COLEÇÃO
DEFESA E
FRONTEIRAS
VIRTUAIS

III

RELAÇÕES INTERNACIONAIS CIBERNÉTICAS (CiberRI)

OPORTUNIDADES E DESAFIOS PARA OS ESTUDOS ESTRATÉGICOS E DE SEGURANÇA INTERNACIONAL

Marcos Aurélio Guedes de Oliveira
Ricardo Borges Gama Neto
Gills Vilar Lopes
ORGANIZADORES

Editora UFPE

RELAÇÕES INTERNACIONAIS CIBERNÉTICAS (CiberRI)

Oportunidades e desafios para os Estudos Estratégicos e de Segurança Internacional

RELAÇÕES INTERNACIONAIS CIBERNÉTICAS (CIBERRI)

OPORTUNIDADES E DESAFIOS PARA OS ESTUDOS ESTRATÉGICOS E DE SEGURANÇA INTERNACIONAL

MARCOS AURÉLIO GUEDES DE OLIVEIRA
RICARDO BORGES GAMA NETO
GILLS VILAR LOPES
ORGANIZADORES

Editora UFPE
RECIFE | 2016

Editor geral da coleção

Marcos Aurélio Guedes de Oliveira

EDITORA ASSOCIADA À
Associação Brasileira
das Editoras Universitárias

Equipe editorial

Diagramação: Pierre Edmilson e Maria Laura Ponessa
Revisora: Ana Maria
Capa e projeto gráfico: Ildembergue Leite
Assistente administrativo: Luciana Belo Guedes
Impressão e acabamento: Editora UFPE

Catalogação na fonte:
Bibliotecária Liliane Campos Gonzaga de Noronha, CRB4-1702

C776 Relações Internacionais Cibernéticas / organizadores: Marcos Aurélio Guedes de Oliveira, Ricardo Borges Gama Neto, Gills Vilar Lopes.
232 p. : il. – (Coleção Defesa e Fronteiras Virtuais, v.3)

ISBN 978-85-415-0633-5 (broch.)

1. Relações Internacionais - Segurança Internacional. 2. Estudos Estratégicos. 3. Ciberespaço. 4. Segurança Cibernética. 5. Defesa. I. Guedes Oliveira, Marcos Aurelio (Org.). II. Gama Neto, Ricardo Borges. III. Vilar Lopes, Gills. IV. Defesa e Fronteiras Virtuais.

327.17 CDD (23.ed.) UFPE (BC2014-198)

Agradecimentos

À Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), que, em parceria com a Secretaria de Assuntos Estratégicos da Presidência da República (SAE/PR), lançou o Edital Pró-Estratégia 2012, viabilizando, assim, o Projeto "*Vigilância nas Fronteiras e Muros Virtuais: um estudo analítico de políticas públicas e sistemas operacionais de proteção às estruturas estratégicas terrestres*".

Aos colegas que atuam na rede de pesquisa sobre Defesa Nacional e Segurança Internacional formada pela Universidade Federal de Pernambuco (UFPE), pelo Instituto Meira Mattos da Escola de Comando e Estado-Maior do Exército (IMM-ECEME) e pela Academia Militar das Agulhas Negras (AMAN), além dos que integram o Centro de Estudos e Sistemas Avançados do Recife (CESAR).

Aos que trabalharam na edição, revisão, tradução, projeto gráfico e divulgação desta obra.

Apresentação dos autores

Ahmina Raiara Solsona Oliveira
Mestra e Bacharel em Relações Internacionais pela Universidade Estadual da Paraíba (UEPB). Pesquisadora do Grupo de Estudos e Pesquisa em Ásia-Pacífico (GEPAP/UEPB/CNPq). Bolsista da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES).

Alcides Eduardo dos Reis Peron
Doutorando e Mestre em Política Científica e Tecnológica pela Universidade de Campinas (Unicamp), com período-sanduiche na *Lancaster University*, na Inglaterra. Bacharel em Relações Internacionais e em Economia pela Faculdades de Campinas (Facamp). Pesquisador do Grupo de Análise de Politicas e Inovação (GAPI-Unicamp). Vencedor do V Concurso Nacional de Dissertações e Teses sobre Defesa Nacional (Categoria Mestrado) do Ministério da Defesa. Bolsista da CAPES.

Alexandre Cesar Cunha Leite
Doutor em Ciências Sociais/Relações Internacionais e Mestre em Economia Política pela Pontifícia Universidade Católica de São Paulo (PUC/SP). Especialista em Relações Internacionais pela Pontifícia Universidade Católica de Minas Gerais (PUC Minas). Economista. Professor do Programa de Pós-Graduação em Relações Internacionais

(PPGRI) da Universidade Estadual da Paraíba (UEPB) e coordenador do Grupo de Estudos e Pesquisa em Ásia-Pacífico (GEPAP/UEPB/CNPq).

Candela Justribó

Licenciada em Ciência Política pela *Universidad de Buenos Aires* (UBA). Assessora da Direção Geral de Planejamento e Estratégia do Ministério da Defesa da Argentina. Pesquisadora do "Observatório da Integração Regional Sul-Americana no século XXI" e da *Escuela de Defensa Nacional* (EDENA). Professora do Programa Sul-Americano de Formação em Defesa, no âmbito da União de Nações Sul-Americanas (UNASUL).

Eduardo Cesar Bohn

Mestre em Estudos Estratégicos Internacionais pela Universidade Federal do Rio Grande do Sul (UFRGS) e Bacharel em Relações Internacionais pela mesma universidade. Foi discente-visitante na *Universität Heidelberg*, na Alemanha. Ex-membro do Centro de Estudos de Governo (CEGOV-UFRGS). Integrou o Projeto "Proteção e Desenvolvimento da Amazônia Azul: Possibilidades e Requisitos de um Projeto Marítimo Brasileiro para o Século XXI", financiado pelo CNPq.

Gills Vilar Lopes

Doutorando e Mestre em Ciência Política (Relações Internacionais) pela Universidade Federal de Pernambuco (UFPE), com período-sanduiche na *Université Laval*, no Canadá. *Specialized Course* em *Cybersecurity: Issues in National and International Security* pela *National Defense University* (NDU),

nos EUA. Internacionalista pela UEPB. Vencedor do VI Concurso de Teses sobre Defesa Nacional (Categoria Mestrado) do Ministério da Defesa. Membro dos NEPI-UFPE, OEPRI-UFPB e O Brasil e as Américas (UFPE). Bolsista do Pró-Estratégia.

Igor Daniel Palhares Acácio

Doutorando e Mestre em Ciência Política pelo Instituto de Estudos Sociais e Políticos da Universidade do Estado do Rio de Janeiro (IESP/UERJ). Bacharel em Relações Internacionais com Habilitação em Estudos Estratégicos pela Universidade Federal Fluminense (UFF). Bolsista do Nacional de Desenvolvimento Científico e Tecnológico (CNPq).

Joanisval Brito Gonçalves

Doutor em Relações Internacionais pela Universidade de Brasília (UnB), Consultor Legislativo do Senado Federal para a área de Relações Exteriores e Defesa Nacional e Consultor para a Comissão Mista de Controle das Atividades de Inteligência do Congresso Nacional (CCAI), advogado e professor. Tem diversas publicações no Brasil e no exterior sobre atividade de Inteligência, entre as quais os livros "Atividade de Inteligência e Legislação Correlata" e "Políticos e Espiões – o controle da atividade de inteligência", ambos pela Editora Impetus. Sítio virtual: www.joanisval.com.

Lucas Ribeiro de Belmont Fonseca

Graduando em Relações Internacionais pela Universidade Federal da Paraíba (UFPB), onde é bolsista CNPq/PIBIC. Membro da Diretoria Acadêmica da Academia Nacional de Estudos Transnacionais (ANET). Aluno selecionado da I Escola de Governança da Internet no Brasil, promovido pelo Comitê Gestor da Internet no Brasil (CGI.Br). Premiado como *Best Delegate* durante o *Harvard National Model United Nations Latin America 2014* (HNMUNLA). Tem artigo sobre Segurança Cibernética publicado na *Security and Defense Studies Review* (SDSR).

Marcos Aurélio Guedes de Oliveira

Doutor em Ciência Politica pela *University of Essex*, na Inglaterra. Coordenador geral do Projeto Vigilância nas Fronteiras e Muros Virtuais: um estudo analítico de políticas públicas e sistemas operacionais de proteção as estruturas estratégicas terrestres. Professor Titular do Programa de Pós-Graduação em Ciência Política da UFPE. Coordenador do Grupo de Estudos "O Brasil e as Américas" e do Núcleo de Estudos Americanos (NEA), ambos da UFPE.

Maurício Reis Nothen

Mestre em Estudos Estratégicos Internacionais pela Universidade Federal do Rio Grande do Sul (UFRGS) e Bacharel em Relações Internacionais pela mesma universidade. 2º lugar do VI Concurso Nacional de Dissertações e Teses sobre Defesa Nacional (Categoria Mestrado) do Ministério da

Defesa. Ex-membro do Centro de Estudos de Governo (CEGOV-UFRGS). Integrou o Projeto "Proteção e Desenvolvimento da Amazônia Azul: Possibilidades e Requisitos de um Projeto Marítimo Brasileiro para o Século XXI", financiado pelo CNPq.

Ricardo Borges Gama Neto

Doutor e Mestre em Ciência Política pela Universidade Federal de Pernambuco (UFPE). Professor Adjunto III e Coordenador do Programa de Pós-Graduação em Ciência Política (PPGCP) da UFPE. Diretor de Pesquisa da Associação Brasileira de Ciência Política (ABCP).

Sol Gastaldi

Licenciada em Ciência Política pela *Universidad de Buenos Aires* (UBA). Mestra em Defesa Nacional pela EDENA e pesquisadora pela mesma instituição. Assessora da Direção Geral de Planejamento e Estratégia do Ministério da Defesa da Argentina. Comentarista convidada do *Council on Hemispheric Affairs* (COHA). Professora do Programa Sul-Americano de Formação em Defesa, no âmbito da União de Nações Sul-Americanas (UNASUL).

