroca – um agricultor e uma costureira dos povoados do Canto do Ferreiro e Detrás do Coco, interior do Piauí – a defender uma dissertação sobre relações internacionais no ciberespaço!

Obrigada aos meus irmãos Italo, Iluska e Iury. Só irmão entende mesmo o jeito um do outro. Obrigada por me dar sentido.

À minha sogra agradeço a inspiração. Sua paixão e seu conhecimento por Shakespeare, pela Universidade e pelos estudantes levantam qualquer um da cadeira catar um livro e estudar.

Agradeço à minha orientadora Professora Cristina, pelos ensinamentos, pelo direcionamento e pela serenidade. De um jeito peculiar, porque muito espontâneo e calmo, acho que "clicamos", e considero minha experiência como sua orientanda muito feliz.

Agradeço também à banca examinadora da defesa do projeto de pesquisa, a Professora Danielly Silva Ramos e o Professor Antônio Jorge Ramalho. Suas considerações na defesa do

projeto melhoraram significativamente este trabalho e aumentaram meu comprometimento. Muito obrigada!

Agradeço, finalmente, aos colegas de aulas, pelas experiências compartilhadas. Aos colegas de trabalho, que muito contribuíram com a elucidação de dúvidas de natureza técnica. A todos os professores que encontrei e reencontrei durante o curso, nominalmente nas figuras de duas professoras brilhantes e mulheres inspiradoras, a professora Norma Breda dos Santos e a professora Maria Helena de Castro Santos. Foi um privilégio vê-las brilhar!

“Quem é que agora está cantando acalantos pra cabeça do século? Ô de marré, de marré deci
Quem é que está fazendo pesadelos na cabeça do século? Ô de marré, de marré deci
Quem é que está passando dinamite na cabeça do século? Ô de marré, de marré deci”

Tom Zé

RESUMO

Esta dissertação apresenta um estudo exploratório de interpretações das Relações Internacionais (RI) sobre a ascensão do ciberespaço. Busca-se identificar tendências gerais dessa produção científica por meio da análise bibliométrica de documentos indexados na *Web of Science* (WoS), bem como identificar, sistematizar e discutir seus principais conceitos e debates por meio da revisão sistemática do núcleo dessa amostra bibliográfica – selecionado conforme os critérios de número de citações e vínculos de citações. Os resultados alcançados apontam para a concentração da literatura de RI sobre a ascensão do ciberespaço indexada na WoS no tema Conflitos Cibernéticos e na subárea de Segurança Internacional; para um processo de amadurecimento do campo de estudos, com conceitos e debates em evolução e a emergência de estudos críticos às perspectivas de guerra cibernética levantadas na literatura inicial; e para a escassez de análises sobre terrorismo cibernético e guerra informacional na amostra bibliográfica revisada. Os esforços aqui empreendidos servem à contextualização do tema e visam contribuir com a elaboração de estudos subsequentes e com a propositura de uma agenda de pesquisa passível de aprofundamento posterior.

Palavras-chave: Ciberespaço. Conflito cibernético. Guerra cibernética. Segurança internacional.

ABSTRACT

This master's thesis presents an exploratory study of International Relations (IR) approaches regarding the rise of cyberspace. It aims to identify general trends in IR literature on the topic through the bibliometric analysis of a sample of documents indexed in the Web of Science (WoS) database, as well as to identify, systematize and discuss the main concepts and debates derived of the core of this bibliographic sample – selected according to number of citations and citation links. The results point to the concentration of IR literature on the rise of cyberspace indexed in WoS in the theme cyber conflicts and in the sub-area of International Security; also, to the evolution of concepts and debates and the emergence of approaches critical to the cyberwar perspectives raised in the initial literature; and to the paucity of analyzes on cyberterrorism and information warfare in the revised bibliographic sample. The efforts here undertaken contextualize the theme and aim to contribute to the elaboration of subsequent studies and to the establishment of a research agenda that can be further deepened.

Keywords: Cyberspace. Cyber Conflict; Cyberwar. International Security.

LISTA DE FIGURAS

Figura 1 Visualização da rede de produção científica sobre fenômenos cibernéticos nas RI

Figura 2 Diagrama resultante da análise dos resultados da busca na WoS por documentos contendo cyber ou cyber* no campo “Tópico”, da área de Relações Internacionais, com o mínimo de 5 citações, pelo VosViewer, com base na funcionalidade Análise de Citação do software.

Figura 3 Núcleo da rede bibliográfica identificada na WoS após análise bibliométrica pelo VosViewer

Figura 4 Nuvem de palavras representando o peso das principais palavras-chave indexadas nos artigos da amostra bibliográfica inicial.

LISTA DE GRÁFICOS

Gráfico 1 Taxas de penetração da internet por regiões geográficas (estimativas de outubro de 2020)
Gráfico 2 Publicação de estratégias nacionais de segurança cibernética por ano
Gráfico 3 Evolução quantitativa da produção científica de RI indexada na WoS por tipo de documento
Gráfico 4 Número de documentos por idioma de publicação

LISTA DE TABELAS

Tabela 1 Quadro-resumo de dados bibliométricos

Tabela 2 Número de documentos publicados por ano por tipo de documento (1996-2020)

Tabela 3 Número de documentos por número de citações

Tabela 4 Número de artigos publicados por periódico

Tabela 5 Número de *proceeding papers* publicados por veículo de publicação

Tabela 6 Resenhas de livros publicadas por veículo de publicação

Tabela 7 Número de publicações por área de pesquisa entre 1996 e 2020

Tabela 8 Palavras-chave mais frequentes e número de vezes em que foram indexadas

Tabela 9 Quadro-resumo de dados bibliométricos da amostra bibliográfica final

Tabela 10 Quadro-resumo das definições conforme elementos constituintes

Tabela 21 Quadro-resumo dos artigos por paradigma da RI dominante

Tabela 12 Amostra bibliográfica inicial

Tabela 13 Amostra bibliográfica final

Tabela 14 Textos adicionados discricionariamente na amostra bibliográfica final

LISTA DE ABREVIATURAS E SIGLAS

APT	Advanced Persistent Threat
C2	Comando e controle
C3I	Comando, controle, comunicações e informação
C4ISR	Comando, Controle, Comunicações, Computadores, Inteligência, Vigilância e Reconhecimento
CCDCOE/OTAN	Cooperative Cyber Defence Centre of Excellence da OTAN
CNA	Computer Network Attacks
CNE	Computer Network Exploitation
CSNU	Conselho de Segurança das Nações Unidas
DDoS	Distributed Denial of Service
DoS	Denial of Service
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
OEWG	Open-ended Working Group on Developments in the Field of ICTs in the Context of International Security
RMA	Revolution in Military Affairs
TTP	Táticas, técnicas e procedimentos
UNGGE	United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.

SUMÁRIO

INTRODUÇÃO 17

Um pouco de história 17

Novas tecnologias 22

Internet das coisas 23

Big Data 23

Inteligência artificial 24

Biotecnologia 24

Blockchain 25

Criptoativos 26

Interpretações para a ascensão do ciberespaço 27

A abordagem do ciberespaço nas RI 30

Breve descrição de casos paradigmáticos 33

Estônia (2007) 33

Geórgia (2008) 34

Stuxnet (2010) 34

Vazamentos da NSA (2013) 35

APT 01 (2013) 36

Guerra russo-ucraniana (2014) 36

Eleições presidenciais dos EUA (2016) 37

Necessidade de sistematização 37

Estrutura desta Dissertação 41

1. CONSIDERAÇÕES METODOLÓGICAS E ANÁLISE BIBLIOMÉTRICA 43

1.1. Considerações Metodológicas 43

1.1.1. Defesa da análise bibliométrica 43

1.1.2. Revisão sistemática de literatura e teoria do enfoque meta-analítico. 43

1.1.3. Amostra bibliográfica inicial e amostra bibliográfica final 46

1.1.4. Detalhamento da definição das amostras bibliográficas....47
1.1.4.1. Parâmetros de busca....47
1.1.4.2. A criação da tabela (arquivo .xlsx) para "manuseio" dos dados bibliométricos 47
1.1.4.3. A definição da amostra bibliográfica final....48
1.1.5. Seções da revisão sistemática de literatura....52
1.1.5.1. Conceitos....53
1.1.5.2. Debates....54
1.1.6. Limites desta revisão sistemática de literatura....54
1.2. Análise bibliométrica: O panorama da produção científica de RI 57
1.2.1. Evolução numérica da produção científica de RI sobre questões cibernéticas ..57
1.2.2. Número de documentos por idioma....60
1.2.3. Número de documentos por número de citações....61
1.2.4. Número de documentos por veículo de divulgação....61
1.2.5. Número de documentos por área de pesquisa por ano....64
1.2.6. Peso das palavras-chave na amostra bibliográfica inicial....65
2. CONCEITOS UTILIZADOS NA INTERPRETAÇÃO DA SEGURANÇA INTERNACIONAL SOBRE CONFLITOS CIBERNÉTICOS 69
2.1. Indefinição conceitual 70
2.2. Ciberespaço 72
2.2.1. As analogias cibernéticas e suas implicações....73
2.2.2. Definições de ciberespaço....75
2.2.3. Baixo custo de entrada, anonimato, assimetrias de vulnerabilidades e dificuldades de atribuição de ataques cibernéticos....80
2.2.4. Ataque e defesa no ciberespaço....84
2.3. Guerra cibernética 87
2.3.1. Definições de guerra cibernética....87
2.3.2. Definições negativas de guerra cibernética....88

2.3.3. Guerra cibernética é guerra? 91
2.3.4. Guerra Cibernética x Guerra Informacional 94
2.3.5. Segurança cibernética x segurança da informação 97
3 PRINCIPAIS DEBATES DA SEGURANÇA INTERNACIONAL SOBRE A ASCENSÃO DO CIBERESPAÇO 106
3.1. O ciberespaço e os paradigmas de RI 107
3.2. A questão central: a ameaça cibernética é exagerada? 109
3.2.1. Eficácia de ataques cibernéticos nas relações internacionais: o efeito multiplicador 112
3.2.2. Dissuasão x risco de escalada cibernética 116
3.2.3. Relações entre atores estatais e não estatais no ciberespaço 120
3.2.4. Securitização do discurso sobre ciberespaço 126
3.3. Considerações sobre poder cibernético 128
CONCLUSÃO 132
REFERÊNCIAS 135
ANEXOS 145
ANEXO I – APRESENTAÇÃO DA AMOSTRA BIBLIOGRÁFICA INICIAL 145
ANEXO II – APRESENTAÇÃO DA AMOSTRA BIBLIOGRÁFICA FINAL 170

INTRODUÇÃO

Um pouco de história

As primeiras máquinas de processamento de dados – baseadas então na separação de cartões perfurados – foram criadas no fim do século XIX por Herman Hollerith[1] (CAPOBIANCO; CURY, 2011, p. 6). Nessa época, pouco se podia prever do que seria possível atingir a partir da integração dessa tecnologia com os controladores de circuitos elétricos patenteados por Nicola Tesla em 1898[2].

Na primeira metade do século XX, seguiu-se uma evolução ainda lenta no desenvolvimento da informática. A chamada primeira geração de computadores eram calculadoras programáveis capazes de armazenar os programas. Por muito tempo essas máquinas, desenvolvidas entre a década de 1930 e o fim da década de 1950, tiveram usos restritos às searas militar e científica. Em 1936, Alan Turing estabeleceu um modelo teórico capaz de descrever aspectos lógicos do funcionamento do que seria um computador moderno (memória, estados e transições). Em 1938, o alemão Konrad Zuse construiu a primeira máquina binária programável do mundo, o computador eletromecânico Z1 (CAPOBIANCO; CURY, 2011, p. 6-7).

Durante a Segunda Guerra Mundial, a informática atingiu um novo nível de relevância, com implicações diretas sobre as relações internacionais e sobre o desenvolvimento do conflito que viria reorganizar toda a ordem internacional. Exércitos e inteligência aliados utilizaram computadores para a realização de cálculos específicos, como aqueles de velocidade aérea e de tabelas de disparos. Versões subsequentes do Mark 1 – computador eletromecânico desenvolvido na Universidade de Harvard, nos EUA – teriam sido utilizadas para comparar métodos de ignição das primeiras bombas atômicas. O Colossus, considerado o primeiro computador inteiramente eletrônico, foi fundamental juntamente à chamada bomba de Turing na quebra da criptografia da máquina de cifração alemã Enigma (COPELAND, 2004). Ambos haviam sido desenvolvidos na Escola de Código e Criptografia do governo britânico

---

1 A máquina criada por Hollerith para auxiliar no recenseamento da população dos EUA fazia a leitura de cartões de papel perfurados em código BCD (*Binary Coded Decimal*) e contagem da informação ali disponível. A estação de leitura era equipada com um pente metálico, em que cada dente era conectado a um circuito elétrico. Os cartões eram colocados sobre uma taça com mercúrio também conectada ao circuito. Quando o pente era colocado sobre o cartão, os dentes que atravessavam as perfurações fechavam o circuito elétrico, acionando os contadores respectivos.

2 Disponível em: https://teslauniverse.com/nikola-tesla/patents/us-patent-611719-electrical-circuit-controller.

(*Government Code Cypher School*) em Bletchley Park e representaram uma vantagem decisiva para a vitória dos aliados.

O período imediatamente após o fim da Segunda Guerra Mundial foi extremamente profícuo no vislumbre e na idealização dos usos futuros da tecnologia computacional, muitos dos quais, tais como a cibernética[3], a inteligência artificial e a internet, efetivamente têm sido desenvolvidos até hoje.

O artigo "*As we may think*", de Vannevar Bush, em julho de 1945, aponta uma mudança de foco nas aplicações da informática, que se movimenta da realização de cálculos em direção ao armazenamento e à análise de informações. Bush, ex-presidente do Comitê de Pesquisa de Defesa Nacional dos Estados Unidos e ex-diretor do Escritório para Desenvolvimento e Pesquisa Científica, instava físicos e cientistas que haviam trabalhado no esforço de guerra a tornar suas descobertas acessíveis por meio de usos pacíficos e a buscar nesses usos o aprimoramento de atributos humanos. Bush descreve em seu artigo o *memex*, um dispositivo elétrico hipotético cujo uso primordial seria gravar, gerenciar e acessar informações de um indivíduo.

> Considere um dispositivo futuro... em que um indivíduo armazena todos os seus livros, registros e comunicações, e que é mecanizado para que possa ser consultado com velocidade e flexibilidade excessivas. É um suplemento íntimo ampliado de sua memória. (BUSH, 1945, tradução da autora)

A descrição do *memex* é considerada um marco importante na idealização das tecnologias de informação e comunicação (TIC) de forma geral e da internet.

A inteligência artificial, que – entre inúmeras outras implicações – potencialmente altera os parâmetros de poder militar, com repercussões diretas na segurança internacional e cujos impactos começam a ser sentidos em maior escala no início do século XXI, tem suas bases teóricas definidas ainda na primeira metade do século XX, a partir dos trabalhos de Norbert Wiener e mais especificamente da conferência *Dartmouth Artificial Intelligence*.

Em 1948, a obra "Cibernética: ou controle e comunicação no animal e na máquina", de Norbert Wiener, inaugurou o campo da Cibernética. Wiener descreveu o princípio do *feedback* em dispositivos eletrônicos, segundo o qual uma ação em determinado sistema gera uma alteração que implica mudança das respostas posteriores. Wiener observa que o mesmo princípio existe na natureza, de plantas a animais complexos. Dessa forma, a obra estabeleceu

[3] Cibernética enquanto aumento das capacidades físicas e mentais humanas por meio da informática.

fundamentos para entendimento do controle em sistemas eletroeletrônicos, mecânicos e orgânicos.

Ainda mais diretamente, em 1956 a conferência *Dartmouth Artificial Intelligence* (AI) inaugurou o campo de estudos da Inteligência Artificial. A conferência contou com pesquisadores convidados com o objetivo de avançar nas questões de "como fazer máquinas utilizarem linguagem, formarem conceitos e abstrações, resolverem tipos de problemas reservados a humanos e se aprimorarem" (MCCARTHY; MINSKY; ROCHESTER; SHANNON, 1955). As discussões tiveram o impacto de convencer os pesquisadores sobre os potenciais de aprendizado e desenvolvimento de inteligência das máquinas, inaugurando estudos continuados até hoje.

Além disso, o desenvolvimento da internet em meados da década de 1960 foi definidor de possivelmente todos os aspectos da sociedade a partir de então, incluídas aí as relações internacionais. A ideia de uma rede universal havia sido descrita no artigo "*On-Line Man Computer Communication*" pelo psicólogo J. C. R. Licklider e pelo arquiteto Welden E. Clark em 1962. Licklider posteriormente seria convidado para chefiar o Escritório de Técnicas de Processamento de Informações (*Information Processing Techniques Office*, IPTO) da *Advanced Research Projects Agency* (ARPA), com a missão de integrar computadores do Departamento de Defesa no Pentágono, no Complexo Militar de Cheyenne Mountain e na sede do Comando Aéreo Estratégico. Os esforços para o estabelecimento dessa rede resultaram, em outubro de 1969, na primeira experiência de conexão bem-sucedida entre computadores geograficamente distantes através da rede telefônica, a Arpanet. Os dois primeiros nós da Arpanet foram um computador na Universidade da Califórnia em Los Angeles (UCLA) e outro no Instituto de Pesquisas de Stanford. Ainda naquele ano a rede incorporou um computador na Universidade da Califórnia em Santa Bárbara e um na Universidade de Utah.

Paralelamente, ainda na década de 1960, a disseminação do uso civil de computadores foi fomentada pela criação e produção em massa de transistores[4]. O surgimento de microprocessadores possibilitou o desenvolvimento de mini e microcomputadores e, eventualmente, o lançamento do computador pessoal (*personal computer* – PC) pela IBM e da interface gráfica de usuários pela Apple – suporte visual de janelas, menus, ícones. Finalmente, o estabelecimento de protocolos de comunicação entre máquinas como o TCP/IP (*transmission control protocol/internet protocol*), utilizado até hoje, contribuiu para a rápida popularização

[4] Condutores e isolantes de corrente elétrica que evitam a geração de calor, possibilitando rapidez e economia na transmissão de corrente elétrica.

da informática nos anos 1980, tornando-a de setor industrial particular em ferramenta para setores como telecomunicações, editoração, cinema e televisão (LÉVY, 1999).

O fim da década de 1980 marcou o início da fase de computadores em rede e da portabilidade. Pierre Lévy argumenta que redes de computadores que vinham se formando desde o final da década de 1970 se aglomeraram conforme o número de pessoas e de computadores conectados começou a crescer exponencialmente.

> Uma corrente cultural espontânea e imprevisível impôs um novo curso ao desenvolvimento tecnoeconômico. As tecnologias digitais surgiram, então, como a infraestrutura do ciberespaço, novo espaço de comunicação, de sociabilidade, de organização e de transação, mas também novo mercado da informação e do conhecimento (LÉVY, 1999, p. 32).

Em meados da década de 1980, a Arpanet havia superado 1.000 nós (*hosts)* e desenvolvido ligações com redes externas na América do Norte, Europa e Austrália. Em 1990, então com aproximadamente 100 mil nós, a rede foi descontinuada, sendo a maior parte dos computadores ligados a ela conectados à NSFNET, rede da Fundação Nacional de Ciências dos EUA (*National Science Foundation*), criada em 1986. Nos anos 1990, o uso da internet explodiu, ensejando a transferência, em 1998, de sua administração do governo dos Estados Unidos (então na forma da NSF) à autarquia *Internet Corporation for Assigned Names and Numbers* (Icann), ligada ao Departamento do Comércio[5].

O termo "*global village*" para referir-se ao impacto de tendências tecnológicas na comunicação havia sido cunhado em 1964 por Marshall McLuhan. A ideia era que a tecnologia estava possibilitando a criação de um "sistema nervoso eletrônico" que rapidamente integrava o planeta, transformando-o num "povoado global"[6]. McLuhan avaliava esse processo como positivo de forma geral, atentando, contudo, para a possibilidade de utilização conjunta de tecnologia e comunicação no desenvolvimento de propaganda extremamente sofisticada. A ideia de vila global tornou-se bastante popular e pode ter contribuído para a naturalização dos desenvolvimentos subsequentes da internet.

Assim, na década de 1990, a internet tomou proporções globais na forma de websites, viabilizando números sem precedentes de comércio, entretenimento e contatos sociais (BETZ; STEVENS, 2011, p. 15). Desde então, presenciamos sua evolução rumo ao que ficou conhecido

---

5 O ano de 1998 marcou o fim do papel direto da NSF na internet. Naquele ano, os pontos de acesso à rede e as funções do árbitro de roteamento foram transferidos para o setor privado e a Administração Nacional de Telecomunicações e Informações do Departamento de Comércio formalizou um acordo com a *Internet Corporation for Assigned Numbers and Names* (Icann), organização sem fins lucrativos para supervisão do registro de nomes de domínio. Disponível em: www.nsf.gov/news/news_summ.jsp?cntn_id=103050. Acesso em: 21 fev. 2021.

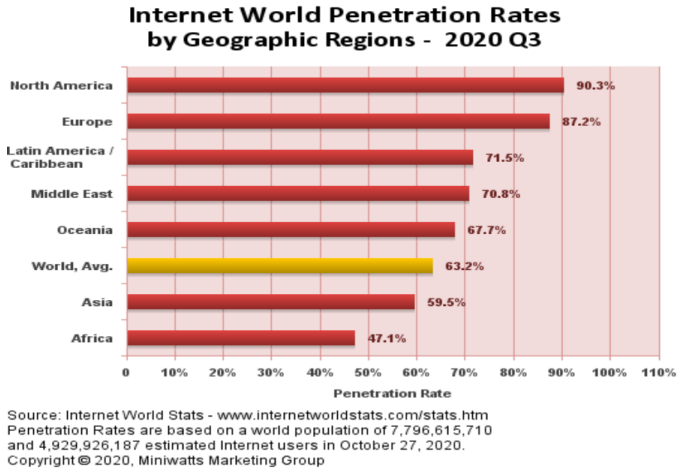
6 *Understanding Media*, McLuhan, 1964.

como Web 2.0 ou Web participativa, com foco não apenas em páginas estáticas, mas na comunicação bidirecional e em conteúdo dinâmico gerado pelos usuários nas primeiras plataformas de mídia social (DINUCCI, 1999; TOLEDANO, 2013).

A intensificação dessa tendência rumo à "internet social" representou uma segunda mudança profunda no caráter da internet e materializou-se na consolidação das mídias sociais como centro de produção e proliferação de conteúdo. A terceira mudança profunda no caráter da internet deriva do aumento exponencial de usuários que acessam a rede por meio de dispositivos móveis[7], provendo de imediatismo e capilaridade sem precedentes as informações disponibilizadas online (GOHDES, 2018, p. 95).

Entre 2000 e 2020, o número de usuários da internet cresceu 1.271%. Em outubro de 2020, o número estimado de usuários no mundo era aproximadamente 4,9 bilhões de pessoas, 63,2% da população mundial estimada para 2021[8]. Desses, 91% acessavam a rede pelo celular[9]. Mais da metade dos usuários (51,8%) estavam na Ásia, onde o potencial de crescimento ainda é muito significativo (o percentual da população conectada representava 59,5% da população do continente). Como observado por Pierre Lévy (1999), as "projeções sobre os usos sociais do virtual devem integrar esse movimento permanente de crescimento de potência, redução nos custos e descompartimentação" (LÉVY, 1999, p. 33).

Gráfico 1 – Taxas de penetração da internet por regiões geográficas (estimativas de outubro de 2020).



Fonte: Internet World Stats. Disponível em: www.internetworldstats.com/stats.htm. Acesso em: 13 fev. 2021

---

7 Em outubro de 2016, pela primeira vez, o número de usuários da internet por dispositivos móveis superou o número de acessos por meio de computadores e notebooks (StatCounter GlobalStats, 2016).

8 Disponível em: www.internetworldstats.com/stats.htm. Acesso em: 13 fev. 2021.

9 Disponível em: www.statista.com/statistics/617136/digital-population-worldwide. Acesso em: 13 fev. 2021.

Atualmente, um mundo sem internet é inimaginável. A rede é um pilar central da moderna sociedade da informação. Conforme Lévy (1999) escreve:

> Durante muito tempo polarizada pela "máquina", anteriormente fragmentada pelos programas, a informática contemporânea – programas e hardware – está desconstruindo o computador em benefício de um espaço de comunicação navegável e transparente, centrado na informação. (LÉVY, 1999, p. 44).

Assim ascendeu o ciberespaço. O desenvolvimento da informática e da internet imprimiu rapidez e volume às trocas de informações e produtos, alterando aspectos fundamentais da vida e organização humanas. O contínuo desenvolvimento das tecnologias de informação e comunicação[10] aumenta exponencialmente a velocidade da coleta e análise de dados a níveis antes cogitados apenas na literatura de ficção científica, possibilitando um fluxo sem precedentes que retroalimenta a ciência e tecnologia.

Novas tecnologias

Em 1984, o romance *Neuromancer*[11] de William Gibson descreveu um futuro – então considerado distópico – em que seres humanos utilizam próteses corpóreas e passam por processos de "reconfiguração neural", "projetam sua consciência desincorporada no ciberespaço", e em que *cowboys*[12] terceirizados invadiam "brilhantes sistemas corporativos, abrindo janelas para fartos campos de dados" em troca de neoienes[13] (GIBSON, 2004, p. 26).

No início do século XXI, diversos avanços científicos e tecnológicos descritos por Gibson foram alcançados e seguem sendo aprimorados. A perspectiva de massificação do uso de tecnologias como a internet das coisas, big data, inteligência artificial, biotecnologia, *blockchain* e criptoativos tende a ter impactos sociais importantes a curto prazo, inclusive nas relações internacionais – por exemplo na alteração do equilíbrio de poder decorrente do domínio dessas tecnologias ou na própria operacionalização de conflitos internacionais, com o desenvolvimento de sistemas automatizados de defesa dotados de inteligência artificial, a

---

[10] Tecnologias de Informação e Comunicação incluem computadores, dispositivos móveis, programas, redes e quaisquer acessórios que facilitem o acesso, armazenamento, processamento e troca de informações.

[11] O livro foi um dos pioneiros no subgênero da ficção científica conhecido por *cyberpunk*, gênero que lida com aspectos sociais da evolução tecnológica, geralmente ambientando suas tramas em um futuro com alta tecnologia contrastada com baixa qualidade de vida (*high-tech, low life*) (CAVALCANTE, John. Neuromancer: o futuro distópico de Willian, Gibson. Quinta Capa. 2019. Disponível em: <https://quintacapa.com.br/janeiro-literario-neuromancer-o-futuro-distopico-de-william-gibson>

[12] *Hackers*.

[13] Neoienes parecem se referir a uma espécie de dinheiro virtual que lembra o que hoje conhecemos por criptoativos.

perspectiva de espionagem cibernética generalizada com a internet das coisas ou a manipulação das capacidades de exércitos com biotecnologia, entre outros.

Internet das coisas

A implementação em larga escala de redes sem fio de alta velocidade, atualmente na forma das redes 5G – com aprimoramentos subsequentes já em fase de estudos e testes (as redes 6G) – representa com grande fidelidade o movimento de crescimento contínuo de potência mencionado por Lévy (1999).

Estima-se que as redes 5G aumentem em 100 vezes a taxa de transferência de arquivos na internet, diminuindo o tempo de latência para praticamente zero (entre 1 e 4 milissegundos), com aumento da cobertura territorial (NOOHANI; MAGSI, 2020, p. 1). A massificação do uso dessa tecnologia não impactará apenas a velocidade de conexão de computadores, tablets e smartphones. O novo patamar de conectividade implicará a conexão de uma grande variedade de objetos à internet, na chamada internet das coisas (*internet of things* – IoT), aumentando substancialmente o nível de automação das atividades humanas.

Exemplos ilustrativos da utilização de IoT são a comunicação entre carros autônomos, entre eles e aplicativos de localização, semáforos e outros sistemas de regulação do tráfego, entre os carros e o portão de nossas casas e entre o portão da casa e a cafeteira para que ela inicie o preparo do café de boas-vindas. Possibilidades menos prosaicas dizem respeito ao desenvolvimento substancial da telemedicina e a realização de cirurgias remotas[14], por exemplo.

Big Data

A quantidade de dados gerada pelo uso de dispositivos eletrônicos conectados (em sua maioria computadores e smartphones) exige grande capacidade computacional e técnicas específicas para sua análise (*Big Data Analytics*). A análise desses grandes volumes de dados objetiva descrever a forma de utilização de serviços e identificar motivos relacionados, além de prever formas de uso e prescrever tomadas de decisão relacionadas à oferta desses serviços.

[14] CUTHBERTSON, Anthony. Surgeon performs world's first remote operation using '5g surgery' on animal in China. The Independent. Disponível em:<www.independent.co.uk/life-style/gadgets-and-tech/news/5g-surgery-china-robotic-operation-a8732861.html >.Acesso em: 01/03/2021.

A perspectiva de aumento exponencial do volume de dados decorrente da popularização da internet das coisas tende a aumentar a relevância da análise de dados e de sua utilização não apenas como suporte à tomada de decisão, mas a sua automação, tornando-se importante instrumento para o refinamento de algoritmos utilizados no aprimoramento da inteligência artificial e de toda a teoria do aprendizado de máquina (*machine learning*), com base no volume dos dados e no princípio de *feedback* descrito por Wiener (1948).

A coleta dos dados que constituem e alimentam a análise de *big data* tem repercussões importantes na privacidade das pessoas e, no caso de uso generalizado de sistemas de decisão automatizados, em sua liberdade de escolha. Na medida em que dados pessoais são coletados, armazenados, processados e refinados, o leque de escolhas de consumo, por exemplo – o exemplo mais trivial –, tende a ser cada vez mais preciso e, portanto, limitado.

Inteligência artificial

De forma geral a inteligência artificial (IA) procura dotar algoritmos utilizados em computadores e máquinas da capacidade de tomar decisões com base nos dados que lhes são alimentados e de aprender conforme aumenta o número de decisões tomadas e o *feedback* a elas, aprimorando continuamente essa capacidade. No entanto, não há definição consensual e o termo funciona como um conceito guarda-chuva que engloba estudos sobre aprendizado de máquinas, raciocínio automatizado, robótica, visão computacional e processamento de linguagem natural (PNL) (DIPLO, 2019).

A tecnologia impacta potencialmente aspectos sociais, políticos e econômicos em todo o mundo. A Indústria 4.0 ou quarta Revolução Industrial, novo paradigma de produção industrial, é focada nos princípios de digitalização, interconectividade e automação e tem na IA, entre outros, um instrumento acelerador da tomada de decisões gerenciais, com impactos na logística e na produção. Diferenças no nível de domínio da tecnologia entre países podem, nesse sentido, alterar o equilíbrio econômico internacionalmente. Também as relações militares entre países podem ser impactadas. O desenvolvimento de sistemas de armas letais autônomas, com o estabelecimento de sistemas automatizados de defesa, tem implicações relevantes – inclusive éticas – para o direito e as relações internacionais.

Biotecnologia

A biotecnologia tem, por um lado, o aspecto do “melhoramento” de capacidades orgânicas, incluídas as de humanos, por meio da utilização de próteses robóticas – como previsto por Gibson em *Neuromancer* – ou da manipulação genética, com a possibilidade de seleção de genes considerados “desejáveis” ou “indesejáveis” em determinados organismos, para fins específicos.

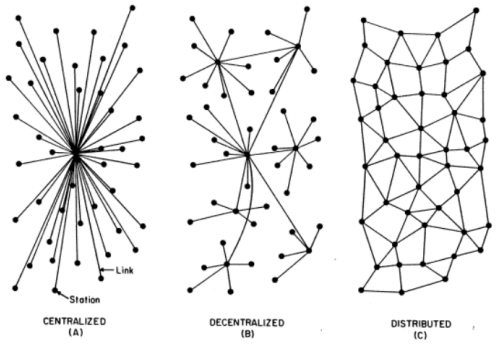
Almeida (2015) defende que o desenvolvimento tecnológico é ao mesmo tempo uma grande oportunidade, mas representa um grande risco no século XXI, tendo seu potencial militar estruturado e institucionalizado, com produção permanente de biotecnologias para uso dual (ALMEIDA, 2015, p. 2264). O uso dual da biotecnologia, em todas as suas formas, bem como suas implicações éticas, são reflexões relevantes para as RI na medida em que tem impactos potenciais, por exemplo e conforme apontado por Almeida (2015), nas organizações militares.

Blockchain

Blockchain é uma arquitetura de redes distribuídas[15], utilizada para registro e autenticação de transações. A tecnologia surgiu a princípio de forma instrumental para viabilizar as operações da primeira moeda virtual (criptomoeda), o *bitcoin*, contudo ela vem sendo testada e utilizada em diversos setores, além da computação, tais como finanças, logística, registros fundiários, saúde e artes (GREVE *et al.*, 2018, p. 2), frequentemente com o objetivo de proporcionar maior transparência e rastreabilidade das informações e transações.

> Todos os nós possuem e mantêm uma réplica do registro de transações efetuadas, materializado na forma de um livro-razão (*ledger*) distribuído, que é imutável, pode ser verificado e auditado, e está sempre disponível. O conjunto e a ordem em que as

[15] Em contraposição a redes centralizadas, em que todos os “nós” da rede se conectam a um nó central, e a redes descentralizadas, que funcionam como um conjunto de redes centralizadas ligadas entre si, nas redes distribuídas não há centros, conforme ilustrado pelo diagrama de Paul Baran a seguir:



> transações são executadas é acordada por todos os participantes da rede, através da realização de um protocolo de consenso (GREVE *et al.*, 2018, p. 2).

Na medida em que estabelece um mecanismo de confiança descentralizado, a utilização generalizada de *blockchain* promete prescindir de autoridades centrais certificadoras, tais como bancos, cartórios e quiçá governos, apresentando um potencial revolucionário em relação à organização institucional em que se baseia boa parte das interações sociais atualmente.

Criptoativos

O desenvolvimento de criptoativos traz para o sistema financeiro a perspectiva de descentralização que a arquitetura de rede *blockchain* implica às áreas em que é utilizada. Trata-se de um caso específico de uso da *blockchain* e, como já explicitado, o primeiro uso para que ela foi pensada.

Em 2019, nota técnica do Fundo Monetário Internacional (FMI) utilizou a seguinte definição para criptoativos: "ativos digitais que usam criptografia para segurança e são moedas ou *tokens* de livros-razão distribuídos e/ou *blockchains*, incluindo *tokens* garantidos por ativos" (CUERVO; MOROZOVA; SUGIMOTO, 2019, p.1, tradução da autora). Isso inclui criptomoedas obtidas por meio de mineração – a utilização de poder computacional para solução de equações e obtenção de *hashes*[16] que permitem transações em *blockchain* – como o Bitcoin (BTC) e o Ethereum (ETH); *stablecoins*, criptoativos com lastro em moedas fiduciárias – versões digitais de moedas nacionais – como o criptorublo, com lastro no rublo russo, e o yuan digital, ambos em fase de testes; criptoativos com lastro em outros bens, como o petro venezuelano, com lastro em barris de petróleo; ou ativos digitais que permitem transações em plataformas específicas, como o Binance Coin (BNB), para transações especificamente dentro de uma corretora de criptoativos. A nota do FMI declara, ainda, que a necessidade de monitoramento e desenvolvimento de marco regulatório adequado aos criptoativos decorre de eles serem o núcleo da revolução tecnológica financeira e fator potencial de volatilidade no mercado de capitais.

O desenvolvimento e a popularização da internet das coisas, de *big data analytics*, inteligência artificial, biotecnologia, *blockchain* e criptoativos tendem a intensificar o processo de ascensão do ciberespaço e potencializar seus efeitos. Na medida em que tem impactos importantes na sociedade, há diferentes abordagens das consequências desse desenvolvimento,

[16] Valores obtidos pela aplicação de uma função que mapeia uma sequência de bits de comprimento arbitrário em uma sequência de bits de comprimento fixo.

sendo a abordagem da disciplina de Relações Internacionais apenas uma lente, ou melhor, um conjunto de lentes através das quais é possível interpretar o fenômeno.

Interpretações para a ascensão do ciberespaço

A ascensão do ciberespaço, enquanto fenômeno com efeitos em possivelmente todos os aspectos da sociedade, é interpretada de formas diversas por diferentes disciplinas. A interpretação da ascensão do ciberespaço pelas RI deve ser, portanto, posta em perspectiva na medida em que representa apenas "parte do elefante", como na parábola indiana e conforme apontado pela professora Nazli Choucri na apresentação do projeto *Explorations in Cyber International Relations*[17]. Nesse sentido, esta seção apresenta interpretações da História, Sociologia e Comércio Internacional sobre a ascensão do ciberespaço de maneira a contribuir com a contextualização do fenômeno.

O historiador israelense Yuval Noah Harari interpreta a ascensão do ciberespaço enquanto processo que altera fundamentalmente a vida e o conjunto de valores humanos. Ele defende que os avanços tecnológicos, notadamente da internet das coisas, *big data*, biotecnologia e inteligência artificial, estão promovendo a substituição de uma visão de mundo antropocêntrica – predominante no século XX – por uma datacêntrica.

Uma relação simbiótica entre ciência e religião estaria no centro desse desenvolvimento. Para Harari (2016), a ciência depende da religião – enquanto legitimadora de normas e valores que permitam a cooperação em larga escala e que viabilize os avanços científicos – e por outro lado a "retrolegitima", na medida em que passa a emitir juízos de valor derivados da religião na forma de declarações factuais científicas. Ao longo do século XX, religiões humanistas[18] localizaram no ser humano a fonte do sentido que legitimava a ciência, de forma que o desenvolvimento dessa última permitiu à humanidade superar os problemas da fome, da peste e da guerra como principais *causae mortis* humanas. A continuidade do ideal humanista deixa como agenda para o século XXI as buscas pela imortalidade, pela felicidade eterna e pela divindade (a capacidade de "manipular" a vida). Contudo, Harari (2016) afirma que "[...] a tentativa de realizar o sonho humanista irá solapar suas fundações, ao desencadear novas

[17] Disponível em: http://ecir.mit.edu. Acesso em: 25 mar. 2021.

[18] "A religião humanista cultua a humanidade e espera que ela assuma na peça o papel que era de Deus no cristianismo e no islamismo e que cabia às leis da natureza no budismo e taoismo. [...] Os humanos devem extrair de suas experiências interiores não apenas o significado da própria vida, mas também o significado de todo o universo." (HARARI, 2016, p. 228).

tecnologias pós-humanistas" (HARARI, 2016, p. 281), desenvolvimento que, em certa medida, presenciamos.

A emergência da agenda da imortalidade, felicidade e divindade ensejaria o surgimento de uma nova religião, o dataísmo, com o estabelecimento dos dados como fonte de sentido que legitima os avanços científicos. Algumas das premissas dessa religião, além da busca por respostas e sentidos nos dados, são a consideração de organismos (inclusive seres humanos) como algoritmos bioquímicos, ainda que altamente sofisticados – igualando organismos a máquinas, como adiantado por Norbert Wiener em 1948 – e a liberdade da informação[19] como valor supremo. Essa mudança filosófica teria importantes repercussões práticas (HARARI, 2016, p. 392).

> Os algoritmos do Google e do Facebook sabem não apenas como você se sente, como sabem 1 milhão de outras coisas a seu respeito das quais você mal suspeita. Consequentemente você deveria parar de ouvir seus sentimentos e começar a ouvir esses algoritmos externos (HARARI, p. 394).

A mudança de uma visão de mundo antropocêntrica para uma datacêntrica poderia implicar mais do que uma revolução filosófica, mas uma revolução prática, retirando do arbítrio humano uma série de decisões que hoje nos são atribuídas, tais como as escolhas de: o que consumir, em quem votar ou o que constitui uma obra de arte de valor.

De forma semelhante a Harari (2016), o sociólogo Manuel Castells (2013) ressalta também a aproximação entre biologia e tecnologia, ao incluir entre as tecnologias de informação e comunicação, juntamente à microeletrônica, à computação e às comunicações, a engenharia genética. Para Castells (2013) a emergência do novo paradigma tecnológico é comparável à Revolução Industrial do século XVIII no potencial de produzir mudanças fundamentais nas bases da economia, sociedade e cultura e é caracterizada pela pervasividade, a saber: "por sua penetração em todos os domínios da atividade humana, não como fonte exógena de impacto, mas como o tecido em que essa atividade é exercida" (CASTELLS, 2013, p. 88).

Castells (2013) avalia as mudanças geradas pela ascensão do ciberespaço na economia, como o aumento de relevância dos setores de finanças e da própria tecnologia; no trabalho, com alteração dos tipos de atividade, locais, jornadas e regimes de proteção dos trabalhadores; na cultura, com o fim da audiência de massa e o surgimento de redes interativas; e nas noções de

---

[19] Harari (2016) faz a ressalva de que a liberdade de informação é diferente de liberdade de expressão. A liberdade de informação é dada à informação e não aos seres humanos, podendo inclusive se chocar com a liberdade de expressão, pois privilegia o direito da informação de circular em detrimento do direito humano de manter seus dados para si.

tempo e espaço. Como consequências dessas mudanças, Castells afirma que "[...] como tendências históricas, as funções e os processos dominantes na era da informação estão cada vez mais organizados em torno de redes" (CASTELLS, 2013, p. 553). Frente à ascensão do ciberespaço, a consequente emergência de uma sociedade em rede representaria um terceiro estágio na relação entre natureza e cultura (enquanto produção humana), um estágio marcado pela autonomia da cultura em relação às bases materiais de nossa existência (CASTELLS, 2013).

Sob um ponto de vista multidisciplinar, mas com foco nos efeitos ao comércio internacional, Pharag Khanna (2016) interpreta a ascensão do ciberespaço enquanto apenas um – o mais recente – entre outros tipos de infraestrutura sobre os quais se constrói a cadeia global de suprimentos que caracteriza o mundo atualmente e a perspectiva do que será o mundo no futuro próximo. Khanna (2016) afirma que a tecnologia já é, juntamente com o ser humano e a natureza, uma das forças mais importantes formatando o planeta, além de, juntamente com a urbanização, constituir uma tendência a se aprofundar no futuro. A conectividade proporcionada – pelo menos em parte – pelas tecnologias de informação e comunicação contribuiu com a emergência do mundo da cadeia global de suprimentos, em que as infraestruturas da própria comunicação, de finanças, transporte e energia ganham centralidade e superam em relevância as tradicionais fronteiras políticas. Como consequência da conectividade, a natureza da competição geopolítica teria mudado da guerra por território para o cabo de guerra por infraestrutura, por natureza menos violento do que conflitos fronteiriços e uma alternativa aos ciclos históricos de conflitos entre grandes potências (KHANNA, 2016).

Além disso, o autor defende que as cidades se tornam mais importantes que os países como unidade política, o que não implicaria o fim do Estado-nação, mas sua superação por uma unidade organizacional mais adequada ao mundo da cadeia global de suprimentos. A globalização, enquanto capacidade crescente de interação global, comprometeria a soberania nacional na medida em que governos renunciam à criação de regulamentações nacionais em favor da aplicação de regras supranacionais e na medida em que a autonomia e a relevância política de cidades e corporações são fortalecidas (KHANNA, 2016). No mundo da cadeia global de suprimentos, as comunidades unem-se a cidades, corporações e Estados como atores relevantes, de forma que esse grupo passa a incluir redes terroristas, unidades *hackers* e grupos religiosos fundamentalistas. A internet é uma grande viabilizadora da formação dessas comunidades, ensejando um senso de identidade mais definido pelo que se faz do que pelo local onde se está (KHANNA, 2016).

Às interpretações da História, da Sociologia e do Comércio Internacional, múltiplas outras se unem na tentativa de compreender as condições e consequências da ascensão do ciberespaço. Enquanto disciplina impactada pela evolução das tecnologias de informação e comunicação, as Relações Internacionais também oferecem lentes através das quais interpretar esses desenvolvimentos. Esta dissertação apresenta um estudo exploratório de interpretações das Relações Internacionais (RI) sobre a ascensão do ciberespaço. A maior parte das abordagens encontradas aqui enquadra-se em estudos de Segurança Internacional, contudo ressalta-se que mesmo dentro das RI há diversidade de interpretações, como por exemplo as que focam nas implicações da ascensão do ciberespaço nas relações econômicas internacionais ou as que analisam os esforços regulatórios e negociações internacionais para o estabelecimento de padrões tecnológicos ou divisões do espectro eletromagnético entre os países.

A abordagem do ciberespaço nas RI

As primeiras interpretações da ascensão do ciberespaço identificadas na produção científica de relações internacionais datam do início dos anos 1990[20], quando principia o processo de massificação da internet. Essa abordagem inicial, bastante limitada numericamente, possuía um caráter ensaístico, buscando prever eventuais consequências do desenvolvimento do ciberespaço para as relações internacionais.

Aproximadamente trinta anos depois, chegamos – talvez o estejamos ultrapassando – ao ponto de ultraconectividade imaginado nos primeiros textos. Se, por um lado, a produção científica de RI relacionada à ascensão do ciberespaço não pode mais ser considerada

[20] ARQUILLA, J.; RONFELDT, D. Cyberwar is coming! *Comparative Strategy*, v. 12, n. 2, p. 141-165, Spring 1993; DE LANDA, M. *War in the Age of the Intelligent Machines*. New York: Zone Books, 1991; BRACKEN, P. *Electronics, Sensors, and Command and Control in the Developing World*: An overview of the issues. draft prepared for discussion at the AAAS Workshop on ad; DRUCKER, P. F. *The new realities*: In government and politics, in economics and business, in society and world view. New York: Harper and Row, 1989. DRUCKER, P. F. *The Coming of the New Organization*. Harvard Business Review, Jan.-Feb. 1988 (reimpresso no livro Revolution in real time: managing information technology in the 1990s, A Harvard Business Review Book, 1990); *Advanced weaponry in the developing world*. Virginia: Westfields Conference Center, June 1992; ARNETT, E. Welcome to hyperwar. *The Bulletin of the Atomic Scientists*, v. 48, n. 7, p. 14-21, Sep. 1992; BENEDIKT, M. (ed.). *Cyberspace*: first steps. Cambridge: MIT Press, 1991; GELERNTER, D. *Mirror worlds, or the day software puts the universe in a shoebox*. How it will happen and what it will mean. New York: Oxford University, 1991; GRIER, P. *The data weapon*. Government Executive, June 1992. p. 20-23; KENNEY, G.; DUGAN, M. J. O*peration Balkan Storm*: here's a plan. The New York Times, Nov. 29 1992; RONFELDT, D. *Cyberocracy, cyberspace, and cyberology*: political effects of the information revolution. Santa Monica: Rand, 1991. RONFELDT, D. Cyberocracy is coming. *The Information Society*, v. 8, n. 4, 1992; TOFFLER, A. *Powershift*: knowledge, wealth, and violence at the edge of the 21st century. New York: Bantam, 1990; VAN CREVELD, M. *The transformation of war*. New York: Free Press, 1991.

incipiente, por outro, sua relevância comparativamente a outros temas tratados na disciplina ainda é pequena (KELLO, 2013).

Em oposição à postura distante da academia de RI, a magnitude das mudanças previstas nas relações internacionais decorrentes do avanço das tecnologias de informação e comunicação e da consequente ascensão do ciberespaço não tem sido negligenciada por elites governamentais. Um importante indicativo da ênfase dada por governos às dinâmicas cibernéticas foi a publicação, entre 2003 e 2017, de 112 estratégias de atuação no ciberespaço 86 países (Gráfico 2) (IZYCKI, 2018). A publicação desses documentos reflete o esforço de preparação governamental para lidar com novos desafios decorrentes da ascensão do ciberespaço. Outro exemplo do interesse governamental no tema, em 2015, a China lançou, no escopo da Nova Rota da Seda (*Belt and Road Initiative* – BRI), a Rota da Seda Digital (*Digital Silk Road)*, com o objetivo de que conjuntamente ao estabelecimento de infraestrutura convencional de energia, transporte e logística, o país viabilize financiamento, construção e assistência a redes de telecomunicação, fomente o desenvolvimento de capacidade em inteligência artificial, computação na nuvem, e-commerce, sistemas de pagamentos móveis, tecnologia de vigilância como reconhecimento facial e cidades inteligentes aos países recipientes[21]. Analogamente, no fim de 2019, a Rússia anunciou sucesso nos testes da Ru.net, uma rede de internet russa que restringe suas conexões à rede global e a tornaria passível de desconexão dessa, objetivando controlar os pontos de entrada e saída de dados do país. Além disso, o país iniciou consultas para o lançamento do criptorrublo, *stablecoin* com lastro no rublo, além de se referir à *blockchain* como a tecnologia do futuro.[22] Também nos Estados Unidos, o Centro para Estudos Internacionais Estratégicos (*Center for Strategic International Studies* – CSIS) recentemente estabeleceu um Programa de Tecnologias Estratégicas[23] que inclui, entre outros temas, "Tecnologia e Inovação" (entre eles inteligência artificial, internet das coisas e tecnologia e guerra), "Inteligência, Privacidade e Vigilância" e "Efeito Político da Internet".