Tiago Medeiros Delgado

Graduando em Direito pela Universidade Federal da Paraíba (UFPB), onde é bolsista CNPq/PIBIC. Membro da Diretoria Aca-

dêmica da Academia Nacional de Estudos Transnacionais (ANET). Premiado como *Outstanding Delegate* durante o *Harvard National Model United Nations Latin America 2014* (HNMUNLA). Tem artigo sobre Segurança Cibernética publicado na *Security and Defense Studies Review* (SDSR).

Walfredo Bento Ferreira Neto

Mestre em Estudos Estratégicos da Defesa e da Segurança pelo INEST/UFF. Especialista em Direito Militar e em Direito em Administração Pública. Bacharel em Direito pela Universidade Estácio de Sá. Possui Licenciatura Plena em Geografia pela UFPE. É Oficial do Exército Brasileiro e Professor da Academia Militar das Agulhas Negras (AMAN) e da Associação Educacional Dom Bosco. Vencedor do IV Prêmio Marechal-do-Ar Casimiro Montenegro Filho, da SAE/PR (Categoria Artigo Científico: Cibernético).

Lista de ilustrações

Lista de abreviaturas e siglas

ATR	sistema de auxílio a reconhecimento e mira
C&T	ciência e tecnologia
C2	comando e controle
C3IGE	comando, controle, comunicações, informática e guerra eletrônica
C4I	comando, controle, comunicação, computadores e inteligência
C4IRS	comando, controle, computação, comunicação, inteligência, vigilância e reconhecimento
CDCiber	Centro de Defesa Cibernética do Exército Brasileiro
CERT	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança da Informação
CIA	Agência Central de Inteligência (EUA)
CiberRI	Relações Internacionais Cibernéticas
CICTE	Comitê Interamericano contra o Terrorismo (OEA)
CITEL	Comissão Interamericana de Telecomunicações (OEA)
CMI	Complexo Militar Industrial (EUA)
CPDN	Ciclo de Planejamento da Defesa Nacional (Argentina)
DIP	Direito Internacional Público
DoD	Departamento de Defesa (EUA)
DoS	negação de serviço
DPDN	Diretriz de Política de Defesa Nacional (Argentina)
ENABED	Encontro Nacional da Associação Brasileira de Estudos de Defesa
END	Estratégia Nacional de Defesa (Brasil)
ENISA	Agência Europeia para a Segurança das Redes e da Informação
EO/IR	eletro-óptica e infravermelho
EUA	Estados Unidos da América
FSB	Serviço Federal de Segurança (Rússia)
GAP	Grupo de Ação Preventiva (Argentina)
GCR	guerra centrada em redes
GICI	Grupo de Infraestruturas Críticas da Informação (Argentina)

GSI-PR	Gabinete de Segurança Institucional da Presidência da República (Brasil)
ICIC	Infraestruturas Críticas de Informação e Segurança Cibernética (Argentina)
Interpol	Organização Internacional de Polícia Criminal
IP	Internet Protocol
KGB	Comitê de Segurança do Estado (antiga URSS)
LBDN	Livro Branco de Defesa Nacional (Brasil)
MIRILADO	material, infraestrutura, recursos humanos, informação, logística, adestramento, doutrina e organização
OEA	Organização dos Estados Americanos
ONG	organização não governamental
ONTI	Gabinete Nacional de Tecnologias de Informação (Argentina)
ONU	Organização das Nações Unidas
OTAN	Organização do Tratado do Atlântico Norte
P&D	pesquisa e desenvolvimento
PDN	Política de Defesa Nacional (Brasil)
PND	Política Nacional de Defesa (Brasil)
PLANCAMIL	Plano de Capacidades Militares (Argentina)
PNICIC	Programa Nacional de Infraestruturas Críticas de Informação e Segurança Cibernética (Argentina)
PPP	parceria público-privada
RAM	revolução nos assuntos militares
REMJA	Reunião de Ministros da Justiça ou de Outros Ministros ou Procuradores-Gerais das Américas (OEA)
RI	Relações Internacionais
SIC	Segurança da Informação e Comunicações (Brasil)
TIC	tecnologias de informação e comunicação
UAS	sistemas aéreos não tripulados
UNASUL	União de Nações Sul-Americanas
USAF	Força Aérea (EUA)
VANT	veículo aéreo não tripulado
VTNT	veículo terrestre não tripulado
WWW	rede mundial de computadores

Sumário

PREFÁCIO

Segurança e Defesa Cibernética neste Admirável Mundo Novo

Joanisval Brito Gonçalves[1]

Nem os maiores escritores de ficção do início do século XX conseguiriam prever quão transformado estaria o mundo cem anos depois. No campo das relações internacionais, potências continuariam disputando poder (entendido como capacidade de influência) e buscando a hegemonia no sistema anárquico (como definiria qualquer realista clássico). A novidade, porém, é que essa disputa por maior influência envolveria outros atores, muitos deles não-estatais, e uma nova dimensão: o espaço cibernético. E esse admirável mundo novo exigiria que estudiosos das relações internacionais revissem seus conceitos, que homens de Estado repensassem como se portar perante a opinião pública e a comunidade das nações, e que todos que se preocupam com segurança e defesa transformassem sua própria percepção de como atuar em prol dos interesses do Estado e para a proteção da sociedade. A própria ideia de soberania assume nova dimensão, assim como a noção de conflito e guerra.

Desde os primórdios da história da humanidade, as relações internacionais se fundamentam em dois alicerces: o comércio e a guerra. E no mundo globalizado do século XXI, onde o comércio entre

1 Os conceitos e opiniões aqui emitidos são exclusivamente do autor e não refletem necessariamente as posições de entidades às quais esteja vinculado.

os povos alcança patamares nunca vistos, a guerra pela defesa das riquezas e pela garantia desse comércio se vê também diante de uma nova dimensão. Assim, enquanto o século XX testemunhou o advento de uma terceira dimensão no fenômeno da guerra (a aeroespacial), o conflito no século XXI defronta-se com outra nova: o espaço cibernético.

Indubitavelmente, entre as grandes transformações do mundo contemporâneo (ou pós-moderno) está o início da era virtual. Certamente, parte significativa da humanidade ainda desconhece muito desse novo universo, ainda que dificilmente sobreviva sem ou fora dele. Quanto aos Estados e outras organizações, as novas tecnologias se mostram determinantes do desenvolvimento. E, como consequência, a necessidade de segurança no novo cenário é premente.

O grande desafio para todos os que nascemos antes da Internet e desse Big Bang tecnológico ocorrido ao final da Guerra Fria é exatamente como entender e se portar na nova realidade em que o mundo está ao alcance de um toque no *smartphone*, em que os sistemas de abastecimento de água e eletricidade, transportes, comunicações, finanças e tudo mais com que lidamos no dia a dia estão conectados a um universo virtual, do qual nos tornamos completamente dependentes. Se isso se aplica no campo pessoal, mais ainda se dá no espaço coletivo, particularmente nas relações entre os povos. Por consequência, tem-se cooperação e conflito, ou seja, a essência da vida humana e das nações.

Como as Relações Internacionais, a Segurança e a Defesa podem ser afetadas por essa realidade cibernética – eis o tema do presente livro. Trata-se de uma obra conjunta de acadêmicos sul-americanos que meritoriamente se aventuram neste novo campo. Sua leitura, portanto, é imprescindível para todo aquele interessado em Segurança e Defesa Cibernética.

O primeiro capítulo volta-se à percepção do ciberespaço sob

o prisma das principais correntes teóricas de Relações Internacionais. Destacando que vivemos hoje em um mundo mais complexo, multipolar no campo político, com novas necessidades para Estados e para as pessoas, o autor, Igor Acácio, assinala que tem por objetivo elencar um panorama teórico explicativo sobre os principais desafios engendrados pelo ciberespaço para os estudos de Segurança Internacional. Assim, neste "novo arranjo geopolítico em constante transformação", os Estados buscam moldar-se frente às novas necessidades, e a análise das Relações Internacionais deve considerar, mais do que nunca, os níveis individual, estatal e sistêmico para tentar explicar a realidade.

Acácio também assinala que cada vez mais cientistas sociais e humanistas têm interferido em um campo dominado tradicionalmente por especialistas em Ciência da Computação: o da Segurança Cibernética. E os internacionalistas, por sua vez, precisam ocupar esse espaço, pois a segurança internacional hoje é indissociável da cibernética.

O ciberespaço, portanto, tem que ser considerado em qualquer paradigma teórico de Segurança nas Relações Internacionais no século XXI (quando se evidenciam novos atores, novos cenários, novas armas e novas modalidades de conflito e de projeção de interesses). Além disso, é algo novo na arte da guerra, e Acácio bem lembra que, "ao contrário do uso estratégico da pólvora ou dos cavalos, que causaram uma verdadeira revolução militar e de outros elementos para a evolução da guerra, o ciberespaço é o único destes que se prostra, simultaneamente, como uma ferramenta (meio) e um ambiente (fim)". Daí a complexidade da análise desse fenômeno.

No segundo capítulo, de Walfredo Ferreira Neto e Gills Vilar Lopes, o foco é na influência do mundo cibernético na percepção das fronteiras interestatais. Tem-se, de fato, com o ciberespaço, uma nova noção de fronteira e, consequentemente, de território. O corolário é, ainda, uma mudança na percepção de soberania.

Assim, os autores discorrem sobre como a percepção weberiana clássica de Estado e soberania tem sido afetada pelo mundo cibernético. O objetivo do capítulo é transpor as questões tradicionais de territorialidade para o ambiente cibernético, uma vez que, "embora destituído de fisicalidade, o ciberespaço é um lugar". Fundamental, portanto, que esse espaço seja protegido.

Os Estudos Estratégicos são tratados no terceiro capítulo, em que Maurício Nothen e Eduardo Bohn buscam contextualizar a inserção das análises sobre o ciberespaço no âmbito desses estudos. Destacam, também, como o tema tem sido tradado no Brasil e assinalam a dificuldade em enquadrar o ciberespaço em padrões analíticos consagrados do conhecimento estratégico, o que "representa uma negação imprudente da oportunidade de análise de um conjunto de fatores de relevância inegável em um cenário de combate contemporâneo centrado em redes e sistemas computadorizados".

Aspecto interessante da análise de Nothen e Bohn é a assinalação do espaço cibernético como novo domínio do combate paralelamente à dificuldade de se validar essa percepção. Observemos, nesse sentido, que tempo se faz necessário para maior reflexão sobre o uso do espaço cibernético no contexto da guerra e, sobretudo, na teorização a respeito. Isso, a nosso ver, requer esforço hercúleo de todos os que se prontifiquem a pensar a guerra e o combate neste novo ambiente e sob diferentes prismas. Eis mais um mérito da presente obra.

O uso da cibernética nas operações de contrainsurgência pelos Estados Unidos da América (EUA) é o tema do quarto capítulo. Nele, Alcides Peron discorre sobre a mudança (importantíssima, que fique claro) no modo como a guerra vem sendo conduzida nas últimas duas décadas: com uma crescente renúncia ao combate direto e sua substituição por novos meios tecnológicos que distanciam o

combatente do campo de batalha, garantindo sua segurança e fazendo com que o conflito se assemelhe a um jogo de videogame.

Em um cenário de conflitos assimétricos, em que, nas democracias, os tomadores de decisão têm que lidar com uma forte pressão da opinião pública contra iniciativas militares nas quais nacionais seus possam sacrificar a vida, países como os EUA têm passado por uma revolução militar e a tecnologia assume papel primordial. Daí Peron assinalar que, "buscando combater o terrorismo, a maioria das operações militares (...) tem sido categorizada enquanto ações 'cirúrgicas', possibilitadas pelo uso de diversos tipos de tecnologias cibernéticas, sistemas informacionais, redes de comunicação via Internet e redes de telefonia móveis, bem como por interfaces de controle remoto, tais quais os chamados *drones* e as Armas Distanciadoras (*Stand-off Weapons*)" e que "as operações militares estadunidenses têm se 'virtualizado', ou seja, têm tornado-se um processo pelo qual a mediação virtual das tecnologias militares resulta em uma reorganização no modo como a violência se atualiza, ao mesmo tempo em que há uma legitimação da forma como ela é lutada, supostamente 'limpa' e precisa".

Particularmente interessante para o leitor brasileiro é o capítulo cinco, de Sol Gastaldi e Candelas Justribó, no qual as autoras argentinas apresentam suas reflexões sobre a Estratégia de Segurança e Defesa Cibernética da Argentina. Afinal, é de extrema relevância que os brasileiros conheçam a maneira como os irmãos platinos têm lidado com o assunto. Convém destacar do capítulo a preocupação argentina com as chamadas "estruturas estratégicas da informação" e com os riscos de ataques cibernéticos contra as infraestruturas críticas (que recentemente passaram a ser denominadas no Brasil de "estruturas estratégicas"). As consequências certamente seriam das mais danosas: de "dano à imagem da organização governamental afetada" e "acesso não autorizado ou alteração de dados pessoais contidos em bancos

de dados" a interferências em serviços essenciais de transporte, comunicações e abastecimento.

Notemos, em se tratando de ataques cibernéticos, que "embora produzidas no âmbito virtual do ciberespaço" essas ações "são resultado do interesse dos Estados em produzir alterações e/ou mudanças no mundo físico", asseveram as autoras. Importante, então, o envolvimento do Estado na proteção do espaço cibernético e na Segurança Cibernética. Atenção deve ser dada ao "Programa Nacional de Infraestruturas Críticas e Segurança Cibernética" argentino, "semente da futura Estratégia Nacional de Segurança Cibernética".

A experiência argentina permite, ainda, uma reflexão sobre a importância de se considerar sistemas de computação e de comunicação militares como estruturas estratégicas, as quais devem estar sempre operacionais. Nesse sentido, quando vislumbramos o cenário brasileiro, aumenta a preocupação sobre nossas vulnerabilidades. Será que o Brasil está em condições de repelir um ataque cibernético contra suas estruturas estratégicas? O que se tem feito de concreto e efetivo a respeito?

A inquietação quanto às vulnerabilidades brasileiras aumenta quando se chega ao sexto capítulo desta obra, de Ahmina Solsona e Alexandre Leite, que trata da condição da República Popular da China (RPC) como potência cibernética. Ao apresentarem um cenário internacional em que os países asiáticos se destacam quando o tema é conflito cibernético, os autores fazem referência à China como "a grande potência", com capacidade para desencadear ataques contra pessoas, organizações e governos: "a China é considerada potência cibernética por parte de países como Estados Unidos, Austrália, França, Reino Unido, Índia, Japão, Alemanha e Coreias, e é, por eles, acusada de atos cibernéticos contra suas redes e sistemas informacionais de governo".

Além de cenário para eventuais incursões ofensivas, com a destruição de dados e capacidades estratégicas de adversários, os chineses

também veriam no espaço cibernético um campo fértil para reunir conhecimento "econômico e tecnológico de seus oponentes", inclusive por meio de espionagem. Daí a necessidade de se estar preparado, em âmbito governamental (mas também privado), para fazer frente às ações chinesas.

O capítulo conduz, finalmente, a uma reflexão sobre como a Segurança Cibernética é tema relevante nas relações entre as grandes potências. A referência é sobre a política externa dos EUA e da RPC no campo cibernético, onde um percebe o outro como ameaça. Nessa "nova Guerra Fria", envolvendo chineses e norte-americanos, o ciberespaço é mais um campo de batalha.

Se os capítulos anteriores enfatizam a dimensão conflitiva, a última contribuição do livro, de autoria de Lucas Fonseca e Tiago Delgado, traz o foco para a cooperação, em especial na cooperação internacional. O caso estudado é o da "Estratégia Interamericana de Combate a Ameaças Cibernéticas", conduzida pela Organização dos Estados Americanos (OEA), em parceria com os Estados e com o terceiro setor. O capítulo destaca a necessidade de construção de uma cultura de Segurança Cibernética latino-americana.

Um dos dilemas tratados no texto de Fonseca e Delgado é exatamente a conciliação entre a liberdade da Internet e a iniciativa de regulação desse meio por alguns governos, sob o argumento da segurança. Nosso descrédito na capacidade regulatória do ambiente virtual permanece, mas o capítulo serve para chamar a atenção para a necessidade de crescente cooperação internacional para se lidar com os problemas da rede, particularmente os relacionados aos crimes cibernéticos. Tem-se aí um grande desafio para as próximas décadas.

Ao concluir a leitura de *Relações Internacionais Cibernéticas*, certamente somos instados a pensar em nossa situação neste ambiente virtual, como indivíduos e cidadãos, e, mais ainda, na atuação de

nossos governos em um cenário tão complexo e imprevisível. A conclusão do internacionalista é de que é impossível pensar as relações internacionais no mundo físico sem pensar naquelas do mundo virtual. Sob a ótica dos Estudos Estratégicos, fica evidente que é inconcebível planejar Defesa e Segurança sem levar em consideração a Defesa e a Segurança Cibernéticas.

No caso do Brasil, o que percebemos é o quanto ainda precisamos evoluir no trato de assuntos tão sensíveis. Ainda que haja referência à Segurança e à Defesa Cibernéticas em políticas de Estado como a Política Nacional de Defesa (PND), muito há a ser feito. O País precisa investir mais na proteção contra ataques cibernéticos, tanto de suas estruturas governamentais quanto do conjunto da sociedade.

Dois anos após as revelações de que nossos sistemas foram devassados por ações de governos estrangeiros, ainda estamos tremendamente vulneráveis. Faltam engajamento governamental e envolvimento dos tomadores de decisão em medidas efetivas que tornem o País e seu povo mais protegidos. Falta o fomento a uma cultura de Segurança Cibernética junto aos agentes públicos e à população em geral.

Neste início de século XXI, fica evidente que temos de aprender a nos conduzir, como indivíduos, sociedade e Estado, neste novo cenário, onde a fronteira entre o ambiente virtual e o físico é tremendamente nebulosa, e onde os acontecimentos e atitudes no ciberespaço afetam diretamente o universo fora dele. Enfim, sobretudo aqueles que nascemos antes do advento da Internet e da expansão do espaço cibernético, temos que reaprender a viver neste admirável mundo novo!

Brasília, janeiro de 2015.

APRESENTAÇÃO

Relações Internacionais Cibernéticas (CiberRI)

Marcos Aurélio Guedes de Oliveira
Ricardo Borges Gama Neto
Gills Vilar Lopes

Este terceiro volume da *Coleção "Defesa e Fronteiras Virtuais"* consolida o trabalho que vem sendo desenvolvido por uma rede de pesquisadores de diferentes áreas do conhecimento – como Ciência Política, Relações Internacionais (RI), Geografia e História – em torno dos temas estratégicos da Defesa Nacional e da Segurança Internacional. Essa rede acadêmica, composta por profissionais de importantes instituições civis e militares de ensino superior do Brasil, surgiu da importância que as questões de Defesa têm tomado no País, sobretudo quanto aos novos alcances estratégicos e político-militares do uso das tecnologias de informação e comunicação (TIC).

Imprescindível para a implantação dessa rede é o patrocínio do *Programa de Apoio ao Ensino e à Pesquisa Científica e Tecnológica em Assuntos Estratégicos de Interesse Nacional* (Pró-Estratégia)[1], financiado pela *Coordenação de Aperfeiçoamento de Pessoal de Ensino Superior* (CAPES) e apoiado pela *Secretaria de Assuntos Estratégicos da Presidência da República* (SAE/PR).

O primeiro volume da coleção, intitulado "Segurança e Defesa Cibernética: da fronteira física aos muros virtuais" e publicado em

1 Sítio virtual oficial do Pró-Estratégia: http://capes.gov.br/component/content/article?id=5157:programa-de-apoio-ao-ensino-e-a-pesquisa-cientifica-e-tecnologica-em-assuntos-estrategicos-de-interesse-nacional-pro-estrategia.

2014, obteve impacto positivo na comunidade de estudiosos de Defesa, sendo lançado durante os Encontros Nacionais da Associação Brasileira de Estudos de Defesa (ENABED) e da Associação Brasileira de Ciência Política (EN-ABCP), bem como no Ministério da Defesa"[2].

O segundo volume da Coleção, "Cooperação Interagências", foi lançado em 2015, abrindo espaço para a discussão sobre os aspectos que envolvem a interação entre agências estratégicas para o Brasil.