[21] COUNCIL FOR FOREIGN RELATIONS. Assessing China's digital silk road initiative: a transformative approach to technology financing or a danger to freedoms? Disponível em: www.cfr.org/china-digital-silk-road.
[22] ERASO FELIPE. 'The cryptoruble is the future' says Russian policymaker. CoinTelegraph. 2020. Disponível em: https://cointelegraph.com/news/the-cryptoruble-is-the-future-says-russian-policymaker.
[23] Disponível em: < https://www.csis.org/programs/strategic-technologies-program>

Gráfico 2 – Publicação de estratégias nacionais de segurança cibernética por ano

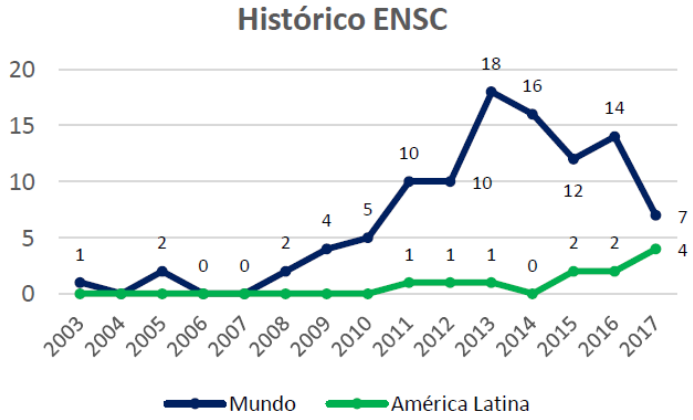


Figure 1. Total de ENSC publicadas anualmente

Fonte: IZYCKI (2018)

Além desses exemplos, a partir de 2007 se percebeu a proliferação de incidentes cibernéticos com causas e/ou implicações nas relações internacionais, corroborando a relevância crescente do ciberespaço na busca de objetivos políticos por governos. O assunto ganhou notoriedade a partir de abril de 2007 (LOBATO; KENKELL, 2015, p. 630), quando uma série de ataques cibernéticos atribuídos à Rússia atingiu instituições governamentais e serviços da Estônia, deixando indisponíveis serviços como sites de notícias, bancos e sistemas de organizações policiais do país.

Aos ataques à Estônia seguiram-se outros incidentes que apontavam para a instrumentalização cada vez maior do ciberespaço em conflitos e questões de segurança internacionais: ataques à Geórgia, em meio ao conflito militar com a Rússia pelos territórios da Abecásia e Ossétia do Sul, em 2008 (MARKOFF, 2008); a publicidade do *malware* Stuxnet em 2010, que teria alterado dados do sistema de controle de usinas de enriquecimento de urânio ao longo dos anos anteriores, de forma a prejudicar o programa nuclear iraniano (RID, 2012); vazamentos, em 2013, comprovando a prática de vigilância cibernética sobre populações e governos praticada pela *National Security Agency* (NSA), dos Estados Unidos (CASADO; KAZ; GREENWALD, 2013); a primeira atribuição contundente de um APT (*Advanced Persistent Threat*) – grupo hacker de atuação ofensiva contínua – a um Estado-nação (conforme relatório da empresa de segurança cibernética Mandiant, que atribuiu o grupo APT 01, de espionagem econômica e industrial, à China) (MANDIANT, 2013); a ampla utilização de ataques cibernéticos no conflito entre Ucrânia e Rússia em 2014, na sequência dos protestos

conhecidos como Euromaidan (Europraça, em tradução livre) e que culminaram com a anexação das regiões da Crimeia e Donbass pela Rússia (GEERS, 2015); interferência externa nas eleições estadunidenses em 2016, com disparo de conteúdos em massa em mídias sociais e vazamentos de e-mails de membros do Partido Democrata, incluindo a então candidata à Presidência Hillary Clinton (US, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, 2017); o "sequestro", em 2017, das informações de cerca de 200 mil computadores em 150 países pelo *ransomware WannaCry*, atribuído à Coreia do Norte, e a exigência do resgate dos computadores infectados em *Bitcoins*; entre outros.

Além de fornecer importantes exemplos da crescente simbiose da condução das políticas nacionais e internacional com o ciberespaço, é possível apreender desses e de outros incidentes especificidades características de conflitos internacionais no domínio cibernético. Ainda, esses incidentes enfatizam que a relevância dos ataques cibernéticos decorre principalmente de suas consequências no mundo não virtual, de suas implicações cinéticas.

Breve descrição de casos paradigmáticos

Os casos apresentados nesta seção objetivam exemplificar formas de instrumentalização do ciberespaço em conflitos e questões de segurança internacionais. Seu conhecimento descritivo é importante, por um lado, porque esses incidentes atestam a crescente importância do tema junto à comunidade política (governos, organizações internacionais e tomadores de decisão) e, por outro, porque representaram um importante estímulo à abordagem científico-acadêmica, sendo frequentemente mencionados na produção acadêmica de RI.

Estônia (2007)

Iniciando em abril de 2007, 22 dias de ataques cibernéticos sobre alvos estonianos – servidores de sites populares e de e-mail, mídia online, entidades do governo, parlamento, polícia e bancos – aconteceram na sequência da transferência do monumento Soldado de Bronze de Tallinn de uma área central da cidade para uma locação periférica.

O monumento, construído em 1947 em homenagem à vitória russa na Segunda Guerra Mundial, havia se transformado em um "ponto focal de tensão entre movimentos pró-Kremlin e movimentos nacionalistas estonianos" e sua movimentação foi acompanhada de manifestações inicialmente pacíficas e em seguida crescentemente violentas, com protestos, confrontos com forças policiais, declaração de um membro do parlamento russo de que o evento

deveria ser a causa de uma guerra e agressão física ao embaixador estoniano durante uma coletiva de imprensa. (OTTIS, 2008, p. 2).

A hipótese de os ataques cibernéticos serem parte de operação de informação do governo russo foi considerada plausível em estudo publicado posteriormente pelo *Cooperative Cyber Defence Centre of Excellence* da Otan (CCDCOE/Otan) (CCDCOE, 2011). "Evidências circunstanciais que ocorreram paralelamente aos ataques consistiram em ataques políticos, econômicos e informacionais à Estônia, bem como em casos isolados de violência física", e foram relacionadas à divergência política entre Estônia e Rússia decorrente da transferência da estátua (OTTIS, 2008, p. 1). Siedler (2016) afirma que os ataques podem ser interpretados como uma tentativa russa de influenciar uma decisão de natureza política estoniana (SIEDLER, 2016, p. 29).

Geórgia (2008)

No ano seguinte, em meio a conflito militar contra a Rússia pelos territórios da Ossétia do Sul e da Abecásia, a Geórgia sofreu uma série de ataques cibernéticos de negação de serviço (*Distributed Denial of Service* – DDoS) sobre alvos governamentais e civis, bem como *defacement* (desfiguração) de sites oficiais e de veículos da mídia e *spamming* das caixas de e-mail de membros do governo (MARKOFF, 2008). O caso foi considerado um marco por ser a primeira vez em que um conflito militar tradicional acontecia apoiado por ataques cibernéticos. Shakarian (2011) argumenta que o objetivo dos ataques teria sido isolar o país da comunidade internacional e silenciar a mídia e a população que apoiava a posição do governo georgiano.

Stuxnet (2010)

Em 2010, a proliferação de publicações sobre o *Stuxnet* – *malware* que afetou o funcionamento de usinas de enriquecimento de urânio do Irã, atrasando em alguns anos o projeto nuclear do país – teve grande impacto sobre a percepção da opinião pública sobre os possíveis efeitos de ataques cibernéticos. Por um lado, ressaltou-se o alto grau de sofisticação

do ataque[24] e a decorrente percepção da elevada capacidade dos atores envolvidos em sua elaboração e execução (RID, 2012); e , por outro, os efeitos diretos do *malware*, ser um ataque a que Siedler (2016) chama "de força bruta", que – ao contrário do observado nos casos da Estônia e da Geórgia – não visava coagir uma mudança de posição política, mas que representou *per se* a mudança pretendida.

Vazamentos da NSA (2013)

Em 2013, o vazamento de documentos da *National Security Agency* (NSA) dos Estados Unidos, comprovando ações de espionagem cibernética da agência sobre populações e governos de outros países, também corroborou a hipótese de atuação sistemática de estados nacionais no ciberespaço. O vazamento confirmou a utilização de inteligência de sinais e espionagem cibernética como forma de influenciar decisões políticas, entre as quais as discussões do Conselho de Segurança das Nações Unidas (CSNU) sobre aplicação de sanções ao Irã em decorrência de seu programa nuclear (CASADO; KAZ; GREENWALD, 2013). O episódio ensejou uma crise diplomática entre Brasil – um dos alvos da espionagem da NSA[25] – e EUA e o patrocínio pelo Brasil e Alemanha – também alvo da agência estadunidense – de duas resoluções intituladas *O direito à privacidade na era digital*, em 2013 e 2014[26], além de fortalecer as iniciativas de normatização da atuação estatal no domínio cibernético. (ABDENUR; GAMA, 2015; SANTORO; BORGES, 2017).

---

[24] O código do *Stuxnet* foi escrito especificamente para dois modelos de controladores lógicos da Siemens usados em Sistemas de Controle Industrial (*Supervisory Control and Data Acquisition* – SCADA) do programa nuclear iraniano, sem acesso à internet ou redes internas (*air gap*). A infecção provavelmente aconteceu através de *pendrive* inserido nos *laptops* de manutenção dos sistemas alvejados. Estima-se que no final de 2010 infecções colaterais tenham chegado a 100 mil servidores em vários países, 60% dos quais no Irã. O *Stuxnet* identificava as configurações do sistema infectado e só prosseguia com o ataque após confirmado o alvo. Por não possuir acesso a redes, toda a programação das ações de sabotagem já estava inserida no código. Uma vez iniciado o ataque, o *software* alterava a frequência de motores, danificando rotores, turbinas e centrífugas ao mesmo tempo em que mostrava dados de funcionamento normal, copiados antes do ataque. (RID, 2012). Para descrição mais detalhada do funcionamento do *Stuxnet*, ver Rid (2012).

[25] Entre os documentos vazados, alguns apontavam o Brasil como alvo prioritário e a realização de vigilância cibernética sobre representações do país no exterior, além da existência de base de coleta de informações de satélites em Brasília até 2002. (CASADO, J.; KAZ, R.; GREENWALD, G. EUA espionaram milhões de e-mails e ligações de brasileiros. País aparece como alvo na vigilância de dados e é o mais monitorado na América Latina. *O Globo* online, 6 jul. 2013. Disponível em: https://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934. Acesso em: 26 nov. 2019.

[26] ASSEMBLEIA GERAL DA ONU (AG). Resolução nº 68/167. AG Index: A/RES/68/167, 18 dez. 2013. Disponível em: http://undocs.org/A/RES/68/167 e ASSEMBLEIA GERAL DA ONU. Resolução nº 69/166. AG Index: A/RES/69/166, 18 dez. 2014. Disponível em: http://undocs.org/A/RES/69/166.

APT 01 (2013)

Também em 2013, a empresa de segurança cibernética estadunidense Mandiant – posteriormente incorporada pela FireEye – atribuiu com elevado grau de certeza o grupo de espionagem cibernética APT[27] 01 à China. O grupo teria espionado, desde 2006, dados de 141 organizações em 20 setores da economia e indústria, tendo mantido acesso às redes dessas empresas por uma média de 365 dias, e atingido o máximo período de quatro anos e dez meses em um dos alvos. O relatório apresenta elementos que indicam que o grupo seja o 2º Escritório do Departamento Geral do Exército de Libertação Popular Chinês, também conhecido como Unidade 61398 (MANDIANT, 2013).

Guerra russo-ucraniana (2014)

Em 2014, após o governo ucraniano rejeitar o acordo de associação do país à União Europeia (UE), que havia sido previamente aprovado pelo parlamento, uma série de protestos que ficaram conhecidos como Euromaidan marcou o início da crise política entre nacionalistas ucranianos e separatistas pró-Rússia, que culminou na ocupação e posterior anexação das regiões de Donbass e da Crimeia pela Rússia. Durante os conflitos, uma série de ataques cibernéticos foi realizada juntamente às campanhas militares tradicionais, incluindo: ataques de negação de serviço e desfiguração contra alvos de ambas as partes (de um lado, sites da mídia *Russia Today* (RT), do outro lado, *sites* da Otan e do CCDCOE), campanhas de espionagem cibernética realizadas por APTs alegadamente baseados na Rússia; vazamentos e bloqueio de telefones celulares de políticos ucranianos; ataque contra a Comissão Central de Eleições da Ucrânia e divulgação de resultados falsos nas eleições de 2014; e utilização de dados da internet para a localizar e alvejar forças militares ucranianas. Além disso, durante a ocupação, tropas especiais russas tomaram o controle de um ponto de troca de tráfego[28], além de cabos de servidores de internet (GEERS, 2015). Durante o conflito, foi registrado o primeiro caso publicamente reconhecido de ataque cibernético bem-sucedido na derrubada prolongada de um sistema elétrico (KOSTYUK, N.; ZHUKOV, Y. M., 2017, p. 1).

---

[27] APT é a sigla de *Advanced Persistent Threat*, ameaças avançadas persistentes, e são grupos *hackers* caracterizados por alta capacidade técnica e sobre os quais frequentemente paira a suspeita de patrocínio de Estados-nação.

[28] Os pontos de troca de tráfego funcionam como *hubs* em que provedores podem conectar seus servidores, facilitando o tráfego de informações. Disponível em: www.techtudo.com.br/noticias/noticia/2014/04/o-que-e-ptt-conhecidos-como-pontos-de-troca-de-trafego-na-internet.html.

Eleições presidenciais dos EUA (2016)

Em outubro de 2016, o governo dos Estados Unidos acusou formalmente a Rússia de interferir nas eleições presidenciais do país através do vazamento de e-mails de membros do Comitê do Partido Democrata. Organizações de inteligência consideraram que os métodos e motivações identificados eram consistentes com a atuação russa. A obtenção de acesso às redes do Comitê do Partido Democrata teria ocorrido em julho de 2015, sendo mantida até pelo menos junho de 2016. O Comitê do Partido Republicano também teria sido hackeado, sem que houvesse vazamento das informações armazenadas ali.

Relatório ostensivo da Comunidade de Inteligência dos Estados Unidos publicado em janeiro de 2017[29] afirma que o uso de vazamentos desse tipo por Moscou não tinha precedentes, contudo convergia com as estratégias russas de uso de mensageria persistente misturada a operações de inteligência (incluindo atividades cibernéticas) com esforços ostensivos de agências governamentais, mídia patrocinada pelo governo e "influenciadores digitais" e *trolls*. (OFFICE FOR THE DIRECTOR OF NATIONAL INTELLIGENCE; NATIONAL INTELLIGENCE COUNCIL, 2017, p. 2).

Os casos mencionados acima têm em comum o envolvimento, direta ou indiretamente, de Estados-nação, visando atingir objetivos de relações internacionais – seja como executores, patrocinadores ou vítimas de ataques cibernéticos. A proliferação desse tipo de incidente a partir de 2007 representou material para a análise de estudiosos de RI, atuando como um incentivo ao desenvolvimento do tema na disciplina.

Necessidade de sistematização

O conhecimento das interpretações atuais da ascensão do ciberespaço na literatura de RI é de importância basilar para o desenvolvimento subsequente do tema. É com essa consideração em mente que se nota a necessidade de maior número de estudos que sistematizem essas interpretações até o presente momento, com vistas a observar, por exemplo, a evolução quantitativa e qualitativa da produção científica em questão, o contexto internacional em que

[29] OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE; NATIONAL SECURITY INTELLIGENCE. *Background to "Assessing Russian Activities and Intentions in Recent US Elections"*: The Analytic Process and Cyber Incident Attribution, 6 jan. 2017. Disponível em: https://apps.washingtonpost.com/g/documents/national/read-the-declassified-report-on-russian-interference-in-the-us-election/2433.

se desenvolveu, principais conceitos e debates identificados e de que forma ela se relaciona às escolas paradigmáticas das RI.

Revisões de Literatura Anteriores

Revisões de literatura sobre a ascensão do ciberespaço nas RI por Reardon e Choucri (2012) e Gorwa e Smeets (2019) apresentam importantes indicadores da produção científica sobre o tema, sem, contudo, aprofundar a sistematização de conceitos e debates do campo de estudos. Ao passo que os primeiros revisam a disciplina de RI como um todo, com foco em debates teóricos da literatura, os últimos apresentam artigos especificamente sobre conflito internacional, com foco em suas abordagens metodológicas.

Reardon e Chourcri (2012) revisam uma amostra bibliográfica composta de 49 artigos publicados em importantes periódicos de relações internacionais e ciência política, em língua inglesa, entre 2001 e 2010. A revisão apresenta, nesse sentido, uma visão ampla da disciplina, identificando cinco áreas temáticas distintas na abordagem da ascensão do ciberespaço pelas RI, a saber: sociedade civil global, governança, desenvolvimento econômico, os efeitos sobre regimes autoritários e segurança. As referidas áreas temáticas se unificariam em torno das questões centrais do esforço de definição do objeto de estudo, dos efeitos qualitativamente transformadores do ciberespaço na política internacional – particularmente o empoderamento de atores anteriormente marginalizados – e de esforços teóricos para compreender a relação entre tecnologia e política (REARDON; CHOUCRI, 2012, p. 4). O trabalho, contudo, não leva em consideração a variação do impacto dos artigos dentro da literatura revisada, de forma que falha em apontar quais desses temas são mais frequentemente abordados dentro da academia de relações internacionais como um todo.

Gorwa e Smeets (2019), por sua vez, revisam a literatura não da disciplina de RI como um todo, mas limitada ao tema conflito cibernético. Sua amostra bibliográfica é constituída de 70 textos publicados entre 1990 e 2018 e selecionados nos cem periódicos mais importantes das áreas de RI e ciência política conforme o índice SciMago[30]. A análise bibliométrica dessa amostra aponta as fontes mais relevantes e artigos de maior impacto sobre o tema, concluindo que, mesmo em comparação com temas recentes das RI, por exemplo as política e governança climáticas, a produção científica existente sobre questões cibernéticas apresenta número médio de citações bastante inferior.

[30] O índice *SCImago Journal Rank* é um indicador de relevância de periódicos com base no número de citações recebidas por um periódico e pela importância ou prestígio dos periódicos de onde essas citações vêm.

Ademais, Gorwa e Smeets (2009) revisam a literatura sob a ótica das metodologias empregadas na elaboração dos artigos. Suas descobertas apontam que a maior parte da amostra não se preocupa em explicitar um desenho de pesquisa; que se caracterizam mais enquanto propostas de natureza teórica e menos enquanto testes de hipóteses anteriores, ou seja, há poucos estudos empíricos; e que a maioria dos artigos sobre conflito cibernético utiliza uma lógica de causalidade baseada em mecanismos e capacidades[31] e que há predomínio de estudos qualitativos em relação a pesquisas quantitativas, percepção corroborada por Kostyuk e Zhukov (2017).

Os achados dos autores dão conta da relevância dos estudos de caso e de sua concentração em quatro casos específicos: os ataques à Estônia (2007), à Geórgia (2008), o *worm* Stuxnet (2010) e o ataque à empresa Sony atribuído à Coreia do Norte, em 2014, sendo a escolha desses casos raramente justificada. Nesse sentido, os autores afirmam:

> A abordagem mais comum em nosso conjunto de dados foi simplesmente selecionar exemplos para apoiar seus argumentos. Em vez de se envolver com um punhado de estudos de caso aprofundados, esses artigos tecem exemplos históricos (e material de fontes primárias e secundárias que incluem relatórios do governo, de empresas de inteligência de ameaças e cobertura da imprensa) em seus argumentos. É claro que isso é compreensível quando existe um número relativamente limitado de casos bem conhecidos que são amplamente reconhecidos como importantes; no entanto, essa abordagem não é sistemática e os casos podem ser facilmente selecionados para se adequar ao argumento que está sendo desenvolvido. (GORWA; SMEETS, 2019, p. 18)

As revisões de literatura de Reardon e Choucri (2012) e Gorwa e Smeets (2019) são pontos de partida muito relevantes para quaisquer estudos que pretendam tratar de questões cibernéticas nas RI. A despeito das diferenças na forma de escolha da amostra bibliográfica, nos períodos abordados e nas próprias abordagens de cada revisão, elas apresentam coesão nas avaliações das características da literatura e nas percepções sobre suas contribuições e limites. Contudo, não há nas referidas revisões a apresentação mais detida dos pontos de divergência nos debates conceituais e tampouco são apresentados em detalhes os argumentos dos debates teóricos identificados.

---

[31] "Brady discute quatro abordagens para causalidade em Ciência Política. Primeiro, há a abordagem da regularidade neo-humeana – voltando a Hume e Mill, que busca determinar a causalidade por meio da 'observação de conjunção e correlação constantes' e 'precedência temporal'. Segundo, há a abordagem de aproximação contrafactual, abordando causalidade por meio da compreensão de situações semelhantes na lógica 'se a causa ocorre, então o efeito ocorre' e 'se o efeito não ocorrer, a causa ainda pode ocorrer'. Terceiro, a abordagem de manipulação busca determinar uma 'receita que produz regularmente o efeito da causa'. Finalmente, há a abordagem de mecanismos e capacidades, com foco no funcionamento do mecanismo ou capacidade que leva da causa ao efeito." (GORWA; SMEETS, 2019, tradução da autora).

Objetivos desta Dissertação

A abordagem do ciberespaço pela disciplina de Relações Internacionais frequentemente menciona a indefinição conceitual como um limite ao desenvolvimento de estudos subsequentes. Especificamente no que tange a conflitos cibernéticos e segurança internacional, Betz e Stevens (2011), Melzer (2011), Schreier (2015) e Kello (2013) chamam a atenção para o fato de que não apenas no ambiente acadêmico, mas também no político, não há clareza quanto às definições, por exemplo, de ataque, uso da força, conflito, guerra, hostilidades e segurança cibernéticas.

A falta de uniformidade nos conceitos utilizados, somada à rapidez no desenvolvimento das tecnologias de informação e comunicação, ao aumento exponencial de sua capacidade de produção e análise de dados e o hermetismo de aspectos técnicos da informática – manifestos notadamente nas linguagens de programação – dificultam a abordagem da questão por cientistas sociais, entre os quais os internacionalistas. Nesse sentido, Kello (2013) afirma que, entre os estudiosos de RI, teria se criado um senso de resignação decorrente da "presunção de inescrutabilidade das tecnologias cibernéticas" e que a manutenção de uma postura de desinteresse ou perplexidade dos acadêmicos de RI em relação ao ciberespaço tende a erodir a relevância de conceitos teóricos das RI, implicando eventualmente a inibição do progresso intelectual da disciplina devido à perda de fertilidade conceitual ou reduzida capacidade de análise (KELLO, 2013), o que justificaria a pouca quantidade de textos sobre o tema e sua relevância ainda tímida comparativamente a outros temas das RI, apontada por Gorwa e Smeets (2019).

Frente ao exposto, os objetivos desta dissertação são:

- Traçar um panorama da produção científica de Segurança Internacional sobre a ascensão do ciberespaço, buscando identificar tendências gerais dessa produção científica;
- Identificar, sistematizar e discutir os principais conceitos e debates dessa literatura;

Inicialmente, a pesquisa realizada pretendia identificar interpretações das RI de forma geral, no entanto, curiosamente, a definição da amostra bibliográfica apresentou resultados aglutinados na subárea de Segurança Internacional, a despeito de a busca por literatura ter sido realizada utilizando parâmetros generalistas que pudessem abarcar resultados em todas as subáreas das RI. Considerações acerca desse fato e da definição da amostra bibliográfica são apresentadas no capítulo 1.

Ressalta-se, ainda, que o desenvolvimento de uma revisão sistemática de literatura apresenta um caráter metadisciplinar, na medida em que seus resultados não dizem respeito diretamente ao objeto de estudo, mas às abordagens sobre esse objeto encontradas na literatura. Dito de outra forma, não são analisados aqui dados primários sobre utilização do domínio cibernético nas relações internacionais, mas as abordagens e temas identificados na literatura de Segurança Internacional, bem como sua sistematização e discussão constituem os principais objetos desta dissertação.

Estrutura desta Dissertação

O Capítulo 1 apresenta as considerações metodológicas da elaboração desta dissertação, entre elas as defesas da análise bibliométrica e da revisão sistemática de literatura como metodologias para conhecer um campo de estudos, detalha a escolha das amostras bibliográficas trabalhadas conforme esses métodos e apresenta as limitações do presente estudo. Além disso, são apresentados os resultados da análise bibliométrica (dados de evolução cronológica da literatura, distribuição por idioma de publicação, número de citações, veículos de divulgação, área de pesquisa em que os documentos foram indexados, palavras-chave e peso das palavras-chave). As observações derivadas da análise bibliométrica permitiram afunilar o escopo pretendido para a revisão sistemática de literatura, limitando-o ao que foi efetivamente encontrado, ou seja, abordagens de Segurança Internacional – e não das Relações Internacionais como um todo – sobre a ascensão do ciberespaço.

O Capítulo 2 apresenta os resultados da revisão sistemática de literatura no que tange os conceitos centrais identificados na literatura revisada, quais sejam, ciberespaço, guerra cibernética e segurança cibernética. A indefinição desses termos é sublinhada, na medida em que representa a dificuldade da comunidade de Segurança Internacional em especificar seus objetos de estudo relacionados à ascensão do ciberespaço e é um limite à evolução dos debates na área. A apresentação e discussão dos conceitos serve, dessa forma, para embasar a discussão apresentada no Capítulo 3 sobre os principais debates identificados na literatura revisada.

Os principais debates identificados na literatura revisada são apresentados no Capítulo 3. São eles: o debate central acerca da gravidade da chamada "ameaça cibernética" e da possibilidade de uma guerra cibernética (feita a ressalva de que não há consenso na utilização do termo); e os debates acessórios a essa discussão na forma das problematizações sobre a efetividade de ataques cibernéticos enquanto instrumento de coerção na política internacional, seu aspecto multiplicador ou independente em relação a outros domínios em situações de

conflito; sobre a possibilidade de uso do ciberespaço em estratégias de dissuasão e/ou sua influência nos riscos de escalada não planejada de conflitos; na discussão sobre a relação de atores estatais e não estatais no domínio cibernético; e na apresentação do argumento de que o discurso sobre segurança cibernética está no centro de um processo de securitização. Além disso, constam no Capítulo 3 uma discussão ontológica acerca do que constitui poder cibernético e se esse apresenta diferenças fundamentais em relação a outras manifestações de poder; e uma seção que explora de que forma as abordagens identificadas se relacionam aos paradigmas das R.I realismo, liberalismo e construtivismo.

Finalmente, a Conclusão procura retomar descobertas apresentadas ao longo dos capítulos anteriores, apontando uma agenda de pesquisa passível de aprofundamento futuro.

1. CONSIDERAÇÕES METODOLÓGICAS E ANÁLISE BIBLIOMÉTRICA

1.1. Considerações Metodológicas

1.1.1. Defesa da análise bibliométrica

Apesar de a aplicação de métodos bibliométricos ser mais popular e significativa nas ciências naturais, sua aplicação nas ciências sociais poderia ser bastante produtiva (VAN LEEUWEN, 2006). Mapas bibliométricos contribuem com a visualização e sumarização de grandes volumes de dados e no estudo de resultados científicos.

Nas RI, Kristensen (2015) fez uso da análise de dados bibliométricos, também de trabalhos indexados na WoS, para avaliar a questão da geografia das RI. Conforme o autor, metodologias bibliométricas especializadas são utilizadas comumente na sociologia da ciência, mas surpreendentemente têm pouco engajamento nas RI (KRISTENSEN, 2015). O método também foi utilizado por Gorwa e Smeets (2019), que apresentaram uma análise bibliométrica da literatura de RI sobre conflitos cibernéticos.

Anyi, Zainab e Anuar (2009) enumeram dados bibliométricos passíveis de análise, bem como algumas de suas aplicações. Por exemplo, a análise da evolução da quantidade de artigos publicados por ano em dado período pode indicar tendências de publicação. Da análise dos meios onde esses artigos foram publicados pode-se inferir a influência de periódicos específicos para a disseminação da pesquisa entre autores do campo. Quanto à análise de conteúdo, Anyi, Zainab e Anuar (2009) mencionam a análise de dados bibliométricos referentes à área de publicação (*issue areas*), às palavras-chave *(keywords*) e à co-ocorrência desses parâmetros, que permitiria avaliar a interação entre diferentes áreas de pesquisa e subtemas. Além disso, a análise do número e distribuição de citações por artigo, periódicos e ano, das redes de cocitações, idade, localização geográfica e distribuição por idioma da literatura mais citada permitem fazer avaliações de relevância de um artigo em relação à produção científica de sua área.

1.1.2. Revisão sistemática de literatura e teoria do enfoque meta-analítico.

A necessidade de sistematizar a busca por literatura relevante e representativa de determinado campo de estudos, com grau de objetividade aceitável na comunidade acadêmica, ensejou a criação de metodologias de revisão bibliográfica.

Helmericks, Nelsen e Unnithan (1991) argumentam que a fragmentação dos temas de ciências sociais entre diversas disciplinas e até mesmo dentro de uma mesma disciplina – entre diferentes abordagens – frequentemente leva a algum grau de arbitrariedade na escolha de teorias para a análise de fenômenos e na seleção da amostra bibliográfica a ser revisada (HELMERICKS, S. G.; NELSEN, R. L.; UNNITHAN, 1991, p. 286). Nesse sentido, procuram estabelecer procedimentos que diminuam essa arbitrariedade ou viés. Em abordagem semelhante, Okoli (2015) defende que "as revisões não deveriam ser apenas bibliografias extensas que listam uma sequência de artigos, mas concentrar-se diretamente em conceitos teóricos e desenvolver, a partir deles, uma história teórica coerente" (OKOLI, 2015, p. 880).

Frente à impossibilidade de efetivamente conhecer toda a produção acadêmica sobre um tópico, o processo de escolha da amostra bibliográfica deve estabelecer um recorte que identifique os autores e publicações mais relevantes para a amostra bibliográfica daquele tema. A validação desses autores e publicações pode acontecer por "consenso" – os mais citados são considerados relevantes e, portanto, devem ser parte da amostra bibliográfica –; ou por "*gatekeepers"* – por meio da consulta dos periódicos e editoras de maior prestígio junto à comunidade acadêmica de determinada área. A validação por "*gatekeepers*" deriva da crença no "controle de qualidade" realizado por eles. (HELMERICKS, S. G.; NELSEN, R. L.; UNNITHAN, 1991, p. 290)

Okoli (2015) diferencia três tipos de revisões sistemáticas de literatura. O primeiro tipo, considerado o mais comum, é o referencial teórico, parte de um artigo científico que busca apresentar fundamentos teóricos e contexto do problema de pesquisa, procurando localizá-lo na discussão acadêmica sobre o tema. O segundo tipo, chamado revisão de literatura de tese, é mais amplo e trata-se da revisão de literatura como capítulo de uma dissertação ou tese de pós-graduação. Finalmente, a revisão autônoma de literatura é o terceiro tipo de revisão sistemática de literatura e analisa em profundidade a produção científica de um tema sem que haja coleta ou análise posterior de dados primários (OKOLI, 2015).

A presente revisão sistemática de literatura sobre interpretações da ascensão do ciberespaço na disciplina de RI assenta-se no terceiro tipo, revisão autônoma de literatura, na medida em que não são analisados dados primários sobre utilização do domínio cibernético nas relações internacionais à luz de abordagens identificadas na literatura. As próprias abordagens e temas identificados, bem como sua sistematização e discussão, constituem os principais objetos desta dissertação.

Okoli (2015) argumenta que a publicação de uma revisão autônoma de literatura beneficia a comunidade acadêmica ao proporcionar a diminuição do tempo e esforço

empregados na pesquisa posterior. Para que esse efeito benéfico seja atingido é necessário que o trabalho de revisão inspire a confiança nos pesquisadores de que tenha sido realizado adequadamente. Sua definição de revisão de literatura autônoma rigorosa exige que os procedimentos adotados na seleção e análise da amostra bibliográfica sejam sistemáticos, explícitos, abrangentes e reprodutíveis. (OKOLI, 2015, p. 880). Nesse sentido, o processo de inclusão e exclusão de fontes deve ser tão transparente quanto seja possível. A publicação explícita e detalhada dos critérios e procedimentos adotados durante a escolha da amostra bibliográfica a ser revisada contribui com a evolução da produção científica na área, pois assume as limitações que podem ter afetado seu resultado. Também Helmericks, Nelsen e Unnithan (1991) afirmam que a transparência dos revisores é uma solução possível – e a preferível – frente à dificuldade de abranger e sistematizar grandes corpos de literatura.

Uma revisão sistemática de literatura deve apresentar, ainda, um elemento analítico crítico. "A revisão não pode simplesmente regurgitar o assunto em questão: ela deve contribuir para o trabalho em sua abordagem dual de sintetizar o material disponível e oferecer a crítica acadêmica da teoria" (KEKÄLE; WEERD-NEDERHOF; CERVAI; BORELLI, 2009 *apud* OKOLI, 2015, tradução nossa).

A união da revisão sistemática de literatura com técnicas de bibliometria deu origem à Teoria do Enfoque Meta-analítico (Temac)[32]. Trata-se de um método de revisão de literatura que visa identificar, inter-relacionar e apresentar a literatura científica mais relevante a respeito de um tema (MARIANO; ROCHA, 2017), acrescentando à Revisão Sistemática de Literatura um aspecto estatístico[33].

Na prática isso significa delimitar parâmetros de busca da literatura que se pretende revisar (palavras-chave, período, áreas de pesquisa, entre outros) a serem aplicados em bases de dados científicas, a exemplo da Web of Science (WoS), Scopus, Scielo, Google Academic e Capes. Os resultados dessa busca são então exportados para *softwares* de análise desses dados (por exemplo, Gephi, VosViewer ou Tableau), que indicam graficamente relações de citação, cocitação, acoplamento bibliográfico (entre outros) entre autores, artigos, periódicos (entre outros). Com base nesse resultado é possível delimitar as publicações de maior relevância para critérios predefinidos, através da visualização dos "nós" de maior peso na rede de produção

[32] Mariano; Rocha (2017).

[33] Glass (1976) foi o primeiro a utilizar o termo meta-análise e com ele procurou se referir à "análise da análise". "Uso-o para referir a análise estatística de uma grande coleção de resultados de análise de estudos individuais para fins de integração dos resultados. O termo conota uma alternativa rigorosa para as discussões narrativas e casuais de estudos de pesquisa que caracterizam as tentativas de compreensão da literatura de pesquisa em rápida expansão." (GLASS, 1976, p. 3)

científica. Definida a amostra bibliográfica a ser revisada, passa-se ao trabalho analítico da literatura.

É importante notar que, como observado por Helmericks, Nelsen e Unnithan (1991), não seria produtivo excluir da bibliografia analisada textos com que porventura se tenha tido contato de forma menos sistemática, como a partir da sugestão de colegas e orientadores, pesquisas em bibliotecas e buscas espontâneas, desde que haja transparência quanto a sua inclusão na amostra bibliográfica revisada.

1.1.3. Amostra bibliográfica inicial e amostra bibliográfica final

Nesta dissertação a base de dados escolhida para realização da pesquisa de bibliografia sobre interpretações da ascensão do ciberespaço na disciplina de RI foi a *Web of Science (*WoS*)*. Trata-se de uma "base multidisciplinar que indexa mais de 12.700 periódicos, nas diferentes áreas científicas, contendo informações desde o início do século XX, sendo atualizada semanalmente" (MARIANO; ROCHA, 2017, p. 430). A informação fornecida pela WoS especificaria os periódicos ativos na cobertura de pesquisa atual e relevante, bem como é proeminente na formatação de campos de pesquisa (AGHAEI CHADEGANI *et al.*, 2013, p. 24).

Nesse sentido, a escolha da WoS permite preencher os requisitos de "consenso" – a avaliação da produção mais citada – e de consulta aos "*gatekeepers*", na medida em que fornece os dados bibliométricos (que incluem o número de citações) e realiza a "curadoria" dos periódicos de maior prestígio junto à comunidade acadêmica de RI, conforme recomendado por Helmericks, Nelsen e Unnithan (1991) para o estabelecimento do recorte que identifique autores e publicações mais relevantes para a amostra bibliográfica daquele tema.

Duas amostras bibliográficas diferentes foram utilizadas na pesquisa. A amostra bibliográfica inicial[34] decorre diretamente da busca realizada na WoS e é trabalhada quantitativamente em uma análise bibliométrica, com vistas a apresentar o panorama e a evolução cronológica da produção sobre a ascensão do ciberespaço pela disciplina de RI.

[34] A amostra bibliográfica inicial é apresentada no Anexo I.

A amostra bibliográfica final decorreu da análise da amostra bibliográfica inicial pelo *software* VosViewer[35]. Foram selecionados os documentos mais relevantes em termos de citação e de número de vínculos com outros documentos e é essa a literatura que constitui prioritariamente o objeto da revisão sistemática de literatura autônoma aqui apresentada. Os documentos dessa amostra foram trabalhados qualitativamente, de forma a extrair dali os principais conceitos e debates identificados. A escolha de outros parâmetros para a seleção de literatura relevante – como a consulta aos índices SciMago JCR de impacto de periódicos e o h-index, de impacto de autores – é possível e de fato o parâmetro de impacto de periódicos foi utilizados no trabalhos de Gorwa e Smeets (2019).

1.1.4. Detalhamento da definição das amostras bibliográficas

1.1.4.1.Parâmetros de busca

A busca na Coleção Principal da *WoS*[36] foi realizada em 26 de fevereiro de 2020, utilizando os termos*: cyber e cyber** no campo "TÓPICO"[37], de forma que abrangesse termos com prefixo "*cyber*" como *cyberspace*, *cyberpower*, *cybersecurity*, *cyberwar* e *cybergovernance*, entre outros, para o período de 1945-2020, utilizando o indicador booleano OR. A busca foi restrita, então, à área de relações internacionais, resultando 517 documentos (artigos científicos, *proceeding papers, book reviews*, entre outros*)*.

1.1.4.2.A criação da tabela (arquivo .xlsx) para "manuseio" dos dados bibliométricos

O resultado da busca na WoS foi disponibilizado em um arquivo do tipo .txt, passível de leitura pelo *software* de análise de dados bibliométricos VosViewer. A WoS exporta os resultados até o limite máximo de 500 documentos e, além disso a limpeza desses dados acarretou a perda de dados de 12 documentos, de forma que o número de documentos da amostra bibliográfica inicial totaliza 488 documentos. A diferença entre os resultados obtidos

---

[35] O VosViewer é uma ferramenta para criação de mapas baseada em dados de rede e para visualização e exploração desses mapas. (WALTMAN; LUDO; VAN ECK, 2019). Manual for VosViewer version 1.6.11. University of Leiben e CWTS, 2019, tradução nossa. Disponível em: https://bit.ly/2RQyERB.

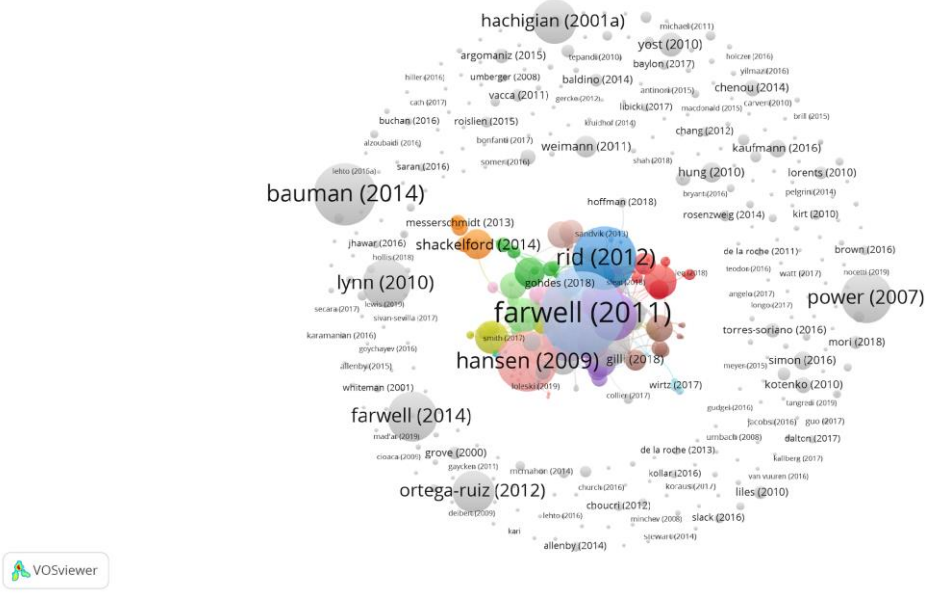
[36] O portal da WoS oferece possibilidade de pesquisa em outras bases de dados compatíveis, a exemplo da Scielo, contudo apenas os resultados referentes à Coleção Principal da WoS foram passíveis de serem exportados para o software de análise de dados VosViewer.

[37] A pesquisa no campo "TÓPICO" inclui os seguintes marcadores: Título, Resumo, Palavras-chave, *Keywords Plus*. Disponível em: http://images-webofknowledge.ez54.periodicos.capes.gov.br/WOKRS532MR24/help/pt_BR/WOS/hs_topic.html.

na busca da WoS e o número de documentos da amostra bibliográfica e representa 5% do total dos documentos resultantes da busca e foi considerada residual.

A Figura 1 apresenta a visualização da amostra bibliográfica inicial (rede de produção científica sobre fenômenos questões cibernéticas nas RI[38] resultante da busca detalhada. O tamanho dos "nós" indica a quantidade de citações, e a ligação entre esses nós diz respeito à "força de associação" (*association strength*[39]) entre eles.

Figura 1 – Visualização da rede de produção científica sobre fenômenos cibernéticos nas RI



A interpretação da Figura 1 indica que parte importante da produção científica sobre fenômenos cibernéticos em RI aglutina-se num núcleo dessa produção. Nota-se, ainda, que há trabalhos de grande peso (alto número de citações representado pelo tamanho dos nós) que estão fora desse núcleo.

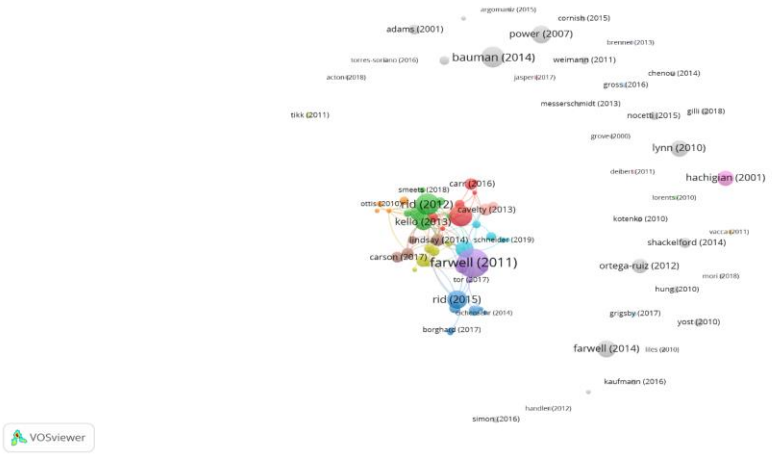
1.1.4.3.A definição da amostra bibliográfica final

[38] A visualização apresentada diz respeito a 500 documentos, já que teve por base o próprio arquivo .txt da WoS.

[39] O método de força de associação é usado para normalizar a força das ligações entre os itens. Trata-se da opção selecionada por padrão pelo VosViewer. Disponível em: www.vosviewer.com/documentation/Manual_VOSviewer_1.6.11.pdf.

Após exportação do registro completo e referências citadas dos documentos resultantes da busca na WoS para o *software* VosViewer, foi realizada a análise de citações[40] restrita a documentos que possuíam o mínimo de cinco citações, de forma a limitar o tamanho da amostra bibliográfica para viabilizar a revisão sistemática de literatura e selecionar documentos de maior impacto, totalizando 85 documentos. A análise dessa amostra intermediária gerou o seguinte diagrama.

Figura 2 – Diagrama resultante da análise dos resultados da busca na WoS por documentos contendo cyber ou cyber* no campo "Tópico", da área de Relações Internacionais, com o mínimo de 5 citações, pelo VosViewer, com base na funcionalidade Análise de Citação do software.

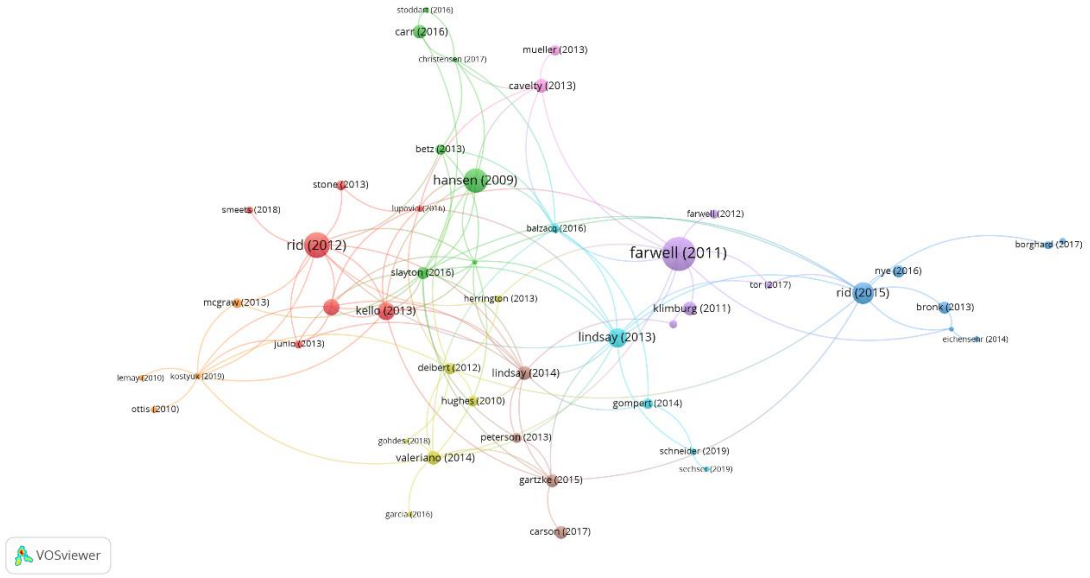


Na Figura 2, o tamanho dos "nós" corresponde ao número de citações totais do documento; a ligação entre esses nós diz respeito à "força de associação" dos vínculos de citação de um documento noutro; e a utilização de cores diferentes representa *clusters*, normalmente referidos na literatura como "comunidades" (WALTMAN; VAN ECK, 2019, p.

[40] Conforme Moraes, Furtado e Tomaél (2015), "a Análise de Citações baseia-se na premissa de que os pesquisadores concebem seus trabalhos a partir de obras anteriores e demonstram isso citando as obras precedentes em seus textos e em uma lista ordenada e padronizada de referências. O comportamento dos cientistas fica evidente a partir do estudo dessas citações (MOREL; MOREL, 1977). Desse modo, e diante da importância que as referências bibliográficas representam num trabalho científico, a análise dessas referências, que são denominadas no campo da bibliometria como Análise de Citação, vem sendo empregada como um importante instrumento metodológico de mapeamento da produção intelectual de diversas áreas do conhecimento. O emprego da Análise de Citação serve para diversas finalidades como a indicação de tendências de temáticas de pesquisa, indicadores de citação e mapeamento de áreas do conhecimento mais citadas em determinada produção científica" (MORAES; FURTADO; TOMAÉL, 2015).

5)[41]. Como é possível apreender do diagrama, um número considerável de documentos não está relacionado com o grupo principal, formado por textos com maior número de citações e vínculos entre si. Nesse sentido, o resultado foi novamente filtrado, de forma a manter na amostra bibliográfica final apenas os documentos participantes do núcleo da produção científica identificada, totalizando 47 documentos.

Figura 3 – Núcleo da rede bibliográfica identificada na WoS após análise bibliométrica pelo VosViewer



Ressalta-se que, conforme a consideração de Helmericks, Nelsen e Unnithan (1991) sobre a validade de incluir na amostra bibliográfica a ser revisada textos com os quais se depara de formas menos sistemáticas (a partir da sugestão de colegas e orientadores, pesquisas em bibliotecas e buscas espontâneas, por exemplo), mas que foram julgados relevantes para a compreensão do tema, ao núcleo da rede bibliográfica identificada no VosViewer (47 documentos) foram adicionados outros 13 artigos, livros e *proceeding papers*, totalizando uma amostra bibliográfica final de 60 documentos[42].

---

41 Waltman e Van Eck (2019) indicam Van Eck, Waltman, Dekker e Van den Berg (2010), Waltman, Van Eck e Noyons (2010), Waltman e Van Eck (2013) e Van Eck e Waltman (2014) para mais informações acerca dos algoritmos utilizados e critérios de determinação dos *clusters* pelo VosViewer.

42 A amostra bibliográfica final, incluindo os documentos adicionados discricionariamente, é apresentada no Anexo II.

1.1.5. Considerações sobre a definição das amostras bibliográficas

A importância do detalhamento de como é escolhida a amostra bibliográfica ficou bastante premente nesta dissertação. Curiosamente, a despeito de ter sido realizada utilizando parâmetros generalistas que pudessem abarcar resultados em todas as subáreas das RI (os filtros utilizados na busca foram a disciplina de RI, os tópicos "cyber" e "cyber*", e o número de citações e vínculos de citação conforme detalhado anteriormente), a pesquisa para definição da amostra bibliográfica apresentou resultados limitados à subárea de Segurança Internacional. De forma diversa, Choucri e Reardon (2012) revisaram a literatura sobre o papel do ciberespaço nas RI entre 2001 e 2010 e identificaram cinco principais subáreas dessa literatura: sociedade civil global, governança do espaço cibernético, desenvolvimento econômico, os efeitos do ciberespaço em regimes autoritários e segurança.

Considerando que o número de artigos selecionados nas duas revisões é próximo (49 artigos por Choucri e Reardon e 60 documentos revisados nesta dissertação), a justificativa para essa diferença parece estar na forma de escolha da amostra bibliográfica a ser revisada. Ao passo que Choucri e Reardon (2012) selecionaram a literatura priorizando as fontes de publicação (26 periódicos de RI escolhidos com base em sua pontuação de impacto, amplitude de tópicos cobertos e metodologias e paradigmas representados) e o tópico (artigos focados em questões relacionadas ao ciberespaço, tecnologias de informação e comunicação, internet e redes sociais, e/ou a "revolução da informação" e artigos que se concentraram principalmente em questões internacionais), esta dissertação optou por realizar a busca em uma base de dados científica específica, a *Web of Science* (WoS), com parâmetros de busca generalistas e com foco no peso dos documentos medido por meio da análise de vínculos e número de citações pelo *software* VosViewer.