Nesse sentido, o terceiro volume da Coleção reflete novamente o crescente interesse acadêmico dado ao tema do ciberespaço nos assuntos de Segurança e Defesa, cuja materialidade pode ser vista com a realização do *I Seminário de Relações Internacionais Cibernéticas* (I CiberRI-UFPB 2014)[3], que contou com o patrocínio do Projeto *Vigilância nas fronteiras e muros virtuais*, no âmbito do Pró-Estratégia. O tema do evento foi praticamente o mesmo do deste volume, a saber: *Tendências, desafios e oportunidades para os Estudos de Segurança Internacional*. A partir dele, alguns contatos com pesquisadores da área de Defesa foram articulados durante o ENABED 2014, em Brasília, com o intuito de produzir a obra que o leitor tem agora em mãos.

Assim como ocorre com a maioria dos conceitos[4] engendrados para debater a Segurança Cibernética[5] e a Defesa Cibernética no âmbito da política internacional, a ideia de se estudar os impactos ciberespaciais nas relações internacionais e vice-versa também nasce com uma analogia. De um lado, *Relações Internacionais Cibernéticas*

2 Cf. http://brasil.gov.br/defesa-e-seguranca/2014/10/defesa-cibernetica-no-brasil-e-tema-de-simposio-em-brasilia.

3 Sítio virtual oficial do CiberRI-UFPB: http://ccsa.ufpb.br/dri/CiberRI.

4 Tais como: Guerra Cibernética, Crime Cibernético, Espionagem Cibernética, Terrorismo Cibernético, Arma Cibernética etc.

5 Com exceção do acrônimo "CiberRI" e do já consagrado substantivo "ciberespaço" – ou espaço cibernético –, opta-se, ao longo dos capítulos, pelo adjetivo "cibernético" após os termos que dizem respeito ao ciberespaço, ao invés do prefixo "ciber". Por exemplo, apesar de a forma "Ciberguerra" ser aceita, prefere-se "Guerra Cibernética".

(CiberRI) surge, no início do século XXI, da necessidade de se criar e defender um subcampo de RI que consiga satisfatoriamente compreender as idiossincrasias e os impactos internacionais do e no ciberespaço, com especial atenção à Guerra Cibernética e à Espionagem Cibernética. Do outro, com o próprio campo de RI não foi diferente: ele surgiu, no início do século XX, com o objetivo principal de compreender, *a priori*, o acontecimento/fenômeno da guerra, para, *a posteriori*, evitá-lo.

Apesar de a designação "Relações Internacionais Cibernéticas" ou "CiberRI" ser utilizada pela primeira vez no Brasil por meio dos trabalhos patrocinados pelo Projeto *Vigilância nas fronteiras e muros virtuais*, trata-se da tradução literal do título de um projeto de pesquisa encabeçado por docentes dos Departamentos de Ciência Política do *Massachusetts Institute of Technology* (MIT) e de *Harvard University*[6]. Todavia, tal trabalho conjunto entre as duas instituições é apenas um exemplo dentre os diversos encontrados alhures, que tratam de temas correlatos a CiberRI[7]. Nesse viés, entendemos que chegou a hora de o Brasil fazer parte também desse novo movimento de (re)descoberta e (re)adaptação dos estudos sobre as relações internacionais.

Assim, podemos vislumbrar CiberRI em quase todo acontecimento internacional que tenha impacto tanto *no* ciberespaço – especialmente, quanto às questões que envolvem a Internet e as redes de telefonia móveis – quanto a partir *dele*. Por certo, os estudos de CiberRI podem ser encaixados nas grades curriculares de graduação ou pós-graduação em Ciência Política e, especialmente, em RI. Algumas universidades[8] já estão até mesmo indo mais além e criando

6 Sítio oficial do projeto *Explorations in Cyber International Relations* (ECIR): http://ecir.mit.edu.

7 Eis algumas universidades que possuem instituto, projeto ou pós-graduação voltado(a) a alguma temática de CiberRI: Aberystwyth University, Cambridge University, Harvard University, MIT, New York University, Oxford University, Stanford University etc.

8 *E.g.*: Universidades Aberystwyth, George Washington, Oxford e de Defesa Nacional (EUA).

pós-graduação (*lato sensu* e *stricto sensu*) em temas concernentes a CiberRI, e não simplesmente voltados exclusivamente a aspectos técnicos ou tecnológicos.

Nesse sentido, o estudo sistematizado de CiberRI pode ser invocado, por exemplo, para analisar, descrever ou explicar os seguintes acontecimentos internacionais: a ação de grupos hacktivistas na Primavera Árabe; a atuação do Partido Pirata no Parlamento Europeu; a utilização de armas e ataques cibernéticos nos conflitos internacionais do século XXI; as reverberações das denúncias de Snowden e do WikiLeaks; as discussões sobre Governança da Internet no âmbito do fórum criado pelas Nações Unidas; a cooperação internacional em matéria de Crimes Cibernéticos, dentre outros.

Como se vê, o leque de inferências é assaz amplo em CiberRI. Por causa disso, fizemos a opção de selecionar, para este terceiro volume, apenas um subcampo de RI que necessariamente vincula estreitamente as questões militares às relações internacionais[9], a saber: (Estudos de) Segurança Internacional ou Estudos Estratégicos (Internacionais).

Todavia, salientamos que, apesar de uma forte escola de pensamento entender que os Estudos de Segurança devam ser conduzidos não apenas em relação aos setores tradicionais – militar e econômico[10] –, este terceiro volume da *Coleção "Defesa e Fronteiras Virtuais"* busca dar ênfase sobretudo ao papel estratégico da caserna e dos serviços de Inteligência de Estado em suas atuações coordenadas no ciberespaço.

Para se ter uma noção da importância deste tema, observa-se que a Política Nacional de Defesa (PND) e a Estratégica Nacional

9 Domício Proença Jr e Eugenio Diniz, *Política de defesa no Brasil: uma análise crítica* (Brasília: UnB, 1998), 2.

10 Barry Buzan, Ole Wæver e Jaap de Wilde, *Security: a new framework for analysis* (Boulder: Lynne Rienner, 1998), 239.

de Defesa (END) brasileiras[11] apregoam justamente que o Setor Estratégico Cibernético (St ciber) é uma das três áreas imprescindíveis para o desenvolvimento e a defesa do País. Mais que isso, a ainda não aprovada Política Nacional de Inteligência (PNI) já apontara, antes mesmos de as revelações de Snowden estourarem, para a necessidade de o Brasil investir sistematicamente em Segurança Cibernética, no que concerne aos serviços de Inteligência de Estado.

Assim, o objetivo deste livro não é trazer acriticamente conceitos técnicos de Segurança da Informação ou de cibernética para RI, mas sim proporcionar um panorama introdutório das principais *oportunidades e desafios* que cercam o recente diálogo entre essas duas áreas. Por isso que, ao contrário do primeiro volume, selecionamos apenas jovens pesquisadores para apresentarem e debaterem os principais temas dessa seara.

Nesse viés, o presente livro foi divido em três grandes partes, oferecendo ao leitor a oportunidade de transitar, não linearmente, entre os capítulos, pelos aspectos teóricos, empíricos e metodológicos[12] que cercam esse novo subcampo de estudo.

Bem-vindos às Relações Internacionais Cibernéticas (CiberRI)!

11 Brasil, *Política Nacional de Defesa (PND) e Estratégia Nacional de Defesa (END)* (Brasília: Ministério da Defesa, 2012), http://www.defesa.gov.br/arquivos/estado_e_defesa/END-PND_Optimized.pdf, acessado em 12 dez. 2014.

12 Um glossário com 28 termos aplicados a CiberRI e uma lista de leitura com mais de 150 referências encontram-se no final deste livro.

PARTE 1

OPORTUNIDADES E DESAFIOS TEÓRICOS

Segurança Internacional no século XXI: o que as teorias de Relações Internacionais têm a dizer sobre o ciberespaço?[1]

Igor Daniel Palhares Acácio

Introdução

É possível afirmar que, na literatura referente a ontologias e epistemologias de Relações Internacionais (RI), as chamadas teorias de inspiração "positivista" não foram capazes de antecipar o fim da Guerra Fria, conquanto seu forte componente preditivo e mesmo normativo. Diante de tais limites explicativos, adiciona-se, ao novo contexto internacional, um novo arranjo geopolítico em constante transformação[2]. O mundo das fixas alianças e das tradicionais guerras interestatais tornou-se mais complexo. A complexidade intensificou-se no Sistema Internacional, desafiando analistas com suas crises humanitárias, guerras civis, unipolaridade militar dos Estados Unidos da América (EUA) e, simultaneamente, espionagem, guerra cibernética etc.[3]

1 Este capítulo é uma versão adaptada e modificada de: Igor D. P. Acácio e Gills Lopes, "Segurança internacional no século XXI: o que as teorias de Relações Internacionais têm a falar sobre o ciberespaço?", *Anais do 36º Encontro Anual da ANPOCS* (Caxambu: ANPOCS, 2012), http://www.anpocs.org/portal/index.php?option=com_docman&task=doc_details&gid=8169&Itemid=76, acessado em 23 dez. 2014.

2 Shiguenoli Miyamoto, "A segurança e a ordem internacionais no limiar do novo século", in *Relações Internacionais: interdependência e sociedade global*, org Odete M. de Oliveira, Arno Dal Ri Júnior, pp. 681-728 (Ijuí/RS: UNIJUÍ, 2003), 681.

3 Kai E. Lehmann, "Unfinished Transformation: the three phases of complexity's emergence into international relations and foreign policy", *Cooperation and Conflict*, Vol. 47, No. 3, pp. 404-413 (2012).

Diante de tal debate internacional e da relativa escassez, no Brasil, de estudos acadêmicos sobre o tema, este trabalho tem como objetivo elencar um panorama teórico-explicativo sobre os principais desafios engendrados pelo ciberespaço para os Estudos de Segurança Internacional, tendo como substrato as Teorias de RI. Nesse intuito, parte-se da visão de quatro correntes teóricas internacionalistas, a saber: Realismo, Escola Inglesa, Neoliberalismo (Institucionalista) e Escola de Copenhague.

Dadas as características inerentes do século XXI – Estados, indivíduos, empresas e estruturas estratégicas cada vez mais conectados ao ciberespaço[4] – a principal hipótese deste texto é a de que os Estados buscam moldar-se frente às novas oportunidades, sendo necessário, portanto, recorrer a uma abordagem que conjugue diferentes campos da teoria de RI. Na chamada era da informação, apresentam-se os desafios de compreensão e ação nos diversos níveis de análise: indivíduo, Estado e sistema.

Nye[5] enfatiza que, até pouco tempo atrás, o subcampo da Segurança Cibernética tem sido dominado por especialistas em Ciência da Computação. Com o crescimento exponencial do uso do ciberespaço – e especialmente da Internet –, tal domínio é pertinente à inferência de cientistas sociais e humanistas. Para que este domínio comece a se abrir à causa internacionalista, por exemplo, faz-se necessário identificar alguns pontos – comuns ou não – entre as questões que envolvem o ciberespaço enquanto fonte de insegurança internacional e as principais correntes teóricas de RI.

A coleta dos dados desta pesquisa foi realizada através de

4 Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem", in *Cyberpower and National Security*, org Franklin D. Kramer, Stuart Starr e Larry K. Wentz (Washington, DC: NDUP, 2009), 24-42.

5 Joseph Nye, "Nuclear lessons for cyber security?", *Strategic Studies Quarterly*, Vol. 5, No. 4, pp. 18-37 (2011), 18.

(re)leituras – contextualizadas à questão cibernética como fonte de insegurança internacional – de determinadas obras clássicas de teóricos das RI e também de autores incluídos no presente debate acadêmico, com o intuito de sistematizar e contrapor visões sobre o tema em tela. Portanto, pauta-se, aqui, por uma pesquisa qualitativa, cuja principal ferramenta é a análise bibliográfica.

O presente texto busca, ainda, categorizar, as abordagens teóricas aqui escolhidas em dois grupos. No primeiro, com características mais ontológicas, estão aquelas que buscam explicar, de maneira atemporal, elementos mais genéricos concernentes ao tema em análise, como: política internacional, guerra e poder. No segundo grupo, cujo caráter explicativo sobre a relação entre ciberespaço e segurança internacional é estudado em termos mais pragmáticos, enquadram-se aquelas teorias mais propícias em lidar com as seguintes questões: novos atores, novos cenários, novas armas, novas modalidades de conflito e projeção de interesses.

O panorama teórico levado a cabo em cada subseção divide-se, para fins expositivos, em dois aspectos:

(1) Em trabalhos seminais de cada corrente teórica analisada à luz de realistas (Hans Morgenthau e Kenneth Waltz), racionalistas da Escola Inglesa (Hedley Bull[6] e Martin Wight), neoliberais (Robert Keohane e Joseph Nye) e da Escola de Copenhague (Buzan, Wæver e Wilde); e
(2) Alguns dos principais autores que tratam o tema do ciberespaço como uma questão de segurança nacional e internacional, enquadrando-os nas escolas teóricas

6 Hedley Bull, *A sociedade anárquica: um estudo da ordem na política mundial* (Brasília e São Paulo: Ed. UnB/IPRI/IOESP, 2002).

supracitadas: Richard Clarke e Robert Knake; John Arquilla e David Ronfeldt; o próprio Joseph Nye; Helen Nissenbaum e Lene Hansen.

Considerando o atual cenário político-internacional multipolar, indaga-se: como as teorias de RI buscam explicar os profundos desafios engendrados pelo ciberespaço? O fato é que a questão do ciberespaço se prostra como um exemplo paradigmático de mudança no foco dos problemas de segurança internacional no contexto contemporâneo.

O restante do presente capítulo se divide da seguinte forma: a próxima seção tece considerações sobre a questão da guerra cibernética e da valorização da questão do ciberespaço como um tema de segurança internacional; as quatro seções seguintes dizem respeito a cada uma das correntes teóricas e suas possíveis utilizações para a questão do

Guerra cibernética: levando a Segurança Internacional até o ciberespaço

O conceito de guerra cibernética encontra muitos significados e, não raras exceções, divergências entre autores. Por exemplo, em uma visão holística e pragmática, Bezerra[7] informa que a guerra cibernética é o "uso da Internet como ferramenta de ação política ou militar". Arquilla e Ronfeldt[8], por sua vez, entendem que esta nova modalidade é mais uma forma de os Estados guerrearem entre si. Já para Clarke e Knake[9], ela é entendida como uma alternativa à guerra convencional - que pode, *de facto*, aumentar a ocorrência de combates tradicionais - cujos principais alvos são civis, pois estes são os que mais dependem

7 Marcelo Bezerra, "Artigo sobre Guerra Cibernética 'Cyberwar'", DSIC/DSI-PR, 2009, http://dsic.planalto.gov.br/artigos/71-artigo-sobre-guerra-cibernetica-qcyberwarq, acessado em 29 set. 2012.

8 John Arquilla e David Ronfeldt, eds, *Athena's Camp: preparing for conflict in the information age* (Santa Monica, CA: RAND Corporation, 1997), Cap. 2, 30.

9 Richard A. Clarke e, Robert K. Knake, *Cyber war: the next threat to national security and what to do about it* (Nova Iorque: HarperCollins, 2010), xi.

de estruturas estratégicas[10] baseadas nas tecnologias de informação e comunicação (TIC)[11]. A possibilidade real de interrupção, sabotagem ou mesmo dano a essas infraestruturas podem potencializar o curso de uma guerra (como ocorreu na guerra russo-georgiana, em 2008) ou mesmo de um ataque não declarado (como no famoso caso Rússia-Estônia, de 2007), sobretudo na era da informação.

Isto posto, prover a defesa estratégico-militar desse espaço recai sobre os ombros das forças armadas, compreendendo, assim, a chamada Defesa Cibernética[12].

Como ocorre na esfera dos Estudos de Segurança e de Defesa, cabe aqui diferenciar Defesa Cibernética de Segurança Cibernética, embora, como lembram Villa e Reis[13], "[...]pode-se dizer que o conceito de segurança tem uma referência defensiva[...]". Segurança Cibernética se refere ao combate e à prevenção dos chamados crimes cibernéticos, na esfera pública, ou seja, no nível político. Já Defesa Cibernética, sendo o "conjunto de ações defensivas, exploratórias e ofensivas, no contexto de um planejamento [estratégico] militar, realizadas no espaço cibernético[...]"[14], deve ser coordenada por um órgão militar. No que tange aos aspectos operacional e tático da defesa do ciberespaço, são as Forças Armadas que aplicam a estratégia, com a finalidade de prevenir ou contra-atacar em caso de guerra cibernética.

---

10 Estruturas estratégicas – antigamente denominadas de infraestruturas críticas – não são apenas as estruturas físicas, mas também os serviços, bens e sistemas que, caso interrompidos ou danificados, podem ter implicações políticas, securitárias e, até mesmo, internacionais.

11 Myrian D. Cavelty e Elgin M. Brunner, "Introduction: information, power and security – an outline of debates and implications", in *Power and Security in the Information Age*, ed M. D. Cavelty, V. Mauer e S.F. Krishna-Hensel (Hampshire: Ashgate, 2007); Myrian D. Cavelty, "Cyberwar: concept, status quo and limitations", *CSS Analysis in Security Policy*, Issue 71, 2010.

12 Paulo S. M. de Carvalho, "A defesa cibernética e as infraestruturas críticas nacionais", *Apresentações do X Ciclo de Estudos Estratégicos*, Rio de Janeiro (2011), 8.

13 Rafael Villa e Rossana Reis, "A segurança internacional no pós-Guerra Fria: um balanço da teoria tradicional e das novas agendas de pesquisa", *BIB: R. bras. de Informação Bibliográfica em Ciências Sociais*, São Paulo, No. 62, pp. 19-51 (2006), 20.

14 Carvalho, "A defesa cibernética", 8.

É o que resume o Quadro 1.

Quadro 1: Diferença entre Defesa Cibernética e Segurança Cibernética no Brasil

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

Fonte: Carvalho, "A defesa cibernética", 8.

O Realismo e o ciberespaço

A vertente inicial[15] do Realismo internacionalista enfatiza o caráter cíclico das relações internacionais, caracterizado por uma visão pessimista da condição humana transplantada para o comportamento dos Estados-Nação – e um privilégio destes ou de um agregado destes interagindo para a análise do cenário internacional.

O pensamento realista busca conferir racionalidade e reflexão científica aos estudos internacionalistas, no sentido de se formularem leis gerais sobre o comportamento dos Estados dentro da política internacional. Assim, princípios gerais[16] seriam sempre necessários e objetivos primeiros de um Estado, os quais poderiam, para sua manutenção e/ou sobrevivência, contar somente com suas próprias capacidades.

Para os realistas, a função primeira do estado é a de se manter enquanto tal, em um mundo cujas relações de força e poder não devem ser desprezadas; pelo contrário, elas devem ser realçadas quando da análise.

15 Cf. Edward H. Carr, *Vinte anos de crise* (Brasília: Ed. UnB/IPRI/IOESP, 2001); Hans J. Morgenthau, *A Política entre as Nações* (São Paulo: Ed. UnB/IOESP/IPRI, 2003).

16 Tais quais: equilíbrio de poder, pelo qual os Estados tenderiam a formar alianças para evitar preponderâncias; interesse nacional, maior justificador da ação internacional de um Estado; poder; e soberania.

Já a anarquia, princípio ordenador importante na perspectiva sistêmica ou estrutural da corrente realista[17] deve ser entendida como a ausência de um governo supraestatal que subjulgue à sua vontade aos demais Estados componentes no sistema internacional.

Em um sistema internacional anárquico no qual prevalecem as relações de poder, a insegurança é um elemento perene, e cada ator potencialmente experimenta diversos tipos de ameaças advindos do nível sistêmico. A anarquia internacional, portanto, implica a necessidade de cada Estado zelar por sua própria segurança, do que decorre que cada Estado adote uma política de defesa visando a este fim. Atualmente, parece ser essa a lógica por trás das políticas nacionais de defesa cibernética: cada Estado busca internamente os mecanismos de defesa contra as ameaças nacionais advindas do ciberespaço.