Gorwa e Smeets (2019) revisaram a literatura de RI sobre o mesmo tema – conflito cibernético –, tendo eles, no entanto, proativamente buscado pelo tema por meio da escolha dos parâmetros de busca *"cyber conflict", "cyber war", "offensive cyber", "offensive cyber operations", "military cyber operations", "cyber weapons"* e *"cyberweapons"* no título ou no resumo de artigos. Diferentemente, nesta dissertação não houve direcionamento da busca ao tema específico de "conflito", mas foi esse o resultado encontrado na amostra bibliográfica da *Web of Science*. Duas hipóteses foram levantadas para explicá-lo: a concentração no tema conflito decorre do filtro pelo número de citações, sendo a literatura sobre esse tema mais citada nas RI de forma geral; ou trata-se de uma aglutinação de artigos sobre o tema conflito derivada da base de dados *Web of Science.*

De toda maneira, a concentração da amostra bibliográfica final definida aqui obriga – em prol da clareza sobre os resultados encontrados nesta pesquisa – a limitar o escopo desses resultados ao que efetivamente foi identificado como o assunto da literatura revisada: o tema conflito cibernético, tratado sob o prisma da Segurança Internacional.

1.1.6. Seções da revisão sistemática de literatura

Na amostra bibliográfica final foram identificados conceitos e debates referentes às interpretações da segurança internacional sobre a ascensão do ciberespaço. Esses conceitos e debates são enumerados abaixo.

1.1.6.1.Conceitos

Seção de Discussão	Objetivo da sessão
Ciberespaço	
As analogias cibernéticas e suas implicações	Apresentar a discussão sobre o uso de analogias na conceituação de ciberespaço e suas implicações
Definições de ciberespaço	Apresentar diferentes conceitos de ciberespaço presentes na literatura revisada e os elementos recorrentes neles.
Baixo custo de entrada, anonimato, assimetrias de vulnerabilidades e dificuldades de atribuição de ataques cibernéticos	Apresentar a discussão sobre a validade dessas características como inerentes ao ciberespaço e suas implicações.
Ataque e defesa no ciberespaço	Apresentar a discussão sobre a validade da máxima de que o ataque é dominante em relação à defesa no ciberespaço.
Guerra cibernética	
Definições de guerra cibernética	Apresentar diferentes conceitos de guerra cibernética.
Definições negativas de guerra cibernética	Apresentar definições negativas de guerra cibernética, ou seja, aquilo a que a literatura explicitamente não se refere no uso do termo, procurando delimitar o objeto de estudo.
Guerra cibernética é guerra?	Apresentar a discussão sobre a possibilidade de ações de guerra cibernética (conforme definições apresentadas na seção anterior) atingirem o *status* de guerra na concepção convencional.
Guerra cibernética x guerra informacional	Apresentar a diferenciação feita na literatura revisada e em países e organizações internacionais entre os conceitos de guerra cibernética e guerra informacional.
Segurança cibernética x segurança da informação	Apresentar a diferenciação entre os conceitos de segurança cibernética e segurança da informação e as iniciativas de governança de segurança cibernética no âmbito das Nações Unidas.

1.1.6.2.Debates

Seção de Discussão	Objetivo da sessão
O ciberespaço e os paradigmas de RI	Apresentar considerações identificadas na literatura acerca da relação da produção científica de RI sobre questões cibernéticas com os principais paradigmas de RI e propor a categorização dos textos da amostra bibliográfica revisada nos paradigmas realista, liberal e construtivista.
A questão central: a ameaça cibernética é exagerada?	Apresentar a discussão central sobre o exagero ou não da "ameaça cibernética" nas relações internacionais, detalhando os argumentos a favor de uma ou outra resposta conforme subtópicos a seguir.
Eficácia de ataques cibernéticos	Apresentar a discussão da eficácia de ataques cibernéticos enquanto instrumentos de coerção política nas relações internacionais.
Dissuasão ou risco de escalada cibernética	Apresentar os argumentos de que o ciberespaço promove um ambiente propício à adoção de estratégias de dissuasão e/ou propício à escalada não planejada de conflitos.
Relação entre atores estatais e não estatais no ciberespaço	Apresentar três discussões sobre a relação entre atores estatais e não estatais no domínio cibernético: os impactos da ascensão do ciberespaço na distribuição de poder entre esses atores; a relação entre crime cibernético e atores estatais; e a relação entre os setores público e privado em arranjos institucionais de segurança cibernética.
Securitização do discurso sobre ciberespaço	Apresentar os argumentos de que os discursos político e científico-acadêmico sobre o ciberespaço passam por um processo de securitização.
Considerações sobre poder cibernético	Apresentar as considerações encontradas na literatura sobre poder cibernético e a discussão se ele constitui um fenômeno fundamentalmente diferente de outras manifestações de poder.

1.1.7. Limites desta revisão sistemática de literatura

O privilégio a conteúdos anglo-saxônicos observado na *Web of Science* (WoS), fonte primordial das amostras bibliográficas analisadas nesta dissertação, deve ser levado em consideração na avaliação do alcance dos resultados deste trabalho. Tal característica foi observada tanto por Aghaei Chadegani *et al.* (2013) quanto por Mariano e Rocha (2017), bem como corroborada na análise dos dados bibliométricos da amostra bibliográfica inicial.

Ainda, a dominância geográfica estadunidense na produção científica das RI. É abordada por Kristensen (2015) e Stuenkel (2018). Por meio do mapeamento das estruturas de redes de autoria e coautoria na produção científica de RI, Kristensen (2015) conclui que os acadêmicos baseados nos Estados Unidos, notadamente da costa leste do país, continuam a

dominar a produção publicada em periódicos de relações internacionais. A utilização do inglês na maior parte das publicações indexadas na WoS pode decorrer de os periódicos mais disseminados e lidos em RI serem editados nesse idioma, algo que ele caracteriza como um argumento sobre quais são os *gatekeepers* da área (KRISTENSEN, 2015, p. 8).

Por sua vez, Stuenkel (2018) afirma que a centralidade da produção acadêmica em língua inglesa ocorreria em detrimento da popularização da produção acadêmica em outros idiomas, implicando o desconhecimento de perspectivas diversas daquelas produzidas e reproduzidas sobretudo nos Estados Unidos. "A maioria dos analistas de assuntos internacionais na angloesfera produz análises provincianas, que celebram e defendem a civilização ocidental como sujeito e ideal normativo de referência da política mundial" (STUENKEL, 2018, p. 9).

No domínio cibernético, a questão torna-se ainda mais premente frente à grande relevância de atores que não utilizam o idioma inglês (Rússia, China, Irã e Coreia do Norte, por exemplo) na operacionalização de ações no domínio cibernético (a elaboração de códigos de *softwares*, por exemplo)[43] e, em alguns casos, na produção acadêmica de RI desses países.

Se considerarmos, ademais, o fenômeno descrito por Nye (2011) e Stuenkel (2018) que consiste na transição de poder de um polo ocidental com centro nos Estados Unidos para um polo oriental com centro na China, a limitação idiomática e seus desdobramentos sobre o acesso a conhecimentos acadêmicos, bem como a fontes primárias, a exemplo de códigos e táticas, técnicas e procedimentos (TTP), é ainda mais notável.

À questão idiomática e geográfica soma-se a importante ressalva de que na literatura analisada frequentemente se menciona "Estado-nação" como uma categoria conceitual, um tipo ideal. No entanto, na definição das características que atribui a esses atores, a maioria dos exemplos apresentados diz respeito a Estados nacionais considerados potências nas áreas de tecnologia da informação e comunicação, de forma que algumas conclusões apresentadas pela literatura no que tange à capacidade ou à atuação dos Estados-nação devem ser relativizadas, quando aplicadas a países considerados potências médias e regionais ou periféricos.

---

[43] Em 2019, o diretor da NSA e comandante do Comando Cibernético dos Estados Unidos fez a seguinte avaliação durante uma entrevista: "Quando olhamos concorrentes próximos, China e Rússia claramente estão no topo da lista porque têm capacidade de operar em todo o espectro de operações no espaço cibernético. Atrás de China e Rússia estão os iranianos e norte-coreanos, que são incomparáveis nas demonstrações tanto de capacidade quanto de intenção de nos atingirem no espaço cibernético" (NAKASONE, P. M. *In*: ELIASON, W. T. *An interview with Paul M. Nakasone*. Joint Forces Quarterly 92. National Defense University, 2019. Disponível em: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_4-9_Nakasone-Interview.pdf, p. 4, tradução nossa).

A publicação preferencial da produção acadêmica das ciências sociais em livros, em contraposição a periódicos – principalmente se comparada com as ciências naturais – é observada por Kristensen (2015). Dessa forma, a prioridade da WoS à indexação de periódicos representaria outro limite à sua utilização em pesquisas das ciências sociais, inclusive na presente revisão sistemática de literatura sobre a interpretação da ascensão do ciberespaço pela disciplina de RI.

Outro limite decorre do fato de que a indexação de textos em bases de dados de produção científica por área ou disciplina pode fazer com que um documento relevante não tenha sido mapeado na escolha da amostra bibliográfica inicial por estar indexado, por exemplo, na área de Ciências da Computação, Segurança de Sistemas de Informação ou Direito, ao invés de RI – naturalmente, a área utilizada como parâmetro para a busca por bibliografia para esta dissertação. Por exemplo, parte da produção sobre governança da internet e normatização da atuação de Estados-nação no ciberespaço está indexada na área do direito, a despeito de ser um tema de grande interesse para as RI.

Em relação à análise quantitativa de dados bibliométricos, é preciso notar que a data de publicação dos documentos (artigos, *proceeding papers*, *book reviews* e outros) pode implicar menor citação de artigos mais recentes. Como equalizar a quantidade de citações dos documentos por suas datas de publicação é um desafio que não foi atacado na metodologia utilizada nesta dissertação.

Finalmente, ficou explícita em ambas as amostras bibliográficas trabalhadas nesta dissertação a centralidade do tema conflito cibernético e das publicações em periódicos da subárea de Segurança Internacional, de forma que, a despeito de a pretensão inicial haver sido revisar sistematicamente a literatura de RI sobre a ascensão do ciberespaço, os resultados alcançados são limitados à subárea da Segurança Internacional.

A despeito dos limites explicitados, não se extingue a validade dos resultados alcançados nesta dissertação. Pelo contrário, eles atuam como elementos que, se por um lado diminuem o escopo das descobertas, por outro lado as torna mais precisas. Ademais, a necessária transparência quanto a sua existência ressalta a qualidade crítica das observações neste trabalho.

1.2. Análise bibliométrica: O panorama da produção científica de RI

A Tabela 1 apresenta um resumo das informações apreendidas da análise bibliométrica da amostra bibliográfica inicial quanto à distribuição de documentos por tipo documental, número de citações, idioma, veículos de publicação, área de pesquisa e palavras-chave. Em seguida é apresentada a análise mais detida desses parâmetros.

Tabela 1 – Quadro-resumo de dados bibliométricos

Tipos de Documentos				
Artigos (265)	Proceeding papers (159)	Resenha/Capitulos de Livros (39)		Outros (25)
Por número de citações				
51-200 citações (11)		11-50 citações (32)		
5-10 citações (40)		1-4 citações (149)		
Idioma				
Inglês (457)	Norueguês (8)	Russo (8)		Outros Idiomas(15)
Principais Publicações de artigos				
Survival (26)	Journal of strategic studies (21)		Bulletin of the atomic scientists (18)	
Internasjonal politikk (11)		Intelligence and national security (10)		
Principais Conferências com trabalhos publicados				
International conference on cyber warfare and security (33)			Conference on cyber conflict (20)	
European conference on cyber warfare and security (20)				
Área de Pesquisa indexada				
Direito e Governo (188)	Computação (61)	Relações Internacionais (170)		Outros (69)
Palavras-Chaves principais				
Security (85)	Space (35)	Terrorism (31)	Attacks (30)	Warfare (27)
War (22)	Internet (21)	Defence (16)	Conflict (14	Russia (14)

1.2.1. Evolução numérica da produção científica de RI sobre questões cibernéticas

Os primeiros indicadores bibliométricos utilizados para trabalhar os dados dos documentos da amostra bibliográfica inicial foram seu ano de publicação e tipo de documento[44], de forma a apresentar a evolução da quantidade e forma de publicação.

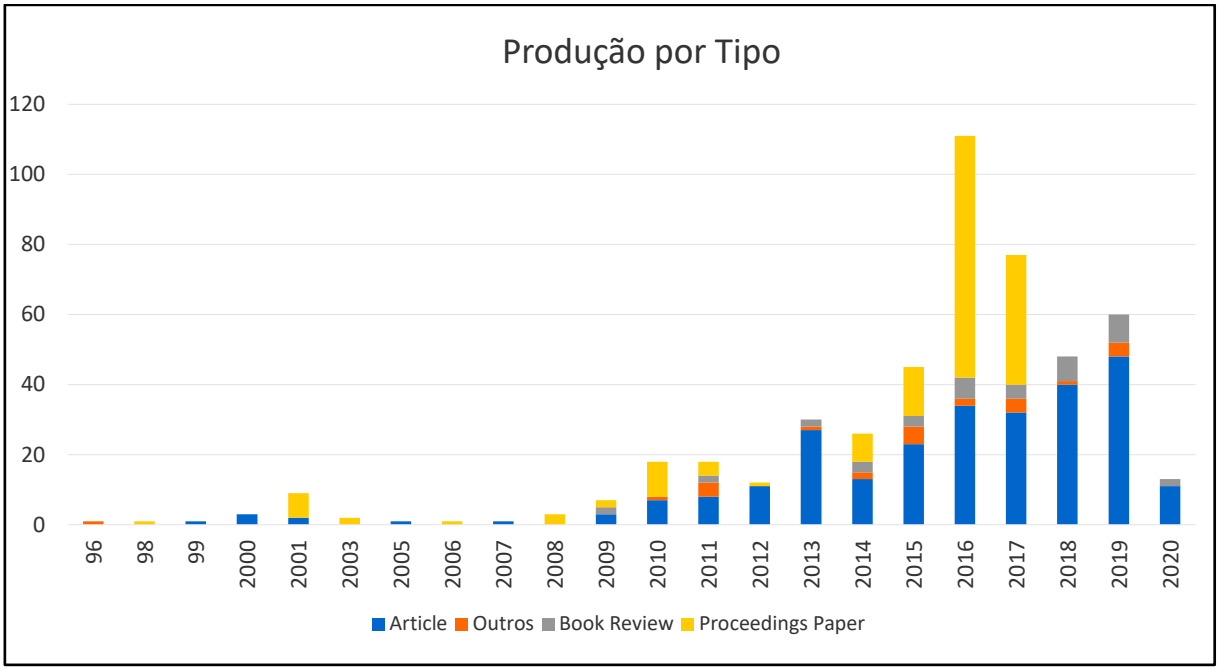
A Tabela 2 e o Gráfico 3 apresentam a evolução quantitativa da produção de RI que trata de fenômenos cibernéticos, diferenciando essa produção por tipo de documento.

[44] O detalhamento sobre a que se refere cada tipo de documento está disponível em: http://images.webofknowledge.com/images/help/WOS/hs_document_type.html#:~:text=News%20Item%3A%20News%2C%20current%20events,paper%20on%20a%20specific%20subject.

Tabela 2 – Número de documentos publicados por ano por tipo de documento (1996-2020)

Tipo de documento	Artigo	Resenha de livros	Material editorial	Carta	Itens de notícia *(news item)*	*Proceedings papers*	Total geral
1996	0	0	1	0	0	0	**1**
1998	0	0	0	0	0	1	**1**
1999	1	0	0	0	0	0	**1**
2000	3	0	0	0	0	0	**3**
2001	2	0	0	0	0	7	**9**
2003	0	0	0	0	0	2	**2**
2005	1	0	0	0	0	0	**1**
2006	0	0	0	0	0	1	**1**
2007	1	0	0	0	0	0	**1**
2008	0	0	0	0	0	3	**3**
2009	3	2	0	0	0	2	**7**
2010	7	0	0	0	1	10	**18**
2011	8	2	2	2	0	4	**18**
2012	11	0	0	0	0	1	**12**
2013	27	2	1	0	0	0	**30**
2014	13	3	0	2	0	8	**26**
2015	23	3	3	2	0	14	**45**
2016	34	6	2	0	0	69	**111**
2017	32	4	4	0	0	37	**77**
2018	40	7	1	0	0	0	**48**
2019	48	8	4	0	0	0	**60**
2020	11	2	0	0	0	0	**13**
Total Geral	**265**	**39**	**18**	**6**	**1**	**159**	**488**

Gráfico 3 – Evolução quantitativa da produção científica de RI indexada na WoS por tipo de documento



A despeito de a busca na WoS ter sido realizada por documentos a partir de 1945, o primeiro documento indexado na área de RI abordando o tema "cyber" e seus derivados data de 1996. Até 2009, a produção científica sobre o tema era baixa, apresentando aumento a partir de 2010, com o pico de 111 documentos em 2016 e diminuição da produção sobre o assunto desde então.

Sharp (2017) em sua sistematização das análises estratégicas sobre o ciberespaço divide a literatura sobre o tema em três fases. Segundo o autor, a primeira fase da análise estratégica focava no caráter revolucionário e nos perigos advindos da ascensão do ciberespaço, a segunda é constituída de artigos mais críticos, que observavam com desconfiança a perspectiva de mudança revolucionária nas relações internacionais e de guerra cibernética levantada nos primeiros estudos e a terceira tende a priorizar estudos empíricos, oferecendo generalizações mais modestas e apresentando as evidências disponíveis de maneira mais sistemática (SHARP, 2017, p. 898-899). Nesse sentido, Gorwa e Smeets (2019) atribuem a redução do número de documentos sobre conflitos cibernéticos a partir de 2016 a uma diminuição do hype sobre o tema decorrente da publicação de artigos mais críticos quanto aos potenciais revolucionários do ciberespaço sobre as relações internacionais – a segunda fase da literatura observada por Sharp (2017).

Considerando toda a produção entre 1996 e 2020 em relação à tipologia de publicação, 54,3% são artigos publicados em periódicos, 32,5% são *proceeding papers* submetidos a

congressos e conferências e 7,9% são resenhas de livros. Os outros tipos de documentos somam 5,1% do total da amostra bibliográfica inicial.

Destaca-se a diferenciação por tipologia de publicação (em especial artigos e *proceeding papers*[45], mais relevantes numericamente) na hipótese de que essa diferenciação implique procedimentos editoriais diferentes que, por um lado, seriam mais rigorosos no caso de artigos científicos e, por outro, mais dinâmicos no caso dos *proceeding papers*. Isso resultaria em maior nível de impacto científico no caso dos primeiros e maior influência sobre tomadores de decisão e membros do governo no caso dos últimos. Reardon e Choucri (2012) diferenciam artigos acadêmicos de *policy papers* em sua revisão de literatura, notando que há uma diferença de abordagem entre eles – ao passo que a perspectiva construtivista predomina nos artigos científicos, abordagens realistas e liberais seriam mais frequentes nos *policy papers.* Contudo, não foram identificados estudos que confirmem a hipótese acerca da influência maior de artigos na comunidade científica e de *proceeding papers* – conforme a divisão da *Web of Science* – em tomadores de decisão, sendo tópico passível de estudo posterior.

1.2.2. Número de documentos por idioma

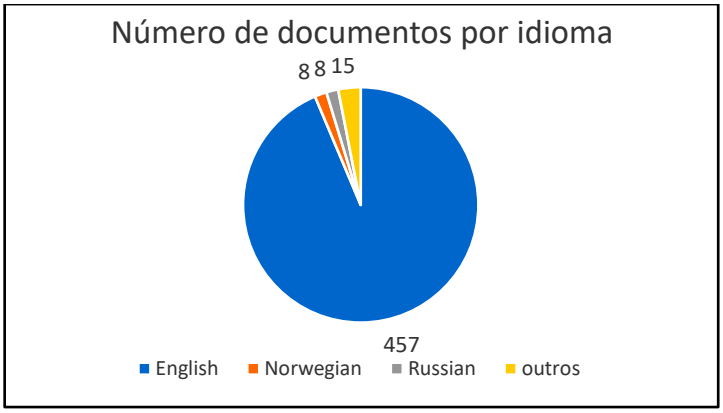
Dos 488 documentos da amostra bibliográfica inicial, 94% são publicados em inglês, 1,6% deles são publicados em russo e 1,6% em norueguês. Note-se que, apesar de o idioma de publicação não ser parâmetro absoluto da origem geográfica dessa produção, a dominância do idioma inglês nos documentos analisados atesta a já mencionada predominância de produção, mas sobretudo de publicação da produção científica de RI nos Estados Unidos e em países anglófonos.

Nesse sentido, Kristensen (2015) defende que a produção científica nos principais periódicos de RI não é aglomerada em redes elitistas com centros na América do Norte, na Europa Ocidental e em Israel. Essas redes não estão completamente confinadas a Estados-nação, tampouco completamente desterritorializadas (KRISTENSEN, 2015, p. 3), de modo que, "mesmo para não americanos, a via para a fama passa por periódicos estadunidenses" (GOLDMANN, 1995, p. 251 *apud* KRISTENSEN, 2015, p. 7).

---

[45] Em 2008 a tipologia *proceeding paper* foi incluída na WoS para designar documentos inicialmente apresentados em uma conferência ou *workshop* e mais tarde adaptada para publicação em um periódico (GONZALES-ALBO; BONDONS, 2011, p. 370).

Gráfico 4 – Número de documentos por idioma de publicação



1.2.3. Número de documentos por número de citações

Tabela 3 – Número de documentos por número de citações

Faixa de citações	Número de documentos	Participação percentual
0 citações	256	52%
Entre 1 e 4 citações	149	31%
Entre 5 e 10 citações	40	8%
Entre 11 e 50 citações	32	7%
Entre 51 e 200 citações	11	2%
Total Geral	488	100%

A avaliação do número de documentos por número total de citações objetiva avaliar a distribuição da relevância deles, com base na análise de citações. Dessa forma, é possível destacar que a "elite" da amostra bibliográfica inicial é constituída de apenas 2% do total (11 documentos), que possuem entre 51 e 200 citações.

A concentração do número de citações em uma parcela tão pequena dessa produção científica pode contribuir com a explicação de porque, após a seleção com base nesse critério, a amostra bibliográfica final apresentou uma temática tão específica (basicamente conflitos cibernéticos, na área de segurança internacional) – a despeito de ter sido realizada uma busca com parâmetros generalistas.

1.2.4. Número de documentos por veículo de divulgação

Considerando apenas artigos – 265 dos 488 documentos –, os itens da amostra bibliográfica inicial foram publicados num total de 81 periódicos. Aproximadamente 25% dos periódicos (20 periódicos) concentram 65% das publicações. Nesta análise, ressalta-se também a produtividade do periódico norueguês, publicado no idioma norueguês, *Internasjonal*

Politikk, que parece indicar forte interesse de estudiosos de RI do país escandinavo em questões cibernéticas.

Tabela 4 – Número de artigos publicados por periódico

Nome da publicação	Total geral
Survival	26
Journal of Strategic Studies	21
Bulletin of the Atomic Scientists	18
Internasjonal Politikk	11
Intelligence and National Security	10
Korean Journal of Defense Analysis	8
Contemporary Security Policy	7
International Affairs	7
International Security	7
International Journal	6
Defence and Security Analysis	5
International Politics	5
Mirovaya Ekonomika i Mezhdunarodnye Otnosheniya	5
Security Studies	5
Studies in Conflict & Terrorism	5
Foreign Affairs	4
Global Policy	4
Revista Unisci	4
Security Dialogue	4
Stanford Journal of International Law	4
Washington Quarterly	4
Outros	95
Total	**265**

Entre *proceeding papers*, os 159 documentos foram publicados num total de 32 veículos de publicação (anais e procedimentos de congressos), sendo 79% das publicações concentradas em 31% dos veículos de publicação (10).

Tabela 5 – Número de *proceeding papers* publicados por veículo de publicação

Nome da publicação	Total geral
International conference on cyber warfare and security	33
Conference on cyber conflict	20
European conference on cyber warfare and security	20
Ethics and policies for cyber operations: a nato cooperative cyber defence centre of excellence initiative	12
Terrorist use of cyberspace and cyber terrorism: new challenges and responses	11
Best practices in computer network defense: incident detection and response	8
Transnational dimension of cyber crime and terrorism	7
Critical infrastructure protection against hybrid warfare security related challenges	6
Countering terrorist recruitment in the context of armed counter-terrorism operations	5
Identification of potential terrorists and adversary planning: emerging technologies and new counter-terror strategies	4
Outros	33
Total Geral	159

As 39 resenhas de livros foram publicadas em 17 veículos de publicação (periódicos, anais e procedimentos de congressos), sendo 72% das publicações em 6 periódicos.

Tabela 6 – Resenhas de livros publicadas por veículo de publicação

Nome da publicação	Total geral
International Affairs	8
Foreign Affairs	6
Survival	6
International Journal of Intelligence and Counterintelligence	4
Naval War College Review	2
Terrorism and Political Violence	2
American Journal of International Law	1
Asian Perspective	1
Bulletin of the Atomic Scientists	1
Common Market Law Review	1
Ethics & International Affairs	1
Foro Internacional	1
International Studies Review	1
Journal of Strategic Studies	1
Obrana a Strategie-Defence & Strategy	1
Small Wars and Insurgencies	1
Strategic Analysis	1
Total geral	39

1.2.5. Número de documentos por área de pesquisa por ano

Ao analisar esse parâmetro é importante ter em mente a ressalva de que os documentos podem ser indexados em diferentes áreas de pesquisa, sendo a mais frequente a indexação em relações internacionais (haja vista ter sido esse o parâmetro utilizado para a busca na WoS). O que essa análise aponta, portanto, é o nível de relacionamento entre a área de relações internacionais e outras áreas de pesquisa na produção científica sobre a ascensão do ciberespaço.

Além de RI, as duas áreas de pesquisa que aparecem com maior frequência são Direito e Governo e Ciência da Computação, revelando maior interesse da comunidade científica de RI na compreensão de implicações políticas e normativas (direito e governo) e aspectos técnico-operacionais (ciência da computação) dos fenômenos cibernéticos nas relações internacionais.

Tabela 73 – Número de publicações por área de pesquisa entre 1996 e 2020

	Direito e governo	Computação	Apenas RI	Outros
1996	0	0	0	1
1998	1	0	0	0
1999	0	0	1	0
2000	2	0	1	0
2001	7	0	2	0
2003	1	1	0	0
2005	0	0	1	0
2006	1	0	0	0
2007	0	0	1	0
2008	3	0	0	0
2009	4	0	1	2
2010	2	10	5	1
2011	11	0	2	5
2012	9	0	1	2
2013	21	0	4	5
2014	7	0	8	11
2015	11	0	21	13
2016	25	50	30	6
2017	15	0	44	18
2018	21	0	25	2
2019	36	0	21	3
2020	11	0	2	0
Total	188	61	170	69

1.2.6. Peso das palavras-chave na amostra bibliográfica inicial

A análise da frequência de indexação das palavras-chave indica os principais temas abordados pela amostra bibliográfica inicial. Dos 488 documentos, 296 indexaram um total de

889 palavras-chave[46]. Os documentos podem indexar mais de uma palavra-chave, de forma que o total de indexações foi 1.617, das quais 410 concentram-se em 21 palavras-chave, apresentadas na Tabela 8.

Tabela 8 – Palavras-chave mais frequentes e número de vezes em que foram indexadas

Palavra-chave	**Número de vezes em que a palavra-chave foi indexada**
Security	85
Space	35
Terrorism	31
Attacks	30
Warfare	27
War	22
Internet	21
Defence	16
Conflict	14
Russia	14
Nato	13
Strategy	12
China	11
Critical Infrastructure	11
Deterrence	11
European Union	10
Stuxnet	10
Weapons	10
Information Security	9
Threat	9
United States	9

A Figura 4 apresenta a nuvem de palavras referente às palavras-chave indexadas na amostra bibliográfica inicial. Com o auxílio das nuvens de palavras, nota-se mais uma vez a já referida centralidade do tema conflito cibernético na amostra bibliográfica inicial.

[46] De forma a facilitar a visualização da nuvem de palavras, o prefixo "*cyber*" foi excluído de palavras-chave, como *cybersecurity*, *cyberterrorism*, *cyberattack.*

Figura 5 – Nuvem de palavras representando o peso das principais palavras-chave indexadas nos artigos da amostra bibliográfica inicial.

A análise bibliométrica da amostra bibliográfica inicial sustenta que há na produção de RI sobre questões cibernéticas indexada na *Web of Science* alto grau de concentração da publicação em periódicos de segurança internacional – fato corroborado pela maior frequência de palavras-chave do campo semântico da segurança (a exemplo de *security*, *terrorismo*, *attacks*, *guerra*, *defesa* e *conflito);* predomínio das publicações em língua inglesa, conforme referido por Kristensen (2015) e Stuenkel (2018); e uma grande concentração do número de citações em poucos artigos, de forma que a elite dessa produção em termos de número de citações é muito pequena, com 83% dos artigos possuindo menos do que 5 citações, ao passo que 2% dos artigos produzidos têm acima de 50 citações.

1.2.7. Análise Bibliométrica da Amostra bibliográfica final

A Tabela 9 apresenta um resumo das informações apreendidas da análise bibliométrica da amostra bibliográfica final (os 47 documentos derivados da amostra bibliográfica inicial mais os 13 documentos indexados discricionariamente) quanto à distribuição de documentos por tipo documental, número de citações, idioma, veículos de publicação, área de pesquisa e palavras-chave. Em seguida é apresentada a análise mais detida desses parâmetros.

Tabela 9 – Quadro-resumo de dados bibliométricos da amostra bibliográfica final

Indexado na WoS				
Sim (52)			Não (8)	
Tipos de Documentos				
Artigos (51)	Proceeding papers (7)		Resenha/Capitulos de Livros (1)	Outros (0)
Por número de citações na WoS				
51-200 citações (9)			11-50 citações (25)	
5-10 citações (17)			1-4 citações (1)	
Idioma				
Inglês (60)				
Principais Publicações de artigos				
Survival (6)	Journal of strategic studies (12)		Security Studies (18)	
International Affairs (4)		International Security (4)		
Principais Conferências com trabalhos publicados				
Conference on cyber conflict (3)			ISA Annual Convention (2)	
Área de Pesquisa indexada				
Direito e Governo (29)	Computação (3)		Relações Internacionais (19)	N/A (9)
Palavras-Chaves principais				
Security (13)	conflict (5)	War (8)	Conflict (5)	Violence (4)
Information (4)	strategic (4)	Stuxnet (4)		

As informações apreendidas da amostra bibliográfica final corroboram as características apreendidas da amostra bibliográfica inicial, indício que indica que a amostra final é de fato representativa da literatura indexada na WoS e analisada bibliograficamente no presente capítulo. No próximo capítulo, a amostra bibliográfica final é objeto de revisão sistemática de literatura, de forma a aprofundar a análise iniciada com o estudo dos índices bibliométricos em direção a discussões conceituais e aos debates teóricos identificados na literatura de segurança internacional indexada na *Web of Science*.

2. CONCEITOS UTILIZADOS NA INTERPRETAÇÃO DA SEGURANÇA INTERNACIONAL SOBRE CONFLITOS CIBERNÉTICOS

A interpretação dos conflitos cibernéticos pela literatura de segurança internacional apresenta dificuldades decorrentes, por um lado, do desconhecimento de aspectos técnicos da informática por estudiosos de RI (KELLO, 2013) e, por outro, da evolução extremamente rápida dos desenvolvimentos tecnológicos. Consequência e ao mesmo tempo catalisadora dessas condições, a indefinição conceitual é um aspecto frequentemente abordado nos artigos revisados nesta dissertação.

Os conceitos centrais identificados na literatura são ciberespaço, guerra cibernética e segurança cibernética. O ciberespaço aparece não apenas como "cenário" onde se desenrolam as relações internacionais, mas como agente dessas relações, na medida em que possuiria caraterísticas que criam incentivos a comportamentos específicos dos atores. Diferentes definições de ciberespaço servem a interpretações de fenômenos diferentes, como "guerra cibernética" ou "guerra informacional", ou a objetivos diferentes como a aplicação do direito internacional ou as iniciativas de criação de um regime de segurança cibernética internacional.

Por sua vez, a noção de guerra cibernética, bem como a probabilidade e os efeitos potenciais de conflitos envolvendo ações no ciberespaço, é o cerne da abordagem da segurança internacional na literatura revisada. De fato, a grande relevância de ataques no ciberespaço decorre da possibilidade de implicarem efeitos cinéticos. Além da discussão sobre definições de guerra cibernética e sua diferenciação de outros fenômenos, a equiparação desse tipo de conflito a formas tradicionais de guerra – o próprio *status* de guerra – e as diferenças entre guerra cibernética e guerra informacional são também problematizados na literatura revisada. Analogamente, é apresentada a diferença entre os conceitos de segurança cibernética e segurança da informação na literatura, acrescidas as percepções divergentes de estados e organizações internacionais sobre o tema e as implicações dessa divergência no estabelecimento de uma governança de segurança cibernética internacional.

Neste capítulo, apresentamos os conceitos centrais e discussões conceituais derivadas da amostra bibliográfica final revisada (Anexo II), com vistas a facilitar a compreensão subsequente do principal debate de segurança internacional sobre conflito cibernético. Eventualmente, a própria apresentação dos conceitos tangenciará o debate apresentado no capítulo 3.

2.1. Indefinição conceitual

A indefinição conceitual na literatura de Segurança Internacional sobre o ciberespaço e conflitos cibernéticos é frequentemente apontada na amostra revisada. Betz e Stevens (2011; 2013), Melzer (2011), Reardon e Choucri (2012), Kello (2013), Junio (2013), Lindsay (2014) e Schreier (2015) tratam do tema, sublinhando a necessidade do estabelecimento de uma base conceitual comum sobre a qual produzir estudos subsequentes da área. O fenômeno não diz respeito apenas à abordagem científico-acadêmica, mas também a divergências nas visões de governos e organizações internacionais envolvidos na governança do ciberespaço (MELZER, 2011). Organizações de cunho técnico como o *National Institute of Standards and Technology* (NIST) dos Estados Unidos apresentam definições que guardam certo nível de consenso na comunidade de segurança cibernética do país, contudo essas definições não foram incorporadas nos estudos de RI, além de não abarcarem todos os fenômenos estudados na disciplina, prescindindo por exemplo, de conceitos importantes para o campo de estudos como guerra cibernética (*cyberwar*).

Conforme aponta Lindsay (2014, p. 7), a ubiquidade e interconectividade de dispositivos computacionais cria desafios para a elaboração de políticas e confusão conceitual para a teoria. Nesse sentido, Kello (2013) defende que o esforço de definição de bases conceituais comuns emolduraria propriedades científicas complexas do ciberespaço de uma forma gerenciável; identificaria atributos das tecnologias e fenômenos considerados mais relevantes – eliminando aqueles não relacionados a questões de segurança nacional e internacional –; e orientaria o desenvolvimento de teorias, facilitando a organização e codificação dos dados coletados a partir de incidentes cibernéticos (KELLO, 2013, tradução nossa).

Betz e Stevens (2011) afirmam que a pouca consistência nas definições governamentais de ciberespaço não é uma questão trivial, haja vista que o que se decide incluir ou excluir do conceito tem implicações significativas nas operações de poder (BETZ; STEVENS, 2011, p. 36). O vácuo conceitual teria dado espaço à utilização de analogias e metáforas na definição de ciberespaço (HANSEN; NISSEMBAUM, 2009; BETZ; STEVENS, 2013; CAVELTY, 2013; LUPOVICI, 2014), com consequências para as interpretações das relações internacionais sobre o tema. A utilização de uma metáfora espacial (ciberespaço como espaço) e de metáforas biológicas no campo da epidemiologia (vide o conceito de vírus de computador) e no campo da ecologia (o ciberespaço como um ecossistema) teria implicações, por um lado, na securitização do discurso sobre o ciberespaço nos ambientes político e científico-acadêmico e, por outro lado,

na descrição do ciberespaço como um domínio cujos desenvolvimentos são "naturais" e espontâneos.

Ademais, a definição dos conceitos tem implicações legais. Melzer (2011) menciona a ausência de definições como "guerra cibernética", "hostilidades cibernéticas" e "conflito cibernético" para fins de direito internacional. Hughes (2010), Melzer (2011) e Goldsmith (2013) prospectam as possibilidades de aplicação da Lei de Conflitos Armados (*Law of Armed Conflict* – Loac) a casos de ataques cibernéticos. Os autores apontam que a definição de critérios que especifiquem, por exemplo, o que constitui "uso da força" ou "legítima defesa" nos termos dos arts. 2.4 e 51 da Carta das Nações Unidas[47], quando aplicados ao ciberespaço, é essencial para qualquer esforço de regulação de conflitos cibernéticos internacionais.

Para Schreier (2015) o termo "guerra cibernética" é muitas vezes utilizado indiscriminadamente para referir-se a diferentes tipos de conflitos, com sujeitos, *modus operandi*, objetos e objetivos diversos. Nesse sentido, o autor defende o rigor conceitual na definição dos tipos de conflitos e ataques cibernéticos como requisito para superar as dificuldades de "determinação da origem e avaliação dos danos" desses ataques (SCHREIER, 2015, p. 7, tradução nossa).

Nesse sentido, é essencial que se diferencie, por exemplo, uma campanha difamatória contra indivíduo por meio da internet, a invasão de servidores governamentais com objetivo de acessar informações classificadas, um ataque de negação de serviço (*Denial of Service*, ou *DoS*) ou sequestro de informações por ataques *ransomwares* com objetivo de obter vantagens financeiras ou um ataque à rede elétrica de determinado país com o efeito de interromper o fornecimento de energia em seu território, entre outros. Note-se que, na maior parte das vezes, mais do que as técnicas utilizadas, o que diferencia esses fenômenos são seus alvos e motivações. Cabe, então, a definição do que constitui efetivamente o objeto de estudo da segurança internacional.

---

[47] O art. 2.4 da Carta das Nações Unidas proíbe o uso da força e o art. 51 estabelece o instituto da legítima defesa nas relações internacionais. "Art. 2º A Organização e seus Membros, para a realização dos propósitos mencionados no Artigo 1, agirão de acordo com os seguintes Princípios: [...] 4. Todos os Membros deverão evitar em suas relações internacionais a ameaça ou o uso da força contra a integridade territorial ou independência política de qualquer Estado, ou qualquer outra ação incompatível com os Propósitos das Nações Unidas."; e "Art. 51. Nada na presente Carta prejudicará o direito inerente de legítima defesa individual ou coletiva no caso de ocorrer um ataque armado contra um Membro das Nações Unidas, até que o Conselho de Segurança tenha tomado as medidas necessárias para a manutenção da paz e da segurança internacionais. As medidas tomadas pelos Membros no exercício desse direito de legítima defesa serão comunicadas imediatamente ao Conselho de Segurança e não deverão, de modo algum, afetar a autoridade e a responsabilidade que a presente Carta atribui ao Conselho para levar a efeito, em qualquer tempo, a ação que julgar necessária à manutenção ou ao restabelecimento da paz e da segurança internacionais" (ONU, 1945).

2.2. Ciberespaço

O conceito de ciberespaço (espaço ou domínio cibernético) é considerado central na literatura revisada, haja vista todos os documentos revisados referirem-se direta ou indiretamente a ele não apenas como cenário em que as relações internacionais cibernéticas acontecem, mas como elemento essencial e definidor dessas relações.

A análise da literatura revisada corrobora com a percepção de Betz e Stevens (2013) de que o ciberespaço é um ambiente que desafia a categorização fácil. Ele tem poucos dos parâmetros definíveis dos domínios físicos tradicionais com limites identificáveis e é caracterizado por uma dinâmica não linear em que os efeitos são imprevisíveis e potencialmente desproporcionais às suas causas aparentes (BETZ; STEVENS, 2013. p. 15).

O *National Institute of Standards and Technology* (NIST) dos EUA apresenta algumas definições de ciberespaço úteis à compreensão das RI. Nesta dissertação, opta-se por uma delas e considera-se ciberespaço como "um domínio global dentro do ambiente de informação que consiste na rede interdependente de infraestruturas de sistemas de informação, incluindo a Internet, redes de telecomunicações, sistemas de computador e processadores e controladores incorporados"[48].

Contudo, na literatura revisada é possível identificar que o conceito, a despeito de sua importância inegável, muitas vezes é tratado como uma noção intuitiva e não tem definição clara apresentada[49]. Nesses casos, as visões sobre o ciberespaço deduzidas da literatura presumem algumas vezes características como baixo custo de entrada, anonimato, assimetrias de vulnerabilidades, dificuldade de atribuição de ataques cibernéticos e primazia do ataque sobre a defesa – discutidas mais detidamente a seguir – ou apenas tratam de dinâmicas relacionadas ao ciberespaço sem, contudo, apresentar uma sentença definidora daquilo a que se referem. Além disso, percebe-se a utilização de metáforas espacial e biológicas enquanto definições, com implicações para os estudos de segurança internacional. Nas definições que se pretendem objetivas, percebe-se divergências sobre a amplitude do conceito de ciberespaço (a

[48] Disponível em: <https://csrc.nist.gov/glossary/term/cyberspace>. Acesso em 04/06/2021.

[49] Isso acontece em Hansen e Nissembaum (2009); Hughes (2010); Inster (2010); Lemay, Fernandeza e Knight (2010); Ottis (2010); Farwell e Rohozinski (2011); Klimburg (2011); Farwell e Rohozinski (2012); Rid (2012); Bronk e Tikk-Ringas (2013); Cavelty (2013); Goldsmith (2013); Junio (2013); Lindsay (2013); McGraw (2013); Mueller, Schmidt e Kerbis (2013); Stone (2013); Eichensehr (2014); Gompert e Libicki (2014); Lindsay (2014); Valeriano e Maness (2014); Rid e Buchanan (2015); Carr (2016); Garcia (2016); Lupovici (2014); Nye (2016); Slayton (2017); Stoddart (2016); Balzacq e Cavelty (2016); Borghard e Lonergan (2017); Carson e Yarhi-Milo (2017); Christensen e Petersen (2017); Sharp (2017); Tor (2017); Efrony e Shany (2018); Gohdes (2018); Smeets (2018); Kostyuk e Zhukov (2019); e Sechser, Narang e Talmadge (2019).

inclusão de infraestruturas físicas, de protocolos e informações transitando entre elas e até da mente humana como parte constituinte do domínio).

2.2.1. As analogias cibernéticas e suas implicações

Betz e Stevens (2013) afirmam que a indefinição conceitual viria dando espaço à utilização de analogias – sobretudo uma espacial e uma biológica – que fomentam a dinâmica de inflação de ameaças (*threat inflation*) no ciberespaço.

A metáfora espacial mostra-se no próprio termo *espaço* cibernético. Conforme Betz e Stevens (2013), "o ciberespaço não é um espaço em nenhum sentido tradicional, [...] mas o experimentamos como se ele possuísse atributos físicos, mesmo que apenas por associação e analogia" (BETZ; STEVENS, 2013, p. 7). A concepção do ciberespaço como um lugar permitiria aplicar as noções de controle e dominação sobre "terras virtuais" e até mesmo estabelecer a imagem de "fronteiras eletrônicas" em paralelismo com a ideia de "fronteira do oeste", sugerindo uma "terra" inexplorada, um local sem lei necessitando de ordem (CAVELTY, 2013, p. 108).

A metáfora espacial apresenta, ainda, uma extensão que é a noção do ciberespaço enquanto um dos *global commons*[50] juntamente a oceanos, ares, espaço e a Antártida (BETZ; STEVENS, 2013; SCHREIER, 2015; GARCIA, 2016).

Schreier (2015) refere-se ao ciberespaço como o mais novo e mais importante entre os *commons*, na medida em que o domínio se sobrepõe a todos os outros e se tornou o "centro de gravidade do mundo globalizado", não apenas para operações militares, mas em todos os aspectos das atividades nacionais como atividades econômicas, financeiras e diplomáticas (SCHREIER, 2015, p. 13).

Garcia (2016) argumenta que a caracterização do ciberespaço como *global common* pode servir às iniciativas de governança desse domínio, pois aproveitaria as experiências já testadas nos outros domínios. Notadamente, a autora aponta cinco características atribuídas aos *commons* aplicáveis nas iniciativas de governança do ciberespaço: primeiramente, os *commons* não podem ser nacionalizados; em segundo lugar, esses domínios devem ser gerenciados cooperativamente; terceiro, todos devem compartilhar os benefícios derivados dos *commons*;

[50] Domínios de recursos que não estão sob a jurisdição de qualquer determinado país e a que todas as nações têm acesso. (OHCHR; OHRLLS; UNDESA; UNEP; UNFPA, 2013)

em quarto lugar, não é permitida a militarização dessas áreas; e quinto, a equidade intergeracional deve ser preservada nesses domínios.

Betz e Stevens (2013) argumentam que, apesar de válida, pois o ciberespaço "trata-se, sem dúvida, de uma parte importante do tecido conectando o sistema internacional" (BETZ; STEVENS, 2013, p. 11), a analogia pode induzir a erro. Diferenças fundamentais que a analogia aos *global commons* não considera são: o fato de o ciberespaço ser artificial, com geografia mutável (*hardware* pode ser desligado ou destruído, deliberada ou acidentalmente) e regras que não obedecem a leis rígidas – como as leis da física que se aplicam à natureza. Além disso, esse domínio não é de fato comum, mas propriedade de entidades públicas ou privadas submetidas às legislações locais de onde suas infraestruturas físicas estão. Se levarmos em conta ainda uma vertente de definições do ciberespaço que considera as mentes dos usuários parte integrante desse domínio[51], "as diferenças sugerem que o espaço cibernético não possui nenhum dos critérios lógicos ou legais de um dos "*commons*" (BETZ; STEVENS, 2013, p. 11).

A metáfora biológica da epidemiologia manifesta-se na utilização dos termos "infecção por vírus", "quarentena" e "sanitização" em relação com o ciberespaço. Cavelty (2013) ressalta que a analogia forneceu *insights* para a programação de *malwares*, como a criação de códigos polimórficos que se alteram (vírus mutantes de computadores) (CAVELTY, 2013, p. 111), ao passo que Betz e Stevens (2013) sublinham que a utilização dessa metáfora tende a "esconder [...] que vírus de computadores são criados por seres humanos com o propósito de invadir os programas de outros seres humanos sem o seu conhecimento" (HELMREICH, 2000, p. 482, *apud* BETZ; STEVENS, 2013, p. 22).

A segunda metáfora biológica, que descreve o ciberespaço como um ecossistema (metáfora biológica ecológica) sugere imagens de uma evolução orgânica, interconectividade e complexidade. É importante notar que a atribuição de um caráter "natural" ao desenvolvimento do ciberespaço deixa de observar o aspecto proativo da atividade humana na construção desse domínio e das dinâmicas ocorrendo nele. Além disso, outra importante implicação da metáfora ecológica e sua visão sistêmica é que a percepção de que a ascensão do ciberespaço aumentaria o potencial para grandes desastres, dada a velocidade e ferocidade com que riscos locais se transfeririam ao sistema (CAVELTY, 2013, p. 108).

Betz e Stevens (2013) afirmam que, apesar de inofensivas quando aplicadas no nível da máquina, as metáforas epidemiológica e ecológica devem ser tratadas com cautela, sobretudo nas discussões sobre segurança cibernética, considerando que o conceito pode se referir – mais

[51] Essa vertente de definições é apresentada com mais detalhes no item Definições de ciberespaço, a seguir.

do que segurança de redes de computadores – a segurança nacional, de forma que é necessário avaliar as implicações dessas analogias nas políticas nacional e internacional (BETZ; STEVENS, 2013).

A despeito de apresentarem algum poder explicativo, útil para traduzir processos técnicos às vezes ininteligíveis para boa parte dos estudiosos do ciberespaço, cabe na academia de RI o aprofundamento da problematização sobre o uso das analogias espacial e biológicas, na medida em que não atuam como mera representação da realidade, mas podem fortalecer um processo de securitização dos discursos político e científico-acadêmico sobre esse domínio, conforme apontado por Hansen e Nissembaum (2009) e Cavelty (2013), e constituindo uma variável relevante para os estudos de segurança internacional sobre a ascensão do ciberespaço.

2.2.2. Definições de ciberespaço

Frente a uma grande diversidade de definições de ciberespaço, categorizações amplas das definições de ciberespaço são propostas em Manjikian (2010), Betz e Stevens (2013) e Cavelty (2013). Essas caracterizações são expostas inicialmente de forma a apresentar as visões gerais do conceito, detalhadas em seguida.

Betz e Stevens (2013) buscam organizar as definições de ciberespaço em duas vertentes. A vertente excludente diz respeito a conceitos que tratam o espaço cibernético como um meio ambiente virtual separado do mundo "real" e limitado por sua infraestrutura física. A vertente inclusiva de definições diz respeito àquelas que consideram tanto aspectos físicos quanto a experiência dos usuários na definição de ciberespaço (BETZ; STEVENS, 2013, p. 7-8).

Analogamente, Cavelty (2013) diferencia dois modelos de conceitualização do ciberespaço enquanto "espaço"[52]. O primeiro modelo considera o novo domínio como o "espaço intermediário entre componentes de hardware, em que a interação acontece (STERLING, 1993), um espaço diferente da realidade, um 'novo lar da mente' (BARLOW, 1996)" (CAVELTY, 2013, p. 107), modelo que se aproxima da vertente excludente de definições a que se referem Betz e Stevens (2013) e que trata o mundo virtual como fundamentalmente separado do mundo real; o segundo modelo de Cavelty (2013) compreende camadas abstratas de informação navegando em camadas físicas de *hardware* (CAVELTY, 2013, p. 109), aproximando-se da vertente inclusiva de definições conforme a organização de Betz e Stevens (2013).

[52] Calvelty (2013) propõe esses modelos considerando conceitualizações de ciberespaço enquanto "espaço", conforme a discussão sobre a analogia espacial apresentada na seção anterior.

Outra proposta de organização das definições de ciberespaço é encontrada em Manjikian (2010), que tem por base a relação dos conceitos com os principais paradigmas das teorias de RI, tema aprofundado no capítulo 3 desta dissertação.