Pode-se inferir, da produção bibliográfica analisada para a realização deste trabalho, que os autores associados a um pensamento realista sobre o ciberespaço, em geral, entendem este campo como um novo domínio operacional para a atuação estatal, em que estes deveriam projetar mais poder e ganhar mais influência *vis-à-vis* outros Estados. Assim, seleciona-se, para sintetizar esta visão, o trabalho de Richard Clarke e Robert Knake, até porque os próprios autores, já no prefácio de seu livro, assumem-se tributários à visão neorrealista predominante na política nuclear estadunidense, própria da Guerra Fria.

Infere-se que a visão desses dois autores, aos olhos das Teorias de RI, é bastante permeada pelo Realismo, pois, para aqueles autores, são os Estados que constituem capacidades cibernéticas e sempre estão buscando maximizar seus interesses no ambiente operacional do ciberespaço[18]. Os autores apresentam a seguinte definição de guerra cibernética:

17 Kenneth Waltz,*Theory of International Politics* (California: Addison-Weasley, 1979).

18 Clarke e Knake, "Cyberwar", 70.

> É a penetração não autorizada em um computador ou rede de uma nação, por / em nome de / em apoio a um governo, ou qualquer outra atividade que afete um sistema computacional, no qual o objetivo é adicionar, alterar ou falsificar dados ou causar rompimento ou danos a um computador ou dispositivo de rede, ou a objetos controlados por computador.[19]

Adicione-se ainda que a abordagem de Clarke e Knake, centrada no Estado, também se constrói em torno da ideia de *National Accountability*, a qual significa que a responsabilidade sobre qualquer ataque cibernético, cuja localização geográfica parta – mesmo que não seja de computadores do governo ou patrocinados por agências governamentais – do Estado A para o Estado B, reside no governo daquele.

Para eles, há três aspectos articulados na questão do ciberespaço que tornariam uma guerra cibernética possível: falhas no desenho da Internet, falhas no *hardware* e no *software* e a crescente colocação *online* de sistemas críticos. Assim, baseados em uma série de eventos narrados, os autores afirmam que incontestavelmente o conflito interestatal envolvendo ataques cibernéticos já começou, desdobrando tal princípio em cinco sentenças sobre a guerra cibernética: (i) é real, (ii) acontece na velocidade da luz, (iii) é global, (iv) prescinde de campo de batalha e (v) já começou[20].

A Escola Inglesa e o ciberespaço

Deve-se frisar que os dois expoentes da Escola Inglesa – Martin Wight e Hedley Bull – não viveram o suficiente para testemunhar os avanços mais recentes nos microcomputadores e, em especial, a criação

19 Ibid., 228.

20 Ibid., 30-31.

da Internet. Busca-se, aqui, uma análise reflexiva sobre com o que ambos os autores poderiam contribuir para se entender melhor determinados acontecimentos políticos que surgem com alguns desafios impostos pelo ciberespaço.

A Escola Inglesa, com sua abordagem racionalista das relações internacionais, nega explicitamente a metodologia *behaviorista* posta pelo Neorrealismo e advoga pela manutenção da metodologia tradicionalista na política internacional. Em outras palavras, para esta corrente de pensamento de RI, o analista internacional deve utilizar-se de ferramentas filosóficas e valorativas holísticas para compreender a política interacional, que é, nas palavras daqueles autores, nada mais que a política do poder. Neste sentido, Wight afirma que "os homens possuem não só territórios, matérias-primas e armas, mas também opiniões e ideologias"[21], e que "seria insensato supor que os estadistas não se deixam levar por considerações de direito e justiça"[22]. Assim, colocar-se no lugar do estadista é uma ferramenta analítica desta corrente. Transpondo essa máxima para fenômenos mais recentes, como a análise política do ciberespaço, é possível utilizar tal técnica, por exemplo, quando das políticas tomadas pelo presidente russo Vladimir Putin, no que diz respeito à atuação estatal no ciberespaço. Ex-funcionário do extinto Comitê de Segurança do Estado (KGB), Putin sabe do papel imprescindível que a informação e a *guerra de informação* – utilização da propaganda para atingir fins políticos – possui. O Serviço Federal de Segurança (FSB), sucessor russo da KGB, é um dos poucos órgãos políticos no mundo que controla quase totalmente as ações tomadas no "vasto e incontrolável ciberespaço" russo[23]. Segundo Clarke e Knake[24], a

21 Martin Wight, *A política do poder* (Brasília: Ed. UnB/IPRI/IOESP, 2002), 69.

22 Ibid., 8.

23 Stanilaw Calandreli, "A batalha russa no ciberespaço" (2011), http://jornalggn.com.br/blog/luisnassif/a-batalha-russa-no-ciberespaco, acessado em 29 ago. 2014.

24 Clarke e Knake, op. cit., 148.

Rússia é um dos Estados mais bem preparados para uma eventual guerra cibernética. Portanto, o fato de se colocar na posição do presidente russo e observar as últimas investidas tomadas por aquele Estado no ciberespaço – cujo ápice está nos ataques cibernéticos, conjugados a bélicos, contra a Geórgia – pode ser uma alternativa à metodologia positivista de, por exemplo, prever os futuros passos russos quanto ao ciberespaço, sem levar em conta o histórico de quem (re)formula a política nacional.

Um importante nome dos estudos atuais da Escola Inglesa, Andrew Hurrell, seguindo preceitos deixados por Bull, utiliza-se das seguintes cinco instituições centrais para pensar um arcabouço (*framework)* analítico sobre a ordem internacional: o direito internacional, a balança de poder, o papel das grandes potências, a diplomacia e a guerra[25]. Como se percebe, a guerra, para essa escola de pensamento, é indissociável da política do poder. A análise que se busca realizar aqui não negligencia tal premissa advinda da Escola Inglesa; pelo contrário, enaltece-se o fato de que até mesmo a sociedade que mais acessa informações em todos os tempos não deixa de lado as possibilidades de se utilizar o ciberespaço como uma ferramenta – ou mesmo, uma extensão – da guerra. É neste sentido que Gills Lopes[26] advoga que essa sociedade hodierna que se utiliza do ciberespaço livre e anárquico como uma extensão de sua política pode ser epitetada de "cibersociedade anárquica".

A manutenção do *equilíbrio de poder* – outra instituições efetiva das relações internacionais, para a Escola Inglesa – em um cenário marcado, à época de Wight e Bull, pelas corridas nuclear e espacial coloca os formuladores de política em uma situação em que cada Estado percebe a ameaça nuclear de uma forma diferente. É o que parece acontecer

25 Andrew Hurrell, *On Global Order* (Oxford, U.K.: OUP, 2007), 4.

26 Gills Lopes M. Souza, "A cibersociedade anárquica: análise do uso das Tecnologias de Informação e Comunicação nos conflitos internacionais do século XXI à luz da Escola Inglesa de Relações Internacionais" (*Monografia do Curso de Relações Internacionais*, Universidade Estadual da Paraíba, 2010).

com alguns Estados atualmente: ao analisar as mais recentes políticas nacionais de defesa, determinados países, por não sofrerem ataques virtuais de grande vulto[27], buscam, no histórico de outros, a justificativa para a tomada de determinadas ações estratégicas no ciberespaço. É o caso, por exemplo, da Alemanha e da Holanda, que, em suas respectivas políticas nacionais de defesa, citam o *worm* Stuxnet[28] como uma ameaça real a ser evitada[29]. O Stuxnet entra neste debate por ser considerado, *grosso modo*, a primeira "arma cibernética" da história, uma vez que foi utilizado para ciberneticamente sabotar estruturas estratégicas do programa nuclear iraniano. A *percepção* dessa ameaça como sendo *real* gera outra máxima oriunda da Escola Inglesa: a de que "possuir armas sem dispor de uma política sólida é o mesmo que não possuí-las quando se fazem necessárias"[30].

A leitura de Wight, no que diz respeito às crises, parece ser bem oportuna às atuais análises sobre a securitização do setor cibernético. Diz ele que crise é "um período de equilíbrio simples" e "é caracterizado pelo aumento de tensão, pela *corrida armamentista*, e pelas inquietantes oscilações no equilíbrio do poder[...]"[31]. Por exemplo, o *McAfee Virtual Criminology Report* – o qual teve significativos impactos nos debates políticos sobre Defesa Cibernética, ao redor do mundo – aponta que vários Estados estão competindo entre si, em uma espécie de "Guerra Fria Cibernética"[32].

---

27 Ao contrário do que ocorreu com a Estônia, em 2007, com a Geórgia, em 2008, com o Irã, desde 2009, e outros países que sofrem diariamente ataques cibernéticos de grande vulto, mas não publicados.

28 Praga virtual que, em 2009, infectou centrífugas de urânio e atrasou o programa nuclear iraniano, danificando, por meio de sabotagem dos sistemas informacionais. Atribui-se a confecção do Stuxnet a uma parceria entre os governos de EUA e Israel.

29 Gills Lopes M. Souza, "Reflexos da digitalização da guerra na política internacional do século XXI: uma análise exploratória da securitização do ciberespaço nos Estados Unidos, Brasil e Canadá", (*Dissertação de Mestrado em Ciência Política*, Universidade Federal de Pernambuco, 2013), 89.

30 Wight, op. cit., 264.

31 Ibid., 169, grifo nosso.

32 MCAFEE. "McAfee Virtual Criminology Report" (2009), 13, http://img.en25.com/Web/McAfee/VCR_2009_EN_VIRTUAL_CRIMINOLOGY_RPT_NOREG.pdf, acessado em 20 dez. 2014.

A corrida armamentista, durante a Guerra Fria, desponta em Wight uma ênfase maior à *instituição efetiva* da guerra. Para ele, levando-se em conta tal corrida, "a arte da guerra já evoluiu tanto que os homens são obrigados a reaprendê-la amiúde a cada dois anos"[33]. Seguindo o pensamento desse autor, há, de fato, não só evoluções, mas verdadeiras revoluções na arte de guerra: "No século XIII foi descoberta a pólvora, e no final do século XV o canhão já era senhor das fortificações medievais e as armas de fogo portáteis estavam desalojando o arco e a flecha". Pode-se completar o raciocínio de Wight com o de John Keegan, quando este vislumbra o importante papel da computação, já nas últimas décadas do século XX, ao modificar a lógica clausewitziana de interpretar a guerra como extensão da política, a partir do momento em que ela torna tangível a percepção de que os custos de uma guerra "claramente superam seus benefícios"[34].

O Neoliberalismo e o ciberespaço

Na literatura internacionalista, esta corrente teórica, não por acaso, também é conhecida como Institucionalismo Neoliberal[35], haja vista que parte de seus principais pressupostos remontam aos liberais clássicos, cujas obras-mor datam das décadas de 1910 e 1930 e a quem Carr epitetou de "utópicos". *Grosso modo*, a corrente liberal clássica de RI utiliza-se de arcabouços filosóficos, jurídicos e históricos de liberais do jusnaturalismo e da economia que impactaram o cenário internacional, tais como Grotius, Vattel, Kant, Adam Smith, e Locke. Uma de suas principais teses é a de que o Estado, enquanto conjunto de indivíduos, encontra no Direito, no comércio e nas organizações internacionais a representatividade e a garantia fundamentais para

33 Wight, op. cit., 249.

34 John Keegan, *Uma história da guerra* (São Paulo: Companhia das Letras, 2006), 92-93.

35 Christian Reus-Smit e Duncan Snidal, eds., *The Oxford Handbook of International Relations* (Oxford: OUP, 2008), 201-266.

sobreviver e cooperar no âmbito internacional. Bebem desta fonte os liberais internacionalistas Norman Angell e Woodrow Wilson, sendo este último o idealizador da malograda Liga das Nações e ex-presidente dos EUA.

Após o fim da Segunda Guerra Mundial, torna-se evidente o fato de a corrente liberal clássica não conseguir explicar o porquê de os Estados – então abarcados pela Liga das Nações – preferirem a guerra a soluções pacíficas. Assim, a corrente realista clássica, liderada por Carr e Morgenthau, projeta-se como *mainstream* das RI, *i.e.*, as abordagens que surgem depois dela buscam ratificar ou retificá-la, como é o caso do Neoliberalismo Institucional.

Os epítetos *neo* e *institucionalista* têm um duplo objetivo: primeiro, o de demonstrar que há certa (e, portanto, não total) ruptura com a corrente clássica; e, segundo, o de enfatizar a influência (mas não sua imprescindibilidade) que as instituições/organizações internacionais (e, portanto, não apenas os Estados) exercem no sistema internacional anárquico. Dois expoentes neoliberais são Robert Keohane e Joseph Nye.

Mas o que interessa aqui diz respeito a dois importantes pressupostos do neoliberalismo: (i) a aceitação realista de que os Estados são os principais atores do sistema internacional anárquico[36]; e (ii) a possibilidade mais corriqueira de os Estados cooperarem entre si para a obtenção conjunta de ganhos. Depreende-se então que as organizações e os regimes internacionais aportam-se como grandes ferramentas de cooperação, capazes de influenciar os Estados[37].

Nesse viés, o sistema internacional propicia aos Estados – os quais continuam sendo, para os neoliberais, racionais e calculistas

36 O uso do prefixo *neo* calha ao fato de esta corrente não seguir estritamente os pressupostos do liberalismo clássico nem uma cartilha estritamente realista.

37 Robert O. Keohane, "International institutions: two approaches", *International Studies Quarterly*, Vol. 32, No. 4 (1988), 379-396.

– ferramentas para diminuir os constrangimentos da anarquia, por intermédio, por exemplo, da cooperação internacional. Em analogia, o ambiente cibernético parece exercer, sobre os mesmos Estados, constrangimentos semelhantes, uma vez que não existe um "ciberleviatã". Acentuando ainda mais a análise, a própria estrutura da Internet foi projetada para ser livre, anárquica, descentralizada, autoexpansível[38] e sem atenção para a questão da segurança[39], tendo em vista que o que norteava os primeiros desbravadores do ciberespaço era o princípio de confiança mútua entre os pais fundadores da ARPANET[40]. Assim, em uma visão neoliberal internacionalista, é possível afirmar que tais constrangimentos à ação do Estado propicia um cenário fecundo para a criação de regimes internacionais – como, por exemplo, aquela pretendida pela Convenção de Budapeste sobre Cibercrimes, de 2001 – e instituições e fomentos à cooperação internacional em matéria de defesa e segurança cibernéticas (como a Organização do Tratado do Atlântico Norte – OTAN).

Ao lado da utilização da pólvora, das duas primeiras revoluções industriais e do advento da tecnologia nuclear, Nye[41] aponta que a revolução da informação é o ponto de inflexão no século XXI, caracterizando, assim, uma revolução nos assuntos militares (RMA). Embora o embrião de tal processo possa ser remontado à criação das máquinas de impressão "gutenbergianas" ou, mesmo, ao uso crescente dos telefones, Nye informa que a atual revolução da informação é a grande responsável pelo crescimento vertiginoso do ciberespaço, um domínio cada vez mais presente e necessário na vida de pessoas físicas e jurídicas neste século.

38 Souza, "Reflexos da digitalização da guerra", 97.

39 Nye, op. cit., 18.

40 Leonard Kleinrock, "History of the Internet and its flexible future", *IEEE Wireless Communications* (2008), 8-18.

41 Nye, op. cit., 18.

Ainda para Nye[42], é nessa nova esfera de influência que um novo tipo de poder emerge: o poder cibernético. Na realidade, o poder em questão é ainda aquele mesmo perseguido pelos grandes estadistas e analisado por teóricos políticos, ao longo da história humana. Todavia, a Revolução da Informação, segundo o autor, molda a natureza desse poder e aumenta extraordinariamente sua difusão. Assim, surge o poder cibernético, ou seja, a capacidade de se obter resultados preferidos por meio do uso dos recursos de informação eletronicamente interligados ao ciberespaço[43].

Assim, com a massificação dos microcomputadores e a quase ubiquidade da Internet, nos dias atuais, o ciberespaço se mostra como um reduto de novas *oportunidades e desafios*. Sendo estes representados pelos vários tipos de: pragas virtuais (*worms*), crimes cibernéticos e, mais recentemente, guerras cibernéticas.

Há alguns anos, organizações internacionais – como a Organização dos Estados Americanos (OEA), a OTAN e a Organização das Nações Unidas (ONU) – têm contribuído com o debate acerca da Defesa Cibernética e, principalmente, da Segurança Cibernética, a ponto de recomendar práticas e fomentar a cooperação interestatal nessas áreas. Percebe-se, assim, uma politização, por meio do uso neoliberal do Direito Internacional e do papel das organizações internacionais para a promoção de regimes internacionais sobre o ciberespaço e a soberania estatal. Por conseguinte, pode-se dizer que está havendo não apenas uma institucionalização, mas também uma *securitização* do ciberespaço, melhor vista na próxima subseção.

42 Joseph Nye, *The future of power* (Nova Iorque: PublicAffairs, 2011), 114.

43 Ibid., 123.

A Escola de Copenhague e o ciberespaço

Buzan, Wæver e Wilde[44] são considerados, dentro do debate teórico de RI, expoentes da chamada Escola de Copenhague[45], que buscou, dentro do contexto de reorganização do sistema internacional no pós-Guerra Fria, ampliar e redefinir as questões a serem tratadas pelos Estudos de Segurança Internacional.

Os pensadores dessa corrente afirmam que o que faz uma questão ser considerada *de segurança* depende do que é discursivamente colocado como "ameaça existencial". Ressaltam ainda que o discurso de segurança tem servido para legitimar ações extraordinárias, situadas além das regras políticas tradicionais – do escopo legal ordinário de um dado país. Demonstrando, neste ponto específico, influência construtivista, Buzan, Wæver e Wilde sustentam que "segurança" é uma prática auto-referencial, ou seja, a ameaça não é objetiva, mas sim definida em um processo intersubjetivo.

A operacionalização deste arcabouço de análise dos assuntos de segurança, na emergente e diversa agenda do pós-Guerra Fria, dá-se pela definição das Unidades de Análise em Segurança (*Units of Security Analysis*), em que: o "Objeto de Referência" seria a coisa existencialmente ameaçada; o "Ator Securitizador" (*Securitizing Actor*) é aquele que securitiza a questão, declarando que o Objeto de Referência está sendo ameaçado; além de existir também o "Ator Funcional" (*Functional Actor*).

O *framework* de análise demonstrado por Buzan *et alii* se traduz por uma visão em que a segurança internacional é uma questão essencialmente discursiva, sendo a Securitização um conceito central,

44 Barry Buzan, Ole Wæver e Jaap de Wilde, *Security: a new framework for analysis* (Londres: Lynne Rienner, 1998).

45 Marianne Stone, "Security according to Buzan: a comprehensive analysis", *Security Discussion Papers*, No. 1 (2009).

sob o qual pode estar teoricamente sujeita qualquer questão pública. Nesse ínterim, as questões confrontar-se-iam em três categorias:

1. não politizado: o Estado não lida com a questão e, por conseguinte, não há debate público;
2. politizado: o tema é parte de política pública, requerendo decisões do governo sobre diversos tipos de alocações;
3. securitizado: face extrema da politização, quando a questão é apresentada como uma ameaça existencial e demanda medidas emergenciais.

Os setores para securitização seriam, assim, as lentes com as quais se observa questões de segurança, devendo o analista ter em mente que: estes estão impingidos de valores e características inerentes, que a natureza das ameaças e das unidades variam de setor para setor e que a securitização pode ser institucional ou *ad hoc*[46].

O tema do ciberespaço não é especificamente abordado por Buzan e seus colaboradores. Entretanto, deve-se ressaltar que Nissenbaum[47], Hansen e Nissenbaum[48] e Hart[49] aplicam a teoria desenvolvida pela Escola de Copenhague ao ciberespaço, propondo, dada a relevância que o tema Segurança Cibernética adquiriu na agenda internacional, a adoção analítica de um Setor Cibernético, com Unidades de Análise em Segurança e dinâmicas próprias, demonstrando que a literatura

46 Buzan et alli, op. cit., 27.

47 Helen Nissenbaum, "Where Computer Security Meets National Security", *Ethics and Information Technology,* No. 7 (2005), 61-73.

48 Lene Hansen e Helen Nissenbaum, "Digital disaster, cyber security and the Copenhagen School", *International Studies Quarterly*, No. 53 (2009), 1555-1575.