Segundo Manjikian (2010), as narrativas liberal e neorrealista oferecem interpretações diversas das características e implicações do ciberespaço nas relações internacionais, sendo que a narrativa liberal se divide, ainda, numa corrente utópica e uma liberal institucionalista.

Nas definições afeitas à visão liberal utópica, o ciberespaço é considerado uma entidade orgânica, evoluindo amplamente por si só, com pouca ou nenhuma regulamentação: uma vila global igualitária e livre (MANJIKIAN, 2010). Essa visão parece estar superada na abordagem da segurança internacional, haja vista ter sido mencionada apenas subsidiariamente na literatura revisada, como visão datada do início dos estudos do ciberespaço pelas RI e frequentemente atribuída a desenvolvedores e cientistas da computação. Nesse sentido, Mueller, Schmidt e Kuerbis (2013) afirmam que uma visão inicial das redes as percebia como horizontais e intrinsecamente igualitárias.

A corrente liberal institucional descreve o ciberespaço como "um universo alternativo criado reflexivamente por meio da ação humana, onde a estrutura do mundo físico, com ênfase no poder, identidade e riqueza, seria menos relevante" (MANJIKIAN, 2010, p. 383). Nessa visão, os participantes do ciberespaço (indivíduos, corporações e estados) são responsáveis pela defesa da informação e da segurança da informação enquanto bens coletivos e devem desenvolver regimes que promovam normas de atuação e capacidade e vontade de autopoliciamento nos atores (MANJIKIAN, 2010, p. 384).

Por outro lado, a narrativa neorrealista das RI para o ciberespaço percebe esse domínio como um campo de batalha virtual (*virtual battlespace)* que não apresenta diferenças fundamentais em relação a outros campos de batalha, sendo uma adaptação tecnológica no sistema internacional existente – ao invés de uma nova criação (MANJIKIAN, 2010, p. 387).

As narrativas apontadas por Manjikian (2010) são análogas à visão de Cavelty (2013) de que duas grandes lógicas separam os discursos sobre o ciberespaço nas relações internacionais. Ao passo em que uma, mais próxima da narrativa neorrealista, vincula ciberespaço a controle e poder estatal, através do discurso de "(re)estabelecer controle e fronteiras" e da menção a "[...] infraestruturas físicas que podem estar sujeitas aos princípios da territorialidade e da soberania", a outra abordagem, mais próxima às narrativas liberais, inspira-se na imagem de redes e interconexão, auto-organização e descentralização (CAVELTY, 2013, p. 113).

A despeito de nem sempre enumerarem representantes de suas categorias, as vertentes de definições propostas por Betz e Stevens (2013) e os modelos de conceitualização de Cavelty (2013) são bem-sucedidos na organização dos conceitos de ciberespaço derivados da literatura revisada aqui, inclusive as versões "intuitivas", que implicam uma ideia do que é o ciberespaço sem que haja a definição declarada do conceito. Argumenta-se que, ao longo da literatura revisada, esses diferentes grupos de conceitos servem a objetos de análise distintos. De forma geral, os conceitos afeitos à vertente excludente de Betz e Stevens (2013), bem como ao primeiro modelo de Cavelty (2013), que convergem na visão de um mundo virtual separado do mundo "real", servem à análise de conflito cibernético enquanto fenômeno que implica violência e atos de agressão virtuais ou cinéticos, com impactos no ciberespaço ou fora dele. Por outro lado, os conceitos pertinentes à vertente inclusiva de Betz e Stevens (2013) ou ao segundo modelo de Cavelty (2013), que consideram aspectos físicos e informacionais do ciberespaço, servem à análise de conflito cibernético enquanto conflito informacional, discutida na seção 2.3.4 deste capítulo e trabalhada, entre outros, por Arquilla e Ronfeldt (1993), Hughes (2010) e Castells (2013) e Schreier (2015). Conceitualizações centradas no aspecto informacional são relevantes sobretudo considerando a crescente importância estratégica das disputas de narrativas, potencializadas no domínio cibernético.

De forma semelhante ao que ocorre com a instrumentalização dos conceitos para objetos de análise distintos, as narrativas ou discursos amplos sobre o ciberespaço que dividem a literatura também servem a fins analíticos específicos: a visão neorrealista (MANJIKIAN, 2010) e/ou de vinculação ao poder estatal (CAVELTY, 2013) é adotada mais comumente quando se discute as perspectivas de guerra cibernética e a visão liberal institucionalista (MANJIKIAN, 2010) e/ou de descentralização (CAVELTY, 2013), quando se trata da busca por um regime de segurança cibernética internacional.

No que tange às definições de espaço cibernético que se pretendem objetivas, primeiramente é preciso reiterar que elas são escassas. Naqueles artigos que oferecem definições explícitas, os conceitos encontrados são muito diversas e apresentam noções mais ou menos amplas do que constitui o espaço cibernético. De forma geral, percebe-se a recorrência de aspectos ou elementos constituintes do ciberespaço combinados de diferentes maneiras. Foram mencionados como elementos do ciberespaço: sua infraestrutura física (cabos, antenas, servidores, *data centers* e dispositivos de acesso, como computadores e celulares); as informações produzidas, armazenadas, processadas e transitadas nessa infraestrutura física; protocolos ou linguagens que permitem a comunicação entre máquinas; o espectro eletromagnético que viabiliza o processamento e trânsito digital da informação; e até mesmo as

mentes humanas, que seriam fundamentalmente impactadas pelo grande volume e rapidez de informações no ciberespaço, passando a constituir parte desse domínio.

Mais comumente (NYE, 2010; MELZER, 2011; VALERIANO; MANESS, 2014) identifica-se a menção a um duplo caráter do ciberespaço: por um lado, espaço cibernético refere-se a infraestrutura física de redes, cabos, *data centers* e dispositivos de acesso como computadores e celulares; por outro lado, há o elemento informacional: os dados que transitam e são armazenados nessa infraestrutura física. Nesse sentido, Nye (2010) define ciberespaço como um "regime híbrido único com propriedades físicas e virtuais" (NYE, 2010, p. 3, tradução nossa). A camada de infraestrutura física possuiria recursos escassos e custos marginais crescentes, sendo limitada também pelo instituto da soberania estatal. A camada virtual ou informacional teria rendimentos crescentes em função da escala e ofereceria dificuldades ao controle governamental. De forma semelhante, Melzer (2011) define espaço cibernético como uma rede global interconectada de informação digital e infraestrutura de comunicações incluindo a internet, redes de telecomunicações, sistemas de computadores e toda a informação ali contida (MELZER, 2011, p. 4). E, por sua vez, Valeriano e Maness (2014) utilizam a terminologia "aspecto físico" e "aspecto sintático" para referir-se ao duplo caráter do ciberespaço, sendo o primeiro aspecto relacionado aos limites físicos de fios, discos rígidos e estrutura e o segundo relacionado à informação armazenada e transitada nesse domínio.

Apesar de não mencionar o aspecto informacional do ciberespaço, a definição de Kello (2013) aborda a questão das formas de conectividade entre dispositivos nesse domínio. O autor afirma que o espaço cibernético é composto de todos os sistemas e redes computacionais existentes, incluindo redes de *air gap* (desligadas da internet) e seria formado por três camadas parcialmente sobrepostas: a internet, incluindo todos os computadores interconectados; a *world wide web*, consistindo apenas dos nós acessíveis através de interface URL[53]; e um "arquipélago" cibernético, contendo todos os outros sistemas computacionais que existem desligados da Internet ou da web (KELLO, 2013, p. 17).

Definições mais amplas de ciberespaço consideram ainda aspectos "semânticos" e "cognitivos". Libicki (2007 *apud* BETZ; STEVENS, 2013) acrescenta à terminologia de "aspecto físico" e "aspecto sintático" utilizada por Valeriano e Maness (2014) o aspecto semântico. Ressalta-se que, diferentemente de Valeriano e Maness (2014), por "aspecto sintático" o autor refere-se a programas e protocolos de comunicação utilizados no ciberespaço, de forma que as informações e ideias transitando no domínio constituiriam o "aspecto

[53] *Uniform resource locator*, endereço virtual de uma página ou website.

semântico". Schreier (2015) também acrescenta uma terceira dimensão à divisão de Valeriano e Maness (2014): o "aspecto cognitivo". O aspecto cognitivo diz respeito aos impactos na mente e comportamento humanos causados pelo acesso muito aumentado a conteúdo e pela quantidade massiva de informações. Dessa forma, as mentes dos usuários são extensão dos aspectos físico e sintático do ciberespaço e são incluídas no conceito. O autor destaca também o papel do espectro eletromagnético[54] na viabilização do ciberespaço e nesse sentido oferece a definição de Kuehl (2009) segundo a qual:

> O ciberespaço é um domínio operacional cujo caráter único e distintivo é definido pelo uso de equipamentos eletrônicos e do espectro eletromagnético para criar, armazenar, modificar, trocar e explorar informação via sistemas baseados em tecnologias de informação e comunicação interconectados e suas infraestruturas associadas (KUEHL, 2009 *apud* SCHREIER, 2015).

Nota-se que a inclusão das mentes dos usuários no conceito de ciberespaço não é uma ideia restrita à discussão conceitual de segurança internacional. Em suas abordagens sociológicas, Castells (2013) e Lévy (1999) referem-se à mente humana como parte constituinte do ciberespaço. Também os editores do romance de William Gibson, *Neuromancer*, convidam o leitor a "mergulhar nessa alucinação coletiva, nesse emaranhado de textos e ideias que, em cada mente, ajudou a construir um verdadeiro ciberespaço consensual" (GIBSON, p. 11, nota ao leitor).

Frente ao exposto, a presente dissertação resume as definições de ciberespaço derivadas da amostra bibliográfica revisada, conforme a amplitude do conceito (Tabela 10). A apresentação e sistematização dos conceitos de ciberespaço, objetivando dar sentindo ao emaranhado de definições que caracteriza a amostra bibliográfica, é uma das contribuições desta revisão sistemática de literatura.

Tabela 10 – Quadro-resumo das definições conforme elementos constituintes

	Infraestrutura Física	**Informações**	**Protocolos e Linguagens**	**Espectro Eletromagnético**	**Usuários**
Nye (2010)	X	X			
Melzer (2011)	X	X			
Betz e Stevens (2013)	X	X	X		
Kello (2013)	X				
Valeriano e Maness (2014)	X	X			
Schreier (2015)	X	X		X	X

[54] Espectro eletromagnético é definido como a gama de frequências de radiação eletromagnética de zero ao infinito, dividido em 26 bandas designadas em ordem alfabética.

Além da menção aos elementos constituintes do ciberespaço (aspectos físico, sintático, semântico e cognitivo) é recorrente na literatura revisada a referência ao que seriam implicações da arquitetura do ciberespaço ou suas características: baixo custo de entrada, com aumento do número de atores potencialmente relevantes, possibilidade de atuação anônima, com consequente dificuldade de atribuição de ataques cibernéticos e assimetrias de vulnerabilidades decorrentes de diferentes níveis de dependência da tecnologia. Essas características do ciberespaço facilitariam, por um lado, ações ofensivas em relação a ações defensivas em conflitos cibernéticos e, por outro, ensejariam a diminuição do poder do Estado-nação[55] enquanto ator central das relações internacionais (NYE, 2010; MANJIKIAN, 2010; KELLO, 2013; SCHREIER, 2015). Esses argumentos e seus corolários são questionados na própria literatura, conforme apresentado adiante.

2.2.3. Baixo custo de entrada, anonimato, assimetrias de vulnerabilidades e dificuldades de atribuição de ataques cibernéticos

O baixo custo de entrada no ciberespaço decorre de serem um computador com acesso à internet e motivação os únicos requisitos necessários para a entrada de indivíduos ou organizações com potencial de realizar ataques e participar de conflitos de relevância internacional. A facilidade de acesso ao ciberespaço aumentaria o número de atores potencialmente relevantes nesse domínio e constituiria fator de instabilidade nas relações internacionais operacionalizadas no espaço cibernético.

O anonimato é outro atributo frequentemente imputado à atuação no ciberespaço (NYE, 2010; HUGHES, 2010; BRONK; TIKKA-RINGAS, 2013; GOLDSMITH, 2013; KELLO, 2013; LINDSAY, 2013; SCHREIER, 2015; GARCIA, 2016; BALZACQ; CAVELTY, 2016; EFRONY; SHANY, 2018). A consequência da possibilidade de atuar anonimamente seria a dificuldade de atribuição de ataques cibernéticos, com diminuição da probabilidade de responsabilização e retaliação por eles. O anonimato e as dificuldades de atribuição atuariam como incentivo à realização de ataques, sendo também considerados fatores de instabilidade nas relações internacionais no ciberespaço.

Nye (2010) e McGraw (2013) mencionam, ainda, uma assimetria de vulnerabilidades inerente ao ciberespaço, decorrente da convivência de atores de diferentes magnitudes nesse domínio. Nye (2010) defende que três principais tipos de atores atuam nesse domínio: governos,

[55] O argumento de que características do domínio cibernético favorecem a erosão do poder do Estado-nação como ator central das relações internacionais é discutido no capítulo 3.

organizações e redes altamente estruturadas, e indivíduos ou redes pouco estruturadas. Ao passo que governos e organizações altamente estruturadas têm como vulnerabilidades um elevado grau de dependência de sistemas informáticos, cujo comprometimento poderia representar até mesmo um risco existencial a essas instituições e impactar um número grande de pessoas, indivíduos teriam por vulnerabilidade o apenas risco da coerção. McGraw (2013) refere-se a isso como um "efeito balanceador da grande vulnerabilidade cibernética no poder", argumentando que "ironicamente, pode ser que países mais desenvolvidos sejam mais vulneráveis à guerra cibernética, por serem mais dependentes de sistemas de alta tecnologia" (MCGRAW, 2013, p. 113).

O baixo custo de entrada, o anonimato e a assimetria de vulnerabilidades combinados teriam o potencial de empoderar atores tradicionalmente pouco relevantes nas relações internacionais e provê-los de um ambiente no qual suas ações dificilmente poderiam ser atribuídas a eles. Nesse sentido, Goldsmith (2013) afirma que há no ciberespaço uma insegurança inerente decorrente da complexidade dos sistemas computacionais – que frequentemente levaria a erros – potencializada pelo número e pelos incentivos dados a atores capazes de explorar vulnerabilidades nesses sistemas. McGraw (2013) argumenta que a falha em construir sistemas efetivamente seguros diminui ainda mais as barreiras de entrada (consideradas já baixas pelo autor) para conflitos cibernéticos motivados por questões geopolíticas (MCGRAW, 2013, p. 113). Bronk e Tikka-Ringas (2013) e Garcia (2016) afirmam que "a atribuição de ataques cibernéticos é uma questão complexa, considerando que a arquitetura de redes de computadores permite a *hackers* habilidosos operar anonimamente" (BRONK; TIKKA-RINGAS, 2013, p. 89); e que o ciberespaço "permite maior anonimato, dificultando atribuição de condutas" (GARCIA, 2016, p. 93).

Há, contudo, na própria literatura revisada, artigos – em geral mais recentes – (LINDSAY, 2013; VALERIANO; MANESS, 2014; GARTZKE; LINDSAY, 2015; RID; BUCHANAN, 2015; SMEETS, 2018) que relativizam essas percepções e discutem em que medida os custos de entrada no ciberespaço são efetivamente baixos, as nuances do anonimato e o processo de atribuição de ataques cibernéticos.

O principal argumento rebatendo a ideia de baixo custo de entrada no ciberespaço é que o custo de entrada só é baixo no ciberespaço para ataques pouco relevantes estrategicamente,

ações de crime ou fraude financeira de pouca expressividade política ou a desfiguração de uma página na internet por motivação ideológica[56].

Gartzke e Lindsay (2015) afirmam que a grande maioria dos ataques cibernéticos, que se utilizam de procedimentos relativamente simples e a baixo custo são, em geral, pouco importantes estrategicamente. Ataques de grande impacto estratégico requerem ações preparatórias de inteligência, ambientes controlados para a realização de testes, recursos humanos altamente qualificados, além de tempo e capacidade computacional, a exemplo do ataque do *worm* Stuxnet ao programa nuclear iraniano. A maior parte dos ataques cibernéticos registrados seria realizada por redes automatizadas de computadores comprometidos (máquinas infectadas com *malwares* que possibilitam aos atacantes controle sobre elas, formando redes de computadores "zumbis", as *botnets*) coordenadas por criminosos em busca de lucros ou por burocracias de espionagem – algo considerado pelos autores de baixa relevância nas questões de segurança e essencialmente diferentes da utilização para execução de ataques terroristas ou militares (GARTZKE; LINDSAY, 2015, p. 324).

Na medida em que demonstram que as principais disputas cibernéticas registradas entre díades de países rivais entre 2001 e 2011 foram regionalizadas e controladas, ao invés de disruptivas e globais, Valeriano e Maness (2014) corroboram a visão de Gatzke e Lindsay (2015), sugerindo que ataques cibernéticos de maior impacto estratégico não são tão quotidianos quanto pode parecer no discurso corrente sobre baixo custo de entrada (VALERIANO; MANESS, 2014).

Ainda Gartzke (2013) e Smeets (2018) mencionam que capacidades cibernéticas são transitórias (SMEETS, 2018) ou do tipo "*use and lose*" (GARTZKE, 2013), pois uma vez aplicadas, as vulnerabilidades computacionais que permitiram seu uso são rapidamente corrigíveis. Nesse sentido, há poucos incentivos à utilização dessas capacidades em ações de pouco impacto estratégico, sem ações de preparação e planejamento ou contra atores com grandes chances de defesa. Essa percepção também põe em questão o alegado baixo custo de entrada no ciberespaço.

Por sua vez, na literatura revisada, o questionamento do anonimato enquanto característica inerente ao ciberespaço é levantado sobretudo na forma da discussão sobre o problema de atribuição de ataques cibernéticos. O processo de atribuição, apesar de não ser absoluto e de exigir tempo e recursos consideráveis, que extrapolam a aplicação de técnicas de

[56] Na seção 2.3.2, sobre definições negativas de guerra cibernética, fica claro que a literatura revisada busca diferenciar seu objeto de estudo de fenômenos com menor impacto estratégico, como crime cibernético, espionagem cibernética e ações de hacktivismo.

análise forense em sistemas de computadores, é possível e tem sido realizado cada vez mais frequentemente com grau aceitável de confiabilidade.

O anonimato no ciberespaço é diretamente questionado por Farwell e Rohozinski (2011), na medida em que afirmam que "trilhas digitais no espaço cibernético inibem o anonimato completo de código ou local" (FARWELL; ROHOZINSKI, 2011, p. 27, tradução nossa). Também Lupovici (2017, p. 9) afirma que o anonimato não é uma característica inerente ao domínio cibernético, mas deve ser compreendido como parte da construção da ideia do ciberespaço, construída e gerenciada através de processos sociais. Tor (2016, p. 100), por sua vez, afirma que "a ideia romântica de anonimato no ciberespaço não se sustenta quando se lida com atores estatais, devido tanto ao contexto estratégico quanto a realidade operacional do comportamento desses atores".

Decorrência do alegado anonimato propiciado pelo ciberespaço, a dificuldade de atribuição de ataques cibernéticos constituiria um incentivo à realização desses ataques, sendo elemento de instabilidade nas relações internacionais. Rid e Buchanan (2015) rebatem esse argumento afirmando que, a despeito de a atribuição de ataques cibernéticos a grupos e/ou governos não ser algo realizado facilmente, tampouco com grau absoluto de certeza, ela é possível e tem sido realizada com sucesso cada vez mais frequentemente. Os autores propõem um modelo para dar a esse processo um grau aceitável de confiança segundo o qual a atribuição não é meramente técnica, mas requer uma variedade de pontos de vista e necessita de equipes multidisciplinares que integrem cientistas da computação, programadores e uma comunidade científica multidisciplinar, incluindo profissionais de RI.

Nesse sentido, Rid e Buchanan (2015) defendem que o trabalho de atribuição de ataques cibernéticos apresenta um nível tático, um operacional e um estratégico. No nível tático, a atribuição demandaria experiência, habilidade e intuição do pessoal técnico; no nível operacional, a atribuição deve ser abordada como uma questão de nuances – e não absoluta –, sendo necessária a atuação de profissionais de diferentes áreas e a observação de aspectos mais amplos do que os vestígios computacionais do ataque – os chamados IoCs (indicadores de comprometimento) ou as características do código utilizado pelos atacantes. No nível estratégico, a atribuição deve ser vista em função daquilo que está em jogo politicamente (RID; BUCHANAN, 2015, p. 7).

Cavelty (2013) e Lupovici (2014) também relativizam a dificuldade de atribuição de ataques cibernéticos e avaliam que a presunção de impossibilidade de determinar as origens de

ataques serve à construção de uma ideia de insegurança no ciberespaço e à securitização[57] dos discursos político e acadêmico sobre o tema (CAVELTY, 2013), além de dificultar o uso de estratégias de dissuasão[58] nesse domínio (LUPOVICI, 2014).

2.2.4. Ataque e defesa no ciberespaço

Juntamente com a dificuldade de atribuição, outra característica do ciberespaço que seria derivada do baixo custo de entrada, do anonimato e de assimetrias em vulnerabilidades seria a maior facilidade de realizar ataques em relação a ações de defesa nesse domínio.

Schreier (2015, p. 12) defende que as alegadas especificidades do ciberespaço (baixo custo de entrada e anonimato e assimetria de vulnerabilidades) contribuiriam para uma dinâmica de conflito em que o ataque seria dominante em relação à defesa: ao passo em que aqueles ocorrem em grande velocidade, com amplo alcance (virtualmente, todos os dados armazenados ou transitando pelo espectro eletromagnético podem ser atingidos) e difícil atribuição de autoria (com a utilização de servidores de IPs falsos e *botnets*, por exemplo), a defesa cibernética enfatiza a detecção de ameaças em detrimento do tratamento ou extinção de vulnerabilidades e conta com protocolos vulneráveis e arquiteturas abertas. Dito de outra forma: no ciberespaço o agressor precisa encontrar uma fragilidade crucial, enquanto o defendente deve encontrar todas elas (KAHN, 1960, *apud* GOLDSMITH, 2013).

Kello (2013) enumera razões pelas quais o ataque é considerado dominante em relação à defesa no ciberespaço, a saber: a imprevisibilidade e indetectabilidade de ataques (por definição, os defensores não conhecem vulnerabilidades *zero-days*[59]); possibilidade de negação de defesa, quando um *malware* priva a defesa da habilidade de gerenciar sua própria proteção (pelo uso de comando e controle remotos ou de *malwares* inteligentes); superfície de defesa complexa, haja vista que o defendente deve proteger continuamente toda a superfície da rede contra o vasto universo de ataques concebíveis; fragmentação da defesa (infraestruturas computacionais críticas são possuídas e operadas pela indústria privada em cooperação com o setor público); e riscos presentes ao longo de toda a cadeia de suprimentos[60].

---

[57] Tratada no item 3.2.4.

[58] Tratada no item 3.2.2.

[59] Falhas de segurança em redes ou programas de computador ainda não publicizadas ou não conhecida pelo alvo.

[60] Exemplo de ataques cibernéticos a cadeias de suprimento, em dezembro de 2020, ataques à plataforma Orion da empresa Solar Winds, *software* de gerenciamento de TI contratado por diversos órgãos do governo dos Estados Unidos e em outros países do mundo, foram publicizados. Os ataques permitiram acesso a sistemas e informações confidenciais de muitas instituições, incluindo o Departamento de Energia (DoE) e a National Nuclear Security Administration (NNSA) dos EUA e teve impactos comparados aos do Stuxnet na mídia especializada.

Gartzke e Lindsay (2015) resumem o argumento de que, no domínio cibernético, o ataque seria dominante em relação à defesa:

> É amplamente aceito que a dependência social da internet e o baixo custo de ferramentas de *hacking* permitem que Estados-nação e *hackers* solitários cruzem fronteiras, sem aviso, para acessar redes vitais de computadores. Uma vez lá dentro, eles podem roubar segredos valiosos ou desativar equipamentos essenciais. Ao mesmo tempo, acredita-se que a ubiquidade, o anonimato e a complexidade da internet minam esforços de desarmamento, defesa e dissuasão. Como a agressão cibernética explora os mesmos canais abertos usados para comércio e comunicação legítimos, as técnicas ofensivas não podem ser simplesmente evitadas ou proscritas. Se os *hackers* conseguirem escapar da detecção e desconsiderar ameaças de retaliação, a dissuasão perde sua credibilidade. Falhas de coordenação entre empresas e atores governamentais, juntamente com a capacidade dos invasores de variar assinaturas mais rápido do que os defensores podem detectá-las, amplificam ainda mais os custos de proteção de rede. Como resultado, tornou-se ideia comum que o ataque domina a defesa no ciberespaço. (GARTZKE; LINDAY, 2015, p. 316, tradução nossa).

Gartzke e Lindsay (2015) desafiam, contudo, essa percepção e sublinham a ausência de evidências empíricas que consubstanciem esse argumento (GARTZKE; LINDSAY, 2015, p. 319). Eles afirmam que, ao invés de implicar uma relação ataque-defesa determinista, o ciberespaço facilita a adoção do que chamam de estratégia de "engano" (*deception*), que serviria tanto a ações ofensivas quanto a ações defensivas. O "engano" é apresentado como uma estratégia protetiva semelhante a suas análogas clássicas (o desarmamento, a dissuasão e a defesa propriamente dita). Porém, ao passo que no domínio cibernético a estratégia do desarmamento não é plausível, haja vista o caráter intrinsecamente dual das ferramentas cibernéticas e a alta dependência que toda a sociedade tem dos usos legítimos do ciberespaço – como as transações comerciais e fluxos de comunicação –, a estratégia do "engano" poderia viabilizar as estratégias protetivas de defesa e de dissuasão no ciberespaço[61] ou funcionar como uma quarta estratégia protetiva *per se*, que seria específica desse domínio.

O engano como estratégia protetiva do ciberespaço refere-se à prática de converter uma invasão de servidores ou redes de computadores em algo que confunda ou prejudique o atacante (GARTZKE; LINDSAY, 2015, p. 336), como a passagem de desinformação, e seria particularmente potente com o advento da internet, de forma semelhante ao que aconteceu com a dissuasão na era nuclear. O engano estaria para a ameaça cibernética assim como a dissuasão para a ameaça nuclear. Nesse sentido, vantagens de ataque ou defesa no domínio cibernético derivariam não de atributos característicos da tecnologia, mas da capacidade organizacional relativa para empregar a estratégia do engano e para integrá-la a estratégias mais amplas

[61] A discussão mais aprofundada sobre dissuasão no domínio cibernético é apresentada no item 3.2.2.

(GARTZKE; LINDSAY, 2015, p. 318), de forma que estados mais poderosos ou redes altamente estruturadas teriam maior probabilidade de uso bem sucedido dessa estratégia.

Frente às discussões conceituais apresentadas, percebe-se que a abordagem do ciberespaço escolhida em determinada literatura geralmente guarda relação com o tema sendo tratado ou o objetivo analítico pretendido. Nesse sentido, definições inclusivas do ciberespaço, que consideram infraestrutura física e aspectos sintáticos e semânticos, são úteis ao estudo de um tipo de conflito cibernético centrado na informação, ao passo que definições focadas em aspectos de infraestrutura física são úteis ao estudo de conflitos cibernéticos centrados na operacionalização de ataques cibernéticos *stricto sensu.* Ademais, a noção do ciberespaço como uma vila global, um domínio livre e igualitário, é utilizada sobretudo quando trata das perspectivas de governança do ciberespaço, ao passo que sua percepção como domínio vinculado ao poder estatal é adotada mais comumente quando se discute as perspectivas de guerra ou conflitos cibernéticos.

Dizer que o ciberespaço possui baixo custo de entrada e que provê anonimato tornou-se praticamente um lugar-comum na apresentação do conceito na literatura inicial. A avaliação mais detida dessas características e de seus corolários (a dificuldade de atribuição e a primazia do ataque em relação à defesa no ciberespaço) deixa claro que essas não são condições incontestes. Nesse sentido, Sharp (2017) afirma que, após uma fase inicial da literatura de RI sobre a ascensão do ciberespaço, que destacava os "perigos" desse domínio, uma segunda fase constituiu-se de textos mais críticos, que passaram a questionar as premissas até então utilizadas como noções absolutas no ciberespaço. A despeito de que no início da produção de segurança internacional sobre conflitos cibernéticos as alegadas características do ciberespaço tenham tido importância fundamental na caracterização desse domínio e possam ter representado possibilidades reais, desde então estados-nação vêm aprimorando suas capacidades de atuação e defesa no espaço cibernético, com altos investimentos em sua própria segurança cibernética, no domínio de novas tecnologias, nos processos de atribuição e em recursos humanos, de forma que o questionamento das características do ciberespaço na literatura é benéfico à capacidade analítica dos estudos de segurança internacional. Nesse sentido, é interessante notar que as discussões acadêmicas sobre ciberespaço na segurança internacional têm contribuído diretamente com o aprimoramento do conceito, mostrando responsividade do campo de estudos e evitando a cristalização de lugares-comuns que podem prejudicar a capacidade analítica da disciplina e ter uma influência limitante em discursos científicos e políticos sobre a questão.

2.3. Guerra cibernética

Analogamente ao que ocorre com o conceito de ciberespaço, tampouco o conceito de guerra cibernética conta com consenso disciplinar na área de segurança internacional, algo apontado em Junio (2013), Kello (2013), McGraw (2013) e Stone (2013) e corroborado pela literatura revisada. Como apontado por Stone (2013), a incerteza em relação ao próprio conceito de guerra *per se* dificulta ainda mais o estabelecimento de um acordo na questão. É interessante notar que institutos de natureza técnica como o NIST, a despeito de apresentarem conceitos para ciberespaço e segurança cibernética, não tem definição de guerra cibernética, algo que aponta para a natureza eminentemente política do fenômeno – mais do que para qualquer particularidade técnica como sua característica principal. Mais do que a dificuldade de se definir guerra cibernética ou ações que constituiriam atos de guerra cibernética, a principal questão identificada na literatura diz respeito ao enquadramento dessas ações e ataques cibernéticos nas noções tradicionais de guerra e suas implicações no direito internacional. Apesar de não haver consenso sobre o *status* de guerra, a literatura revisada aponta para enorme concordância sobre o potencial estratégico desses ataques.

2.3.1. Definições de guerra cibernética

Como ocorre com o conceito de ciberespaço, há poucas definições categóricas de guerra cibernética. De forma geral, contudo, é possível apreender as noções de guerra cibernética utilizadas nos documentos revisados conforme suas argumentações. As principais divergências entre os conceitos de guerra cibernética derivados da literatura podem ser organizados com base na presença ou não de efeitos cinéticos, às vezes referidos como violência ou, mais especificamente, letalidade. Ao passo que alguns autores defendem que, para constituir um ato de guerra, um ataque cibernético deve necessariamente implicar o efeito cinético de destruição física, violência ou letalidade (RID, 2012; MCGRAW, 2013). Outra parte da literatura considera que os efeitos de ataques cibernéticos, ainda que não imitem efeitos cinéticos de atos de guerra convencionais, podem ser tão relevantes estrategicamente quanto os últimos (JUNIO, 2013; LEMAY; FERNANDEZA; KNIGHT, 2010).

Hughes (2010) define “guerra cibernética” como qualquer guerra levada a cabo no ciberespaço por atores estatais e não estatais significativos – sem definir ciberespaço tampouco explicar a que se refere com o adjetivo “significativos”. O autor exemplifica o que poderia ser considerado guerra cibernética: “a condução de operações cibernéticas ofensivas ou defensivas

de sistemas de informação e comunicação, infraestruturas críticas, sistemas de armas e centros de comando militar" (HUGHES, 2010, p. 525), porém não impõe a necessidade de efeitos cinéticos àquilo que chama de atos de guerra cibernética. Analogamente, Junio (2013) oferece a seguinte definição para guerra cibernética: "ato coercivo envolvendo ataques a redes de computadores", referindo-se por "ataque a redes" à interrupção, adulteração ou destruição de informação, e por "coercivo" ao uso da força para alterar ou preservar um *status quo* político (JUNIO, 2013, p. 2), sem mencionar a necessidade de impactos cinéticos.

De forma diversa, para McGraw (2013) guerra cibernética requer impacto no mundo físico, ou "efeito cinético" no jargão militar, ainda que seus meios sejam virtuais, o impacto de uma ação deve ser físico para que seja considerada guerra cibernética (MCGRAW, 2013, p. 112).

Numa abordagem teórica, o conceito de guerra cibernética para Lindsay (2014) é um entre quatro cenários possíveis, consideradas as combinações entre os extremos dos debates sobre conflitos e ascensão do espaço cibernético. O debate sobre a ascensão do espaço cibernético questiona se a ascensão do ciberespaço constituiria uma mudança tecnológica evolutiva a partir de outras tecnologias ou uma mudança tecnológica revolucionária. O debate sobre conflitos cibernéticos questiona se o domínio cibernético constituiria um meio ambiente político competitivo ou cooperativo (LINDSAY, 2014). Na hipótese de a ascensão do espaço cibernético ser uma mudança tecnológica revolucionária num ambiente político competitivo, tem-se o cenário de guerra cibernética (*cyber warfare)*, no qual se presume que o espaço cibernético é um ambiente anárquico e perigoso, com distribuição assimétrica de capacidades e no qual o ataque é dominante em relação à defesa (LINDSAY, 2014, p. 12). Os outros cenários possíveis no modelo de Lindsay (2014) são: internet aberta (ascensão do ciberespaço como mudança tecnológica evolutiva em ambiente político cooperativo), regime de segurança cibernética (ciberespaço como mudança tecnológica revolucionária em meio ambiente político cooperativo) e espaço cibernético disputado (mudança tecnológica evolutiva em meio ambiente político competitivo) (LINDSAY, 2014).

2.3.2. Definições negativas de guerra cibernética

É frequente na literatura revisada (HUGHES, 2010; LINDSAY, 2013; KELLO, 2013; LINDSAY, 2014; SIEDLER, 2016) a utilização de estratégias negativas de definição de guerra cibernética. Na medida em que os autores declaram a que *não* se referem em seus estudos, buscam diferenciar seu objeto de estudo de outros fenômenos que não teriam relevância para a

segurança internacional, tais como criminalidade cibernética com objetivos financeiros, espionagem cibernética e hacktivismo[62]. Essa distinção é importante e constitutiva no sentido de separar o que faz parte ou não dos estudos da segurança internacional.

Conforme aponta McGraw (2013), a confusão entre os conceitos de guerra cibernética, espionagem cibernética e crime cibernético decorre de os três fenômenos terem a mesma raiz: uma forte dependência de sistemas inseguros que perpetua medo e incerteza na questão da segurança cibernética. Daí a importância do desenvolvimento de sistemas seguros desde sua concepção (*security by design*), em oposição à abordagem atual de segurança cibernética de caça de ameaças (*threat hunting*) (MCGRAW, 2013). Também nesse sentido, Klimburg (2011) afirma que ações de guerra ou crime cibernético não são fundamentalmente diferentes, divergindo basicamente quanto a sua motivação.

Parte da literatura, no entanto, diferencia ações de guerra cibernética de crime cibernético, ciberespionagem e hacktivismo com base no impacto estratégico dessas ações: ações de guerra cibernética, consideradas raras, implicariam maior importância estratégica nas relações internacionais, em comparação a menor relevância – e maior frequência – de crimes cibernéticos com objetivos financeiros, espionagem cibernética e hacktivismo.

Nesse sentido, Hughes (2010), na proposta de criação de um *Tratado para o ciberespaço*, exclui de seu objeto de análise as ações de *hacking* recreacional ou motivado socialmente ("hacktivismo") (HUGHES, 2010, p. 525), sem, no entanto, fazer a mesma ressalva quanto a ações de crime cibernético e espionagem cibernética. Nesse sentido, ações de espionagem e crime no ciberespaço[63] seriam assemelhadas a guerra cibernética e são também objeto da iniciativa de normatização proposta por Hughes (2010).

Por sua vez, Kello (2013), Junio (2013), Schreier (2015) e Siedler (2016) diferenciam entre ataques a redes de computadores (*Computer Network Attacks*, CNA) e exploração de redes de computadores (*Computer Network Exploitation*, CNE) – Kello (2013) diferencia, ainda crime cibernético e hacktivismo. Ataques a redes de computadores (CNA) dizem respeito à utilização de código para interferir na funcionalidade de um sistema computacional com propósito político ou estratégico e efeitos nem sempre limitados ao espaço cibernético ao passo que exploração de redes de computadores (CNE) refere-se à invasão de sistema computacional adversário, de forma a acessar a informação sem danificá-la (ciberespionagem). A exploração

---

62 Kello (2013) define hacktivismo como ataques cibernéticos com propósito de chamar atenção para uma causa, em defesa de uma ideologia e sendo realizado por atores privados (KELLO, p. 20).

63 A relação entre crime cibernético e guerra cibernética é abordada por Farwell e Rohozinksi (2011) e apresentada na seção 3.2.3, sobre a relação entre atores estatais e não estatais no ciberespaço.

de redes de computadores depende de discrição e indetectabilidade, havendo por consequência baixos incentivos para prejudicar o sistema acessado. No entanto, conforme também aponta Lindsay (2013), a técnica poderia ser utilizada como instrumento para ataques cibernéticos futuros (KELLO, 2013, p. 21).

De acordo com a Lei de Conflitos Armados (Loac[64]) – argumenta Kello (2013) –, exploração e ataques a redes de computadores implicariam consequências políticas e legais diferentes. Como forma de espionagem, a exploração de redes de computadores não implicaria efeitos adversos diretos e não é proibida pelo direito internacional. Em contraste, um ataque cibernético de grande impacto poderia constituir uso de força ou mesmo um ataque armado sob obrigações de tratados (KELLO, 2013, p. 21). Nesse sentido, Junio (2013), conceitua ataques a redes de computadores como atos que alteram, degradam ou destroem sistemas computacionais adversários, incluindo a informação ali transitante, e exploração de redes de computadores como monitoramento e espionagem de sistemas computacionais, sem caráter destrutivo. Atos de guerra cibernética incluiriam ataques a redes de computadores, mas não sua exploração (JUNIO, 2013).

Para Lindsay (2013), que também define negativamente guerra cibernética com base na diferença de impactos estratégicos entre esse e outros fenômenos, as perspectivas mais graves para esse fenômeno iriam além do uso militar em tempo de guerra e dizem respeito à possibilidade de ataques cibernéticos interromperem o funcionamento ou destruírem sistemas de controle industrial, a exemplo de controladores de redes de energia elétrica, distribuição de água, controle de tráfego aéreo e de armas ou redes financeiras e industriais[65]. Isso implicaria efeitos estratégicos significativos, de forma que esses ataques poderiam até mesmo atuar como substitutos de ataques convencionais (LINDSAY, 2013, p. 11). Contudo, o autor faz a ressalva de que ações de espionagem cibernética, consideradas menos relevantes do que ações de guerra cibernética, seriam potencialmente mais graves do que crime cibernético e hacktivismo por empregar muitas vezes *malwares* e ferramentas instrumentalizáveis na realização de ataques de grande impacto (LINDSAY, 2013). Além disso, ações de ciberespionagem podem minar o poder de um ator mais forte pelo roubo de propriedade intelectual e segredos comerciais (uma tese que é referida na literatura como "morte por mil cortes" (LEMAY; FERNANDEZA; KNIGHT, 2010; LINDSAY, 2013; LINDSAY, 2014), tendo importância estratégica relevante.

---

64 A Loac abarca o direito governando a legalidade de ir à guerra (*jus ad bellum*), manifesto nos arts. 2.4 e 51 na *Carta das Nações Unidas*, e o direito governando o comportamento durante a guerra (*jus in bello*), direito internacional humanitário.

65 A discussão sobre ataques cibernéticos a infraestruturas críticas aparece mais frequentemente na literatura relacionado ao conceito de "segurança cibernética" e é abordado nesta dissertação na seção 2.3.5.

Note-se que a diferenciação de fenômenos conforme o impacto estratégico, ou a severidade dos danos causados é também considerada pelo setor privado responsável, juntamente com instituições públicas, pela segurança cibernética de infraestruturas críticas nos EUA. Nesse sentido, Carr (2016) afirma que o setor diferencia entre ameaças de baixo nível como ataques de perturbação, *hackers* individuais e hacktivistas e a proteção contra ataques à segurança nacional (CARR, 2016) – que, presume-se, incluiriam ataques e exploração a redes de computadores.

Siedler (2016) qualifica ainda mais a questão do impacto estratégico, diferenciando dentre ataques a redes de computadores entre aqueles de coerção e aqueles de força bruta. Segundo a autora, ataques de coerção têm por objetivo principal a demonstração de poder, a exemplo do que teriam sido os ataques à Estônia em 2007, e têm baixa capacidade para alterar o comportamento de um adversário em situação de conflito devido a dúvidas quanto à atribuição dos ataques e à ausência de consequências cinéticas. Por outro lado, ataques de força bruta teriam efeitos cinéticos palpáveis, a exemplo do Stuxnet e, portanto, maior efetividade na consecução de objetivos políticos (SIEDLER, 2016, p. 29).

2.3.3. Guerra cibernética é guerra?

Para além da definição do que constituiriam atos de guerra cibernética, um debate conceitual relevante na literatura revisada é a possibilidade ou não de igualar ações de guerra cibernética (em suas várias definições) na visão tradicional de guerra, sendo a ausência de consequências cinéticas, de caráter violento ou letalidade, por vezes utilizada como argumento para desconsiderar ataques cibernéticos como atos de guerra. Essa discussão relaciona-se com a questão da eficácia de ataques cibernéticos enquanto elementos de coerção política nas relações internacionais.

Kello (2013) resume algumas dificuldades identificadas na definição de ataques cibernéticos enquanto atos de guerra:

> Noções tradicionais de guerra confrontam cinco dificuldades em sua aplicação a ataques cibernéticos [...]. Em primeiro lugar, falta aos ataques cibernéticos aproximação causal a ferimentos (danos físicos) e eles podem inclusive não ser violentos. Em segundo lugar, a concepção da guerra como o uso de forças armadas estabelece um limite muito alto em termos de escopo, duração e intensidade, que as ações cibernéticas podem não atender. Terceiro, os perpetradores de um ataque cibernético podem ser atores não estatais, normalmente não considerados sujeitos de direito internacional e que, portanto, não estão sujeitos às suas penalidades. Quarto, uma operação cibernética ofensiva conduzida por atores não tradicionais, como aquela contra a Estônia (2007), não precisaria envolver objetivos estratégicos dos Estados ou de seus militares. Quinto, pelo menos no caso de um ataque cibernético generalizado,

> a importante distinção entre alvos militares e civis se dissolve devido à ampla difusão de sistemas de computadores na sociedade e suas interdependências (KELLO, 2013, p. 25, tradução nossa).

De fato, o principal ponto de controvérsia sobre o conceito de guerra cibernética atingir o *status* de guerra encontrado na literatura revisada é a necessidade ou não de violência e letalidade na caracterização de um ato de guerra. Rid (2012), baseando-se na definição clássica de guerra de Clausewitz, afirma que, para ser considerada um ato de guerra, determinada ação deve implicar violência, possuir caráter instrumental e ter objetivos políticos (RID, 2012, p. 7-8). O autor argumenta que nenhum dos incidentes cibernéticos conhecidos até então apresentaria os três atributos simultaneamente. Em ataques cibernéticos, o elemento "uso da força", essencial a qualquer ato de guerra, tende a ser "uma sequência bem mais indireta e complexa de causas e consequências que finalmente resultem em violência e baixas" (RID, 2012, p. 9), ao contrário do uso da força direto e denso identificado nos conflitos usualmente classificados como guerra. A conclusão de Rid (2012), explícita em seu título *Cyberwar will not take place*, é que os conflitos cibernéticos conhecidos não atingem o *status* de guerra e que não há perspectiva da ocorrência de uma guerra cibernética.

De forma análoga, Kello (2013) afirma que, já que armas cibernéticas não são abertamente violentas, é pouco provável que seu uso atinja os critérios de guerra interestatal. Apenas no caso de os efeitos de um ataque cibernético produzirem destruição física significativa ou perda de vidas, a ação poderia ser rotulada como guerra, no entanto a maior parte dos ataques não atinge esses critérios (KELLO, 2013). O autor, no entanto, defende que, a despeito de não necessariamente terem o *status* de ato de guerra, o impacto de ataques cibernéticos não deve ser subestimado. O desenvolvimento de capacidades cibernéticas estaria expandindo o espectro de possibilidades de danos e resultados entre os conceitos de guerra e paz, com consequências importantes para a segurança nacional e internacional (KELLO, 2013, p. 8).

Para Stone (2013), em contraposição a Rid (2012), ataques cibernéticos, a despeito de não apresentarem necessariamente letalidade, podem sim constituir atos de guerra, na medida em que "podem resultar em grandes quantidades de violência, letal ou não". Nesse sentido, ele afirma em seu título que a ciberguerra acontecerá (*Cyberwar will take place!*). Para o autor, a necessidade de letalidade como requisito para caracterizar atos de guerra deve ser relativizada, considerando-se sobretudo que desenvolvimentos ocidentais na forma de guerrear têm se pautado pela diminuição do número de baixas e pela precisão e rapidez em atingir componentes materiais e meios de resistência dos adversários (STONE, 2013, p. 105).

A expressão “grandes quantidades de violência, letal ou não” referidas por Stone (2013) refere-se a danos físicos que não atinjam necessariamente pessoas, mas impactos cinéticos a prédios e instalações. No entanto, Rid (2012) diferencia atos de sabotagem de atos de guerra precisamente pelo fato de os primeiros, na hipótese de utilização de violência, alvejarem “coisas” e não “pessoas”; e por prescindirem de atribuição. Ele argumenta que, apesar de sempre instrumentais, atos de sabotagem isoladamente não constituiriam atos de guerra porque os sabotadores podem deliberadamente evitar violência e atribuição política (RID, 2012, p. 16). Stone (2013), por sua vez, afirma que, mesmo que não apresentem caráter necessariamente violento, ataques cibernéticos podem implicar violência e que nada impede que formas futuras de guerra envolvam atos de força não atribuídos.

Uma abordagem intermediária é apresentada por Lemay, Fernandeza e Knight (2010). Os autores referem-se ao conceito “espectro de guerra”, cunhado para abordar técnicas de guerra assimétrica e descrito em documentos da doutrina militar canadense, para avaliar o *status* de guerra cibernética enquanto guerra. Conforme os autores, em um extremo do “espectro de guerra” estaria a paz e no outro um estado de guerra cinética de alta intensidade. Seu argumento é que uma guerra cibernética de baixa intensidade, em que uma série de ataques cibernéticos não podem ser correlacionados, pode ser tão devastadora quanto uma guerra cibernética de alta intensidade, causando uma “morte por mil cortes” (*death by a thousand cuts)* e, no entanto, são negligenciados na análise de guerra cibernética pela academia e por tomadores de decisão.

Diante da discussão apresentada, é possível concluir que, de forma geral, para a literatura, as definições de guerra cibernética que prescindem de efeitos cinéticos dificilmente podem ser classificáveis como atos de guerra convencionais. Mesmo entre as definições que implicam consequências cinéticas, observações acerca do contexto em que determinada ação foi tomada – notadamente o que está em jogo politicamente e o estado das relações políticas e diplomáticas entre os atores envolvidos – seriam necessárias para sua classificação como ato de guerra. Essa perspectiva busca a um só tempo não excluir a possibilidade de um ataque cibernético constituir ato de guerra, ao mesmo tempo em que relativiza um temor generalizado e generalista de guerra constante e total no ciberespaço. Ademais, a cautela em classificar ataques cibernéticos como atos de guerra não impacta de forma nenhuma o reconhecimento do potencial estratégico do uso desses instrumentos, podendo inclusive aumentar sua relevância, na medida em que diminui os incentivos à retaliação.

2.3.4. Guerra Cibernética x Guerra Informacional

Na literatura revisada nota-se imprecisão e às vezes sobreposição entre os conceitos de guerra cibernética e guerra informacional. Essa distinção de abordagens é mais notável em definições institucionais (de organizações internacionais ou nacionais, de diferentes países), com a visão de Estados Unidos e Otan referindo-se a guerra cibernética enquanto fenômeno diferenciado de guerra informacional e mais limitado a aspectos técnicos e computacionais, ao passo que a visão de China, Rússia e da Organização de Xangai para a Cooperação (*Shangai Cooperation Organization – SCO*)[66] tratam de ataques cibernéticos de forma geral como ações de guerra informacional, ignorando a ideia de uma guerra cibernética isolada.

Na discussão conceitual identificada na literatura, em geral a noção de guerra cibernética é mais limitada, com a presunção do uso de ferramentas cibernéticas ou a definição de alvos cibernéticos na realização de ataques com ou sem efeitos cinéticos, de forma a atingir objetivos políticos. A guerra informacional, por sua vez, diria respeito ao esforço pela predominância de uma narrativa em relação a outras, não se utilizando necessariamente de instrumentos cibernéticos.

Na visão de Schreier (2015), as operações informacionais têm espectro bastante mais amplo do que as guerras cibernéticas. O autor explica que, no fim dos anos 1970, surgiu na doutrina militar dos EUA o que foi chamado de guerra informacional e guerra de comando e controle, reconhecendo a informação como elemento de poder nacional em tempos de paz, conflito ou guerra. Atualmente a maior parte das forças armadas consideraria as operações de informação como capacidade essencial e a informação tanto uma arma quanto um alvo. Nesse sentido, Schreier (2015) apresenta a doutrina para operações de informação da Otan, segundo a qual operações de informação abarcariam operações psicológicas, desinformação militar, operações de segurança, operações em redes de computadores e guerra eletrônica (NATO, 2009).

---

[66] Moraes (2010) explica que a SCO se tornou uma organização permanente com a entrada do Uzbequistão em 2001, somando-se aos então chamados "Cinco de Xangai", a saber: China, Rússia, Cazaquistão, Tajiquistão e Quirguistão. O foco da SCO está em questões regionais de segurança e questões geopolíticas; seu objetivo seria o combate a problemas transnacionais de segurança, tais como o terrorismo, o tráfico de drogas e o fundamentalismo, assim como a questão do separatismo nas províncias chinesas do Tibete e Xinjiang. (MORAES, 2010).

Nos EUA, a doutrina de guerra informacional teria sido atualizada na Revolução de Assuntos Militares (*Revolution in Military Affairs* – RMA)[67] no final dos anos 1990, devido à forte crença na burocracia militar do país sobre a importância da guerra informacional no futuro dos conflitos (HUGHES, 2010, p. 528). Hughes (2010) considera que o valor da informação foi aprimorado pela tecnologia, com a utilização generalizada de redes, sistemas de tecnologia da informação e bancos de dados computacionais. Isso permitiria maior consciência situacional, maior sincronicidade de comando, controle e inteligência e, portanto, melhor utilização da informação em superioridade de combate. Nesse sentido, a transformação mais importante causada pela ascensão do ciberespaço estaria não na tecnologia em si, mas no deslocamento do foco da dimensão física para a dimensão informacional (SCHREIER, 2015, p. 19).

Betz e Stevens (2013), por sua vez, afirmam que foi a partir das discussões sobre o impacto das tecnologias da informação e comunicação (TIC) na guerra, no início da década de 1990, que surgiu a ideia de "guerra de informação estratégica", mas não haveria definição clara do conceito (BETZ; STEVENS, 2013, p. 8-9). Por sua vez, Melzer defende que "guerra de informação" se refere exclusivamente às operações de informação conduzidas em situações de conflito armado e exclui operações de informação ocorridas em tempo de paz (MELZER, 2011, p. 22).

Arquilla e Ronfeldt (1993) introduzem o conceito de guerras de rede (*netwar*[68]). Ao passo que guerras cibernéticas se utilizam de diversas formas de tecnologia, notadamente com efeitos em C3I (comando, controle, comunicações e informação) – não estando restritas à noção de guerras eletrônicas, computadorizadas ou automatizadas –, as guerras de rede aproximam-se da ideia de "guerra informacional" e são direcionadas à opinião pública e manipulação de sistemas pelo pensamento, sendo em sua maioria não militares e não violentas. O advento das guerras cibernéticas poderia implicar ainda amplas ramificações nas doutrinas e organização militares, como de fato foi percebido na Revolução dos Assuntos Militares. Já as guerras de redes podem surgir entre governos de nações rivais, mas também entre atores estatais e não estatais, por exemplo, governos contra grupos ilícitos, organizações terroristas, ou contra

---

[67] "Uma Revolução nos Assuntos Militares (*Revolution in Military Affairs – RMA*) é uma mudança significativa na natureza da guerra causada pela aplicação inovadora de tecnologias que, combinadas com mudanças dramáticas nos aspectos doutrinário, operacional e organizacional militares, alteram fundamentalmente o caráter e a condução de operações militares" (MCKITRICK, s/d, tradução nossa).

[68] "Netwar refere-se ao conflito informacional em alto nível, entre nações ou sociedades. Significa tentar interromper, danificar ou modificar o que uma população-alvo "sabe" ou pensa que sabe sobre si mesma e o mundo ao seu redor. Uma guerra de rede pode se concentrar na opinião pública ou da elite, ou em ambas. Pode envolver medidas de diplomacia pública, propaganda e campanhas psicológicas, subversão política e cultural, engano ou interferência na mídia local, infiltração de redes de computadores e bancos de dados e esforços para promover um movimentos dissidentes ou de oposição em redes de computadores" (ARQUILLA, 1993, p. 28).

políticas de grupos de interesse como questões ambientais, direitos humanos e questões religiosas. Atores não estatais podem ou não ser ligados a outros atores estatais ou estar organizados em grandes redes/coalizões transnacionais. (ARQUILLA; RONFELDT, 1993, p. 28).

Também Farwell e Rohozinski (2011) afirmam que instrumentos cibernéticos podem ser utilizados como ferramenta para descreditar, desestabilizar e enfraquecer a autoridade de regimes adversários. Analogamente, Betz e Stevens (2011) trazem a ideia de "poder cibernético produtivo" como a capacidade de produção, reprodução e fortalecimento de discursos como possivelmente a forma mais importante de poder cibernético (BETZ; STEVENS, 2011).

Por sua vez, Hughes (2010) apresenta os desenvolvimentos da noção de guerra informacional e sua relação com ataques cibernéticos em alguns países, afirmando que, embora desde a Guerra Fria houvesse a previsão de guerra informacional – em grande parte em conflitos convencionais –, no século XXI muitos aspectos da "guerra de informação" mudaram do campo de batalha militar tradicional para a esfera pública (HUGHES, 2010, p. 528). Conforme Hughes (2010, p. 532), por exemplo, em 2003:

> O então diretor do departamento de guerra eletrônica do Exército de Libertação Popular chinês, Dai Qingmin, propôs um esforço abrangente de guerra de informação, incluindo ataques cibernéticos, eletrônicos e cinéticos coordenados em operações militares (HUGHES, 2010, p. 532).

Na mesma linha, Junio (2013), Darczewska (2014) e Kostyuk e Zhukov (2017) mencionam a centralidade da noção de guerra informacional nas visões de China e Rússia. Junio (2013) ressalta que livros de doutrina militar chinesa recomendam ofensivas informacionais através de ataques a redes de computadores em antecipação a guerras convencionais (JUNIO, 2013, p. 7). Por sua vez, Darczewska (2014) afirma que a teoria russa de guerra informacional foi construída em oposição à visão dos EUA e da Europa Ocidental, que prioriza o uso de novas tecnologias computacionais para atingir objetivos militares e de inteligência. A autora afirma que "a maior parte dos autores russos compreende guerra informacional como a busca por influência sobre consciência das massas, parte da rivalidade entre sistemas civilizacionais diferentes, adotados por países diferentes no espaço informacional" (DARCZEWSKA, 2014, p. 12). No mesmo sentido, Kostyuk e Zhukov (2017) explicam que a doutrina militar russa coloca forte ênfase no uso estratégico da informação durante a guerra (KOSTYUK; ZHUKOV, 2017, p. 5).

De fato, em 2009, a Organização de Xangai para Cooperação (*Shanghai Cooperation Organization* – SCO), organização com foco em questões geopolíticas e questões regionais de

segurança, adotou os seguintes conceitos de guerra, armas e infraestrutura informacionais, sem mencionar o conceito de "guerra cibernética":

> "Guerra informacional" significa um confronto entre dois ou mais estados no espaço informacional com o objetivo de danificar sistemas, processos e recursos de informação, estruturas criticamente importantes e outras, minar sistemas políticos, econômicos e sociais, manipular psicologicamente massas da população para desestabilizar a sociedade e o Estado, e obrigar o Estado a tomar decisões no interesse da parte contrária;
> "Infraestrutura de Informação" significa uma gama de ferramentas técnicas e sistemas para formação, geração, transformação, transmissão, uso e armazenamento de informação;
> "Armas de informação" significa tecnologias de informação, ferramentas e métodos usados para fins de guerra de informação (Anexo I do Acordo sobre Cooperação para Garantir a Segurança da Informação Internacional entre os Estados-Membros da Organização de Cooperação de Xangai. Disponível em: https://ccdcoe-admin.aku.co/wp-content/uploads/2018/11/SCO-090616-IISAgreement.pdf, tradução nossa).

Apesar de possuir uma interface importante com a ascensão do ciberespaço, a guerra informacional é um fenômeno que apresenta clara diferenciação daquilo que a maioria dos autores na literatura revisada trata como guerra cibernética. A guerra informacional não iniciou com a ascensão do espaço cibernético, mas pode ser – e há importantes indícios de que o seja – potencializada pela ubiquidade do novo domínio e por seu potencial de transmissão e armazenamento de informações. A literatura de segurança internacional revisada faz bem em diferenciar guerra cibernética de guerra informacional, no entanto os estudos sobre impactos da ascensão do ciberespaço na segurança internacional poderiam se beneficiar muito em sua capacidade analítica de maior ênfase ao tema da guerra informacional *per se*, sobretudo se considerada a centralidade desse conceito na visão de potências militares e tecnológicas como China e Rússia.

2.3.5. Segurança cibernética x segurança da informação

Decorrência da indefinição conceitual de guerra cibernética e guerra informacional, também as noções de segurança cibernética e segurança da informação por vezes confundem-se, sobretudo em arranjos institucionais de governos e organizações internacionais. Nesse sentido, ecoando a separação entre guerra cibernética e guerra informacional, Lindsay (2014) aponta que, ao passo em que a noção ocidental de segurança cibernética enfatiza ameaças de natureza técnica, o conceito de segurança informacional, adotado por Rússia, China e outros países da Organização para Cooperação de Xangai, enfatiza ameaças ideológicas e considera o

controle do conteúdo das informações tão importante quanto – talvez mais – do que a segurança técnica das redes (LINDSAY, 2014, p. 15). Na literatura revisada, contudo, é notável a prioridade dada à noção de segurança cibernética em detrimento das abordagens de segurança da informação. Dentro da questão da "segurança cibernética", o tema da governança de segurança cibernética é o mais abordado, sendo a definição do termo instrumental no estabelecimento de arranjos de governança de segurança cibernética (nacional e internacionalmente) eficazes.

O conceito de "segurança cibernética" também compartilha da imprecisão conceitual característica das questões cibernéticas na segurança internacional (BETZ;STEVENS, 2013; KELLO, 2013). Esse seria um dos motivos pelos quais não tem sido possível estabelecer um regime internacional de regras e normas de conduta no ciberespaço (KELLO, 2013, p. 18).

A indefinição conceitual de "segurança cibernética" também aparece na relação entre noções nacionais e internacional do conceito. Para Hughes (2010), a segurança cibernética é uma questão tanto de aplicação da lei domesticamente quanto de defesa militar, abordagem que se relaciona, por um lado, aos impactos do crime cibernético em jurisdições nacionais e, por outro, às possibilidades de conflitos cibernéticos internacionais. Hughes (2010) aponta, então, que conforme a segurança cibernética entra na seara das políticas de segurança nacional, muitos governos passam a desenvolver capacidades cibernéticas que levam a questão a seus adversários internacionalmente (HUGHES, 2010, p. 530).

Levando em consideração os aspectos nacional e internacional da segurança cibernética, Cavelty (2013) sistematiza os discursos sobre o tema conforme os atores que o proferem e as principais ameaças elencadas por eles. A abordagem da comunidade técnica considera segurança cibernética a segurança de computadores e redes de computadores, tendo por principais ameaças *malwares*, *hackers* e perturbações da rede. Atores corporativos como a indústria de antivírus e a comunidade de inteligência e aplicação da lei buscariam a proteção de redes do setor privado e de informações classificadas – no caso de redes do governo –, tendo por principais ameaças crime cibernético, espionagem cibernética e ameaças persistentes avançadas (APT)[69]. A comunidade de defesa civil e segurança interna prioriza a segurança de infraestruturas críticas no conceito de segurança cibernética e concentra-se nas ameaças a essas infraestruturas, nos potenciais efeitos-cascata de um ataque sobre elas, em terroristas cibernéticos e comandos cibernéticos de estados adversários. Finalmente, a comunidade militar preocupa-se com a segurança de redes das forças armadas e seu impacto no Estado-nação,

[69] Grupos *hackers* de alta sofisticação técnica frequentemente ligados a Estados-nação.

considerando principais ameaças ataques a infraestruturas críticas, terroristas cibernéticos, ciberespionagem e comandos cibernéticos de estados rivais (CAVELTY, 2013, p. 109).

Em uma abordagem empírica, Carr (2016) afirma que o conceito de segurança cibernética utilizado atualmente é muito amplo, referindo-se ao mesmo tempo a coisas tão diversas quanto a integridade da privacidade pessoal online, à segurança de infraestruturas críticas e do comércio eletrônico (*e-commerce*) e a direitos de propriedade intelectual, aspectos que apresentam em comum apenas a tecnologia que utilizam. A autora avalia arranjos institucionais de segurança cibernética nos EUA e no Reino Unido, de forma a compreender a separação de papéis e responsabilidades entre o setor público e o setor privado, concluindo que falta clareza nos conceitos e nas competências e responsabilidades na parceria público-privada para governança de segurança cibernética, pondo em questão a eficácia desses arranjos.

Ademais, Lemay, Fernandeza e Knight (2010), Cavelty (2013) e Carr (2016) sublinham a forte ligação que o conceito de segurança cibernética tem com as "infraestruturas críticas"[70]. Um ataque a essas infraestruturas segue como um dos temas dominantes em segurança cibernética. Em geral, essas infraestruturas são discutidas em termos de "setores" regulados pelo governo por meio de agências ou departamentos, contudo em sua maior parte são administradas pela iniciativa privada. Num cenário de ausência de instrumentos eficazes de *accountability* e *compliance* do setor privado como parte integrante da segurança nacional, há poucos incentivos para que esse setor invista em medidas robustas de segurança cibernética (LEMAY; FERNANDEZA; KNIGHT, 2010, p. 192). A esse respeito é notável a escassez na literatura revisada de estudos sobre a possibilidade de utilização de ataques a infraestruturas críticas por organizações terroristas, sobretudo em face de ser esse um dos principais riscos decorrentes da ascensão do ciberespaço a governos e países. Note-se que, conforme notado acima, a menção a esse risco e a seu grande potencial existe, contudo, não foram identificados estudos que aprofundem o tema.

Iniciativas de governança de segurança cibernética internacionalmente têm por desafio a aplicação da Lei de Conflito Armado (Loac) – incluindo o direito governando a legalidade de ir à guerra (*jus ad bellum*), manifesto nos arts. 2.4 e 51[71] na *Carta das Nações Unidas* e o direito governando o comportamento durante a guerra (*jus in bello*), direito internacional humanitário

---

[70] Infraestruturas críticas são definidas nos Estados Unidos como "sistemas e bens, físicos ou virtuais, tão vitais para a nação que sua destruição ou incapacidade teriam efeito debilitante na segurança nacional, segurança econômica nacional, saúde e segurança públicas, ou qualquer combinação desses elementos" (WILSHUSEN, 2011, p. 2).

[71] O art. 2.4 da *Carta da ONU* proíbe "a ameaça ou o uso da força" nas relações internacionais, ao passo que o art. 51 autoriza ações de legítima defesa em casos de "ataque armado".

– a ataques cibernéticos. Esse desafio decorre em grande parte do desacordo entre países membros quanto às noções de segurança cibernética e segurança da informação.

De fato, a possibilidade de aplicação do direito internacional a ações estatais no domínio cibernético já foi afirmada em relatório do *United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (UNGGE)[72] de 2013. Também o Comitê de Guerra Informacional Ofensiva do Conselho Nacional de Pesquisas dos EUA e especialistas convidados pelo *Cooperative Cyber Defence Centre of Excellence* da Otan (CCDCOE/OTAN) para elaboração do *Manual de Tallinn de Direito Internacional aplicável à Guerra Cibernética* (*Tallinn Manual on the International Law Applicable to Cyber Warfare*) confirmaram a possibilidade de aplicação da Loac a ataques cibernéticos (HUGHES, 2010; EICHENSEHR, 2014). Contudo, a determinação do significado das expressões "uso da força" (art. 2.4 da *Carta da ONU*) e "ataque armado" (art. 51 da *Carta da ONU*) no ciberespaço permanece como ponto de divergência (HUGHES, 2010; MELZER, 2011; GOLDSMITH, 2013; EICHENSEHR, 2014; SCHREIER, 2015; GARCIA, 2016).

Outras dificuldades referidas por Hughes (2010) na aplicação dos princípios da Loac para conflitos no espaço cibernético dizem respeito à dificuldade em separar alvos militares e não militares, considerando a ubiquidade e a interconectividade características do domínio cibernético; ao fato de os ataques poderem ser lançados de locais diferentes de onde estão seus executores; e a falta de clareza acerca do que constitui uma arma cibernética – agravada pelo que outros autores se referem como natureza intrinsecamente dual das ferramentas cibernéticas. Nesse sentido, Goldsmith (2013) afirma que é cético quanto à aplicação do direito internacional no caso de ataques cibernéticos, sobretudo em decorrência das dificuldades de atribuição. Para o autor:

> As leis da guerra não seriam tão eficazes ou teriam o mesmo nível de relevância normativa se as nações que as violaram não pudessem ser identificadas e publicamente envergonhadas. As normas não podem muito em um mundo sem atribuição séria; o anonimato é um destruidor de normas. Essa, infelizmente, é a situação no domínio cibernético (GOLDSMITH, 2013, p. 136, tradução da autora).

[72] Grupo de especialistas governamentais nos desenvolvimentos no campo das telecomunicações e informação no contexto da segurança internacional, traduzido pela autora. Posteriormente, o grupo foi renomeado para *United Nations Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, ou Grupo de Especialistas Governamentais das Nações Unidas para o Avanço do Comportamento Estatal Responsável no Ciberespaço no Contexto da Segurança Internacional (traduzido pela autora).

De forma a suprir as lacunas em relação à aplicação do direito internacional em casos de ataques cibernéticos, em 2009 o CCDCOE/Otan propôs a um grupo de especialistas (advogados, acadêmicos e profissionais técnicos) o esforço de elaboração de um documento que facilitasse a regulação de operações cibernéticas pelo direito internacional. Esse esforço resultou na publicação em 2013 do já mencionado *Manual de Tallin de Direito Internacional aplicável à Guerra Cibernética*. Eichensehr (2014) explica que o *Manual de Tallinn* não tem por objetivo dar diretrizes ou estabelecer melhores práticas, mas descrever a aplicação da lei existente a conflitos cibernéticos e que, nesse sentido, provê uma análise de como o *jus ad bellum* e o *jus in bello* podem ser traduzidos para o ciberespaço, bem como apresenta as questões mais contenciosas a serem resolvidas no debate e prática estatal (EICHENSEHR, 2014, p. 585). As principais divergências incluem algumas já mencionadas: se um ataque cibernético que causa extensos efeitos negativos, mas não necessariamente causa danos físicos, morte ou destruição pode ser considerado ataque armado; se a introdução de um *malware* em infraestrutura cibernética de outro estado sem que isso cause danos físicos, mas sirva por exemplo à espionagem cibernética, constitui violação de soberania; se um estado viola o direito internacional ao falhar no adequado monitoramento de atividades cibernéticas internas de forma que possibilite o uso de sua infraestrutura cibernética interna no ataque de terceiros a outros estados.

Mesmo considerando seu escopo limitados, Efrony e Shany (2018) afirmam que a aceitação dos Estados das regras descritas no Manual de Tallin não está clara e que na verdade há interesses divergentes na promoção de segurança jurídica internacional no ciberespaço.

> As críticas dirigidas à adequação de certos aspectos das Regras de Tallinn e a relação entre elas e a prática estatal pós-Tallinn convidam a uma avaliação do grau em que os Estados aceitaram, ou estão interessados em aceitar, as premissas dessas regras [...]: de que os danos causados por operações cibernéticas são comparáveis aos causados por ataques cinéticos; de que o direito internacional governa operações cibernéticas; de que os Estados exercem soberania ou controle sobre partes do ciberespaço; de que ataques cibernéticos podem ser regulados por regras de *jus ad bellum* e *jus in bello* análogas àquelas aplicáveis na esfera cinética; e de que os Estados podem incorrer em responsabilidade sobre operadores privados no ciberespaço. [...]. Embora as Regras de Tallinn tenham sido criticadas por alguns como não indo longe o suficiente para limitar a capacidade dos Estados de conduzir operações no ciberespaço, vemos alguns Estados alegando o contrário e outros indo ainda mais longe do que isso, desafiando a própria adequação do *jus ad bellum* e *jus in bello* para operações cibernéticas. (EFRONY; SHANY, 2018, p. 653, tradução da autora)

Observações de Hughes (2010), Melzer (2011) e Schreier (2015) apontam, ainda, para uma ausência importante na literatura revisada, no que tange à discussão sobre segurança cibernética: a avaliação de iniciativas de criação de uma governança internacional de segurança

cibernética nas Nações Unidas. Stauffacher (2019) supre em parte essa carência, descrevendo brevemente as iniciativas do UNGGE e do *Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security (OEWG)*[73].

Atualmente, duas frentes de trabalho aparentemente desconectadas atuam nos esforços de normatização da atuação estatal cibernética nas Nações Unidas: o já referido UNGGE (cuja primeira "edição" aconteceu ainda em 2003) e o *OEWG* (criado em 2018). A interação entre esses grupos e a evolução de seus trabalhos são aspectos importantes a conhecer para compreender as perspectivas para a governança de segurança cibernética internacional.

Stauffacher (2019) explica que o UNGGE foi criado em 2003 por iniciativa da delegação russa nas Nações Unidas, no escopo do Primeiro Comitê da Assembleia-Geral da ONU, que cobre assuntos de desarmamento e segurança internacional. Os Grupos de Especialistas Governamentais (*Group of Governmental Experts* – GGE) são mecanismos para estudo de um tópico novo, com objetivo de gerar recomendações para negociações futuras de acordos multilaterais sobre o tema. Após algumas edições bem-sucedidas, com a adoção de relatórios que sublinhavam o uso crescente de TICs por Estados-nação como instrumentos de guerra e inteligência e o risco de escalada de tensões devido à ausência de normas de conduta (UNGGE, 2010); que afirmavam que o direito internacional é aplicável ao espaço cibernético e essencial à manutenção da paz, estabilidade e acessibilidade nesse domínio (UNGGE, 2013); e que instavam ao estabelecimento de uma norma proibindo o ataque a infraestruturas críticas provedoras de serviços públicos, além de abrir a possibilidade de participação de outros grupos de interesse (setor privado, academia e organizações civis) (UNGGE, 2015), a partir de 2016 discordâncias quanto a definições de "uso da força", "ataques armados" e "segurança cibernética" teriam minado a efetividade do UNGGE enquanto foro para o desenvolvimento das normas de atuação no ciberespaço[74].

Um dos motivos que teriam levado ao esvaziamento do UNGGE foi a inabilidade de potências cibernéticas de chegar a um acordo quanto ao conceito de segurança cibernética, com Rússia e China defendendo uma visão que incluía a informação como passível de instrumentalização para ataques e, portanto, uma das ameaças à segurança nacional, posição diversa da noção de segurança cibernética defendida pelos Estados Unidos, que ressalta a proteção a aspectos técnicos (STAUFFACHER, 2019, p. 7)

---

[73] Grupo de Trabalho Aberto sobre Desenvolvimentos no Campo das TICs no Contexto da Segurança Internacional (tradução da autora).

[74] UNGA (2010); UNGA (2013); UNGA (2015).
https://bit.ly/2QvSr8d; https://undocs.org/A/70/174.

Dessa forma, em 2018, a delegação russa apresentou a proposta de formação do *Open-Ended Working Group* (OEWG), fórum em que qualquer Estado-membro da ONU poderia participar, que prevê a participação de atores não estatais e que incorporava elementos acordados anteriormente no GGE e medidas do Código de Conduta em Segurança da Informação Sino-Russo de 2015. No mesmo ano, os EUA defenderam uma resolução autorizando nova edição do GGE para o ano seguinte. A existência desses dois fóruns de discussão nas Nações Unidas, com visões divergentes de segurança cibernética e, portanto, do que se pretende atingir com a normatização da atuação estatal no domínio cibernético, é um elemento que dificulta o estabelecimento de regime internacional de segurança cibernética.

Mais, a adoção do que Garcia (2016) chama de governança securitária preventiva (*preventive security governance*), incluindo a codificação ou especificação de normas já existentes que esclareçam regras de comportamento nas áreas cibernética, deve também considerar o regime internacional de direitos humanos, a lei de responsabilidade estatal e o "direito dos comuns". Nesse sentido, a autora defende que a promoção de normas cibernéticas nas Nações Unidas é essencial para prevenir a escalada de tensões no caso de ataques cibernéticos e para remediar problemas decorrentes de ataques realizados cooperativamente (GARCIA, 2016, p. 100).

Frente ao exposto, percebe-se que os conceitos centrais identificados na literatura revisada são "ciberespaço", "guerra cibernética" e "segurança cibernética", sendo a definição de ciberespaço basilar na medida em que é utilizada não apenas como cenário para as relações internacionais, mas como parte integrante dessas relações. Na literatura inicial, a atribuição das características de baixo custo de entrada, anonimato, assimetria de vulnerabilidades e dominância do ataque em relação à defesa no ciberespaço criaram a ideia desse domínio como instável e perigoso, em que comportamentos temerários seriam favorecidos. Contudo, mais recentemente, o questionamento dessas características como inerentes ao ciberespaço foi o principal motor da evolução dos estudos de segurança internacional sobre a ascensão desse domínio em direção a uma produção científica mais crítica e com maior embasamento empírico.

A literatura revisada aponta, ainda, que os conceitos de ciberespaço e sua caracterização variam conforme os fenômenos sendo abordados e os objetivos da análise. De forma que definições inclusivas (ciberespaço como infraestrutura física e aspectos sintáticos, semânticos e cognitivos) seriam mais úteis ao estudo de guerra informacional, ao passo que definições focadas em aspectos de infraestrutura física servem ao estudo de conflitos cibernéticos centrados na operacionalização de ataques cibernéticos *stricto sensu.* Ademais, a noção do ciberespaço como um domínio livre e igualitário (visão liberal, na caracterização de Manjikian

(2010)), é utilizada sobretudo quando trata das perspectivas de governança do ciberespaço, ao passo que sua percepção como domínio vinculado ao poder estatal é adotada mais comumente quando se discute as perspectivas de guerra ou conflitos cibernéticos.

Por sua vez, diferentes conceituações de guerra cibernética implicam avaliações diversas acerca da eficácia de ataques cibernéticos enquanto instrumento para consecução de objetivos políticos nas relações internacionais. A noção de guerra cibernética como ações iniciadas no ciberespaço, porém com consequências não virtuais, cinéticas, é o conceito mais frequente apreendido da literatura. A diferenciação de guerra cibernética dos fenômenos crime cibernético, espionagem cibernética e hacktivismo mostrou-se bem aceita na literatura e ajuda a esclarecer melhor o objeto de análise da segurança internacional sobre a ascensão do ciberespaço.

De forma geral, o principal argumento levantado na literatura contrário à classificação de ataques cibernéticos como atos de guerra é a percepção frequente de ausência de efeitos físicos ou cinéticos. A proposta por Siedler (2016) de divisão entre ataques a redes de computadores de coerção e ataques de redes de computadores de força bruta, apesar de aparentemente não encontrar forte eco no resto da literatura, pode contribuir com o refinamento do conceito de guerra cibernética. Nesse sentido, propõe-se aqui que atos de guerra cibernética podem ser definidos como ataques a redes de computadores – na definição de Kello (2013) – ou seja, "utilização de código para interferir na funcionalidade de um sistema computacional com propósito político ou estratégico e efeitos nem sempre limitados ao espaço cibernético", diferenciados de crime cibernético, espionagem cibernética e hacktivismo em suas motivações e impacto estratégico, e de força bruta (na definição de Siedler, 2016), ou seja, cuja consecução do objetivo não depende da tomada de decisão por parte de um adversário, mas exclusivamente de ser o ataque cibernético bem sucedido.

Finalmente, divergências no conceito de guerra cibernética e guerra informacional e segurança cibernética e segurança da informação, sobretudo na abordagem institucional de Estados e organizações internacionais, têm se mostrado um dos principais óbices ao avanço das discussões sobre o estabelecimento de uma governança internacional de segurança cibernética. A separação entre esses conceitos é relevante e benéfica às análises da Segurança Internacional, contudo, o foco da literatura em estudos que priorizam a noção ocidental mais focada nos aspectos técnicos, deixa de lado o aspecto fundamental da informação e de seu controle ou manipulação enquanto elemento da segurança internacional. Essa parece ser uma fragilidade crucial da literatura revisada.

O capítulo a seguir apresenta debates identificados na literatura revisada que são diretamente influenciados pelos conceitos discutidos neste capítulo e que pretendem expor as principais preocupações dos analistas de segurança internacional no que concerne à ascensão do ciberespaço.

3 PRINCIPAIS DEBATES DA SEGURANÇA INTERNACIONAL SOBRE A ASCENSÃO DO CIBERESPAÇO

Este capítulo procura, tendo por base a discussão conceitual apresentada, sistematizar os principais debates identificados na literatura de segurança internacional sobre a ascensão do ciberespaço. Conforme adiantado, a centralidade dos conceitos de ciberespaço, guerra cibernética e segurança cibernética fazem com que parte desses debates tenha sido tangenciada na discussão das definições.

Inicialmente, a relação entre as abordagens da ascensão do ciberespaço e os paradigmas das relações internacionais é apresentada de forma a embasar os debates apresentados na sequência.

Em seguida, o debate mais amplo identificado na literatura – em relação ao qual a quase totalidade da amostra bibliográfica se posiciona direta ou indiretamente – é apresentado. Esse debate se constrói acerca de variações do questionamento: a ameaça cibernética é exagerada? O questionamento é abordado em quatro debates subsidiários sobre: a eficácia de ataques cibernéticos e seu caráter acessório ou independente em situações de conflito; as possibilidades de *détente* e dissuasão cibernética ou da escalada não planejada de conflitos cibernéticos – inclusive para embates cinéticos; a relação entre atores estatais e não estatais no ciberespaço; e a ocorrência de um processo de securitização do discurso político e científico-acadêmico sobre questões cibernéticas nas relações internacionais.

Em resposta ao debate amplo, dois grupos diferenciam-se: por um lado, parte da literatura defende que características do ciberespaço, sobretudo baixo custo de entrada, anonimato, assimetrias de vulnerabilidade e dificuldade de atribuição – e nesse ponto a discussão conceitual sobre ciberespaço é basilar para compreender o que está em jogo – permitem a ascensão de um número sem precedentes de atores potencialmente influentes e dotados de um ambiente que seria mais propício ao ataque do que à defesa, representando uma revolução nas relações internacionais e na disciplina de RI. No outro lado do debate, autores às vezes referidos como “céticos”, ainda que por vezes admitam a existência de algumas das características acima mencionadas, veem o desenvolvimento cibernético como o surgimento de uma nova ferramenta a ser utilizada numa lógica já conhecida, não representando impacto fundamental na natureza das relações internacionais, tampouco a necessidade de uma revolução nas interpretações da disciplina de RI, mas sua mera adaptação.

Finalmente, a literatura revisada é também apresentada à luz de considerações ontológicas, a saber: discussões sobre o que constituiria poder cibernético e se ele tem especificidades em relação a outras manifestações de poder.

3.1. O ciberespaço e os paradigmas de RI

Os paradigmas clássicos das RI apresentam abordagens diferentes acerca do significado da ascensão do ciberespaço nas relações internacionais. Manjikian (2010) sistematiza essas visões e defende que desde o início da década de 1990 dois discursos principais (neoliberal e neorrealista) coexistem na tentativa de descrever e analisar o ciberespaço. Desenvolvedores técnicos e acadêmicos adotariam preferencialmente uma narrativa neoliberal, ao passo que estudos estratégicos e militares optariam por uma narrativa neorrealista (MANJIKIAN, 2010, p. 383).

Enquanto a narrativa liberal, em uma vertente utópica e outra pragmática,[75] sublinha o potencial revolucionário do espaço cibernético e é otimista quanto ao potencial democratizante do novo domínio, a visão ciberrealista percebe o espaço cibernético como um campo de batalha virtual (*virtual battlespace)* que não apresenta diferenças fundamentais em relação a outros campos de batalha, apenas uma adaptação tecnológica no sistema internacional existente – em vez de uma nova criação.

Na visão liberal utópica, o ciberespaço constituiria uma "vila global", utilizando a expressão cunhada e popularizada por McLuhan (1964), extraterritorial, governada por regras próprias derivadas de sua programação, noção manifesta na máxima "*the code is the code*". Considerando um nível maior de influência da realidade política nas dinâmicas do ciberespaço, a visão liberal institucionalista considera que a abordagem do ciberespaço deveria se focar em esforços internacionais para preservá-lo e habilitá-lo para uso comum.

De maneira diversa, os neorrealistas cibernéticos defendem que as mudanças nas tecnologias de informação e comunicação (TIC) não criaram uma entidade nova. Nesse sentido, a ascensão do ciberespaço não implica mudança no cálculo de custos e benefícios, tampouco dos objetivos dos atores no sistema internacional. O ciberespaço apenas fez com que os

[75] "A tradição liberal apresenta uma vertente utópica e uma vertente liberal pragmática. Na primeira vertente a ascensão do ciberespaço é considerada um processo orgânico e espontâneo, e o resultado desse processo é uma sociedade civil virtual, sem fronteiras, um domínio igualitário e livre. A visão liberal pragmática (reguladores) percebe a ascensão do ciberespaço como fruto de cooperação internacional concentrada, gerando um universo alternativo criado reflexivamente por meio da ação humana, onde a estrutura do mundo físico, com ênfase no poder, identidade e riqueza, seria menos relevante" (MANJIKIAN, 2010, p. 383).

Estados-nação adaptassem suas estratégias a esse novo domínio (MANJIKIAN, 2010, p. 383-385). Nesse sentido, Rid (2012) defende que "[...] todos os ataques cibernéticos presentes e passados são meramente versões sofisticadas de três atividades que são tão antigas quanto a própria guerra: subversão, espionagem e sabotagem. É improvável que isso mude nos anos subsequentes".

O paradigma construtivista na interpretação da ascensão do ciberespaço na literatura de RI é ressaltado por Reardon e Choucri (2012). Essa abordagem seria dominante na literatura acadêmica revisada pela dupla – em contraposição aos *policy papers*, em que a visão realista seria predominante.

> [...] os construtivistas dominaram a literatura acadêmica sobre política cibernética ao longo da década. Isso é verdadeiro mesmo na área de Segurança, na qual o realismo costuma ser predominante. Metade dos artigos da pesquisa encontrados em periódicos acadêmicos são construtivistas. Isso é paradoxal. Teorias realistas podem ajudar a explicar como os estados usam tecnologias cibernéticas para promover seus interesses em segurança e como eles podem responder às capacidades cibernéticas de outros estados. Embora muitos construtivistas não contestem a existência material de ameaças, eles argumentam que a rotulagem de diversas atividades como "ameaça à segurança nacional" é um produto de interpretação intersubjetiva ao invés de algo determinado materialmente. Também pode ser que o número maior de abordagens construtivistas reflita uma relutância por parte dos realistas em estudar o ciberespaço. (READON; CHOURCI, 2012, p. 6).

A importância da abordagem construtivista na década de 2000-2010, período dos artigos revisados por Reardon e Choucri (2012), pode representar uma reação à literatura inicial de segurança internacional sobre a ascensão do ciberespaço e o que Sharp (2017) e Gorwa e Smeets (2019) chamam de *hype* da guerra cibernética, que parece ter se caracterizado pela inflação de ameaças e pela noção de insegurança relacionada ao ciberespaço. Nesse sentido, a literatura construtivista teria atuado de forma a trazer o debate sobre guerra cibernética "de volta à Terra", para usar a expressão de Gartzke (2013).

A amostra bibliográfica revisada nesta dissertação foi categorizada conforme os paradigmas das RI considerados dominantes nos artigos. Ressalta-se que a categorização, quando possível, não foi feita com base em declarações explícitas acerca do paradigma preferencial dos documentos, mas muitas vezes inferidas a partir dos tópicos abordados, do tratamento de Estados-nação como unitários ou não, entre outros indícios.

Tabela 11 – Quadro-resumo dos artigos por paradigma da RI dominante

Realismo	Liberalismo	Construtivismo	Sem paradigma dominante
• Arquilla; Ronfeldt (1993) • Lemay; Fernandeza; Knight (2010) • Lynn (2010) • Klimburg (2011) • Farwell; Rohozinski (2011) • Deibert; Rohozinski, Nishihata (2012) • Farwell; Rohozinski (2012) • Rid (2012) • Bronk;Tikka-Ringas (2013) • Gartzke (2013) • Goldsmith (2013) • Junio (2013) • Kello (2013) • Lindsay (2013) • McGraw (2013) • Peterson (2013) • Stone (2013) • Darczewska (2014) • Gompert; Libicki (2014) • Gartzke; Lindsay (2015) • Siedler (2016) • Carson;Yarhi-Milo (2017) • Tor (2017)	• Nye (2010) • Hughes (2010) • Betz; Stevens (2011) • Melzer (2011) • Herrington; Aldrich (2013) • Mueller; Schmidt; Kerbis (2013) • Eichensehr (2014) • Carr (2016) • Garcia (2016) • Nye (2016) • Stoddart (2016) • Christensen; Petersen (2017) • Sharp (2017) • Efrony; Shany (2017) • Gohdes (2018) • Stauffacher (2019)	• Hansen; Nissembaum (2009) • Cavelty (2013) • Betz; Stevens (2013) • Lupovici (2014) • Balzacq; Cavelty (2016)	• Inkster (2010) • Manjikian (2010) • Ottis (2010) • Reardon; Choucri (2012) • Lindsay (2014) • Valeriano; Maness (2014) • Rid; Buchanan (2015) • Slayton (2017) • Smeets (2018) • Sechser; Narang; Talmadge (2019) • Gorwa; Smeets (2019) • Kostyuk; Zhukov (2019)

Fonte: Elaboração da autora.

3.2. A questão central: a ameaça cibernética é exagerada?

O debate mais importante identificado na literatura revisada diz respeito a divergências sobre a perspectiva de o espaço cibernético representar uma alteração revolucionária ou marginal nas relações internacionais, manifesta no questionamento: a ameaça cibernética é exagerada?

Note-se que nessa questão a noção de ameaça pode significar, por um lado, algo que põe em risco as relações de poder atuais, o *status quo* das relações internacionais, com a perspectiva de difusão de poder na forma do empoderamento de atores antes negligenciados e consequente erosão papel do Estado-nação enquanto ator central do sistema internacional; por outro lado, "ameaça" pode se referir a algo que põe em risco vidas ou o funcionamento da sociedade (como poderia acontecer em casos de guerra cibernética segundo as definições mais comuns desse conceito na amostra bibliográfica revisada, quais sejam aquelas que implicam algum grau de impactos físicos, cinéticos).

Kello (2013) e Lindsay (2014) exemplificam o primeiro caso:

> Poucas questões no futuro de estudos cibernéticos serão mais importantes do que aquela de determinar a medida em que a era presente representa uma nova fase nas relações internacionais – se padrões de competição de segurança serão alterados significativamente ou se continuarão essencialmente os mesmos, apenas com novos instrumentos à disposição dos atores (KELLO, 2013, p. 39).

> O debate tecnológico concentra-se na discussão se as redes onipresentes criam perigos revolucionários ou apenas evoluções marginais de crimes cibernéticos, inteligência de sinais e guerra eletrônica. Um lado desse debate argumenta que a infraestrutura interconectada e as ferramentas de *hacking* facilmente acessíveis tornam as potências industriais avançadas particularmente vulneráveis a sérias interrupções de estados mais fracos ou mesmo de atores não-estatais. O outro lado argumenta que a indústria de defesa e o *establishment* de segurança nacional exageram muito a ameaça cibernética (LINDSAY, 2014, p. 9)

No segundo caso, a ascensão do espaço cibernético é percebida enquanto ameaça a vidas ou ao funcionamento da sociedade. Nesse sentido, analogias a ataques como Pearl Harbor, a Blitz, Hiroshima e o 11 de Setembro são mencionadas em Hughes (2010). Em geral autores que consideram esse significado para a "ameaça cibernética" priorizam a noção de guerras cibernéticas com efeitos cinéticos e acreditam não apenas em sua plausibilidade, mas até mesmo probabilidade. Sob essa abordagem, é notável o diálogo estabelecido entre os artigos de Arquilla e Ronfeldt (1993), Thomas Rid (2012) e Stone (2013), nomeados respectivamente *Cyberwar is coming!*, *Cyberwar will not take place* e *Cyberwar will take place!*

Ambos os entendimentos sobre ameaças – ameaças ao *status quo* das relações internacionais e ameaças a vidas e ao funcionamento da sociedade – são considerados no debate central identificado. Parte desse debate debruça-se sobre a possibilidade de novas formas de guerrear decorrentes da ascensão do ciberespaço implicarem eficácia aumentada de ataques cibernéticos e/ou efeito multiplicador a ataques cinéticos como elementos de mudança revolucionária nas relações internacionais (ARQUILLA; RONFELDT, 1993; HUGHES, 2010; KELLO, 2013; STONE, 2013; JUNIO, 2013). Nesse sentido, Arquilla e Ronfeldt (1993) defendem que a revolução da informação implica mudanças tanto na forma como as sociedades iniciarão conflitos quanto nas próprias formas de guerrear das corporações militares (ARQUILLA; RONFELDT, 1993, p. 27). Analogamente, Hughes (2010) considera que, para além de o espaço cibernético tornar-se "o próximo campo de batalha", poder-se-ia vislumbrar uma corrida armamentista cibernética que reformataria a forma de guerrear do século XXI (HUGHES, 2010, 523). Mais cautelosamente, Kello (2013) considera que a ascensão do ciberespaço não altera fundamentalmente a guerra, contudo o potencial das armas cibernéticas e complicações em relação à defesa representariam um perigo à estabilidade das relações internacionais – além das já discutidas dificuldades de atribuição e primazia do ataque sobre a defesa, Kello (2013) menciona a volatilidade tecnológica, possibilidades de escalada de

conflitos, pouca profundidade estratégica[76] e o aumento no número de atores capazes de causar ou influenciar um conflito como elementos de uma instabilidade instrumental.

Stone (2013) e Junio (2013) não argumentam necessariamente pela alta gravidade da ameaça cibernética, no entanto defendem a plausibilidade de uma guerra, com ou sem efeitos cinéticos, ser iniciada no ciberespaço. Nesse sentido, levado em conta o framework teórico a respeito das causas da guerra, Junio (2013) defende que a teoria de RI identifica diversos mecanismos pelos quais armas cibernéticas podem causar escaladas violentas, de forma que há razões para crer que a guerra cibernética é plausível e até mesmo provável (JUNIO, 2013, p. 1-3).

A probabilidade de guerras cibernéticas é defendida também por Farwell e Rohozinski (2012), contudo essa probabilidade não decorreria de escaladas não planejadas ou erros estratégicos, mas, pelo contrário, do fato de o combate cibernético ser mais adequado ao moderno sistema global de comércio do que formas de engajamento cinético, apresentando um cálculo estratégico diferente, de forma que os Estados estão corretos em temer a guerra cibernética (FARWELL; ROHOZINSKI, 2012, p. 109). Ressalta-se aqui que o conceito de guerra cibernética utilizado pelos autores parece prescindir de efeitos cinéticos.

Outra abordagem (ARQUILLA; RONFELDT, 1993; NYE, 2010) localiza sobretudo no aumento do número de atores potencialmente relevantes e em consequentes mudanças na importância relativa de instituições – entre elas o Estado-nação – o possível caráter revolucionário do ciberespaço nas relações internacionais. Nesse sentido Arquilla e Ronfeldt (1993) afirmam que:

> A revolução da informação, tanto em seus aspectos tecnológicos quanto não tecnológicos, coloca em movimento forças que desafiam o *design* de muitas instituições. Isso perturba e corrói hierarquias em torno das quais as instituições normalmente são projetadas. Ela difunde e redistribui o poder, muitas vezes para o benefício dos que podem ser considerados atores menores e mais fracos. Ela cruza fronteiras e redesenha limites e responsabilidades das instituições. Ela expande os horizontes espaciais e temporais que os atores devem levar em consideração. E assim geralmente obriga sistemas fechados a se abrirem. Embora isso possa dificultar a existência sobretudo para instituições grandes, burocráticas e envelhecidas, a forma institucional em si não está se tornando obsoleta. Instituições de todos os tipos continuam sendo essenciais para a organização da sociedade. As organizações responsivas e capazes adaptarão suas estruturas e processos à era da informação. Muitas evoluirão de modelos de organização hierárquicos tradicionais para modelos de organização novos e flexíveis. Seu sucesso dependerá do aprendizado de como

[76] A pouca profundidade estratégica a que Kello (2013) se refere é o curto período e algumas vezes a incapacidade de resposta de que dispõem os governos em relação a ações no domínio cibernético. Os precedentes tradicionais que regulam o papel dos governos na conduta da defesa nacional podem ser de difícil interpretação em uma emergência cibernética.

> entrelaçar princípios hierárquicos e de rede (ARQUILLA; RONFELDT, 1993, p. 26, tradução nossa).

Nye (2010) acredita ser improvável que potências tradicionais tenham tanto domínio sobre o ciberespaço quanto em outros "ambientes" (notadamente mares e espaço aéreo), considerando as características do espaço cibernético. No entanto, o fenômeno de difusão do poder – que ele considera característico do início do século XXI – não significa igualdade de poder, de forma que governos e Estados-nação permaneceriam centrais no sistema internacional.

Os questionamentos apresentados acerca da validade e do caráter absoluto de características do ciberespaço, abalam as premissas sobre as quais se embasa o argumento de a ascensão do ciberespaço representar uma alteração revolucionária nas relações internacionais. No caso de o custo de entrada no ciberespaço não ser tão baixo como se propala e o anonimato não ser absoluto, com a possibilidade de atribuição de ataques cibernéticos guardando um grau aceitável de confiabilidade, e na hipótese de o ataque não ser dominante em relação à defesa no ciberespaço, o número de atores realmente influentes no ciberespaço com incentivos para realizar ataques cai consideravelmente, diminuindo as chances de execução de ataques cibernéticos de grande impacto cinético e de forma que o domínio cibernético pode ser instrumentalizado por atores tradicionais que teriam seu poder aumentado – em oposição à ideia de erosão do poder do Estado-nação.

A seguir, a avaliação da eficácia de ataques cibernéticos e sua relação com manifestações de "uso da força" convencionais; a comparação das potencialidades de uso desse domínio em estratégias de dissuasão ou o risco aumentado de escaladas cibernéticas; a análise de diferentes interações entre Estados-nação e atores não estatais no ciberespaço; e a apresentação do argumento de securitização dos discursos político e acadêmico-científico sobre a ascensão do ciberespaço fortalecem a ideia de que a ameaça cibernética, da forma como é apresentada na literatura revisada nesta dissertação, é em grande medida exagerada.

3.2.1. Eficácia de ataques cibernéticos nas relações internacionais: o efeito multiplicador

A eficácia de ataques cibernéticos como instrumento de influência ou alteração do comportamento de outros atores é um dos elementos levados em consideração no debate sobre o caráter revolucionário da ascensão do ciberespaço. O primeiro aspecto abordado em relação a esse debate é a questão dos efeitos temporários de ataques cibernéticos.

Alguns atributos específicos da guerra cibernética enumerados por Gartzke (2013) são o caráter temporário dos danos que podem ser infligidos – o que contribui para a baixa eficácia da guerra cibernética enquanto instrumento de coerção – e a dificuldade de utilizar capacidades cibernéticas para dissuadir um oponente, haja vista que essas capacidades perdem sua eficácia, uma vez publicizadas, o que ele chama de capacidades *use and lose*.

> Capacidades *use and lose* não conseguem coagir ou impedir comportamentos, porque evidências da capacidade de infligir danos é, em si, utilizável para a ameaça. Se, ao contrário, a guerra cibernética é realizada ao invés de ameaçada, então a natureza temporária do dano cibernético dita que um inimigo suceda ataques na internet de ação cinética (GARTZKE, 2013, p. 60, tradução livre).

A conclusão é que "a internet é, em geral, um substituto inferior às forças terrestres ao performar as funções de coagir e conquistar" (GARTZKE, 2013, p. 42, tradução livre) e que o ciberespaço "torna-se um domínio adjunto às formas mais tradicionais da guerra" (GARTZKE, 2013, p. 70, tradução livre). Nesse sentido, o autor afirma que os efeitos danosos passíveis de serem atingidos por meio de armas cibernéticas são limitados e temporários, de forma que um ator pode se beneficiar de ações de guerra cibernética quase que exclusivamente se for capaz de combiná-la com outros métodos – normalmente ataques cinéticos (GARTZKE, 2013, p. 57-58).

Analogamente ao conceito de capacidades *use and lose*, Smeets (2018) refere-se à "transitoriedade das armas cibernéticas", apontando que a necessidade de emprego rápido e rápida obsolescência de "armas cibernéticas" faz com que sejam necessários reinvestimentos constantes para o desenvolvimento de capacidade ofensiva sustentável no ciberespaço. Nesse sentido, atores menores (indivíduos e redes pouco estruturadas) teriam mais dificuldades de manter capacidade cibernética relevante, frente à limitação de recursos para realização de testes e aprimoramento de ferramentas. Ademais, quando atores ofensivos investem recursos significativos em uma arma cibernética, eles têm o incentivo de não atacar contrapartes de alta capacidade, dado o receio de que as vulnerabilidades exploradas sejam facilmente descobertas e corrigidas. Essas circunstâncias fazem com que, ao contrário da noção normalmente defendida de que a entrada de atores no domínio cibernético é facilitada e de baixo custo, Smeets conclua que "armas cibernéticas são na verdade para os fortes" (SMEETS, 2018, p. 26).

Outro aspecto levantado na literatura (ARQUILLA; RONFELDT, 1993; HUGHES, 2010; GARTZKE, 2013; GOMPERT; LIBICKI, 2014; LINDSAY, 2014; KOSTYUK; ZHUKOV, 2017), que implica a avaliação de eficácia de ataques cibernéticos, é a sua utilização como ferramenta "multiplicadora de efeito", em oposição a sua utilização independentemente

de mecanismos mais convencionais de ataques. A utilização de ataques cibernéticos enquanto ferramenta acessória de métodos convencionais de ataques, bem como a alegada incapacidade dos primeiros de servirem como instrumento de coerção política *per se*, aponta para a eficácia limitada de ataques cibernéticos em situações de conflito, o que corrobora para certo exagero na noção de ameaça cibernética conforme apontada na literatura inicial e por vezes, até mesmo para seu potencial como elemento de estabilidade.

A perspectiva de utilização de ferramentas cibernéticas enquanto multiplicador de força de métodos tradicionais aparece já em Arquilla e Ronfeldt (1993). Os autores citam uma análise do general Colin Powell sobre a Guerra do Golfo, segundo a qual "uma força reduzida e um orçamento de defesa cada vez menor resultam em maior dependência da tecnologia, que deve fornecer o multiplicador de força necessário para garantir uma dissuasão militar viável" (POWELL, C. *apud* ARQUILLA; RONFELDT, 1993). "Multiplicador de força" é um termo militar que descreve uma arma ou tática que, quando adicionada e empregada juntamente com outras forças de combate, aumenta significativamente o potencial de combate dessa força (HUGHES, 2010, p. 533). O autor sublinha a consideração sobre o efeito multiplicador dos ataques cibernéticos na Doutrina da Guerra Cibernética da Rússia, na qual a estratégia cibernética é "projetada para ser um multiplicador de força junto com ações militares mais tradicionais, incluindo ataques de armas de destruição em massa" (HUGHES, 2010, p. 532).

Analogamente, Gompert e Libicki (2014) defendem que ataques cibernéticos não reduzem significativamente a capacidade do inimigo de lançar ataques semelhantes em resposta, motivo pelo qual uma guerra cibernética *per se* (sem implicar consequências cinéticas) não geraria instabilidade e crise. Para fazê-lo, deve ser utilizada conjuntamente a capacidades cinéticas (GOMPERT; LIBICKI, 2014, p. 12). Também Lindsay (2014) aborda as implicações de ataques cibernéticos a métodos tradicionais de conflito, afirmando que um ataque cibernético bem-sucedido seria capaz de prejudicar ou até mesmo paralisar redes de comunicação, causando danos à estrutura de C4ISR (Comando, Controle, Comunicações, Computadores, Inteligência, Vigilância e Reconhecimento – *Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance*) e, consequentemente, ao desempenho de armamentos ou outras funções críticas. Num conflito, o prejuízo a essas funções militares seria mais vantajoso no início dos enfrentamentos, daí decorrendo maior probabilidade da execução de ataques cibernéticos desse tipo no início ou como prelúdio de um ataque cinético (LINDSAY, 2014, p. 11).

Por outro lado, Farwell e Rohozinski (2011) investigam os efeitos da utilização do ciberespaço independentemente de ataques cinéticos, em sua substituição. Nesses casos, o

ciberespaço ofereceria boas oportunidades para atingir inimigos com risco diminuído em relação a meios militares tradicionais, sendo também uma forma mais barata de fazê-lo. Além dos benefícios estratégicos possíveis de ataques cibernéticos, a consecução de objetivos políticos com menos perdas de vidas humanas e danos sobre alvos civis seria fator de estabilidade nas relações internacionais.

Outro aspecto levantado na análise da eficácia de ataques cibernéticos diz respeito não apenas à avaliação do potencial destrutivo desses ataques ou a seu uso independente ou acessório a métodos tradicionais, mas ao cálculo de custos e benefícios de sua utilização. Rid (2012), Gartzke (2013) e Nye (2016) apontam que não é porque um ataque cibernético de grande impacto é possível, que ele acontecerá. Em geral os custos (notadamente custos reputacionais e risco de retaliação) excedem os benefícios desse tipo de ataque. Haveria, nesse sentido, uma superestimativa do potencial revolucionário de uma guerra cibernética entre estudiosos do assunto (GARTZKE, 2013). Rebatendo a percepção de perigo constante de guerra cibernética, o autor argumenta que o uso da força (virtualmente ou não) é custoso, arriscado e improdutivo na maioria das vezes, de maneira que um eventual agressor em geral tem mais incentivos para não atacar do que para atacar. "Devemos nos perguntar não sobre o que poderia acontecer, mas por que razões indivíduos, grupos ou nações podem agir" (GARTZKE, 2013, p. 53, tradução livre). Analogamente, para Nye (2016) a desconsideração de cálculos de custo-benefício pelos atores é um dos elementos do exagero da ameaça cibernética, já que não é porque um ataque potencialmente destrutivo é possível, que ele acontecerá, conclusão semelhante à que chega Rid (2012) quando defende que "*Cyberwar will not take place*".

Ademais, avaliações empíricas relativizam a "ameaça cibernética". Siedler (2016) investiga a efetividade de ataques a redes de computadores (*Computer Network Attacks, CNAs)*, "o método de *hard power* por excelência no ciberespaço", para consecução de objetivos políticos e conclui que a utilização desse método como meio de coerção – compreendida aqui como uma forma de barganha que objetiva demonstrar poder de forma a alterar a percepção de custo-benefício dos outros atores – é prejudicada por desafios quanto à credibilidade de atribuição e a baixa severidade dos danos causados. Quando utilizados como "força bruta", ou seja, como a aplicação de capacidades em busca de interesses sem que se apele ao poder de decisão do adversário, mas simplesmente levando a ação a cabo – como no caso de invasão e alteração de computadores e redes de adversários, a exemplo da utilização do *worm* Stuxnet na campanha contrária ao programa nuclear iraniano, entre 2010 e 2011 – Siedler (2016) considera que CNAs têm eficácia considerável (SIEDLER, 2016, p. 24).

Em abordagem empírica e quantitativa, Kostyuk e Zhukov (2017) apresentam uma análise da relação entre atividades cibernéticas e violência física durante a guerra entre Rússia e Ucrânia no período de 2014 a 2016 e no conflito entre forças contra e pró-governo na Síria entre 2011 e 2016. Analogamente à diferenciação de CNAs por Siedler (2016), eles diferenciam dois objetivos amplos que ataques cibernéticos costumam buscar: propaganda ou acarretamento de danos (*disruption*)[77]. A análise quantitativa realizada pelos autores considera apenas ataques do segundo tipo – em consonância com a abordagem dominante na literatura, de guerra cibernética, implicando efeitos físicos. Esses ataques buscam minar a capacidade dos oponentes de operar nos domínios físico e eletrônico, incluindo atividades de baixa sofisticação, como a execução de ataques de negação de serviço (*Denial of Service – DoS* e *Distributed Denial of Service – DDoS)* e atividades de alta sofisticação, como o desenvolvimento e emprego de códigos maliciosos para atingir sistemas de infraestruturas críticas e alvos militares (KOSTYUK; ZHUKOV, 2017, p. 5-6), como no caso do Stuxnet. Kostyuk e Zhukov (2017) concluem que os ataques cibernéticos analisados têm pouca ou nenhuma relação com os eventos de violência física do conflito russo-ucraniano. Sua afirmação é categórica no sentido de que ataques cibernéticos ainda não funcionam como ferramentas efetivas de coerção durante a guerra, podendo, contudo apoiar operações no solo, prejudicando o comando e controle dos adversários, coletando inteligência e criando oportunidades para exploração cinética.

3.2.2. Dissuasão x risco de escalada cibernética

A possibilidade de utilização do ciberespaço como instrumento de dissuasão em conflitos (*cyber deterrence*) aponta para um potencial estabilizador desse domínio nas questões de segurança internacional. Esse argumento é utilizado na defesa de que a ameaça cibernética – enquanto elemento revolucionário sobre o *status quo* do sistema internacional – é exagerada. O outro lado do debate central, que defende que a ascensão do ciberespaço representa fator de instabilidade e uma ameaça – seja à estrutura de poder nas relações internacionais, seja a vidas

[77] A separação de Kostyuk e Zhukov (2017) entre operações cibernéticas com objetivo de propaganda e *disruption* assemelha-se à divisão proposta por Siedler (2016) entre ataques de coerção e força bruta, na medida em que ações de propaganda cibernética buscam influenciar a opinião pública e indiretamente minar o recrutamento ou financiamento do adversário, influenciando em seu cálculo de custo-benefício (KOSTYUK; ZHUKOV, 2017, p. 4). Operações nessa categoria incluem vazamentos de informação privada comprometedora, publicação *online* de conteúdo partidário de um dos lados e a criação de sites e fóruns para promover a mensagem de um grupo armado.

e ao funcionamento da sociedade – argumenta que as perspectivas de escalada não planejada de conflitos e erros de cálculo estratégico seriam aumentadas com a ascensão do ciberespaço.

Conforme Nye (2016), dissuasão significa convencer alguém a não agir de determinada forma, levando-o a crer que os custos da ação pretendida excederiam os benefícios de sua execução (NYE, 2016, p. 45). O autor enumera quatro principais métodos por meio dos quais a dissuasão é viabilizada no domínio cibernético: a ameaça de retaliação; a negação por defesa; o "emaranhamento" (*entanglement*) e tabus normativos.

A ameaça de retaliação diz respeito ao perigo de respostas retaliatórias por parte da vítima de um ataque cibernético. Importante notar que essa resposta pode ocorrer por meio cibernético, mas também diplomático, econômico, cinético e até mesmo nuclear (LIBICKI *apud* NYE, 2016). Essa é a base da chamada "ambiguidade escalatória" manifesta na estratégia cibernética dos EUA de 2011. A "ambiguidade escalatória" relaciona-se ao princípio da equivalência que baseia as abordagens dos Estados Unidos e da Otan para ataques cibernéticos[78], segundo o qual os efeitos diretos e indiretos de um ataque, em vez de seu método, é que determinam a força e severidade da retaliação, que pode acontecer inclusive por meio de ataques cinéticos. De fato, Nye (2016) refere-se a "ambiguidade escalatória calculada", deixando explícito que a vagueza no princípio de equivalência adotado pelos EUA e pela Otan é deliberada de forma a deixar as opções de retaliação abertas. Apesar de potencialmente menos eficaz do que outras formas de dissuasão por depender de um elevado grau de certeza do processo de atribuição – algo que nem sempre é possível no espaço cibernético –, a ameaça de retaliação é parte importante da dissuasão cibernética (NYE, 2016, p. 55).

A dissuasão por negação diz respeito ao controle dos impactos de ataques cibernéticos pela manutenção de estruturas de rede atualizadas e boas práticas de segurança cibernética de maneira geral. Melhores defesas podem aprimorar a dissuasão na medida em que mitigam os efeitos danosos de ataques cibernéticos e permitem que governos se concentrem em ameaças mais sofisticadas. Mesmo atuando como dissuasão, a defesa deve ser complementada por outros métodos (NYE, 2016, p. 57).

O emaranhamento refere-se à interdependência inerente à utilização do domínio cibernético. Esse atributo atua como meio de dissuasão, pois muitas vezes um ataque

[78] "Todos os estados possuem o direito inerente à autodefesa e reconhecemos que certos atos hostis conduzidos por meio do ciberespaço podem obrigar a ações condizentes com os compromissos que temos com nossos parceiros do tratado militar. Nós nos reservamos o direito de usar todos os meios necessários – diplomáticos, informacionais, militares e econômicos – conforme apropriado e consistente com o direito internacional aplicável, a fim de defender nossa nação, nossos aliados, nossos parceiros e nossos interesses" (WHITE HOUSE, 2011).

bem-sucedido em um adversário pode implicar consequências graves para o próprio atacante (NYE, 2016, p. 58).

Finalmente, considerações normativas podem atuar como dissuasão ao impor custos reputacionais ao "*soft power*" de determinado ator, maiores do que as vantagens obtidas por determinado ataque. Para Nye (2016) a desconsideração de cálculos de custo-benefício pelos atores é um dos elementos do exagero da ameaça cibernética, já que não é porque um ataque potencialmente destrutivo é possível, que ele acontecerá, conforme antecipado.

Ainda sobre as possibilidades de dissuasão cibernética, Lupovici (2014) propõe uma clarificação sobre esse conceito. Segundo o autor, na maior parte das abordagens sobre o tema – que seriam pouco informadas pela teoria de RI e em sua maior parte voltadas à definição de políticas –, a dissuasão cibernética refere-se normalmente à prevenção do uso de capacidades cibernéticas por adversários ou à proteção a infraestruturas cibernéticas do defendente. O autor defende que é importante contemplar de que forma a dissuasão cibernética se relaciona com outros modos de dissuasão e propõe que seja incluída no conceito de dissuasão cibernética a hipótese da utilização de ameaças de emprego de meios cibernéticos para desincentivar atividades indesejadas, ainda que essas sejam de natureza não virtual, ou cinética. Nesse sentido, ele propõe como conceito para dissuasão cibernética a utilização de meios cinéticos ou cibernéticos para impedir ataques cibernéticos e/ou a utilização de meios cibernéticos para impedir ataques cinéticos ou cibernéticos (LUPOVICI, 2014, p. 4). Assim, Lupovici (2014, p. 5) aborda a questão da intersecção entre meios cinéticos e cibernéticos em situações de conflito. Do ponto de vista dos atores, esses meios se complementariam para desincentivar ataques e para incentivar a opção por estratégias cibernéticas na execução de ataques, haja vista as possibilidades de retaliações cinéticas serem menores nesses casos.

De forma diversa, Gartzke e Lindsay (2015) apontam os limites da utilização da estratégia de dissuasão ou *détente* no espaço cibernético. Primeiramente, para que a dissuasão seja bem-sucedida, presume-se que os adversários pensem e ajam racionalmente – algo que não é possível presumir automaticamente como verdadeiro, sobretudo considerando o aumento no número e nos tipos de atores atuantes no espaço cibernético. Além disso, a demora e a incerteza inerentes ao processo de atribuição de ataques cibernéticos e a necessidade de manutenção do

segredo em relação a ferramentas cibernéticas, decorrentes da caracterização delas como capacidades *use and lose*[79], dificultam a dinâmica de dissuasão.

O outro lado do debate sobre o exagero da ameaça cibernética argumenta que, ao invés de representar fator de estabilidade para a Segurança Internacional enquanto provedora de novas estratégias de dissuasão, a ascensão do ciberespaço aumenta as chances de escaladas imprevistas de conflitos. Curiosamente, essa possibilidade baseia-se também em parte na "ambiguidade escalatória", segundo a qual um país pode se reservar o direito de retaliar ataques cibernéticos com quaisquer meios julgados convenientes (FARWELL; ROHOZINSKI, 2011; KELLO, 2013; VALERIANO; MANESS, 2014).

Kello (2013) explica que a ambiguidade escalatória, para além do princípio da equivalência, decorre também da dificuldade de interpretação de ações cibernéticas por conta de sinalização turva, quebra ou interferência de canais de comunicação, normas compartilhadas rudimentares ou inaplicáveis e dificuldades de atribuição.

> A ausência de "tabelas de conversão" claras para orientar a interpretação do princípio da equivalência pode levar a uma resposta excessiva da vítima de um ataque; a falta de padrões acordados de proporcionalidade pode produzir contrarrespostas irracionais; e, ao mesmo tempo, a falta de medidas de fortalecimento da confiança pode impedir as tentativas de desacelerar ou encerrar a crise (KELLO, 2013, p. 26, tradução da autora).

O desenvolvimento de "sistemas ativos de defesa" – sistemas autorizados a responder a ataques cibernéticos ou comprometimento de redes com retaliações automáticas – é também levantado como fator de instabilidade no ciberespaço que pode levar a escalada não planejada de conflitos. Betz e Stevens (2011) afirmam que, mais do que consolidar violações de soberania como toleráveis, a adoção desses sistemas as torna automáticas. Para lidar com o paradoxo formado, no qual violações de soberania no ciberespaço são norma e exceção – dependendo da perspectiva e das exigências políticas e diplomáticas do período –, iniciativas de governança no ciberespaço têm se fortalecido entre nações "com ideias semelhantes", não apenas como meio de dissuasão, mas para sinalizar o que é e o que não é aceitável entre os membros desses "blocos" (BETZ; STEVENS, 2011, p. 63).

Finalmente, a consideração de fatores políticos domésticos – como o controle estatal sobre operações cibernéticas – e especificidades do ciberespaço – tais como dificuldade de

[79] Segundo Gartzke e Lindsay (2015), "vantagens cibernéticas ofensivas são capacidades do tipo *use and lose*. Revelar a capacidade de causar danos através da internet normalmente significa dar ao inimigo dicas sobre vulnerabilidades que podem ser corrigidas, ao passo que iniciar o ataque raramente tem efeito duradouro no equilíbrio de poder" (GARTZKE, 2013, p. 60, tradução nossa). Discussão análoga sobre a transitoriedade de armas cibernéticas é apresentada em Smeets (2018).

atribuição e complexidade computacional – são consideradas por Junio (2013) fatores que aumentam as chances de erro nos cálculos de custos e benefícios na decisão sobre a realização de ataques cibernéticos ou de retaliações contra alvos errados (JUNIO, 2013, p. 2). Ele conclui que a ocorrência de uma guerra cibernética é, no mínimo, plausível o suficiente para que receba atenção da academia e de formuladores de política.

3.2.3. Relações entre atores estatais e não estatais no ciberespaço

As relações entre atores estatais e não estatais no ciberespaço aparecem de três diferentes formas na literatura revisada. A forma mais comum e com implicações mais relevantes para o debate sobre as consequências da ascensão do ciberespaço para as relações internacionais diz respeito a mudanças relativas de poder entre governos e Estados e atores não estatais que seriam causadas pela multiplicação e empoderamento de atores não estatais no ciberespaço. A segunda forma da relação entre atores estatais e não estatais abordada na literatura é a cooperação de governos e Estados com atores não estatais, sobretudo *hackers* patrióticos e mesmo a comunidade de crime cibernético de determinado país, na execução de ataques cibernéticos contra adversários por meio de *proxies* não estatais, de forma que a atribuição de ataques a Estados-nação seja ainda mais dificultada (HUGHES, 2010; FARWELL; ROHOZINSKI, 2011; KLIMBURG, 2011). Ainda, a literatura revisada aponta arranjos institucionais nacionais de governança de segurança cibernética como circunstâncias de relações muito próximas e pouco transparentes entre atores estatais e não estatais, na forma do setor público e do setor privado de tecnologias de informação e comunicação de dado país.

A abordagem mais frequente das relações entre atores estatais e não estatais no ciberespaço, adotada entre outros por Arquilla e Ronfeldt (1993), Nye (2010), Betz e Stevens (2011) e Kello (2013), menciona a ascensão de um número sem precedentes de atores não estatais potencialmente influentes nas relações internacionais e avalia os impactos que esse desenvolvimento pode representar à posição central dos Estados-nação no sistema internacional. Nye (2010), após a análise de recursos e vulnerabilidades dos tipos de atores atuantes no domínio cibernético – a saber: governos; organizações e redes altamente estruturadas; e indivíduos e redes pouco estruturadas –, afirma que, apesar da difusão de poder no espaço cibernético, o Estado-nação permanece como ator dominante na política internacional, agora em um ambiente em que o controle é dificultado.

Por sua vez, Kello (2013) afirma que um dos motivos pelos quais o impacto revolucionário da mudança tecnológica altera o quadro básico da sociedade internacional é que a tecnologia empodera atores não reconhecidos (KELLO, 2013, p. 31). Nesse sentido, o grande número de atores atuantes no ciberespaço decorrente da alegada facilidade de entrada nesse domínio poderia perturbar a estabilidade estratégica pela dificuldade de cooperação entre Estados-nação enquanto atores unitários racionais; e internamente, entre os atores domésticos, prejudicando a própria atuação estatal como ente unitário e racional. Ainda Kello (2013) refere-se à dispersão de poder para fora dos controles governamentais, com o empoderamento de atores não tradicionais como grupos religiosos extremistas, ativistas políticos, organizações criminosas e indivíduos.

A questão da soberania no domínio cibernético é mencionada por Inkster (2010) ao apresentar brevemente a visão e prática chinesas no ciberespaço:

> Falando em uma conferência organizada em Dallas, Texas, pelo Instituto Leste-Oeste, em maio de 2010, Liu Zhengrong, vice-diretor-geral do Escritório de Assuntos da Internet do Escritório de Informações do Conselho de Estado, pediu cooperação internacional para proteger o ciberespaço internacional, acrescentando que "a soberania da internet de cada país deve ser respeitada e as diferentes condições nacionais e culturais levadas em consideração". (INKSTER, 2010, p. 63, tradução nossa).

O instituto da soberania é analisado mais detidamente por Betz e Stevens (2011). Valendo-se da classificação de Krasner (1999) acerca da soberania (soberania doméstica, de interdependência, legal internacional e westfaliana), os autores analisam a influência do ciberespaço separadamente em cada um desses tipos.

A soberania legal internacional diz respeito ao estabelecimento de entidades políticas e seu reconhecimento como iguais pelo direito internacional. O ciberespaço não representaria ameaça a esse instituto como fonte de autoridade (BETZ; STEVENS, 2011, p. 58). À perspectiva defendida por alguns teóricos de que o ciberespaço conquiste reconhecimento como ente soberano *per se*, os autores rebatem com o argumento de que nunca a disposição dos Estados-nação foi tão pequena nessa direção (BETZ; STEVENS, 2011, p. 60).

Por sua vez, a soberania westfaliana refere-se à identificação dos entes soberanos com territórios físicos dentro dos quais a autoridade política doméstica é a única fonte legítima de organização institucional. No espaço cibernético, operações de ataque a Estados-nação perturbariam a soberania westfaliana da mesma maneira que tradicionais ações militares, não representando de fato uma novidade capaz de acabar com o instituto da soberania (BETZ; STEVENS, 2011, p. 61). No entanto, os autores, conforme já brevemente abordado, traçam um

cenário em que o desenvolvimento de "sistemas ativos de defesa" venha consolidar violações de soberania westfaliana não apenas como toleráveis, mas automatizadas e eventualmente o *status quo.*

De maneira diversa, a soberania doméstica é fortemente afetada no espaço cibernético: a autoridade e o controle internos dos Estados são continuamente postos à prova, em variados contextos políticos (de regimes autoritários a democracias liberais). Em contrapartida, os Estados nacionais, novamente independentemente de seus contextos políticos, têm respondido aumentando os controles[80] sobre atividades cibernéticas domésticas.

Finalmente, a soberania da interdependência (a possibilidade de regular o fluxo transnacional de bens, pessoas, ideias, poluentes, doenças) é considerada a mais afetada pelos processos de globalização, entre eles o desenvolvimento do ciberespaço (BETZ; STEVENS, 2011, p. 69). De fato, uma parte importante do intercâmbio de informação no domínio cibernético converte-se em capital, bens e serviços. Por outro lado, parte das trocas serve também à facilitação de ilícitos transnacionais, recrutamento de agentes, disseminação de propaganda com os mais variados intentos, além de permitir acesso a equipamentos e instalações sensíveis dos Estados nacionais. A preocupação com os efeitos do intenso fluxo informacional sobre a população tem também fortalecido os controles estatais sobre o espaço cibernético, a exemplo da proibição de vídeos de recrutamento para organizações terroristas e da legislação alemã que responsabiliza empresas de tecnologia pela publicação de posts com discurso de ódio[81]. Nesse sentido, Gohdes (2018) analisa a relação entre a ascensão das tecnologias de informação e comunicação em conflitos violentos e conclui que, a despeito das perspectivas iniciais de que a internet seria um território livre, no qual os cidadãos teriam acesso igualitário à informação, atualmente a pesquisa demostra quanto da experiência do usuário médio de internet é formatado por leis e regulamentações nacionais (DEIBERT *et al.* 2010; 2011 *apud* GOHDES, 2018). Betz e Stevens resumem então como característica definidora do ambiente político no espaço cibernético o conflito entre o controle daquilo que é desejável aos Estados-nação (bens, serviços e capital) e o controle daquilo que lhes representa ameaça

---

[80] Esses controles dividem-se em controles de 1ª, 2ª e 3ª geração. Controles de 1ª geração procuram limitar acesso a recursos online através da manipulação do tráfego na internet em vários níveis (do indivíduo ao servidor de internet ou *gateways* nacionais, por exemplo). Controles de 2ª geração são multifacetados e incluem abordagens técnicas e legais/normativas, como obrigatoriedade de registro junto a autoridades governamentais e de conformidade com suas diretrizes. Controles de 3ª geração não dizem respeito ao controle físico, mas à efetivação de mudanças cognitivas na população através de propaganda, vigilância e *data mining* (BETZ;STEVENS, 2011)

[81] A *Network Defensement Act* entrou em vigor em 2018 e objetiva restringir o discurso de ódio e os conteúdos ilegais e ofensivos na internet (DEUTSCHE WELLE BRASIL, 2018).

(terrorismo, dissidência política, acesso não autorizado a infraestruturas críticas) (BETZ; STEVENS, 2011, p. 72).

Conforme notado na discussão conceitual, parte da produção científica mais recente passa a questionar não apenas as características do ciberespaço, mas a própria validade do corolário de erosão do poder do Estado-nação no domínio cibernético. Nesse sentido, Rid e Buchanan (2015) e Gatzke (2013) discordam da erosão do poder tradicional de Estados-nação no domínio cibernético e defendem que pode ocorrer precisamente um efeito inverso de fortalecimento e maior concentração de capacidades nos Estados-nação. Para Rid e Buchanan (2015):

> Uma segunda visão banalizada é que a internet está tirando o poder dos Estados e dando-o a atores não estatais, entidades privadas e criminosos; que a tecnologia está nivelando o campo de jogo. No processo de atribuição, o caso é o inverso: apenas os Estados têm os recursos para atribuir as operações mais sofisticadas com um alto nível de certeza (RID; BUCHANAN, 2010, p. 31, tradução nossa).

Para Gartzke (2013) uma decorrência do caráter acessório de ataques cibernéticos a ações militares convencionais seria a guerra cibernética ser particularmente atraente a Estados com alta capacidade, confrontando oponentes mais fracos. Dessa forma, ao invés de ameaçar subverter a ordem mundial, a guerra cibernética deve perpetuar ou até mesmo acentuar a desigualdade militar atual (GARTZKE, 2013, p. 63, tradução livre).

A avaliação empírica de Valeriano e Maness (2014) acerca de incidentes cibernéticos também corrobora com a ideia de que a suposta difusão de poder entre atores não estatais não é tão verdadeira assim, na medida em que demonstra que as principais disputas cibernéticas registradas entre díades de países rivais entre 2001 e 2011 foram regionalizadas e controladas, ao invés de disruptivas e globais. Os autores concluem que a ameaça cibernética nesse sentido é sobrevalorizada e que, a despeito da importância inegável de estudar o assunto, as análises "devem ser trazidas de volta ao mundo real".

A segunda abordagem identificada na literatura revisada para análise das relações entre atores estatais e não estatais é apresentada em Farwell e Rohozinski (2011) e diz respeito à cooperação de atores estatais e não estatais como forma de blindagem dos primeiros contra a atribuição de ataques cibernéticos. Farwell e Rohozinski (2011) mencionam a possibilidade de "confluência entre o crime cibernético e a atuação estatal", afirmando que os Estados estão "capitalizando a tecnologia cujo desenvolvimento é impulsionado pelo crime cibernético e talvez terceirizando ataques cibernéticos a atores não atribuíveis, incluindo organizações criminosas". Nesse sentido, eles afirmam:

> Quase todos os eventos cibernéticos significativos relatados desde 2005 envolvem táticas, técnicas e códigos ligados à comunidade do crime cibernético. Críticos afirmam que a China terceirizou a pirataria cibernética contra os Estados Unidos a terceiros que agiram fora da lei, ou pelo menos capitalizou suas atividades. *Botnets* aproveitados por operadores criminosos russos efetuaram a negação de serviço que interrompeu as redes nacionais da Estônia em maio de 2007. Essas *botnets* são parte de uma economia clandestina de kits de *crimeware* e recursos que são comprados, vendidos e comercializados e normalmente usados para guerra corporativa para derrubar concorrentes políticos e comerciais offline (FARWELL; ROHOZINSKI, 2011, p. 26, tradução da autora).

Analogamente, Klimburg[82] (2011) afirma que a operacionalização de uma guerra cibernética ou ações de crime ou terrorismo cibernético não são fundamentalmente diferentes e que a distinção entre esses fenômenos repousaria basicamente em sua motivação. Para o autor esse fato atesta a presunção de que atores não estatais podem ser utilizados pelo Estado, ostensiva ou secretamente, para execução de ataques cibernéticos passíveis de negação plausível. "Isso significa que estados têm interesse em manter ou tolerar organizações *proxy* que poderiam ser implicadas nesse tipo de atividade" (KLIMBURG, 2011, p. 42, tradução da autora). Também Ottis (2010, p. 98) afirma que, ainda que não haja laços formais entre um governo e uma milícia cibernética online, o governo ainda pode utilizá-la como instrumento de poder, de forma a distanciar o Estado dos ataques. Ainda, Hughes (2010) exemplifica o fenômeno abordado por Farwell e Rohozinski (2011) e Klimburg (2011) afirmando que a Rússia abriga um número considerável de especialistas em informática mal remunerados, que atacariam sistemas e operações online de adversários russos com a conivência e possivelmente o apreço ou incentivo governamental, atuando como "*hackers* patrióticos" civis (HUGHES, 2010, p. 532).

A terceira abordagem da influência da ascensão do ciberespaço na relação de atores estatais e não estatais analisa os arranjos de governança em segurança cibernética nacionais, em que os setores público e privado interagem com proximidade, porém frequentemente pouca transparência e clareza nas definições de responsabilidades. Hansen e Nissenbaum (2009), Lemay, Fernandeza e Knight (2010), Mueller, Schmidt e Kuerbis (2013) e Carr (2016) defendem que os discursos nacionais sobre segurança cibernética são construídos de maneira a eliminar as fronteiras entre as atuações desses atores, fato que, segundo Hansem e Nissembaum (2009), contribui e é um indicador de um processo de securitização dos discursos sobre o ciberespaço.

---

[82] O artigo de Klimburg (2011) é muito interessante para este tópico especificamente, pois descreve formas de recrutamento de pessoal capacitado para atuação no ciberespaço pelos governos da China, EUA e Rússia.

> O cenário da RAND mostra apropriadamente como o discurso sobre segurança cibernética se move perfeitamente entre distinções normalmente consideradas cruciais para os estudos de segurança: entre segurança individual e coletiva, entre autoridades públicas e instituições privadas e entre segurança econômica e político-militar (HANSEN; NISSENBAUM, 2009, p. 1161, tradução nossa).

Ademais, a falta de definições de responsabilidades claras entre o setor público e o setor privado poria em questão a durabilidade e a eficácia desses arranjos (CARR, 2016). A autora explica que, em geral, a parceria público-privada é operacionalizada sobretudo no compartilhamento de informações, com o papel do governo limitado à recomendação de melhores práticas. Ainda assim, o mero compartilhamento de informações seria dificultado, haja vista que para o setor privado as decisões são tomadas dentro de um modelo de negócio que responde à necessidade por lucro e à defesa do interesse de acionistas, o que nem sempre está de acordo com a noção de transparência e de bem público; ao passo que as informações provenientes do governo guardam a necessidade de obedecer a regras de acesso e confidencialidade. Analogamente, Lemay, Fernandeza e Knight (2010) apontam que o setor privado, por ser direcionado pelo lucro e não estar imbuído de preocupações de segurança nacional, tem poucos incentivos para adotar medidas de *compliance* em segurança cibernética, a despeito de ser um setor central em sua operacionalização.

Mueller, Schmidt e Kuerbis (2013) abordam a compatibilidade entre a governança da internet, caracterizada por ser necessariamente em rede, e o fato de a abordagem dos fenômenos cibernéticos por parte de Estados nacionais ocorrer, na maior parte das vezes, sob uma lógica de organização e controle baseada em estruturas hierárquicas. Nesse sentido, uma das perguntas a que os autores buscam responder é: "os Estados-nação organizados hierarquicamente entram em conflito com as formas de organização descentralizada e em rede encontradas na internet, ou têm se adaptado a elas?" (MUELLER; SCHMIDT; KUERBIS, 2013, p. 87, tradução nossa). A resposta a que chegam é que, com base em casos empíricos, os governos têm tendido a responder de forma a adaptar-se à governança de rede ao invés de alterá-la, buscando se inserir em redes técnicas e operacionais de modo a formatar padrões e práticas em um ambiente de múltiplos interesses.

A avaliação das três formas de relação entre atores estatais e não estatais identificadas na literatura corroboram o argumento de que a ascensão do espaço cibernético não representa uma ameaça ao *status quo* das relações internacionais. O Estado-nação teria seu papel como ator principal da política internacional garantido e, alguns defendem, até fortalecido. Ataques cibernéticos realizados por atores não estatais têm em geral menor impacto estratégico, devido à ausência de ações preparatórias, da possibilidade da realização de testes, de recursos

financeiros escassos, de forma que não representam um risco real ao domínio estatal em conflitos cibernéticos. Governos e Estados-nação estariam ainda incorporando atores não estatais a suas estratégias no ciberespaço de forma a distanciar-se da atribuição desses ataques e aumentando suas possibilidades de ação.

3.2.4. Securitização do discurso sobre ciberespaço

A securitização, conforme abordagem da Escola de Copenhagen, "é um ato de discurso que 'securitiza', ou seja, que constitui um ou mais objetos de referência – historicamente a nação ou o Estado – ameaçados em sua sobrevivência física ou ideacional e, portanto, que necessitam de proteção urgente" (HANSEN; NISSENBAUM, 2009, p. 1156). Hansen e Nissembaum (2009) debruçam-se sobre a análise do conceito de segurança cibernética e o processo de securitização dos discursos sobre ascensão do ciberespaço. Para as autoras, o conceito de segurança cibernética deixou de ser um mero conceito técnico de segurança computacional, quando proponentes urgiram que ameaças derivadas de tecnologias digitais poderiam ter efeitos sociais devastadores (HANSEN; NISSENBAUM, 2009, p. 1155).

A securitização de "segurança cibernética" seria particularmente bem-sucedida em relação à securitização de outras áreas (por exemplo, da questão ambiental) graças a uma "gramática de securitização" que relaciona diretamente objetos de referência, ameaças e atores da securitização, através, nesse caso, das estratégias de hipersecuritização, práticas cotidianas de segurança e a tecnificação do discurso sobre segurança cibernética. A hipersecuritização do discurso manifesta-se na forma contundente com que a segurança cibernética se apoia em cenários de desastres multidimensionais, com ameaças severas de efeitos irreversíveis e rápido desenvolvimento ocorrendo em cascata; e no fato de que nenhum desses cenários efetivamente já ocorreu. (HANSEN; NISSEMBAUM, 2009, p. 1164). Em segundo lugar, a responsabilidade pela segurança cibernética e suas implicações na segurança nacional e até mesmo internacional é transferida ou compartilhada não apenas com o setor empresarial privado, mas com cada indivíduo usuário das tecnologias digitais, estratégia a que Hansen e Nissembaum (2009) se referem como "práticas cotidianas de segurança". A combinação de práticas de segurança cotidiana com efeitos cascata catastróficos e potencialmente imediatos que fazem com que o conceito "segurança cibernética" saia do âmbito da "segurança corporativa" ou "confiança do consumidor" para as modalidades de segurança social, segurança nacional e – acrescenta-se aqui, segundo a mesma lógica – segurança internacional. Em terceiro lugar, a tecnificação do setor despolitiza o processo de securitização, na medida em que sugere que se trata de uma

agenda neutra do ponto de vista político e normativo (HUYMANS, 2006, p. 6-9 *apud* HANSEN; NISSENBAUM, 2009). Apesar de essa estratégia não ser utilizada exclusivamente no setor cibernético, nesse caso ela tem sido capaz de atingir uma posição mais privilegiada do que em outros setores.

Também as analogias espacial e biológicas utilizadas na definição do ciberespaço[83] atuam como poderosos formatadores de percepção e ferramentas utilizadas ativamente no discurso político (CAVELTY, 2013, p. 118). Essas analogias servem ao processo de inflação de ameaças destinado a "adicionar urgência aos apelos por ação". Nesse sentido, Betz e Stevens (2011) alertam para a necessidade de cautela quanto à forma como o discurso da segurança cibernética estrutura nosso pensamento, canalizando-o para modalidades enganosas (BETZ; STEVENS, 2013, p. 3). Calvelty (2013) ressalta ainda o uso frequente de linguagem militar para tratar de questões relacionadas à ascensão do ciberespaço e que isso sugere que a segurança cibernética pode e deve ser administrada como uma questão militar por atores militares. A autora declara que a facilidade com que o domínio digital foi submetido à retórica e às práticas da Guerra Fria é alarmante (CAVELTY, 2013, p. 119).

Do outro lado do debate, Kello (2013) argumenta que a ligação entre segurança de computadores e segurança nacional e internacional precisaria ser aprofundada. Para o autor:

> [...] as percepções públicas da questão cibernética exibem as seguintes tendências: (1) uma propensão a pensar em "ameaças cibernéticas" como linhas de código perniciosas – em vez de se concentrar nos agentes humanos que as utilizam e em seus motivos para fazê-lo; (2) uma inclinação para conceber "segurança" como a segurança de um sistema de computador ou rede – sem prestar atenção suficiente à segurança da atividade crítica (por exemplo, enriquecimento nuclear) que está além do ciberespaço, mas depende da funcionalidade do computador; e (3) o hábito de rotular qualquer ação cibernética hostil – do roubo de dados pessoais à destruição de turbinas nucleares – como um "ataque", ignorando as conotações potencialmente graves desse termo em um contexto internacional. (KELLO, 2013, p. 16).

A percepção da securitização do discurso sobre segurança cibernética e, de forma mais ampla, sobre a ascensão do ciberespaço, apontada por Hansen e Nisembaum (2009), Betz e Stevens (2011), Cavelty (2013) e mencionada também em Lupovici (2014) são corroboradas pela presente revisão sistemática de literatura. Não à toa o principal debate identificado nessa literatura questiona a presença de uma "ameaça" às relações internacionais advinda do ciberespaço. Percebe-se, no entanto, que o apontamento desse processo de securitização tem tido o efeito positivo de relativizar os cenários cibernéticos catastróficos presentes na literatura

[83] Discutidas no item 2.2.1.

inicial sobre o tema e a fazer avançar os estudos em direção a uma produção científica mais embasada em evidências empíricas e mais ponderada em suas conclusões.

3.3. Considerações sobre poder cibernético

Um recorte ontológico do debate central identificado na literatura pesquisada busca compreender se poder cibernético constitui um fenômeno fundamentalmente diferente de poder em suas manifestações tradicionais ou se seria uma adaptação marginal, derivada do surgimento do domínio cibernético como novo ambiente de competição por influência entre os atores.

A despeito de não haver consenso sobre o que significa poder, Baldwin (2016) afirma que há um consenso generalizado acerca de sua importância central nos estudos de relações internacionais. Ao fazer a revisão do conceito de poder nas RI, ele se utiliza daquilo que chama de conceito dahliano de poder.

> Embora houvesse muitos pontos de desacordo, os estudiosos que trabalhavam na tradição de Laswell e Kaplna, Dahl, Simon e March concordaram em pelo menos quatro pontos: primeiro, que o poder era um conceito causal; segundo, que o poder deve ser visto como um conceito relacional em vez de absoluto; terceiro, que poder é um conceito multidimensional; e que as bases de poder são muitas e variadas, sem hierarquia permanente entre elas (BALDWIN, 2016, p. 3, tradução nossa).

Em consonância com a definição dahliana de poder apresentada, Nye (2010) defende que poder é algo que depende de contexto e que o rápido crescimento do espaço cibernético é um contexto importante na política mundial. As características do domínio cibernético reduziriam diferenciais de poder entre os atores, fornecendo um bom exemplo da difusão de poder que caracteriza a política global no século XXI.

Diversamente, Betz e Stevens (2011) defendem que o poder cibernético é meramente a manifestação do poder no espaço cibernético, obedecendo aos mesmos princípios gerais que se aplicam a manifestações fora desse domínio. Nesse sentido eles inspiram sua análise do poder cibernético no framework de Barnett e Duvall (2005). Conforme seu argumento, há quatro formas através das quais se pode observar o exercício de poder no espaço cibernético. Elas constituiriam as quatro formas de poder cibernético: os poderes cibernéticos compulsório, institucional, estrutural e produtivo (BETZ; STEVENS, 2011, p. 45). O poder cibernético compulsório, que consiste no uso de coerção direta por um ator no espaço cibernético com o objetivo de modificar o comportamento e as condições de existência de outro ator, geralmente ocorre na forma do controle de máquinas ou redes (BETZ; STEVENS, 2011, p. 45-46). Esse

conceito assemelha-se à utilização de ataques a redes de computadores (CNAs) como força bruta, segundo a sistematização de Siedler (2016).

O poder cibernético institucional, por sua vez, diz respeito à utilização de recursos de um ator – geralmente um Estado-nação – de modo a estabelecer uma série de normas e padrões a serem obedecidos por todos os usuários do espaço cibernético. O governo estadunidense exerceria esse poder, por exemplo, através da *Internet Corporation for Assigned Names and Numbers* – ICANN, que gerencia a alocação dos nomes dos domínios; Rússia e China, por sua vez, exerceriam esse poder respectivamente na *International Telecommunication Union* (ITU) e na Organização de Xangai para Cooperação, na qual buscariam promover interesses nacionais na governança da internet (BETZ; STEVENS, 2011, p. 47-48).

O terceiro tipo de poder cibernético elencado por Betz e Stevens é o estrutural, que atuaria de forma a manter posições relativas de poder entre os atores e que em grande medida possibilita ou constrange as ações que eles possam pôr em prática. No caso do espaço cibernético, no entanto, em função da organização em rede, o poder estrutural apresenta natureza dual. Nas palavras de Betz e Stevens, "O poder cibernético estrutural [...] funciona tanto para manter o *status quo* quanto para perturbá-lo" (BETZ; STEVENS, 2011, p. 50).

Finalmente, o quarto tipo de poder cibernético seria o produtivo (em tradução livre), que diz respeito à produção, reprodução e fortalecimento de discursos. Os autores defendem que, em uma era de "comunicação estratégica", essa seja, talvez, a forma mais importante de poder cibernético (BETZ; STEVENS, 2011). O conceito de poder produtivo aproxima-se das noções de guerra informacional e segurança da informação discutidas e da abordagem sino-russa quanto ao potencial das tecnologias de informação e comunicações.

Analogamente à visão de poder produtivo de Betz e Stevens (2011), Castells (2013) analisa o poder da comunicação na atual sociedade em rede, caracterizada como "a estrutura social construída ao redor de [...] redes digitais de comunicação" (CASTELLS, 2013, p. 4, tradução nossa). O autor argumenta que "o processo de construção e exercício das relações de poder é transformado definitivamente no novo contexto organizacional e tecnológico derivado da ascensão de redes digitais globais de comunicação" (CASTELLS, 2013, p. 4, tradução da autora). Nesse sentido, os processos de globalização e ascensão da sociedade de redes decorrentes do desenvolvimento do domínio cibernético impactam sobremaneira a atuação dos Estados nacionais, na medida em que processam conhecimento e pensamentos para criar ou destruir "confiança[84]" – considerada por ele a fonte decisiva de poder estatal (CASTELLS,

[84] O termo "confiança", aqui, parece referir-se ao conceito de legitimidade.

2013, p. 16). Também Nye parece concordar com esse argumento: “Na Era da Informação, não se trata apenas de qual exército vence, mas qual história vence” (NYE, 2005 *apud* BETZ; STEVENS, 2011, tradução livre).

Também Schreier (2015) ressalta que as novas formas de conteúdo e conectividade transformam a maneira com que a influência pode ser exercida, inclusive no exercício de *soft power* e *smart power*[85] na busca por objetivos estratégicos dentro e fora do espaço cibernético (SCHREIER, 2015). Para o autor poder cibernético é a capacidade de controlar sistemas e redes de tecnologia da informação dentro e através do ciberespaço e seria moldado por fatores tecnológicos, organizacionais e informacionais, sendo apenas uma dimensão da noção mais ampla de poder informacional e apoiando o exercício de outros tipos de poder. O autor defende que o uso, a ameaça do uso ou as expectativas acerca dos efeitos causados por capacidades cibernéticas de um Estado podem ser transformados em elemento de barganha política através da estratégia.

Por sua vez, Klimburg (2011) apresenta considerações mais específicas sobre poder cibernético. Para Klimburg (2011), o poder cibernético de um Estado depende de três dimensões: aspectos de coordenação operacional e de políticas entre diferentes estruturas governamentais; coerência com outras políticas cibernéticas por meio de alianças internacionais; e estruturas legais e cooperação com atores cibernéticos não estatais (KLIMBURG, 2011, p. 43). Embora as duas primeiras dimensões sejam importantes, Klimburg (2011) considera que a natureza do ciberespaço implica grande parte das capacidades cibernéticas de um Estado estar fora do controle direto do governo nos setores privado e na sociedade civil, sendo a cooperação com atores não estatais fundamental para a criação da capacidade cibernética de um Estado.

As discussões sobre poder cibernético encontradas na literatura revisada não permitem concluir que haja alguma especificidade à análise desse tipo de poder em relação a manifestações mais tradicionais, sobretudo em face da prioridade dada à noção de guerra enquanto forma de infligir efeitos cinéticos danosos contra um adversário. Desse ponto de vista, não há nada de muito novo em relação ao poder cibernético. De fato, como discutido no tópico anterior, a eficácia de ataques cibernéticos na consecução de objetivos políticos tem, inclusive, um caráter acessório e complementar a estratégias mais tradicionais de exercício de poder. No entanto, um importante aspecto que merece atenção e que é abordado apenas lateralmente na

---

[85] *Smart power* (poder inteligente, em português) é um conceito de Joseph Nye (2004) e refere-se à utilização de alianças, parcerias e instituições, busca por desenvolvimento global, diplomacia pública e inovação e tecnologia para exercício de poder.

amostra bibliográfica revisada é o papel do ciberespaço como domínio propício e instrumentalizável ao exercício do poder informacional (ou produtivo, na terminologia de Betz e Stevens). Esse parece ser o elemento de maior impacto estratégico nas políticas nacional e internacional decorrente da ascensão do ciberespaço e, no entanto, é negligenciado em grande parte na literatura revisada.

CONCLUSÕES

Uma primeira conclusão desta dissertação é de natureza metodológica e diz respeito à necessidade de adequar a forma de escolha da amostra bibliográfica a ser trabalhada na elaboração de uma revisão sistemática de literatura ao objetivo que se pretende atingir. A utilização de uma base de dados científicos e da análise de citações como alicerce para a elaboração de trabalhos que pretendam traçar um panorama de determinado campo de estudos pode se mostrar inadequada. De fato, nesta dissertação esse método para a escolha da amostra bibliográfica a ser revisada gerou uma amostra limitada à Segurança Internacional, ao invés de representativa da disciplina de RI como um todo. Esse fato não implica, contudo, a invalidação dos resultados aqui apresentados, mas sua necessária localização em um campo de estudos mais específico, que, ademais, representa – se considerado o maior número de citações utilizado como parâmetro – um campo bastante relevante em termos de impacto científico na literatura de RI de forma geral.

Em segundo lugar, as deduções da análise bibliométrica da produção de RI sobre a ascensão do ciberespaço permitem corroborar as visões sobre a centralidade da produção em língua inglesa nas RI, da concentração da literatura em publicações específicas da área de Segurança Internacional e no tema conflito cibernético. Do ponto de vista metodológico, as diferenças de impacto de diferentes tipos de documentos (artigos e *proceeding papers*) em comunidades diferentes emergiu como tópico passível de aprofundamento posterior – a hipótese é que, por um lado, *proceeding papers* informem mais diretamente tomadores de decisão e a comunidade de política, ao passo que artigos moldariam as visões da comunidade científico-acadêmica. Além disso uma análise mais detida sobre a relação entre o contexto político e variações do número de documentos produzidos pode trazer *insights* sobre motivações e dinâmicas de incentivos na elaboração de artigos científicos, a exemplo de como é criada uma tendência de pesquisa.

Conjuntamente, a análise bibliométrica da literatura de RI sobre a ascensão do ciberespaço e a revisão sistemática do núcleo dessa literatura permitiram identificar conceitos e debates em evolução, bem como um processo de amadurecimento desse campo de estudos. Nota-se constantes referências à indefinição conceitual e à grande variedade de fenômenos tratados na literatura. Porque não há acordo em torno dos conceitos centrais na abordagem do tema – notadamente ciberespaço, guerra cibernética e segurança cibernética, as inferências que

se fazem dizem respeito a fenômenos variados, com autores por vezes utilizando o mesmo conceito, porém com definições diferentes, para embasar conclusões divergentes.

Prevalece, contudo, o predomínio da noção de guerra cibernética enquanto fenômeno interestatal e com efeitos cinéticos como a principal abordagem de conflito cibernético trabalhada na literatura. A probabilidade desse fenômeno, inicialmente percebida como alta, possibilitada pela noção de um ciberespaço anárquico e perigoso, avança na direção mais parcimoniosa da busca por evidências empíricas que a consubstanciem. Baixo custo de entrada, anonimato, assimetrias de vulnerabilidades e a consequente dificuldade de atribuição de ataques cibernéticos não são mais presunções inquestionáveis como no início da produção de segurança internacional sobre a ascensão do ciberespaço. A despeito de um processo de difusão de poder, o Estado-nação é ainda percebido como o tipo de ator mais poderoso nas relações internacionais operacionalizadas no ciberespaço e a ideia de uma ameaça cibernética ao *status* quo das relações internacionais ou ao funcionamento da sociedade por conta de ataques cibernéticos de alto impacto foi relativizada ao longo desses aproximadamente trinta anos desde o início das abordagens de questões cibernéticas pelas RI. Nesse sentido, a percebida ausência de evidências empíricas da "ameaça cibernética" pela literatura mais recente contribui para a percepção de que o debate central sobre o exagero dessa ameaça tende a conclusões cada vez mais próximas do argumento de que a ameaça cibernética é – ou pelo menos foi, na literatura inicial – exagerada.

Ademais, a revisão sistemática da literatura de segurança internacional sobre a ascensão do ciberespaço permite estabelecer duas ausências notáveis: uma delas é a falta de trabalhos sobre a instrumentalização do ciberespaço em ações de terrorismo. A despeito de a análise bibliométrica identificar trabalhos indexando "*terrorism*" como palavra-chave, nenhum dos trabalhos mais citados e que constituíram o objeto da revisão sistemática de literatura aprofunda a questão. Trata-se de um aspecto notável também pelo fato de muitos trabalhos se referirem a ataques cibernéticos a infraestruturas críticas como um dos maiores riscos levantados pela ubiquidade do ciberespaço, ignorando o potencial de sua utilização não em conflitos interestatais, mas em ataques terroristas.

A segunda ausência notável diz respeito a estudos de segurança internacional que levem em consideração não apenas a probabilidade de uma guerra cibernética interestatal com efeitos cinéticos, mas a instrumentalização do ciberespaço em ações de guerra informacional. Parte da abordagem científico-acadêmica e importantes atores da política internacional localizam no aspecto informacional, naquilo que Betz e Stevens (2011) chamam de poder produtivo, que Nye (2010) chama de ganhar "corações e mentes", o principal ativo estratégico possibilitado pelo

ciberespaço. Nesse sentido, a despeito da importância inegável de prescrutar efeitos cinéticos de ações cibernéticas, estudos de segurança internacional que ignorem a utilização do ciberespaço em operações de informação e suas possibilidades na desestabilização de regimes domesticamente ou internacionalmente, ficam sujeitos a perder importância analítica e poder explicativo.

A presente dissertação deixa como principal contribuição a reunião e a tentativa de sistematização de conceitos e debates de um campo relativamente novo e complexo de estudos nas relações internacionais, qual seja o estudo das implicações da ascensão do ciberespaço na subárea da Segurança Internacional. Mais do que certezas categóricas, o que decorre da revisão dessa literatura é uma agenda de pesquisa passível de aprofundamento futuro. Ressalta-se aqui, além da necessidade de estudos sobre a instrumentalização do ciberespaço em atos de terrorismo e em operações de informação, também a necessidade de aprofundar e detalhar os impactos de novas tecnologias individualmente (como Internet das Coisas, Big Data, Inteligência Artificial, Biotecnologia, Blockchain e Criptoativos) em conflitos internacionais. De fato, as perspectivas levantadas na literatura revisada referem-se à ascensão do ciberespaço enquanto processo amplo e foram levantadas há anos. O campo de estudos poderia se beneficiar de estudos mais recentes e detalhados acerca do funcionamento dessas tecnologias e suas implicações na segurança internacional. Ainda, a avaliação de iniciativas de criação de um regime internacional de segurança cibernética nas Nações Unidas – ou fora delas – também merece atenção, na medida em que tem um papel importante na manutenção da paz e estabilidade no ciberespaço. Passíveis de aprofundamento também são os estudos empíricos acerca da utilização de ataques cibernéticos simultaneamente a situações de conflito cinético, como realizadas por Kostyuk e Zhukov (2017) e Gohdes (2018), de forma a compreender melhor a interação entre as realidades virtual e não virtual em circunstâncias de conflito atualmente. Nesse sentido, espera-se que este estudo aumente o interesse de pesquisadores de RI pelo tema, bem como que tenha contribuído com a contextualização do campo de estudos.

REFERÊNCIAS

ABDENUR, A. E.; GAMA, C. F. *Triggering the Norms Cascade*: Brazil's Initiative for Curbing Electronic Espionage. 2015.

ABRAMO, G.; D'ANGELO, C. A. Evaluating research: from informed peer review to bibliometrics. *Scientometrics*, v. 87, n. 3, p. 499-514, 2011.

ADRIAANSE, L.; RENSLEIGH, C. Web of Science, Scopus and Google Scholar: A content comprehensiveness comparison. *The Electronic Library*, v. 31, n. 6, p. 727-744, 2013.

ALMEIDA, Maria Eneida de. The permanent relation between biology, power and war: the dual use of the biotechnological development. Ciênc. saúde coletiva, Rio de Janeiro , v. 20, n. 7, p. 2255-2266, July 2015 .

ANI, K. W. U.; ZAINAB, A. N.; ANUR, N. B. Bibliometric studies on single journals: A review. *Mala. J. Lib. & Inf. Sci.*, v. 14, n. 1, p. 17-55, 2009.

APT1. Alexandria, VA: Mandiant, 18 Feb. 2013.

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

ASSEMBLEIA GERAL DA ONU (AG). *Resolução 68/167*. AG Index: A/RES/68/167, 18 dez. 2013. Disponível em: http://undocs.org/A/RES/68/167.

ASSEMBLEIA GERAL DA ONU. *Resolução 69/166*. AG Index: A/RES/69/166, 18 dez. 2014. Disponível em: http://undocs.org/A/RES/69/166.

BALZACQ, T.; CAVELTY, M. D. A theory of actor-network for cyber-security. *European Journal of International Security*, v. 1, n. 2, p. 176-198, 2016.

BARNETT, M.; DUVALL, R. *Power in International Politics, International Organization*. Cambridge University Press, v. 59, n. 1, p. 39-75, 2005.

BETZ, D. J.; STEVENS, T. Analogical reasoning and cyber security. *Security Dialogue*, 2013.

BETZ, D. J.; STEVENS, T. *Cyberspace and the State*: toward a strategy for cyber-power. Londres: International Institute for Strategic Studies, 2011.

BORGHARD, E. D.; LONERGAN, S. W. The Logic of Coercion in Cyberspace. *Security Studies*, 2017.

BORNMANN, L.; DANIEL, H. D. What do citation counts measure? A review of studies on citing behavior. *Journal of documentation*, v. 64, n. 1, p. 45-80, 2008.

BOTELHO, L. L. R.; ALMEIDA CUNHA, C. C.; MACEDO, M. O método da revisão integrativa nos estudos organizacionais. *Gestão e Sociedade*, v. 5, n. 11, p. 121-136, 2011.

BRONK, C.; TIKK-RINGAS, E. The Cyber Attack on Saudi Aramco. *Survival*, 2013.

BROOME, M. E. Integrative literature reviews for the development of concepts. Concept development in nursing: foundations, techniques and applications. Philadelphia: WB Saunders Company, 2000. 231-50.

BUSH, V. As We May Think. *The Atlantic Monthly*, v. 176, n. 1, p. 101-108, Jul. 1945.

CAPOBIANCO, L.; CURY, Ligia. *Princípios da História das Tecnologias da Informação e Comunicação*. Grandes Invenções, 2011, VIII Encontro Nacional de História da Mídia. Guarapuava: Unicentro, 28-30 abr. 2011.

CARR, M. Public-private partnerships in national cyber-security strategies. *International Affairs*, 2016.

CARSON, A; YARHI-MILO, K. Covert Communication: The Intelligibility and Credibility of Signaling in Secret. *Security Studies*, 2017.

CASADO, J.; KAZ, R.; GREENWALD, G. EUA espionaram milhões de e-mails e ligações de brasileiros. País aparece como alvo na vigilância de dados e é o mais monitorado na América Latina. *Jornal O Globo online*, 6 jul. 2013. Disponível em: https://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934. Acesso em: 26 nov. 2019.

CASTELLS, M. *A Sociedade em Rede*. São Paulo: Paz e Terra, 2013.

CASTELLS, M. *Communication Power*. Oxford: Oxford University, 2013.

CAVELTY, M. D. From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review*, 2013.

CHI, P.-S. Bibliometric characteristics of political science research in Germany. Proceedings of the American Society for Information Science and Technology. 2012. 49.10.1002/meet.14504901115.

CHRISTENSEN, K. K.; PETERSEN, K. L. Public-private partnerships on cyber security: a practice of loyalty. *International Affairs*, 2017.

COBO, M. J.; LÓPEZ-HERRERA, A. G.; HERRERA- VIEDMA, E.; HERRERA, F. SciMAT: A new science mapping analysis software tool. *Journal of the Association for Information Science and Technology*, v. 63, n. 8, p. 1609-1630, 2012.

COPELAND, B. J. *Colossus*: Its Origins and Originators. IEEE Annals of the History of Computing. Nov. 2004.

COUNCIL FOR FOREIGN RELATIONS. *Assessing China's digital silk road initiative*: a transformative approach to technology financing or a danger to freedoms? Disponível em: www.cfr.org/china-digital-silk-road.

CUERVO, C; MOROZOVA, A; SUGIMOTO, N. Regulation of crypto assets. FinTech notes. *International Monetary Fund.* Washington, DC, 2019.

DARCZEWSKA, J. *The anatomy of Russian information warfare the Crimea operation*: a case study. 2014. Disponível em: https://bit.ly/3ap26nY.

DEIBERT, R. J.; ROHOZINSKI, R.; CRETE-NISHIHATA, M. Cyclones in cyberspace: Information shaping and denial in the 2008 Russia-Georgia war. *Security Dialogue*, 2012.

DEUTSCHE WELLE BRASIL. *Lei contra discurso de ódio na internet entra em vigor na Alemanha*, 2 jan. 2018. Disponível em: www.dw.com/pt-br/lei-contra-discurso-de-%C3%B3dio-na-internet-entra-em-vigor-na-alemanha/a-41996447.

DILMA cancela viagem aos Estados Unidos. *Jornal O Estado de S. Paulo online*, 17 set. 2013. Disponível em: https://bit.ly/3ej6xlp. Acesso em: 26 nov. 2019.

DOCUMENTOS da NSA apontam Dilma Rousseff como alvo de espionagem. *Portal G1*, 1 set. 2013. Disponível em: http://g1.globo.com/politica/noticia/2013/09/documentos-da-nsa-apontam-dilma-rousseff-como-alvo-de-espionagem.html. Acesso em: 26 nov. 2019.

EFRONY, D.; SHANY, Y. A rule book on the shelf? Tallinn manual 2.0 on cyberoperations and subsequent state practice. *American Journal of International Law*, 2018.

EICHENSEHR, K. E. Tallinn Manual on the International Law Applicable to Cyber Warfare. *American Journal of International Law*, 2014.

ENTENDA o caso de Edward Snowden, que revelou espionagem dos EUA. *Portal G1*, 2 jul. 2013. Disponível em: http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html. Acesso em: 26 nov. 2019.

FARWELL, J. P.; ROHOZINSKI, R. Stuxnet and the Future of Cyber War. *Survival*, v. 53, n. 1, p. 23-40, 2011.

FARWELL, J. P; ROHOZINSKI, R. The New Reality of Cyber War. *Survival*, 2012.

GARCIA, D. Future arms, technologies, and international law: Preventive security governance. *European Journal of International Security*, 2016.

GARNER, J.; ROBERTSON, S. *Conducting a literature review*. 2002. Disponível em www.lib.unimelb.edu.au/postgrad/litreview/gettingstarted.html. Acesso em: 12 jul. 2017.

GARTZKE, E. The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. *Quarterly Journal*: International Security, 2013.

GARTZKE, E.; LINDSAY, J. R. Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace. *Security Studies*, 2015.

GEERS, K. (ed.). Cyber War in Perspective: Russian Aggression against Ukraine. Tallinn: NATO CCD COE, 2015.

GLASS, G. V. Primary, secondary, and meta-analysis of research. *Educational researcher*, v. 5, n. 10, p. 3-8, 1976.

GOHDES, A. R. Studying the Internet and Violent conflict. *Conflict Management and Peace Science*, 2018.

GOLDSMITH, J. How Cyber Changes the Laws of War. *European Journal of International Law*, 2013.

GOMIDE, R.; SOUZA, L. Espiões da era digital. *Revista Época online*, 27 jul. 2013. Disponível em: https://epoca.globo.com/tempo/noticia/2013/07/bespioesb-da-era-digital.html. Acesso em: 26 nov. 2019.

GOMPERT, D. C.; LIBICKI, M. Cyber Warfare and Sino-American Crisis Instability. *Survival*, 2014.

GONZÁLEZ-ALBO, B.; BORDONS, M. Articles vs. Proceedings Papers: Do they differ in research relevance and impact? A case study in the Library and Information Science field. *Journal of Informetrics*, v. 5, n. 3, p. 369-381, 2011.

GORWA, Robert; SMEETS, M. *Cyber Conflict in Political Science*: A Review of Methods and Literature. 2019.

GREENWALD, G; GOMIDE, R.; SOUZA, L. A carta em que o embaixador americano agradece o apoio da NSA. *Revista Época Online*, 2 ago. 2013. Disponível em: https://epoca.globo.com/tempo/noticia/2013/08/carta-em-que-o-atual-bembaixadorb-americano-no-brasil-bagradece-o-apoio-da-nsab.html. Acesso em: 26 nov. 2019.

GREVE, F. G. *et al. Blockchain e a revolução do consenso sob demanda*. Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC) – Minicursos, [S.l.], may 2018. Disponível em: http://143.54.25.88/index.php/sbrcminicursos/article/view/1770. Acesso em: 13 fev. 2021.

GUEDES, V. L.; BORSCHIVER, S. Bibliometria: uma ferramenta estatística para a gestão da informação e do conhecimento, em sistemas de informação, de comunicação e de avaliação científica e tecnológica. *Encontro Nacional de Ciência da Informação*, v. 6, p. 1-18, 2005.

GUZZINI, S. Structural power: the limits of neorealist power analysis. *International Organization*, v. 74, n. 3, p. 443-478, 1993. Disponível em: http://cadmus.eui.eu//handle/1814/23701.

HAASTER, J. van. Assessing Cyber Power. *In*: PISSANIDIS, N.; RÕIGAS, H.; VEENENDAAL, M. (Org.). *8th International Conference on Cyber Conflict*: Cyber Power. Tallinn: NATO CCD COE Publications, 2016. p. 7-21. Disponível em: https://ccdcoe.org/sites/default/files/multimedia/pdf/CyCon_2016_book.pdf.

HANSEN, L.; NISSENBAUM, H. Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, 2009.

HARZING, A. W.; ALAKANGAS, S. Google Scholar, Scopus and the Web of Science: a longitudinal and cross-disciplinary comparison. *Scientometrics*, v. 106, n. 2, p. 787-804, 2016.

HELMERICKS, S. G.; NELSEN, R. L.; UNNITHAN, N. P. The researcher, the topic, and the literature: A procedure for systematizing literature searches. *The Journal of Applied Behavioral Science*, v. 27, n. 3, p. 285-294, 1991.

HERRINGTON, L.; ALDRICH, R. The Future of Cyber-Resilience in an Age of Global Complexity. *Politics*, 2013.

HIRSCH, J. E. An index to quantify an individual's scientific research output. *Proceedings of the National academy of Sciences of the United States of America*, v. 102, n. 46, p. 165-69, 2005.

HISTORY.COM (ed.). *Arab Spring*. Disponível em: history.com/topics/middle-east/arab-spring

HUGHES, R. A treaty for cyberspace. *International Affairs*, 2010.

HUSSAIN, E. H. *International Studies Review*. 2013.

INKSTER, N. China in Cyberspace. *Survival*, 2010.

ISMAIL, S.; NASON, E.; MARJANOVIC, S.; GRANT, J. Bibliometrics as a tool for supporting prospective R&D decision-making in the health sciences: Strengths, weaknesses and options for future development. *Rand health quarterly*, v. 1, n. 4, 2012.

IZYCKI, E. Estratégias nacionais de segurança cibernética na América Latina Oportunidades para convergência de interesses e construção de consenso. Revista Iberica de Sistemas e Tecnologias de Informacao, 2018.

JUNIO, TJ. How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate. *Journal of Strategic Studies*, 2013.

KAZ, R.; CASADO, J. NSA e CIA mantiveram em Brasília equipe para coleta de dados filtrados de satélite. *Jornal O Globo*, 8 jul. 2013. Disponível em: https://oglobo.globo.com/mundo/nsa-cia-mantiveram-em-brasilia-equipe-para-coleta-de-dados-filtrados-de-satelite-8949723. Acesso em: 26 nov. 2019.

KELLO, L. The Meaning of the Cyber Revolution Perils to Theory and Statecraft. *International Security*, 2013.

KLIMBURG, A. Mobilising cyber power. *Survival*, 2011.

KOSTYUK, N.; ZHUKOV, Y. M. Invisible digital front: can cyber attacks shape battlefield events? *Journal of Conflict Resolution*, 2019.

KRISTENSEN, P. M. (2015). Revisiting the "American Social Science" – Mapping the Geography of International Relations. International Studies Perspectives, 16(3), 246-269.

LEMAY, A.; FERNANDEZA, J. M.; KNIGHT, S. Pinprick attacks, a lesser included case? *Conference on Cyber Conflict, Proceedings 2010*, 2010.

LIANG, L.; ZHONG, Z.; ROUSSEAU, R. Uncited papers, uncited authors and uncited topics: A case study in library and information science. *Journal of Informetrics*, v. 9, n. 1, p. 50-58, 2015.

LIFF, A. P. Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War. *Journal of Strategic Studies*, 2012.

LIMA, R. A.; VELHO, L. M. L. S.; DE FARIA, L. I. L. Bibliometria e "avaliação" da atividade científica: um estudo sobre o índice h. *Perspectivas em Ciência da Informação*, v. 17, n. 3, p. 3-17, 2012.

LINDSAY, J. R. Stuxnet and the Limits of Cyber Warfare. *Security Studies*, 2013.

LINDSAY, J. R. The Impact of China on Cybersecurity Fiction and Friction. *International Security*, 2014.

LINMANS, A. J. M. Why with bibliometrics the humanities does not need to be the weakest link. *Scientometrics*, v. 83, n. 2, p. 337-354, 2010.

LOBATO, L. C.; KENKEL, K. M. A ciberguerra é moderna! Uma Investigação sobre a relação entre tecnologia e modernização na guerra. *Contexto Int.* [online]. v. 37, n. 2, p. 629-660, 2015.

LOBATO, L. C.; KENKEL, K. M. Discourses of cyberspace securitization in Brazil and in the United States. *Revista Brasileira de Política Internacional*, v. 58, n. 2, p. 23-43, 2015. https://dx.doi.org/10.1590/0034-7329201500202.

LOPES, S.; COSTA, M. T.; FERNÁNDEZ-LLIMÓS, F.; AMANTE, M. J.; LOPES, P. F. A Bibliometria e a Avaliação da Produção Científica: indicadores e ferramentas. *In*: *Actas do Congresso Nacional de Bibliotecários, Arquivistas e Documentalistas*, n. 11, 2012 Oct.

LUPOVICI, A. The "Attribution Problem" and the Social Construction of "Violence": Taking Cyber Deterrence Literature a Step Forward. *International Studies Perspectives*, 2016.

LYNN, W. J. Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs*, v. 89, n. 5, p. 97-108, 2010. Disponível em: www.jstor.org/stable/20788647. Acesso em: 18 mar. 2021.

MACFARLANE, B. *Researching with integrity*: The ethics of academic inquiry. New York; London: Routledge, 2009.

MANJIKIAN, M. M. From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik. *International Studies Quarterly*, v. 54, n. 2, p. 381-401, 2010. Disponível em: www.jstor.org/stable/40664172.

MARIANO, A. M.; CRUZ, R. G.; GAITÁN, J. A. Meta-análises como instrumento de pesquisa: Uma revisão sistemática da bibliografia aplicada ao estudo das alianças estratégicas internacionais. *In*: *Congresso Internacional de Administração-Inovação Colaborativa e Competitividade*. 2011.

MARIANO, A. M.; ROCHA, M. S. Revisão da Literatura: Apresentação de uma Abordagem Integradora. *In*: *AEDM International Conference–Economy, Business and Uncertainty*: Ideas for a European and Mediterranean industrial policy. Reggio Calabria, Italia, 2017.

MARKOFF, J. Georgia takes a beating in the cyberwar with Russia. *The New York Times*, 11 Ago. 2008.

MCCARTHY, J.; MINSKY, M.; ROCHESTER, N.; SHANNON, C. E. A proposal for the Dartmouth Summer Research Project on Artificial Intelligence. ago. 1955. Disponível em: http://raysolomonoff.com/dartmouth/boxa/dart564props.pdf. Acesso em: 18 fev. 2021.

MCGRAW, G. Cyber War is Inevitable (Unless We Build Security In). *Journal of Strategic Studies*, 2013.

MCKITRICK, J.; BLACKWELL, J.; LITTLEPAGE, Fred; KRAUS, Georges, BLANCHFIELD, Richard; HILL, Dale. *The Battlefield of the Future*: 21st Century Warfare Issues. Cap. 3, p. 1. Air University. Disponível em: www.cdsar.af.mil/battle.bfoc.html.

MELZER, N. *Cyber Warfare and International Law*. Genebra, Unidir Resources: 2011. Disponível em: http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf.

MORAES, M.; FURTADO, R. L.; TOMAÉL, M. I. Redes de Citação: estudo de rede de pesquisadores a partir da competência em informação. *Em Questão*, Porto Alegre, v. 21, n. 2, p. 181-202, maio/ago. 2015.

MORAES, R. F. *Instituições de segurança e potências regionais*: a Organização para a Cooperação de Xangai (SCO) e a Comunidade Econômica dos Estados da África Ocidental (ECOWAS). 2010.

MUELLER, M.; SCHMIDT, A.; KUERBIS, B. Internet Security and Networked Governance in International Relations. *International Studies Review*, v. *15*, n. 1, p. 86-104, 2013.

MYERS, S. L. Cyberattack on Estonia stirs fear of 'virtual war'. *The New York Times Online*. Disponível em: Nationalgeographic.com/culture/topics/reference/arab-spring-cause. Acesso em: 18 maio 2007.

NATO. *Allied Joint Publication (AJP) 3.10*. Allied Joint Doctrine for Information Operations, 23 nov. 2009.

NOOHANI, M. Z.; MAGSI, K. U. *A Review Of 5G Technology*: Architecture, Security and wide Applications. International Research Journal of Engineering and Technology (IRJET), 2020. Disponível em: https://bit.ly/3amRDJQ. Acesso em: 29 mar. 2021.

NYE, J. *Cyberpower*. Cambridge: Belfer Center for Science and International Affairs. Harvard Kennedy School, 2010. Disponível em: www.belfercenter.org/sites/default/files/files/publication/cyber-power.pdf.

NYE, J. S. Deterrence and Dissuasion in Cyberspace. *International Security*, 2016

NYE, J. S. The future of power. New York: PublicAffairs, 2011.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE. Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution. Disponível em: < https://www.dni.gov/files/documents/ICA_2017_01.pdf>.

OHCHR; OHRLLS; UNDESA; UNEP; UNFPA. Global governance and governance of the global commons in the global partnership for development beyond 2015. Thematic Think Piece. 2013. Disponível em: <https://bit.ly/3mYf5Cg>.

OKOLI, C. A Guide to Conducting a Standalone Systematic Literature Review. Communications of the Association for Information Systems. 2015. p. 37. hal-01574600.

ONU. Carta das Nações Unidas. 1945. Disponível em: <http://www.onu.org.br/conheca-a-onu/documentos/>.Acesso em: 19/03/2021.

OTTIS, R. Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective. Tallinn: CCD COE, 2008. Disponível em: www.etis.ee/Portal/Publications.

OTTIS, R. From pitchforks to laptops: volunteers in cyber conflicts. *Conference on Cyber Conflict, Proceedings 2010*, 2010.

PETERSON, D. Offensive Cyber Weapons: Construction, Development, and Employment. *Journal of Strategic Studies*, 2013.

PIHELGAS, M. (ed.) *Mitigating risks arising from false-flag and no-flag cyber attacks*. CCDCOE, 2015.

REARDON, R; CHOUCRI, N. *The role of cyberspace in international relations*: a view of the literature. Paper prepared for the 2012 ISA Annual Convention, San Diego, CA, 2012.

RID, T. Cyber war will not take place. *Journal of Strategic Studies*, v. 35, p. 5-32, 2012. Disponível em: <www.tandfonline.com/doi/abs/10.1080/01402390.2011.608939>.

RID, T.; BUCHANAN, B. Attributing cyber attacks. *Journal of Strategic Studies*, 2015.

SANTORO, M; BORGES, B. Brazilian Foreign Policy Towards Internet Governance. Rev. Bras. Polít. Int., 60(1): e003, 2017.

SECHSER, T. S.; NARANG, N.; TALMADGE, C. Emerging technologies and strategic stability in peacetime, crisis, and war. *Journal of Strategic Studies*, 2019.

SCHNEIDER, J. The capability/vulnerability paradox and military revolutions: Implications for computing, cyber, and the onset of war. *Journal of Strategic Studies*, 2019.

SCHREIER. *On Cyberwarfare*. Genebra: Geneva Centre for the Democratic Control of Armed Forces (DCAF), 2015. Disponível em: www.dcaf.ch/Publications/On-Cyberwarfare.

SHAKARIAN, P. *The 2008 Russian Cyber Campaign Against Georgia*. Military Review, 2011.

SHARP, T. Theorizing cyber coercion: The 2014 North Korean operation against Sony. *Journal of Strategic Studies*, 2017.

SIEDLER, R. E. Hard Power in Cyberspace: CNA as a Political Means. *In*: PISSANIDIS, N.; RÕIGAS, H.; VEENENDAAL, M. (org.). *8th International Conference on Cyber Conflict*: Cyber Power. Tallinn: NATO CCD COE Publications, 2016. p. 23-36. Disponível em: https://ccdcoe.org/sites/default/files/multimedia/pdf/CyCon_2016_book.pdf.

SLAYTON, R. What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment. *International Security*, 2016.

SMEETS, M. A matter of time: On the transitory nature of cyberweapons. *Journal of Strategic Studies*, 2018.

SOUZA, M. T.; SILVA, M. D.; CARVALHO, R. Revisão integrativa: o que é e como fazer. *Einstein*, v. 8, n. 1, pt. 1, p. 102-6, 2010.

STAUFFACHER, D. *UN GGE and UN OEWG*: How to live with two concurrent UN Cybersecurity processes. Remarks for the ICT4Peace to Jeju Forum. May 2019.

STODDART, K. UK cyber security and critical national infrastructure protection. *International Affairs*, 2016.

STONE, J. Cyber war will take place! *Journal of Strategic Studies*, 2013.

STUENKEL, O. *O mundo pós-ocidental*: potências emergentes e a nova ordem global. Rio de Janeiro: Zahar, 2018.

TOR, U. "Cumulative Deterrence" as a New Paradigm for Cyber Deterrence. *Journal of Strategic Studies*, 2017.

U.S. OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE. *Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections*. 6 jan. 2017. Disponível em: www.dni.gov/files/documents/ICA_2017_01.pdf.

UNITED NATIONS GENERAL ASSEMBLY (UNGA). Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/65/201, 30 de julho de 2010. Disponível em: < https://eucyberdirect.eu/wp-content/uploads/2019/10/ungge2010.pdf >.

UNGA. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98*, 24 de junho de 2013. Disponível em: < https://eucyberdirect.eu/wp-content/uploads/2019/10/ungge-2013.pdf>.

UNGA. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, 22 de julho de 2015. Disponível em: < https://undocs.org/A/70/174>

UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH UNIDIR. *The Cyber Index*. International Security Trends and Realities. Nova York; Genebra, 2013. Disponível em: www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf.

VALERIANO, B.; MANESS, R. The dynamics of cyber conflict between rival antagonists, 2001-11. *Journal of Peace Research*, v. 51, p. 347, 2014. Originally published online 1 Apr. 2014.

VAN ECK, N J; WALTMAN, L. Manual for VOSviewer version 1.6.11. Universiteit Leiden. 2019.

VAN LEEUWEN, T. N. The application of bibliometric analyses in the evaluation of social science research. Who benefits from it, and why it is still feasible. *Scientometrics*, v. 66, n. 1, p. 133-154, 2006.

WHITE HOUSE. *International Strategy for Cyberspace*. 2011. Disponível em: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf. Acesso em: 26 mar. 2021.

WILSHUSEN, G. C. *Cyber security*: continued attention needed to protect our nation's critical infrastructure and federal information systems. Testimony before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Committee on Homeland Security, House of Representatives. Washington DC: US Government Accountability Office, 16 mar. 2011.

WILSON, M. I.; COREY, K. *The role of ICT in Arab Spring Movements 2012 netcom*.

ANEXOS

ANEXO I – APRESENTAÇÃO DA AMOSTRA BIBLIOGRÁFICA INICIAL

A Tabela 12 apresenta a amostra bibliográfica inicial, cujos dados bibliométricos foram analisados quantitativamente no capítulo 1.

Tabela 12 – Amostra bibliográfica inicial

Autor	Título	Publicação	Ano
Gordon, D	Where in the (Cyber) world is Carlos Salinas?	Bulletin of the atomic scientists	1996
Marks, AF	Social science networking in a changing Europe	Information dissemination and access in Russia and eastern Europe: problems and solutions in east and west	1998
Cooper, J	New skills for cyber diplomats	World today	1999
Smith, R	Fit to govern?	World today	2000
Bunker, RJ	Weapons of Mass Disruption and Terrorism	Terrorism and political violence	2000
Grove, GD; Goodman, SE; Lukasik, SJ	Cyber-attacks and international law	Survival	2000
Cuellar, MF	The civil aviation analogy - Part III - Past as prologue: International aviation security treaties as precedents for international cooperation against cyber terrorism and cyber crimes	Transnational dimension of cyber crime and terrorism	2001
Sofaer, AD	Toward an international convention on cyber security	Transnational dimension of cyber crime and terrorism	2001
Sofaer, AD; Grove, GD; Wilson, GD	Draft international convention to enhance protection from cyber crime and terrorism	Transnational dimension of cyber crime and terrorism	2001
Goodman, SE	The civil aviation analogy - Part I - International cooperation to protect civil aviation against cyber crime and terrorism	Transnational dimension of cyber crime and terrorism	2001
Putnam, TL; Elliott, DD	International responses to cyber crime	Transnational dimension of cyber crime and terrorism	2001
Whiteman, HH	The civil aviation analogy - Part II - Cyber terrorism and civil aviation	Transnational dimension of cyber crime and terrorism	2001
Sofaer, AD; Goodman, SE	Cyber crime and security - The transnational dimension	Transnational dimension of cyber crime and terrorism	2001
Adams, J	Virtual defense	Foreign affairs	2001
Hachigian, N	China's cyber-strategy	Foreign affairs	2001
Kamal, A	New forms of confrontation: Cyber-terrorism and cyber-crime	International seminar on nuclear war and planetary emergencies - 27th session	2003

Salvador, T; Sherry, JW; Urrutia, AE	Less cyber, more cafe - Design implications for easing the digital divide with locally social cyber cafes	Organizational information systems in the context of globalization	2003
Gallemore, C	Of lords and (cyber)serfs: eGovernment and poststructuralism in a neomedieval Europe	Millennium-journal of international studies	2005
Hung, CF	The politics of cyber participation in the PRC: The implications of contingency for the awareness of citizens' rights	Issues & studies	2006
Power, M	Digitized virtuosity: Video war games and post-9/11 cyber-deterrence	Security dialogue	2007
Minchev, Z; Shalamanov, V	Operational analysis support to energy security in South East Europe: a Bulgarian academic community approach	Energy security: international and local issues, theoretical perspectives, and critical energy infrastructures	2008
Umbach, F; Nerlich, U	Asset criticality in European gas pipeline systems - increasing challenges for NATO, its Member States and industrial protection of critical energy infrastructure	Energy security: international and local issues, theoretical perspectives, and critical energy infrastructures	2008
Umberger, H; Gheorghe, A	Cyber security: threat identification, risk and vulnerability assessment	Energy security: international and local issues, theoretical perspectives, and critical energy infrastructures	2008
Deibert, RJ	Cyber-Security and Threat Politics: US Efforts to Secure the Information Age	International studies review	2009
Westby, J	Stability inspite of cyber war What would be necessary for peace in the digital area	Internationale politik	2009
Cioaca, C	The importance and role of nato in cyber-security	15th international conference the knowledge-based organization: military sciences. security and defense, conference proceedings 1	2009
Cotoara-Nicolae, A; Nastasescu, V; Barbu, C	Technical and technological dimension of security and defence	15th international conference the knowledge-based organization: military sciences. security and defense, conference proceedings 1	2009
Whelan, R	Proceedings of the NATO Advanced Research Workshop on Responses to Cyber Terrorism	Terrorism and political violence	2009
Weitz, R	China, Russia, and the Challenge to the Global Commons	Pacific focus	2009
Hansen, L; Nissenbaum, H	Digital Disaster, Cyber Security, and the Copenhagen School	International studies quarterly	2009
Kaminski, RT	Escaping the cyber state of nature: cyber deterrence and international institutions	Conference on cyber conflict, proceedings 2010	2010
David-West, A	Alleged North Korean Cyber Attacks Unconfirmed	North Korean review	2010
[Anonymous]	Cyberterrorism: The Invisible Threat Stealth Cyber Predators in a Climate of Escalating Risk	Foreign affairs	2010
Starr, S; Kuehl, D; Pudas, T	Perspectives on building a cyber force structure	Conference on cyber conflict, proceedings 2010	2010

Carver, T	Materializing the Metaphors of Global Cities: Singapore and Silicon Valley	Globalizations	2010
Bernier, M; Treurniet, J	Understanding cyber operations in a canadian strategic context: more than C4ISR, more than CNO	Conference on cyber conflict, proceedings 2010	2010
Kirt, T; Kivimaa, J	Optimizing it security costs by evolutionary algorithms	Conference on cyber conflict, proceedings 2010	2010
Hare, F	The cyber threat to national security: why can't we agree?	Conference on cyber conflict, proceedings 2010	2010
Lorents, P; Ottis, R	Knowledge based framework for cyber weapons and conflict	Conference on cyber conflict, proceedings 2010	2010
Liles, S	Cyber warfare: as a form of low-intensity conflict and insurgency	Conference on cyber conflict, proceedings 2010	2010
Lemay, A; Fernandeza, JM; Knight, S	Pinprick attacks, a lesser included case?	Conference on cyber conflict, proceedings 2010	2010
Ottis, R	From pitchforks to laptops: volunteers in cyber conflicts	Conference on cyber conflict, proceedings 2010	2010
Kotenko, I; Konovalov, A; Shorov, A	Agent-based modeling and simulation of botnets and botnet defense	Conference on cyber conflict, proceedings 2010	2010
Inkster, N	China in Cyberspace	Survival	2010
Hung, CF	China's Propaganda in the Information Age: Internet Commentators and the Weng'an Incident	Issues & studies	2010
Yost, DS	NATO's evolving purposes and the next Strategic Concept	International affairs	2010
Hughes, R	A treaty for cyberspace	International affairs	2010
Lynn, WJ	Defending a New Domain The Pentagon's Cyberstrategy	Foreign affairs	2010
Repez, F; Deaconu, G	Cyber attacks - unprecedented threat to security	Proceedings international conference military science universe, selected papers	2011
Gaycken, S	Get Cyber Real!	Survival	2011
Tikk, E	Get Cyber Real! Reply	Survival	2011
Gaycken, S	Computer Wars Why is it so difficult to protect against military Cyber attacks	Internationale politik	2011
Platt, V	Still the fire-proof house? An analysis of Canada's cyber security strategy	International journal	2011
Tertrais, B	Cyber War: The Next Threat to National Security and What To Do About It	Survival	2011
Zelin, AY	Internationa Press News form Cyber-Dschihadistan Global or local act - that is the Debate since 9/11	Internationale politik	2011
Jurjan, I	New trends in terrorism	17th international conference the knowledge-based organization, conference proceedings 1: management and military sciences	2011

Kis, A	The human security as global common	17th international conference the knowledge-based organization, conference proceedings 1: management and military sciences	2011
Stoica, M; Nemes, A	Romania's involment in the fight against terorrism	17th international conference the knowledge-based organization, conference proceedings 1: management and military sciences	2011
Michael, G	Cyber War: The Next Threat to National Security and What To Do About It	Terrorism and political violence	2011
de la Roche, AB	Space, security and resilience: Reflections on the debate	Space policy	2011
Vacca, WA	Military Culture and Cyber Security	Survival	2011
Deibert, R	Ronald Deibert: Tracking the emerging arms race in cyberspace	Bulletin of the atomic scientists	2011
Tikk, E	Ten Rules for Cyber Security	Survival	2011
Weimann, G	Cyber-Fatwas and Terrorism	Studies in conflict & terrorism	2011
Klimburg, A	Mobilising Cyber Power	Survival	2011
Farwell, JP; Rohozinski, R	Stuxnet and the Future of Cyber War	Survival	2011
Gercke, M	Legal Responses to Terrorist Use of the Internet	Enhancing cooperation in defence against terrorism	2012
Bronk, C; Monk, C; Villasenor, J	The Dark Side of Cyber Finance	Survival	2012
Bendiek, A; Wagner, B	The Constitution of the Internet The EU needs to develop a common Strategy for Cyber Security	Internationale politik	2012
Lin, H	A virtual necessity: Some modest steps toward greater cybersecurity	Bulletin of the atomic scientists	2012
Choucri, N; Goldsmith, D	Lost in cyberspace: Harnessing the Internet, international relations, and global security	Bulletin of the atomic scientists	2012
Chang, LYC	Responsive Regulation and the Reporting of Information Security Incidents-Taiwan and China	Issues & studies	2012
Handler, SG	The new cyber face of battle: developing a legal approach to accommodate emerging trends in warfare	Stanford journal of international law	2012
Farwell, JP; Rohozinski, R	The New Reality of Cyber War	Survival	2012
Deibert, RJ; Rohozinski, R; Crete-Nishihata, M	Cyclones in cyberspace: Information shaping and denial in the 2008 Russia-Georgia war	Security dialogue	2012
Liff, AP	Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War	Journal of strategic studies	2012
Ortega-Ruiz, R; Del Rey, R; Casas, JA	Knowing, Building and Living Together on Internet and Social Networks: The ConRed Cyberbullying Prevention Program	International journal of conflict and violence	2012
Rid, T	Cyber War Will Not Take Place	Journal of strategic studies	2012

Young-do, K; Jin-sung, K; Kyung-ho, L	Major Issues of the National Cyber Security System in South Korea, and its Future Direction	Korean journal of defense analysis	2013
Carr, J	The misunderstood acronym: Why cyber weapons aren't WMD	Bulletin of the atomic scientists	2013
Tertrais, B	Cyber War Will Not Take Place	Survival	2013
Johnsen, R	Cyber Warfare and defence operational capability	Internasjonal politikk	2013
Lango, HI	The academic debate on cyber security	Internasjonal politikk	2013
Kritsiotis, D	Enforced Equations	European journal of international law	2013
Sandvik, KB	Cyber War and International law	Internasjonal politikk	2013
Kaufmann, M	Cyber-resilience in the EU	Internasjonal politikk	2013
Mitchell, PT	Cyberspace and the State: Toward a Strategy for Cyber-Power	Journal of strategic studies	2013
Nye, JS	From bombs to bytes: Can our nuclear history inform our cyber future?	Bulletin of the atomic scientists	2013
de la Roche, AB	The merger of two global commons: The need for new governance	Space policy	2013
Liff, AP	The Proliferation of Cyberwarfare Capabilities and Interstate War, Redux: Liff Responds to Junio	Journal of strategic studies	2013
Cardash, SL; Cilluffo, FJ; Ottis, R	Estonia's Cyber Defence League: A Model for the United States?	Studies in conflict & terrorism	2013
Inkster, N	Chinese Intelligence in the Cyber Age	Survival	2013
Rid, T	More Attacks, Less Violence	Journal of strategic studies	2013
Segal, A	The code not taken: China, the United States, and the future of cyber espionage	Bulletin of the atomic scientists	2013
Brenner, JF	Eyes wide shut: The growing threat of cyber attacks on industrial control systems	Bulletin of the atomic scientists	2013
Messerschmidt, JE	Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm Shearman & Sterling Student Writing Prize in Comparative and International Law, Outstanding Note Award	Columbia journal of transnational law	2013
Goldsmith, J	How Cyber Changes the Laws of War	European journal of international law	2013
Herrington, L; Aldrich, R	The Future of Cyber-Resilience in an Age of Global Complexity	Politics	2013
Junio, TJ	How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate	Journal of strategic studies	2013
McGraw, G	Cyber War is Inevitable (Unless We Build Security In)	Journal of strategic studies	2013
Peterson, D	Offensive Cyber Weapons: Construction, Development, and Employment	Journal of strategic studies	2013
Stone, J	Cyber War Will Take Place!	Journal of strategic studies	2013

Betz, DJ; Stevens, T	Analogical reasoning and cyber security	Security dialogue	2013
Mueller, M; Schmidt, A; Kuerbis, B	Internet Security and Networked Governance in International Relations	International studies review	2013
Bronk, C; Tikk-Ringas, E	The Cyber Attack on Saudi Aramco	Survival	2013
Cavelty, MD	From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse	International studies review	2013
Kello, L	The Meaning of the Cyber Revolution Perils to Theory and Statecraft	International security	2013
Lindsay, JR	Stuxnet and the Limits of Cyber Warfare	Security studies	2013
Bicakci, S	NATO's Emerging Threat Perception: Cyber Security in the 21st Century	Uluslararasi iliskiler-international relations	2014
Holt, MW	Aligning National Cyber Security Strategies to International Guidance: A First Step Toward Improving Incident Response Capabilities Across NATO	Best practices in computer network defense: incident detection and response	2014
Kello, L	Correspondence A Cyber Disagreement Reply	International security	2014
Kelly, PJ	Cyber war will not take place	International affairs	2014
Bentley, D	Cyber operations and the use of force in international law	International affairs	2014
Lindner, F; Gaycken, S	Back to Basics: Beyond Network Hygiene	Best practices in computer network defense: incident detection and response	2014
Kruidhof, O	Evolution of National and Corporate CERTs - Trust, the Key Factor	Best practices in computer network defense: incident detection and response	2014
Rigoni, A; Lindstrom, G	Computer Network Defense: New Threats and Trends	Best practices in computer network defense: incident detection and response	2014
van den Heuvel, E; Baltink, GK	Coordination and Cooperation in Cyber Network Defense: the Dutch Efforts to Prevent and Respond	Best practices in computer network defense: incident detection and response	2014
McMahon, D	Beyond Perimeter Defense: Defense-in-Depth Leveraging Upstream Security	Best practices in computer network defense: incident detection and response	2014
Stewart, JN	Advanced Technologies/Tactics Techniques, Procedures: Closing the Attack Window, and Thresholds for Reporting and Containment	Best practices in computer network defense: incident detection and response	2014
McGuffin, C; Mitchell, P	On domains: Cyber and the practice of warfare	International journal	2014
Lindsay, JR	Correspondence A Cyber Disagreement	International security	2014
Horowitz, MC	Coming next in military tech	Bulletin of the atomic scientists	2014
Allenby, BR	Are new technologies undermining the laws of war?	Bulletin of the atomic scientists	2014
Purser, S	Standards for Cyber Security	Best practices in computer network defense: incident detection and response	2014

Rosenzweig, P	International law and private actor active cyber defensive measures	Stanford journal of international law	2014
Baldino, D; Goold, J	Iran and the emergence of information and communications technology: the evolution of revolution?	Australian journal of international affairs	2014
Eichensehr, KE	Tallinn Manual on the International Law Applicable to Cyber Warfare	American journal of international law	2014
Chenou, JM	From Cyber-Libertarianism to Neoliberalism: Internet Exceptionalism, Multi-stakeholderism, and the Institutionalisation of Internet Governance in the 1990s	Globalizations	2014
Gompert, DC; Libicki, M	Cyber Warfare and Sino-American Crisis Instability	Survival	2014
Shackelford, SJ; Craig, AN	Beyond the new "digital divide": analyzing the evolving role of national governments in internet governance and enhancing cybersecurity	Stanford journal of international law	2014
Valeriano, B; Maness, RC	The dynamics of cyber conflict between rival antagonists, 2001-11	Journal of peace research	2014
Lindsay, JR	The Impact of China on Cybersecurity Fiction and Friction	International security	2014
Farwell, JP	The Media Strategy of ISIS	Survival	2014
Bauman, Z; Bigo, D; Esteves, P; Guild, E; Jabri, V; Lyon, D; Walker, RBJ	After Snowden: Rethinking the Impact of Surveillance	International political sociology	2014
Khan, Z	Strategizing Cyber Revolution within the Domain of Security Studies	Ipri journal	2015
Brill, A	The Use of Internet Technology by Cyber Terrorists & Cyber Criminals: The 2014 Report	Terrorist use of cyberspace and cyber terrorism: new challenges and responses	2015
Houston, N	How Human Issues Impact Confronting Cyber Terrorism	Terrorist use of cyberspace and cyber terrorism: new challenges and responses	2015
Mele, S	The Italian Strategic Response Against Cyber Threats and the Terrorist Use of Cyberspace	Terrorist use of cyberspace and cyber terrorism: new challenges and responses	2015
Houston, N	Cultural Aspects of Information Sharing and Collaboration	Terrorist use of cyberspace and cyber terrorism: new challenges and responses	2015
Freedman, LD	Cyber Blockades	Foreign affairs	2015
Schmitt, MN	The law of cyber targeting	Naval war college review	2015
Lindsay, JR	Debating the Chinese Cyber Threat Reply	International security	2015
Meyer, P	Seizing the Diplomatic Initiative to Control Cyber Conflict	Washington quarterly	2015
Tripathi, S	Cyber: Also a Domain of War and Terror	Strategic analysis	2015

Kallberg, J	Bringing Fear to the Perpetrators: Humanitarian Cyber Operations as Evidence Gathering and Deterrence	Strategic analysis	2015
Borah, CK	Cyber war: the next threat to national security and what to do about it?	Strategic analysis	2015
Marguery, T; Summers, S	The Emergence of EU Criminal Law. Cyber Crime and the Regulation of the Information Society	Common market law review	2015
Dortmans, PJ; Thakur, N; Ween, A	Conjectures for framing cyberwarfare	Defence and security analysis	2015
Chiesa, R	Cyber-Attacking a Country: What Terrorists Haven't Done So Far (and they could do)	Terrorist use of cyberspace and cyber terrorism: new challenges and responses	2015
Macdonald, S	Assessing and Responding to the Cyberterrorism Threat	Terrorist use of cyberspace and cyber terrorism: new challenges and responses	2015
Shore, JJM	An Obligation to Act: Holding Government Accountable for Critical Infrastructure Cyber Security	International journal of intelligence and counterintelligence	2015
Brill, A	Virtual Currencies and Terrorist Financing: Basics for Anti-Terrorist Professionals	Terrorist use of cyberspace and cyber terrorism: new challenges and responses	2015
Parker, GN	The Terror Next Door: A Security Analysis of the Escalating Threat of Lone Wolf Terrorists	Lone actors - an emerging security threat	2015
Gordon, T; Sharan, Y; Florescu, E	Possible Evolution of Lone Wolf and SIMAD Terrorism	Lone actors - an emerging security threat	2015
Simonovski, I	The Use Of Cyber Space For Terrorist Purposes - With Special Reference To The Financing Terrorist Activity	Terrorist use of cyberspace and cyber terrorism: new challenges and responses	2015
Antinori, A	Gen-T. Terrorist Infosphere and i-Volution of Lone Wolf Terrorism	Lone actors - an emerging security threat	2015
Zweig, E	From Al-Qaeda To The Islamic State (ISIS), Jihadi Groups Engage in Cyber Jihad: Beginning with 1980s Promotion Of Use Of 'Electronic Technologies' Up To Today's Embrace Of Social Media to Attract A New Jihadi Generation	Terrorist use of cyberspace and cyber terrorism: new challenges and responses	2015
Minchev, Z	Human Factor Dual Role in Modern Cyberspace Social Engineering	Terrorist use of cyberspace and cyber terrorism: new challenges and responses	2015
Geun-hye, K; Kyung-bok, L; Jong-in, L	CBMs for Cyberspace beyond the Traditional Security Environment: Focusing on Features for CBMs for Cyberspace in Northeast Asia	Korean journal of defense analysis	2015
Lobato, LC; Kenkel, KM	Discourses of cyberspace securitization in Brazil and in the United States	Revista brasileira de politica internacional	2015
Allenby, BR	The paradox of dominance: The age of civilizational conflict	Bulletin of the atomic scientists	2015
Kavanagh, C	Cybersecurity, Sovereignty, and U.S. Foreign Policy	American foreign policy interests	2015
Brenner, J; Lindsay, JR	Debating the Chinese Cyber Threat	International security	2015

Brocato, AL	Tackling Terrorists' Use of the Internet: Propaganda Dispersion & the Threat of Radicalization	Terrorist use of cyberspace and cyber terrorism: new challenges and responses	2015
Pyung-Kyun, W	The Russian Hybrid War in the Ukraine Crisis: Some Characteristics and Implications	Korean journal of defense analysis	2015
Gross, O	Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents	Cornell international law journal	2015
Cavaiola, LJ; Gompert, DC; Libicki, M	Cyber House Rules: On War, Retaliation and Escalation	Survival	2015
Daugirdas, K; Mortenson, JD	United States Responds to Alleged North Korean Cyber Attack on Sony Pictures Entertainment	American journal of international law	2015
Pace, S	Security in space	Space policy	2015
Gompert, DC; Libicki, M	Waging Cyber War the American Way	Survival	2015
Inkster, N	Cyber Attacks in La-La Land	Survival	2015
Yong-joon, L; Hyuk-jin, K; Jaeil, L; Dong-kyoo, S	Development of Countermeasures against North Korean Cyberterrorism through Research Case Studies	Korean journal of defense analysis	2015
Roislien, HE	When The Generation Gap Collides With Military Structure: The Case of Norwegian Cyber Officers	Journal of military and strategic studies	2015
Argomaniz, J	European Union responses to terrorist use of the Internet	Cooperation and conflict	2015
Cornish, P	Governing Cyberspace through Constructive Ambiguity	Survival	2015
Nocetti, J	Contest and conquest: Russia and global internet governance	International affairs	2015
Carr, M	Power Plays in Global Internet Governance	Millennium-journal of international studies	2015
Gartzke, E; Lindsay, JR	Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace	Security studies	2015
Rid, T; Buchanan, B	Attributing Cyber Attacks	Journal of strategic studies	2015
Burke, I; van Heerden, RP	Automating Cyber Offensive Operations for Cyber Challenges	Proceedings of the 11th international conference on cyber warfare and security (ICCWS 2016)	2016
Gudgel, JE	Cyber War versus Cyber Realities: Cyber Conflict in the International System	Small wars and insurgencies	2016
Nocetti, J	Cyber war versus cyber realities: cyber conflict in the international system	International affairs	2016
Teodor, M; Teodor, BA	Cyber Threats in Hybrid Warfare: the Ukrainian Case	Countering hybrid threats: lessons learned from Ukraine	2016
Hiller, B	Cyber Security and CIP: A Potential Role for OSCE	Critical infrastructure protection against hybrid warfare security related challenges	2016
Lehto, M; Limnell, J	Cyber Security Capability and the Case of Finland	Proceedings of the 15th European conference on cyber warfare and security (ECCWS 2016)	2016

Tatar, U; Karabacak, B; Gheorghe, A	An Assessment Model to Improve National Cyber Security Governance	Proceedings of the 11th international conference on cyber warfare and security (ICCWS 2016)	2016
Lehto, M	Theoretical Examination of the Cyber Warfare Environment	Proceedings of the 11th international conference on cyber warfare and security (ICCWS 2016)	2016
Alzoubaidi, AR; Prodan-Palade, D; Ekici, S	Terrorist Recruitment and Counter Measures in the Cyber World	Countering terrorist recruitment in the context of armed counter-terrorism operations	2016
Harry, C	A Framework for Categorizing Disruptive Cyber Activity and Assessing its Impact	Proceedings of the 11th international conference on cyber warfare and security (ICCWS 2016)	2016
Young-ju, L	Establishment of a Feasible Cyber Organization Structure to Enhance the Capabilities of Cyberspace Operations in the ROK's Defense Forces	Korean journal of defense analysis	2016
Greiman, V	Cyberwarfare: From the Trenches to the Clouds	Proceedings of the 11th international conference on cyber warfare and security (ICCWS 2016)	2016
Ormrod, D; Turnbull, B	The Military Cyber-Maturity Model: Preparing Modern Cyber-Enabled Military Forces for Future Conflicts	Proceedings of the 11th international conference on cyber warfare and security (ICCWS 2016)	2016
Ivers, A; Segal, A	Adam Segal: Life in the hacked world order	Bulletin of the atomic scientists	2016
Huttenlocher, E	Cyber-Warfare and Cyber-Terrorism: Step to Learning to Knowing the Difference	Proceedings of the 11th international conference on cyber warfare and security (ICCWS 2016)	2016
Machin, N; Gazapo, M	Cybersecurity as a critical factor for the Security of the European Union	Revista Unisci	2016
Baldassarre, G	Critical Infrastructure Protection Against Hybrid Warfare Security Related Challenges	Critical infrastructure protection against hybrid warfare security related challenges	2016
Zholdoshbaev, R	Assessing the Risks of Cyber Terrorism in Central Asian countries	Countering terrorist recruitment in the context of armed counter-terrorism operations	2016
Duvenage, P; Jaquire, V; von Solms, S	Conceptualising Cyber Counterintelligence: Two Tentative Building Blocks	Proceedings of the 15th European conference on cyber warfare and security (ECCWS 2016)	2016
Allenby, B	Cyber-Humans: Our Future with Machines	Bulletin of the atomic scientists	2016
Cuozzo, G	Critical Infrastructure Cyber-Attack Through Firmware Exploitation	Critical infrastructure protection against hybrid warfare security related challenges	2016
Rid, T	Dark Territory: The Secret History of Cyber War	Survival	2016
Kallberg, J	Assessing India's Cyber Resilience: Institutional Stability Matters	Strategic analysis	2016
Goychayev, R	On International Cooperation in Nuclear and Cyber Security	Peace review-a journal of social justice	2016
Nocetti, J	The real cyber war: the political economy of internet freedom	International affairs	2016
Kuusisto, T; Kuusisto, R	Leadership for Cyber Security in Public-Private Relations	Proceedings of the 15th European conference on cyber warfare and security (ECCWS 2016)	2016

Deschaux-Dutard, D	Cyber security in the European Union: resilience and adaptability in governance policy	International affairs	2016
Ionatamishvili, EL; Svetoka, S	Strategic Communications and Social Media in the Russia-Ukraine Conflict	Critical infrastructure protection against hybrid warfare security related challenges	2016
Couzigou, I	The Challenges Posed by Cyber-Attacks to the Law on Self-Defence	International law and..., vol. 5	2016
Black, K; David, M	War in 1s and 0s: Framing the Lexicon for the Digital age	Proceedings of the 11th international conference on cyber warfare and security (ICCWS 2016)	2016
Au, H; Diallo, M; Lee, K	Multi-Stage Analysis of Intrusion Detection Logs for Quick Impact Assessment	Proceedings of the 15th European conference on cyber warfare and security (ECCWS 2016)	2016
Mohideen, F	The Cyber-Security State of our Nation: A Critique of South Africa's Stance on Cyber-Security in Respect of the Protection of Critical Information Infrastructure	Proceedings of the 11th international conference on cyber warfare and security (ICCWS 2016)	2016
Chen, J; Duvall, G	On Dynamic Cyber Defense and its Improvement	Proceedings of the 11th international conference on cyber warfare and security (ICCWS 2016)	2016
Pawlak, P	Capacity Building in Cyberspace as an Instrument of Foreign Policy	Global policy	2016
Holczer, T; Gazdag, A; Miru, G	Intrusion Detection in Cyber Physical Systems Based on Process Modelling	Proceedings of the 15th european conference on cyber warfare and security (ECCWS 2016)	2016
Efthymiopoulos, MP	Cyber Security in Smart City of Dubai	Proceedings of the 11th international conference on cyber warfare and security (ICCWS 2016)	2016
Lynton, E; Gullion, JG; Williams, JL	Countering Terrorist Recruitment: Social Media, Cyber Terror, and Peaceful Platforms	Countering terrorist recruitment in the context of armed counter-terrorism operations	2016
Mileham, P	Human conflict and universal ethics (part 2)	Defence and security analysis	2016
Church, A	Military Strategy as a Guide for Cybersecurity	Proceedings of the 15th European conference on cyber warfare and security (ECCWS 2016)	2016
Glezos, S	Virtuous networks: Machiavelli, speed and global social movements	International politics	2016
Van Vuuren, JCJ; Plint, G; Leenen, L; Zaaiman, J; Kadyamatimbaand, A; Phahlahmohlaka, J	Building Blocks for National Cyberpower	Proceedings of the 11th international conference on cyber warfare and security (ICCWS 2016)	2016
Chen, C	Opportunities and Challenges Faced by the Belt and Road in the Era of Big Data	Proceedings of symposium of policing diplomacy and the belt & road initiative, 2016	2016
Boettinger, K; Hansch, G; Filipovic, B	Detecting and Correlating Supranational Threats for Critical Infrastructures	Proceedings of the 15th European conference on cyber warfare and security (ECCWS 2016)	2016
Yucel, C; Koltuksuz, A; Yagci, H	Clandestine Cell Based Honeypot Networks	Proceedings of the 15th European conference on cyber warfare and security (ECCWS 2016)	2016
Falk, C	An Ontology for Threat Intelligence	Proceedings of the 15th European conference on cyber warfare and security (ECCWS 2016)	2016

Sample, C; John, M	Cultural Comparison Between and Attackers and Victims	Proceedings of the 15th European conference on cyber warfare and security (ECCWS 2016)	2016
Hurley, J; Watkins, L; Wendt, V; Gravattand, A; McGibbon, M	Quantifying Decision Making in the Critical Infrastructure	Proceedings of the 11th international conference on cyber warfare and security (ICCWS 2016)	2016
Hurley, J; Watkins, L	Cyberspace: The new Battlefield	Proceedings of the 11th international conference on cyber warfare and security (ICCWS 2016)	2016
Polunina, O	Cyberwarfare as a new Challenge for Latin America	Proceedings of the 11th international conference on cyber warfare and security (ICCWS 2016)	2016
Cavallaro, F; Chiappetta, A; De Santis, M; Pinnarelli, A	Critical Infrastructure Protection: Smart Grids	Critical infrastructure protection against hybrid warfare security related challenges	2016
Schmidt-Felzmann, A	Sweden Under Attack! Lessons from Past Incidents for Coping with a Comprehensive Synchronized Attack on Critical Energy and Information Infrastructure	Critical infrastructure protection against hybrid warfare security related challenges	2016
Jaitner, ML; Kantola, H	Reflexive Control in Cyber Space	Proceedings of the 15th European conference on cyber warfare and security (ECCWS 2016)	2016
Rovinskaya, TL	Establishment of the "pirate movement" in the USA	Mirovaya ekonomika i mezhdunarodnye otnosheniya	2016
Surma, I	Pushing the Boundaries of Digital Diplomacy: The International Experience and the Russian Practice	Proceedings of the 11th international conference on cyber warfare and security (ICCWS 2016)	2016
Kobek, LP; Caldera, E	Cyber Security and Habeas Data:The Latin American Response to Information Security and Data Protection	Oasis-observatorio de analisis de los sistemas internacionales	2016
Bryant, I; Maple, C; Watson, T	A Cross-Disciplinary Approach to Modelling and Expressing Adversity	Proceedings of the 15th European conference on cyber warfare and security (ECCWS 2016)	2016
Enache, AC; Sgarciu, V	Designing Real-Time Anomaly Intrusion Detection Through Artificial Immune Systems	Proceedings of the 15th European conference on cyber warfare and security (ECCWS 2016)	2016
Dvorak, M	A Method to Generate SQL Queries Filtering Rules in SIEM Systems	Proceedings of the 15th European conference on cyber warfare and security (ECCWS 2016)	2016
Mar'yasis, DA	Spheres of innovative breakthrough in Israel	Mirovaya ekonomika i mezhdunarodnye otnosheniya	2016
Nagaraj, SK; Bryant, A	Barriers to Extending Malware Detection Research	Proceedings of the 11th international conference on cyber warfare and security (ICCWS 2016)	2016
Sun, NX	Piercing the veil of national security: does China's banking it security regulation violate the tbt agreement?	Asian journal of WTO & international health law and policy	2016
Coldea, F	Building National Capabilities and Countering Hybrid Threats: Lessons Learned	Countering hybrid threats: lessons learned from Ukraine	2016
Heydari, V; Yoo, SM	Securing Critical Infrastructure by Moving Target Defense	Proceedings of the 11th international conference on cyber warfare and security (ICCWS 2016)	2016

Dvorak, J; Konecny, J; Jankova, M	Options of risk modelling in limit situations of a learning organization	Proceedings of the 11th international scientific conference public administration 2016	2016
Shalamanov, V; Minchev, Z	Terrorist Organizations Recruitment Success Reduction in Support to NATO's Operations: CIMIC IT Tools	Countering terrorist recruitment in the context of armed counter-terrorism operations	2016
Shapiro, J	Russian Hybrid Warfare: Not New, Well-Accomplished, and Limited in Scope	Countering hybrid threats: lessons learned from Ukraine	2016
Filiol, E; Gallais, C	Combinatorial Optimization of Operational (Cyber) Attacks Against Large-Scale Critical Infrastructures: The Vertex Cover Approach	Proceedings of the 11th international conference on cyber warfare and security (ICCWS 2016)	2016
Chen, J; Dinerman, A	On Cyber Dominance in Modern Warfare	Proceedings of the 15th European conference on cyber warfare and security (ECCWS 2016)	2016
Brantly, AF	Aesop's wolves: the deceptive appearance of espionage and attacks in cyberspace	Intelligence and national security	2016
Lemay, A; Knight, S; Fernandez, J; Leblanc, S	The Sound a Rattling Cyber-Sabre Makes: Cases Studies in Cyber Power Projection	Proceedings of the 15th European conference on cyber warfare and security (ECCWS 2016)	2016
Yilmaz, K; Gunestas, M; Basibuyuk, O	Cyber Terrorism: Motivation and Method on Global Scale and the Situation in Turkey	Countering terrorist recruitment in the context of armed counter-terrorism operations	2016
Jacobs, V; Bulters, J; van Wieren, M	Modeling the Impact of Cyber Risk for Major Dutch Organizations	Proceedings of the 15th European conference on cyber warfare and security (ECCWS 2016)	2016
Somer, T; Hallaq, B; Watson, T	Utilising Journey Mapping and Crime Scripting to Combat Cyber Crime	Proceedings of the 15th European conference on cyber warfare and security (ECCWS 2016)	2016
Fliegauf, MT	In Cyber (Governance) We Trust	Global policy	2016
Scully, T	Cyber Security and the 2016 Defence White Paper	Security challenges	2016
Viggiano, E	The Role of Cultural Intelligence in Cyber Warfare	Proceedings of the 11th international conference on cyber warfare and security (ICCWS 2016)	2016
Karamanian, A; Sample, C; Kolenko, M	Hofstede's Cultural Markers in Successful Victim Cyber Exploitations	Proceedings of the 11th international conference on cyber warfare and security (ICCWS 2016)	2016
Afful-Dadzie, E; Nabareseh, S; Oplatkova, ZK; Klimek, P	Framing Media Coverage of the 2014 Sony Pictures Entertainment Hack: A Topic Modelling Approach	Proceedings of the 11th international conference on cyber warfare and security (ICCWS 2016)	2016
Edwards, N; Kao, G; Hamlet, J; Bailon, J; Liptak, S	Supply Chain Decision Analytics: Application and Case Study for Critical Infrastructure Security	Proceedings of the 11th international conference on cyber warfare and security (ICCWS 2016)	2016
Schmidt-Felzmann, A	After the war in Ukraine: peace building and reconciliation in spite of the external aggressor	International crisis management: NATO, EU, OSCE and civil society: collected essays on best practices and lessons learned	2016
Bernik, I	Compliance With Information Security Policies in the Slovene Insurance Sector	Proceedings of the 15th European conference on cyber warfare and security (ECCWS 2016)	2016

Futter, A	War Games redux? Cyberthreats, US-Russian strategic stability, and new challenges for nuclear security and arms control	European security	2016
Buchan, R	Cyber Warfare and the Status of Anonymous under International Humanitarian Law	Chinese journal of international law	2016
Saran, S	Striving for an International Consensus on Cyber Security: Lessons from the 20th Century	Global policy	2016
Jhawar, R; Mauw, S; Zakiuddin, I	Automating Cyber Defence Responses Using Attack-Defence Trees and Game Theory	Proceedings of the 15th European conference on cyber warfare and security (ECCWS 2016)	2016
Ben-Asher, N; Morris-King, J; Thompson, B; Glodek, W	Attacker Skill, Defender Strategies and the Effectiveness of Migration-Based Moving Target Defense in Cyber Systems	Proceedings of the 11th international conference on cyber warfare and security (ICCWS 2016)	2016
Grant, T; van Eijk, E; Venter, HS	Assessing the Feasibility of Conducting the Digital Forensic Process in Real Time	Proceedings of the 11th international conference on cyber warfare and security (ICCWS 2016)	2016
Kollar, D; Melkova, M	Positives and Negatives of the European Digitle Single Market	Proceedings of the 3rd international conference on European integration 2016 (ICEI 2016)	2016
Mtsweni, J; Shozi, NA; Matenche, K; Mutemwa, M; Mkhonto, N; van Vuuren, JJ	Development of a Semantic-Enabled Cybersecurity Threat Intelligence Sharing Model	Proceedings of the 11th international conference on cyber warfare and security (ICCWS 2016)	2016
Botha, J; Eloff, M; Swart, I	Pro-Active Data Breach Detection: Examining Accuracy and Applicability on Personal Information Detected	Proceedings of the 11th international conference on cyber warfare and security (ICCWS 2016)	2016
Kawasaki, T	Where does Canada fit in the US-China strategic competition across the Pacific?	International journal	2016
Awan, J; Memon, S	Threats of Cyber Security and Challenges for Pakistan	Proceedings of the 11th international conference on cyber warfare and security (ICCWS 2016)	2016
Slack, C	Wired yet Disconnected: The Governance of International Cyber Relations	Global policy	2016
Brown, A; Andel, T	What's in Your Honeypot?	Proceedings of the 11th international conference on cyber warfare and security (ICCWS 2016)	2016
Ghimire, S	Making security sector reform organic: infrastructures for peace as an entry point?	Peacebuilding	2016
Buchanan, B	The Life Cycles of Cyber Threats	Survival	2016
Cohen, MS; Freilich, CD; Siboni, G	Israel and Cyberspace: Unique Threat and Response	International studies perspectives	2016
Eun, YS; Amann, JS	Cyberwar: Taking Stock of Security and Warfare in the Digital Age	International studies perspectives	2016
Clark, B	Undersea cables and the future of submarine competition	Bulletin of the atomic scientists	2016
Jarvis, L; Macdonald, S; Whiting, A	Analogy and Authority in Cyberterrorism Discourse: An	Global society	2016

	Analysis of Global News Media Coverage		
Colbert, E; Sullivan, D; Hutchinson, S; Renard, K; Smith, S	A Process-Oriented Intrusion Detection Method for Industrial Control Systems	Proceedings of the 11th international conference on cyber warfare and security (ICCWS 2016)	2016
Stoddart, K	UK cyber security and critical national infrastructure protection	International affairs	2016
Torres-Soriano, MR	The Hidden Face of Jihadist Internet Forum Management: The Case of Ansar Al Mujahideen	Terrorism and political violence	2016
Garcia, D	Future arms, technologies, and international law: Preventive security governance	European journal of international security	2016
Gross, ML; Canetti, D; Vashdi, DR	The psychological effects of cyber terrorism	Bulletin of the atomic scientists	2016
Lupovici, A	The "Attribution Problem" and the Social Construction of "Violence": Taking Cyber Deterrence Literature a Step Forward	International studies perspectives	2016
Kaufmann, M	Exercising emergencies: Resilience, affect and acting out security	Security dialogue	2016
Simon, L	The 'Third' US Offset Strategy and Europe's 'Antiaccess' Challenge	Journal of strategic studies	2016
Slayton, R	What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment	International security	2016
Nye, JS	Deterrence and Dissuasion in Cyberspace	International security	2016
Carr, M	Public-private partnerships in national cyber-security strategies	International affairs	2016
Roscini, M	Military Objectives in Cyber Warfare	Ethics and policies for cyber operations: a NATO cooperative cyber defence centre of excellence initiative	2017
Smith, F; Ingram, G	Organising cyber security in Australia and beyond	Australian journal of international affairs	2017
Radek, M	Cybernetic safety of selected world villages and Slovakia	International relations 2017: current issues of world economy and politics	2017
Nathan, AJ	Cyber Dragon: Inside China's Information Warfare and Cyber Operations	Foreign affairs	2017
Secara, D	National and international security policies. Defense in the online	Debating globalization. identity, nation and dialogue: history, political sciences, international relations	2017
Collier, J	Strategies of Cyber Crisis Management: Lessons from the Approaches of Estonia and the United Kingdom	Ethics and policies for cyber operations: a NATO cooperative cyber defence centre of excellence initiative	2017
Cath, CNJ; Glorioso, L; Taddeo, M	NATO CCD COE Workshop on 'Ethics and Policies for Cyber Warfare' - A Report	Ethics and policies for cyber operations: a NATO cooperative cyber defence centre of excellence initiative	2017

Cho, Y; Chung, J	Bring the State Back In: Conflict and Cooperation Among States in Cybersecurity	Pacific focus	2017
Cimbala, SJ	Nuclear deterrence and cyber warfare: coexistence or competition?	Defence and security analysis	2017
Kallberg, J; Burk, RA	The Flaw of Immediate Cyber Counter Strikes	Strategic analysis	2017
Parker, E	Dark Territory: The Secret History of Cyber War	Foreign affairs	2017
Kaivo-Oja, J	Identifying Terrorists in Cyber Space: Evaluating the Potential Role of Emerging Radical Technologies and Technology Disruption in Terrorism Foresight	Identification of potential terrorists and adversary planning: emerging technologies and new counter-terror strategies	2017
Adamsky, D	The Israeli Odyssey toward its National Cyber Security Strategy	Washington quarterly	2017
Bigelow, B	Mission Assurance: Shifting the Focus of Cyber Defence	2017 9th international conference on cyber conflict: defending the core (Cycon)	2017
Mazo, J	The Cyber Effect: A Pioneering Cyberpsychologist Explains How Human Behavior Changes Online	Survival	2017
Jenkins, R	Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare	Ethics & international affairs	2017
Mele, S	Terrorism and the Internet: Finding a Profile of the Islamic "Cyber Terrorist"	Countering terrorism, preventing radicalization and protecting cultural heritage: the role of human factors and technology	2017
Hwang, JJ	China's Cyber Strategy: A Taiwanese Perspective	Korean journal of defense analysis	2017
Bogdanoski, M; Veljovski, G	The Presence of Militant Religious Extremism in the Cyber Battlefield	Countering terrorism in south eastern Europe	2017
Biller, J	The Misuse of Protected Indicators in Cyberspace: Defending a Core Aspect of International Humanitarian Law	2017 9th international conference on cyber conflict: defending the core (Cycon)	2017
Shackelford, SJ; Russell, S; Kuehn, A	Defining Cybersecurity Due Diligence Under International Law: Lessons from the Private Sector	Ethics and policies for cyber operations: a NATO cooperative cyber defence centre of excellence initiative	2017
Bousfield, D	Revisiting Cyber-Diplomacy: Canada-China Relations Online	Globalizations	2017
Gunaratna, R	Global threat forecast	Revista Unisci	2017
Stockburger, PZ	Control and Capabilities Test: Toward a New Lex Specialis Governing State Responsibility for Third Party Cyber Incidents	2017 9th international conference on cyber conflict: defending the core (Cycon)	2017
Gordon, TJ; Florescu, E; Sharan, Y	Emerging Technologies and Potential Measures for the Pre-Detection of Terrorism Intent	Identification of potential terrorists and adversary planning: emerging technologies and new counter-terror strategies	2017
Sivan-Sevilla, I	Trading Privacy for Security in Cyberspace: A Study Across the Dynamics of US Federal Laws and Regulations Between 1967 and 2016	2017 9th international conference on cyber conflict: defending the core (Cycon)	2017

Stytz, MR; Banks, SB	The Nexus Between Cybercrime and Cyberterrorism	Countering terrorism in south eastern Europe	2017
Maric, M	Who Acts-Cyber Identity Issues	Identification of potential terrorists and adversary planning: emerging technologies and new counter-terror strategies	2017
Barrett, E	On the Relationship Between the Ethics and the Law of War: Cyber Operations and Sublethal Harm	Ethics & international affairs	2017
Antinori, A	The "Swarm Wolf". Understanding to Prevent the Evolution of Terror	Identification of potential terrorists and adversary planning: emerging technologies and new counter-terror strategies	2017
McDonald, J	Blind Justice? The Role of Distinction in Electronic Attacks	Ethics and policies for cyber operations: a NATO cooperative cyber defence centre of excellence initiative	2017
Singer, TVP	Update to Revolving Door 2.0: The Extension of the Period for Direct Participation in Hostilities Due to Autonomous Cyber Weapons	2017 9th international conference on cyber conflict: defending the core (Cycon)	2017
Rowe, NC	Challenges of Civilian Distinction in Cyberwarfare	Ethics and policies for cyber operations: a NATO cooperative cyber defence centre of excellence initiative	2017
Gonchar, M	The Impact of Russian Aggression Against Ukraine on CEI	Addressing emerging security risks for energy networks in south Caucasus	2017
Alred, L; Kelly, SM; Rubly, M; Shokh, Y; Tsitsishvili, M; Weitz, R	US policy towards Central Asia under Trump	Revista Unisci	2017
Pierazzi, F; Apruzzese, G; Colajanni, M; Guido, A; Marchetti, M	Scalable Architecture for Online Prioritisation of Cyber Threats	2017 9th international conference on cyber conflict: defending the core (Cycon)	2017
Eaves, E; Matheny, J	IARPA Director Jason Matheny advances tech tools for US espionage	Bulletin of the atomic scientists	2017
Hansel, M; Ruhnke, S	A revolution of democratic warfare? Assessing regime type and capability-based explanations of military transformation processes	International journal	2017
Jolicoeur, P; Seaboyer, A	ISIS Social Media Exploitation in the SEE	Countering terrorism in south eastern Europe	2017
FitzGerald, B; Parziale, J	As technology goes democratic, nations lose military control	Bulletin of the atomic scientists	2017
Chivvis, CS	Hybrid war: Russian contemporary political warfare	Bulletin of the atomic scientists	2017
Longo, R; Pintore, F; Rinaldo, G; Sala, M	On the Security of the Blockchain BIX Protocol and Certificates	2017 9th international conference on cyber conflict: defending the core (Cycon)	2017
Geers, K	Core Illumination: Traffic Analysis in Cyberspace	2017 9th international conference on cyber conflict: defending the core (Cycon)	2017
Finlay, CJ	The concept of violence in international theory: a Double-Intent Account	International theory	2017

Bubnova, NI	U.S. - Russia relations and arms control: breating the clinch	Mgimo review of international relations	2017
Strohmeier, M; Smith, M; Schafer, M; Lenders, V; Martinovic, I	Crowdsourcing Security for Wireless Air Traffic Communications	2017 9th international conference on cyber conflict: defending the core (Cycon)	2017
Yusgiantoro, P	Developing Indonesia's Basic Defense Forces	Korean journal of defense analysis	2017
Koraus, A; Veselovska, S; Kelemen, P	Cyber security as part of the business environment	International relations 2017: current issues of world economy and politics	2017
Smeets, M	Organisational Integration of Offensive Cyber Capabilities: A Primer on the Benefits and Risks	2017 9th international conference on cyber conflict: defending the core (Cycon)	2017
Happa, J; Fairclough, G	A Model to Facilitate Discussions About Cyber Attacks	Ethics and policies for cyber operations: a NATO cooperative cyber defence centre of excellence initiative	2017
Cornish, P	Deterrence and the Ethics of Cyber Conflict	Ethics and policies for cyber operations: a nato cooperative cyber defence centre of excellence initiative	2017
Hoisington, M	Regulating Cyber Operations Through International Law: In, Out or Against the Box?	Ethics and policies for cyber operations: a NATO cooperative cyber defence centre of excellence initiative	2017
Kallender, P; Hughes, CW	Japan's Emerging Trajectory as a "Cyber Power': From Securitization to Militarization of Cyberspace	Journal of strategic studies	2017
Macak, K	From the Vanishing Point Back to the Core: The Impact of the Development of the Cyber Law of War on General International Law	2017 9th international conference on cyber conflict: defending the core (Cycon)	2017
Angelo, P	The Colombian Peace Process: Trial and Error	Survival	2017
Casanovas, P	Cyber Warfare and Organised Crime. A Regulatory Model and Meta-Model for Open Source Intelligence (OSINT)	Ethics and policies for cyber operations: a NATO cooperative cyber defence centre of excellence initiative	2017
Bonfanti, A	Hacking by Law Enforcement Agencies: Remarks About the European Union Study on Legal Frameworks for Hacking by Law Enforcement	Diritti umani e diritto internazionale	2017
Taddeo, M	Just Information Warfare	Ethics and policies for cyber operations: a nato cooperative cyber defence centre of excellence initiative	2017
Watt, E	The Role of International Human Rights Law in the Protection of Online Privacy in the Age of Surveillance	2017 9th international conference on cyber conflict: defending the core (Cycon)	2017
Mastriano, D	Putin - the masked nemesis of the strategy of ambiguity	Defence and security analysis	2017
Guo, S; Ding, W; Lanshina, T	Global Governance and the Role of the G20 in the Emerging Digital Economy	Vestnik mezhdunarodnykh organizatsii-international organisations research journal	2017

Libicki, M	The Coming of Cyber Espionage Norms	2017 9th international conference on cyber conflict: defending the core (Cycon)	2017
Osawa, J	The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem?	Asia-Pacific review	2017
Nussbaum, BH	Communicating Cyber Intelligence to Non-Technical Customers	International journal of intelligence and counterintelligence	2017
Fischerkeller, M	Incorporating Offensive Cyber Operations into Conventional Deterrence Strategies	Survival	2017
Dalton, MG	How Iran's hybrid-war tactics help and hurt it	Bulletin of the atomic scientists	2017
Huang, ZX; Macak, K	Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches	Chinese journal of international law	2017
Wirtz, JJ	Life in the "Gray Zone": observations for contemporary strategists	Defence and security analysis	2017
Baylon, C	Lessons from Stuxnet and the Realm of Cyber and Nuclear Security: Implications for Ethics in Cyber Warfare	Ethics and policies for cyber operations: a NATO cooperative cyber defence centre of excellence initiative	2017
Inkster, N	Measuring Military Cyber Power	Survival	2017
Carrapico, H; Barrinha, A	The EU as a Coherent (Cyber)Security Actor?	JCMS-journal of common market studies	2017
Sharp, T	Theorizing cyber coercion: The 2014 North Korean operation against Sony	Journal of strategic studies	2017
Christensen, KK; Petersen, KL	Public-private partnerships on cyber security: a practice of loyalty	International affairs	2017
Jasper, SE	U.S. Cyber Threat Intelligence Sharing Frameworks	International journal of intelligence and counterintelligence	2017
Grigsby, A	The End of Cyber Norms	Survival	2017
Borghard, ED; Lonergan, SW	The Logic of Coercion in Cyberspace	Security studies	2017
Carson, A; Yarhi-Milo, K	Covert Communication: The Intelligibility and Credibility of Signaling in Secret	Security studies	2017
Lee, YJ; Kwon, HJ; Lee, JI; Shin, DK	The Countermeasure Strategy Based on Big Data against North Korean Cyber-attacks	Korean journal of defense analysis	2018
Artusy, DV; Gioe, DV	Cyber Dragon: Inside China's Information Warfare and Cyber Operations	International journal of intelligence and counterintelligence	2018
Shah, MA	Cyber Compellence: An Instrument of Technology-Driven Strategy	IPRI journal	2018
Sleat, M	Just cyber war?: Casus belli, information ethics, and the human perspective	Review of international studies	2018
Hansel, M	Cyber-attacks and psychological IR perspectives: explaining misperceptions and escalation risks	Journal of international relations and development	2018

Biller, J	Cyber Mercenaries: The State, Hackers, and Power	Naval war college review	2018
Chen, K	Cyber weaponry: issues and implications of digital arms	International affairs	2018
Siroli, GP	Considerations on the Cyber Domain as the New Worldwide Battlefield	International spectator	2018
Maurer, T	Cyber Proxies and Their Implications for Liberal Democracies	Washington quarterly	2018
Freedman, LD	Hacking the Bomb: Cyber Threats and Nuclear Weapons	Foreign affairs	2018
Cai, CH	China and Global Cyber Governance: Main Principles and Debates	Asian perspective	2018
Rid, T	The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age	Survival	2018
Freedman, LD	Digital World War: Islamists, Extremists, and the Fight for Cyber Supremacy	Foreign affairs	2018
Joo, YM; Tan, TB	Smart Cities: A New Age of Digital Insecurity	Survival	2018
Lopes, GV; Medeiros, MD	CyberIR or the introduction to the systematic studies on cyberspace in the International Relations tripod teaching-research-extension	Meridiano 47-journal of global studies	2018
Ayhan, K	Branding Korea as "My Friend's Country": The Case of VANK's Cyber Public Diplomats	Korea observer	2018
Whyte, C	Dissecting the Digital World: A Review of the Construction and Constitution of Cyber Conflict Research	International studies review	2018
Hollis, DB; Ohlin, JD	What if Cyberspace Were for Fighting?	Ethics & international affairs	2018
Stritecky, V; Hynek, N	Comparing global security regimes: a power-analytical synthesis	International politics	2018
Bowers, I	The use and utility of hybrid warfare on the Korean Peninsula	Pacific review	2018
Zdravkovski, A	Cyber sheiks and grassroots jihadis: the war in Syria and the devolution of the Bosnian Salafi communities	Small wars and insurgencies	2018
Ziegler, CE	International dimensions of electoral processes: Russia, the USA, and the 2016 elections	International politics	2018
Schaefer, D	Australia's new alliance dynamics, US-China rivalry and conflict entrapment in outer space	Australian journal of international affairs	2018
Golub, K; Golub, Y	Collective Security Treaty Organization: Origins of the Multidimensional Mandate and Modern Means for its Implementation	Vestnik mezhdunarodnykh organizatsii-international organisations research journal	2018
Wirtz, JJ	Cyber War versus Cyber Realities	International journal of intelligence and counterintelligence	2018

Wirtz, JJ	The Cyber Pearl Harbor redux: helpful analogy or cyber hype?	Intelligence and national security	2018
Sharp, T	Hiding in Plain Sight: Political Effects of Cyber Operations	Survival	2018
Brantly, AF	When everything becomes intelligence: machine learning and the connected world	Intelligence and national security	2018
Armenia, S; Tsaples, G	Individual Behavior as a Defense in the "War on Cyberterror": A System Dynamics Approach	Studies in conflict & terrorism	2018
Khanijo, R	Post-Pokhran II: Emerging Global Nuclear Order and India's Nuclear Challenge	Strategic analysis	2018
Kanet, RE	Russia and global governance: the challenge to the existing liberal order	International politics	2018
Boeke, S; Broeders, D	The Demilitarisation of Cyber Conflict	Survival	2018
Jacobsen, JT	A "digital Geneva Convention" is not in Denmark's interest	Internasjonal politikk	2018
Gioe, DV	Cyber operations and useful fools: the approach of Russian hybrid intelligence	Intelligence and national security	2018
Boys, JD	The Clinton administration's development and implementation of cybersecurity strategy (1993-2001)	Intelligence and national security	2018
Jordaan, SM	Resilience for power systems amid a changing climate	Bulletin of the atomic scientists	2018
Hoffman, W; Volpe, TA	Internet of nuclear things: Managing the proliferation risks of 3-D printing technology	Bulletin of the atomic scientists	2018
Stevens, T	Cyberweapons: power and the governance of the invisible	International politics	2018
Lantis, JS; Bloomberg, DJ	Changing the code? Norm contestation and US antipreneurism in cyberspace	International relations	2018
Wilner, AS	Cybersecurity and its discontents: Artificial intelligence, the Internet of Things, and digital misinformation	International journal	2018
Poznansky, M; Perkoski, E	Rethinking Secrecy in Cyberspace: The Politics of Voluntary Attribution	Journal of global security studies	2018
Efrony, D; Shany, Y	A rule book on the shelf? Tallinn manual 2.0 on cyberoperations and subsequent state practice	American journal of international law	2018
Mori, S	US Defense Innovation and Artificial Intelligence	Asia-pacific review	2018
Gohdes, AR	Studying the Internet and Violent conflict	Conflict management and peace science	2018
Acton, JM	Escalation through Entanglement How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War	International security	2018

Adamsky, D	From Moscow with coercion: Russian deterrence theory and strategic culture	Journal of strategic studies	2018
Smeets, M	A matter of time: On the transitory nature of cyberweapons	Journal of strategic studies	2018
Gilli, A; Gilli, M	Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage	International security	2018
Sharikov, PA	Evolution of American cyber security policies	Mirovaya ekonomika i mezhdunarodnye otnosheniya	2019
Mad'ar, T	Lagging colossus or a mature cyber-alliance? 20 years of cyber defence in NATO	Obrana a strategie-defence & strategy	2019
Jensen, MS	Cyber resilience, sectoral principle and responsibility placement - Nordic experience	Internasjonal politikk	2019
Sander, B	Democracy Under The Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections	Chinese journal of international law	2019
Willett, M	Assessing Cyber Power	Survival	2019
Hoffman, W	Is Cyber Strategy Possible?	Washington quarterly	2019
Orozco, GAP	The international cybersystem: elements of analysis	Oasis-observatorio de analisis de los sistemas internacionales	2019
Tangredi, SJ	Full-bodied cyber without the hype	Naval war college review	2019
Fucik, J	CSIRT: On the frontline of combating cyber threats	Obrana a strategie-defence & strategy	2019
Lewis, J	Hacking the Bomb: Cyber Threats and Nuclear Weapons	Survival	2019
Jacobsen, JT	NATO offensive cyberspace operations. Opportunities and challenges for NATO's research-driven and impact-based approach	Internasjonal politikk	2019
Jasper, SE	The Decision to Attack: Military and Intelligence Cyber Decision-Making	International journal of intelligence and counterintelligence	2019
Nocetti, J	The perfect weapon: war, sabotage, and fear in the cyber age	International affairs	2019
Nocetti, J	The perfect weapon: war, sabotage, and fear in the cyber age	International affairs	2019
Muller, LP	Into the gray zone: deterrence as a defense of cyberspace?	Internasjonal politikk	2019
Clemens, WC	The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age	Asian perspective	2019
Arora, B	Teaching cyber security to non-tech students	Politics	2019
Christensen, KK; Liebetrau, T	A new role for 'the public'? Exploring cyber security controversies in the case of WannaCry	Intelligence and national security	2019
Coslovi, D	The Devil is in the Details: An Examination of Hybrid Cyber Operations and International Law	Journal of military and strategic studies	2019

Kristiansen, M; Hoem, N	Deterrence as an element of cybersecurity strategy from a small state perspective	Internasjonal politikk	2019
Shackelford, SJ	Should cybersecurity be a human right? exploring the 'shared responsibility' of cyber peace	Stanford journal of international law	2019
Babb, C; Wilner, A	Passwords, pistols, and power plants: An assessment of physical and digital threats targeting Canada's energy sector	International journal	2019
[Anonymous]	US Military Undergoes Restructuring to Emphasize Cyber and Space Capabilities	American journal of international law	2019
Kelton, M; Sullivan, M; Bienvenue, E; Rogers, Z	Australia, the utility of force and the society-centric battlespace	International affairs	2019
Lutz, CKG; Lutz, BJ; Lutz, JM	Russian Foreign Policy Management and Manipulation with the Soviet Successor States	Terrorism and political violence	2019
O'Malley, S	Assessing Threats to South Korea's Undersea Communications Cable Infrastructure	Korean journal of international studies	2019
Taillat, S; Douzet, F	Collective security and strategic instability in the digital domain	Contemporary security policy	2019
Finnemore, M	Talking Past Each Other: Government, Business and Civil Society Discussing Cyber Security	Mgimo review of international relations	2019
Svenungsen, B	Internet as geopolitical arena?	Internasjonal politikk	2019
Larsdotter, K	Military strategy in the 21st century	Journal of strategic studies	2019
Lequesne, C	Why Studying State Foreign Services Remains a Research Priority	Diplomacy & statecraft	2019
Riehle, K; May, M	Human-cyber Nexus: the parallels between 'illegal' intelligence operations and advanced persistent threats	Intelligence and national security	2019
Nye, JS	Soft Power and Public Diplomacy Revisited	Hague journal of diplomacy	2019
Mori, S	US Technological Competition with China: The Military, Industrial and Digital Network Dimensions	Asia-pacific review	2019
Carrea, S	The ECHR in the Cyberspace: Does the Power to Infringe Always Entail the Duty to Protect?	Diritti umani e diritto internazionale	2019
Leonova, OG	SHARP POWER - THE NEW TECHNOLOGY OF INFLUENCE IN A GLOBAL WORLD	Mirovaya ekonomika i mezhdunarodnye otnosheniya	2019
Arbatov, AG	DREAMS AND REALITIES OF ARMS CONTROL	Mirovaya ekonomika i mezhdunarodnye otnosheniya	2019
Gunaratna, R	GLOBAL THREAT FORECAST 2019	Revista unisci	2019
Gjesvik, L; Overbo, EJ	Deter who? The importance of strategic culture for cybersecurity	Internasjonal politikk	2019
Cunningham, FS; Fravel, MT	Dangerous Confidence? Chinese Views on Nuclear Escalation	International security	2019

Gill, AS	Artificial Intelligence and International Security: The Long View	Ethics & international affairs	2019
Kari, MJ; Pynnoniemi, K	Theory of strategic culture: An analytical framework for Russian cyber threat perception	Journal of strategic studies	2019
Tromblay, DE	Gray Day: My Undercover Mission to Expose America's First Cyber Spy	International journal of intelligence and counterintelligence	2019
Couzigou, I	The Criminalization of Online Terrorism Preparatory Acts Under International Law	Studies in conflict & terrorism	2019
Blasko, DJ	The PLA army after 'below the neck' reforms: contributing to China's joint warfighting, deterrence and MOOTW Posture	Journal of strategic studies	2019
Hare, FB	Precision cyber weapon systems: An important component of a responsible national security strategy?	Contemporary security policy	2019
Gompert, DC; Libicki, M	Cyber War and Nuclear Peace	Survival	2019
Leuprecht, C; Szeman, J; Skillicorn, DB	The Damoclean sword of offensive cyber: Policy uncertainty and collective insecurity	Contemporary security policy	2019
Demchak, CC	China: Determined to dominate cyberspace and AI	Bulletin of the atomic scientists	2019
Petersen, KL	Three concepts of intelligence communication: awareness, advice or co-production?	Intelligence and national security	2019
Lakomy, M	Let's Play a Video Game: Jihadi Propaganda in the World of Electronic Entertainment	Studies in conflict & terrorism	2019
Loleski, S	From cold to cyber warriors: the origins and expansion of NSA's Tailored Access Operations (TAO) to Shadow Brokers	Intelligence and national security	2019
Jensen, B; Valeriano, B; Maness, R	Fancy bears and digital trolls: Cyber strategy with a Russian twist	Journal of strategic studies	2019
Gomez, MAN	Sound the alarm! Updating beliefs and degradative cyber operations	European journal of international security	2019
Lin, H	The existential threat from cyber-enabled information warfare	Bulletin of the atomic scientists	2019
Drezner, DW	Technological change and international relations	International relations	2019
Aaronson, SA	What Are We Talking about When We Talk about Digital Protectionism?	World trade review	2019
Kostyuk, N; Zhukov, YM	Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?	Journal of conflict resolution	2019
Sechser, TS; Narang, N; Talmadge, C	Emerging technologies and strategic stability in peacetime, crisis, and war	Journal of strategic studies	2019
Schneider, J	The capability/vulnerability paradox and military revolutions: Implications for computing, cyber, and the onset of war	Journal of strategic studies	2019

Cavelty, MD; Wenger, A	Cyber security meets security politics: Complex technology, fragmented politics, and networked science	Contemporary security policy	2020
Madrid, M	International Relations in the Cyber Age. The Co-Evolution Dilemma	Foro internacional	2020
Mathews, JT	The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats	Foreign affairs	2020
Georgieva, I	The unexpected norm-setters: Intelligence agencies in cyberspace	Contemporary security policy	2020
Klimburg, A	Mixed Signals: A Flawed Approach to Cyber Deterrence	Survival	2020
Blagden, D	Deterring Cyber Coercion: The Exaggerated Problem of Attribution	Survival	2020
Dossi, S	On the asymmetric advantages of cyberwarfare. Western literature and the Chinese journal Guofang Keji	Journal of strategic studies	2020
Lindsay, JR	Demystifying the Quantum Threat: Infrastructure, Institutions, and Intelligence Advantage	Security studies	2020
Egloff, FJ	Contested public attributions of cyber incidents and the role of academia	Contemporary security policy	2020
Shires, J	Cyber-noir: Cybersecurity and popular culture	Contemporary security policy	2020
Dover, R	SOCMINT: a shifting balance of opportunity	Intelligence and national security	2020
Wilner, AS	US cyber deterrence: Practice guiding theory	Journal of strategic studies	2020
Stevens, C	Assembling cybersecurity: The politics and materiality of technical malware reports and the case of Stuxnet	Contemporary security policy	2020

ANEXO II – APRESENTAÇÃO DA AMOSTRA BIBLIOGRÁFICA FINAL

A Tabela 13 apresenta a amostra bibliográfica final preliminar – decorrente dos filtros aplicados sobre a amostra bibliográfica inicial após análise de citações pelo *software* VosViewer (mínimo de 5 citações e com vínculos entre si) – que totaliza 47 textos.

Tabela 13 – Amostra bibliográfica final preliminar

ID	Autores	Texto	Periódico	Ano
1	Hansen, L; Nissenbaum, H	Digital Disaster, Cyber Security, and the Copenhagen School	International Studies Quarterly	2009
2	Hughes, R	A treaty for cyberspace	International Affairs	2010
3	Inkster, N	China in Cyberspace	Survival	2010
4	Lemay, A; Fernandeza, JM; Knight, S	Pinprick attacks, a lesser included case?	Conference on Cyber Conflict, Proceedings 2010	2010
5	Ottis, R	From pitchforks to laptops: volunteers in cyber conflicts	Conference on Cyber Conflict, Proceedings 2010	2010
6	Farwell, JP; Rohozinski, R	Stuxnet and the Future of Cyber War	Survival	2011
7	Klimburg, A	Mobilising cyber power	Survival	2011
8	Deibert, RJ; Rohozinski, R; Crete-Nishihata, M	Cyclones in cyberspace: Information shaping and denial in the 2008 Russia-Georgia war	Security Dialogue	2012
9	Farwell, JP; Rohozinski, R	The New Reality of Cyber War	Survival	2012
10	Liff, AP	Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War	Journal of Strategic Studies	2012
11	Rid, T	Cyber war will not take place	Journal of Strategic Studies	2012
12	Betz, DJ; Stevens, T	Analogical reasoning and cyber security	Security Dialogue	2013
13	Bronk, C; Tikk-Ringas, E	The Cyber Attack on Saudi Aramco	Survival	2013
14	Cavelty, MD	From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse	International Studies Review	2013
15	Goldsmith, J	How Cyber Changes the Laws of War	European Journal of International Law	2013
16	Herrington, L; Aldrich, R	The Future of Cyber-Resilience in an Age of Global Complexity	Politics	2013
17	Junio, TJ	How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate	Journal of Strategic Studies	2013
18	Kello, L	The Meaning of the Cyber Revolution Perils to Theory and Statecraft	International Security	2013
19	Lindsay, JR	Stuxnet and the Limits of Cyber Warfare	Security Studies	2013
20	McGraw, G	Cyber War is Inevitable (Unless We Build Security In)	Journal of Strategic Studies	2013

21	Mueller, M; Schmidt, A; Kuerbis, B	Internet Security and Networked Governance in International Relations	International Studies Review	2013
22	Peterson, D	Offensive Cyber Weapons: Construction, Development, and Employment	Journal of Strategic Studies	2013
23	Stone, J	Cyber war will take place!	Journal of Strategic Studies	2013
24	Eichensehr, KE	Tallinn Manual on the International Law Applicable to Cyber Warfare	American Journal of International Law	2014
25	Gompert, DC; Libicki, M	Cyber Warfare and Sino-American Crisis Instability	Survival	2014
26	Lindsay, JR	The Impact of China on Cybersecurity Fiction and Friction	International Security	2014
27	Valeriano, B; Maness, RC	The dynamics of cyber conflict between rival antagonists, 2001-11	Journal of Peace Research	2014
28	Gartzke, E; Lindsay, JR	Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace	Security Studies	2015
29	Rid, T; Buchanan, B	Attributing cyber attacks	Journal of Strategic Studies	2015
30	Carr, M	Public-private partnerships in national cyber-security strategies	International Affairs	2016
31	Garcia, D	Future arms, technologies, and international law: Preventive security governance	European Journal of International Security	2016
32	Lupovici, A	The “Attribution Problem” and the Social Construction of “Violence”: Taking Cyber Deterrence Literature a Step Forward	International Studies Perspectives	2016
33	Nye, JS	Deterrence and Dissuasion in Cyberspace	International Security	2016
34	Slayton, R	What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment	International Security	2016
35	Stoddart, K	UK cyber security and critical national infrastructure protection	International Affairs	2016
36	Balzacq; Cavelty			2016
37	Borghard, ED; Lonergan, SW	The Logic of Coercion in Cyberspace	Security Studies	2017
38	Carson, A; Yarhi-Milo, K	Covert Communication: The Intelligibility and Credibility of Signaling in Secret	Security Studies	2017
39	Christensen, KK; Petersen, KL	Public-private partnerships on cyber security: a practice of loyalty	International Affairs	2017
40	Sharp, T	Theorizing cyber coercion: The 2014 North Korean operation against Sony	Journal of Strategic Studies	2017
41	TOR			2017
42	Efrony, D; Shany, Y	A rule book on the shelf? Tallinn manual 2.0 on cyberoperations and subsequent state practice	American Journal of International Law	2018
43	Gohdes, AR	Studying the Internet and Violent conflict	Conflict Management and Peace Science	2018
44	Smeets, M	A matter of time: On the transitory nature of cyberweapons	Journal of Strategic Studies	2018
45	Kostyuk, N; Zhukov, YM	Invisible digital front: can cyber attacks shape battlefield events?	Journal of Conflict Resolution	2019
46	Schneider, J	The capability/vulnerability paradox and military revolutions: Implications for computing, cyber, and the onset of war	Journal of Strategic Studies	2019
47	Sechser, TS; Narang, N; Talmadge, C	Emerging technologies and strategic stability in peacetime, crisis, and war	Journal of Strategic Studies	2019

A Tabela 14 apresenta os textos adicionados discricionariamente à amostra bibliográfica final, sendo também objeto da revisão sistemática de literatura.

Tabela 14 – Textos adicionados discricionariamente à amostra bibliográfica final.

ID	Autores	Texto	Periódico	Ano
1	Arquilla, J.; Ronfeldt, D.	Cyberwar is coming!	Comparative Strategy	1993
2	Lynn, W. J.	Defending a New Domain: The Pentagon's Cyberstrategy	Foreign Affairs	2010
3	Manjikian, M. M.	From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik	International Studies Quarterly	2010
4	Nye, J.	Cyberpower	Belfer Center for Science and International Affairs	2010
5	Betz, D. J.; Stevens, T.	Cyberspace and the State: toward a strategy for cyber-power	LIVRO	2011
6	Melzer, N.	Cyber Warfare and International Law	Unidir Resources	2011
7	Reardon, R.; Choucri, N.	The role of cyberspace in international relations: a view of the literature	Paper prepared for the 2012 ISA Annual Convention, San Diego, CA	2012
8	Gartzke, E.	The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth	Quarterly Journal: International Security	2013
9	Darczewska, J.	The anatomy of Russian information warfare the Crimea operation, a case study	Point of View n.42. Centre for Eastern Studies. Warsaw.	2014
10	Schreier, F.	On Cyberwarfare	Geneva Centre for the Democratic Control of Armed Forces (DCAF)	2015
11	Siedler, R. E.	Hard Power in Cyberspace: CNA as a Political Means	8th International Conference on Cyber Conflict: Cyber Power	2016
12	Gorwa, R.; Smeets, M.	Cyber Conflict in Political Science: A Review of Methods and Literature	Working Paper Prepared for the 2019 ISA Annual Convention	2019
13	Stauffacher, D.	UN GGE and UN OEWG: How to live with two concurrent UN Cybersecurity processes	Remarks by Dr. Daniel Stauffacher, Founder and President, ICT4Peace to Jeju Forum May 2019	2019