49 Catherine Hart, "Mobilizing the Cyberspace Race: the Securitization of the Internet and its Implications for Civil Liberties", *Cyber-Surveillance in Everyday Life: an International Workshop* (Toronto: Universidade de Toronto, 12-15 maio 2011).

internacionalista também caminha para a aplicação do instrumental da Escola de Copenhague à questão da Segurança Cibernética. Selecionam-se, assim, dois trabalhos para serem sublinhados neste capítulo.

A principal contribuição ao debate em Segurança Cibernética feita pela Escola de Copenhague é oferecida por Hansen e Nissenbaum, que conceituam Segurança Cibernética como algo oriundo da agenda pós-Guerra Fria em resposta à mistura de inovações tecnológicas e às mudanças nas condições geopolíticas internacionais. As autoras realizam três perguntas: quais são as ameaças e os Objetos de Referência que distinguem o Setor Cibernético dos demais Setores?; Como as instâncias concretas da "securitização cibernética" podem ser analisadas? Como os Estudos Críticos de Segurança podem levar o "discurso cibernético" a sério?

O argumento central das autoras está em não ser plausível manter o tema inscrito nos cinco setores já teorizados pela Escola de Copenhague – setores político, societal, econômico, militar e ambiental –, dada a relevância[50] que o tema da segurança cibernética está adquirindo no cenário contemporâneo da Segurança Internacional; cabendo, em algum parâmetro, atualizá-la.

As autoras comparam a dinâmica do Setor Econômico com a do Cibernético, devido à constante interdependência e aos problemas em definir limites geográficos e competências, inclusive com o alto grau de responsabilidade da esfera privada. Todavia, o potencial de securitização é maior do que a economia. Há uma ligação muito mais forte com a questão da segurança militar e da velocidade de adaptação às novas TIC, pois o elo com essa segurança reside no fato de o *backbone*

50 Por exemplo, as diversas iniciativas estatais, tais como: a Comissão para Proteção de Infraestruturas Críticas nos EUA, em 1996; a localização proeminente da Segurança Cibernética dentro do *Department of Homeland Security*, em 2003; a formulação da *National Strategy to Secure Cyberspace*, no âmbito do Pentágono; e a criação de um centro de defesa cibernética da OTAN, em 2008.

da RMA estar nas tecnologias digitais[51]

Torna-se nítido que as autoras retomam ideias de Ronald Deibert, o qual argumenta que a Segurança Cibernética se divide em quatro tipos de discurso – conforme os objetos de referência, as ameaças, as opções de política e as ordens mundiais –, quais sejam: segurança nacional, segurança estatal, segurança privada e segurança de redes[52].

Buscando desenvolver o *insight* anterior, Hansen e Nissenbaum argumentam, retomando Buzan e seus colaboradores, que existe uma gramática de segurança específica – como objetos de referência, discurso securitário e dinâmica de ameaças – para o que chamam de "setor cibernético":

> *a)* *hipersecuritização*: cujo pressuposto maior é colocar o tema como ameaça existencial em função da possibilidade de danos a serem causados por ataques cibernéticos nos âmbitos social, econômico e militar, atraindo, assim, objetos de referência desses respectivos setores. As autoras destacam a semelhança entre os discursos sobre prováveis danos catastróficos e os discursos presentes no Setor Ambiental, em que o destino do planeta estaria irreversivelmente condenado, se medidas emergenciais não fossem tomadas. Contudo, a diferença fundamental reside na velocidade com que os efeitos cascata de um ataque cibernético maciço podem atingir as pessoas e Estados[53];

51 Hansen e Nissenbaum, op. cit., 1162.

52 Ibid., 1163.

53 Ibid., 1164.

b) *práticas diárias de segurança*: a gramática dos Estudos de Segurança é utilizada para a aceitação da Audiência, uma vez que os discursos mencionam constantemente aspectos da Segurança Cibernética que atingem ao cidadão – tais como fraudes de cartão de crédito, invasões a *e-mails* e servidores-*web* Os objetivos que os Atores de Securitização típicos do Setor Cibernético veem em tal gramática são: assegurar a parceria dos indivíduos para protegerem as redes (como a utilização de antivírus); e, principalmente, tornar a hipersecuritização mais aceitável, pois os indivíduos passariam a ligar os elementos catastróficos de ataques cibernéticos às práticas que observam em seu cotidiano[54]. Um aspecto interessante a mencionar sobre o teor dos discursos é que a construção social do mundo digital vista como algo perigoso se dá pelo uso de termos como "vírus" e "infeções", contra os quais o cidadão comum deve proteger-se constantemente. Nesse sentido, o procedimento discursivo é análogo à securitização de questões de saúde[55];
c) *tecnificações*: a ideia presente nessa terceira gramática, de acordo com as autoras "copenhagueanas", é a de que o ambiente hipotético e especulativo da Segurança Cibernética gera espaço para discursos técnicos e especializados. Muitas vezes, o conhecimento necessário para entender determinadas questões de ordem técnica o qual suplanta as habilidades de um pesquisador de Segurança Internacional.

54 Ibid., 1165.

55 Ibid., 1166.

> Progressivamente, o que ocorre nessa gramática é a *despolitização* da questão já presente na agenda de Segurança estatal, restringindo-a a opinião dos especialistas em Segurança da Informação e fazendo com que esta seja utilizada no discurso político[56].

Criar um Setor específico para a questão cibernética ocorre pela especificidade da dinâmica de ameaças e unidades de análise em Segurança. Assim, o Setor de Segurança Cibernética ligaria Objetos de Referência, como redes cibernéticas ou indivíduos, à segurança de regimes políticos e das estruturas do Estado. O propósito central de Hansen e Nissenbaum é definir as três gramáticas de Segurança no referido setor, pois estes não podem ser encontrados na dinâmica de outro Setor apresentado pela Escola de Copenhague.

Ainda assim, as autoras enaltecem a contribuição fundamental que a Teoria da Securitização, desenvolvida pela Escola de Copenhague, oferece aos estudos em Segurança Cibernética, ou seja, desvelar as perigosas consequências normativas e políticas de um processo de "securitização do ciberespaço" [57].[58]

Considerações finais

Após analisar brevemente quatro abordagens teóricas de RI e algumas de suas aproximações para a temática da Segurança

56 Ibid.: 1167.

57 Ibid., 1172.

58 Para a relação intrínseca entre esse processo e a questão filosófica da inevitabilidade da técnica moderna, dialogando com Escola de Copenhague, ver: Marcial A. G. Suarez e Igor D. P. Acácio, "Reflections on virtual to real: modern technique, international security studies and cyber security environment", in *Cyberspace and International Relations*, ed Jan-Frederik Kremer e Benedikt Müller (Berlin: Springer, 2014), 269-280. Para o caso brasileiro, cf: Igor D. P. Acácio, "Segurança Cibernética: Análise sobre a Política de Defesa Brasileira (2000-2011)", (*Monografia de Relações Internacionais*, Niterói: Universidade Federal Fluminense, 2011). Para um estudo comparativo, cf. Souza, op. cit.

Cibernética, o resultado a que se chega, aqui, é que tanto o Realismo quanto a Escola Inglesa podem ser alocados em um grupo de abordagens em que é possível auferir considerações mais genéricas e cujo escopo está associado a questões mais metafísicas; já o Neoliberalismo e a Escola de Copenhague podem ser enquadrados em um segundo grupo, caracterizado por apresentar arcabouços mais contextualizados sobre o tema em questão, pelos quais é possível derivar *insights* promissores de pesquisa. É o que aponta o Quadro 2.

Quadro 2: As teorias de Relações Internacionais e o ciberespaço

Escopo quanto à insegurança do ciberespaço	Abordagem teórica	O que diz (ou pode dizer) sobre a insegurança do ciberespaço
Generalista, define a estrutura básica	Realismo	- ciberespaço é um novo domínio operacional no qual Estados devem agir para mitigar insegurança ocasionada por ameaças a suas infraestruturas críticas, buscando projetar poder e influência, maximizando seus interesses
	Escola Inglesa	- ciberespaço enquanto instituição efetiva da sociedade da informação
Analítico	Neoliberalismo	- Direito internacional, regimes internacionais e organizações internacionais (OEA, OTAN, ONU) podem fomentar cooperação internacional - *cyber power*
	Escola de Copenhague	- temática da segurança cibernética é passível de Securitização por Estados ou demais agentes dentro das sociedades, em processos discursivos que revelam a percepção do ciberespaço como fornecedor de ameaças existenciais - Há enormes riscos em processos de securitização do ciberespaço, porque estes podem fortalecer mecanismos de exceção como a violação de privacidade e da neutralidade da rede em atendimento à agenda de segurança

Fonte: Acácio e Lopes, op. cit., 20-21 (com adaptações).

Vale frisar, ademais, que Nye[59] cunha o termo "*soft power*" para designar manifestações outras do poder que não apenas as militares e econômicas ("*hard power*"), como, por exemplo, a influência de valores culturais de uma nação em relação a outra. Portanto, tem-se, no século XXI, a configuração de que algo novo emerge na arte de guerrear e que se utiliza do próprio ambiente – ciberespaço – para tomar algum tipo de vantagem na política internacional.

Deve-se ressaltar, entretanto, a fluidez – inerente a qualquer abordagem teórica que se diz internacionalista – com que as reflexões sobre o ciberespaço se interpenetram. Dada a necessidade de se explicar um novo acontecimento internacional, e tendo em vista a complexidade do atual contexto de Segurança Internacional, elementos de diferentes correntes teóricas podem, e devem, ser utilizados com o fito da obtenção de explicações mais sólidas acerca do tema estudado.

Ao contrário do uso estratégico da pólvora ou dos cavalos, que causaram uma verdadeira revolução militar[60] e de outros elementos para a evolução da guerra, o ciberespaço é o único destes que se prostra, simultaneamente, como uma ferramenta (meio) e um ambiente (fim). Portanto, trata-se de um ambiente complexo de ser analisado e mensurado tecnicamente e apenas à luz direta de teóricos de RI, que tem servido, também, para uma miríade de discursos políticos de securitização[61].

O que se argumentou neste trabalho diz respeito à impossibilidade da utilização de tipos teóricos puros. É necessário, pois, construir agendas de pesquisa sobre o tema do ciberespaço – e das questões de Segurança – que integrem a perspectiva das RI e dos Estudos Estratégicos à já presente visão técnica e dos especialistas

59 Joseph S. Nye, *Soft power: the means to success in world politics* (Nova Iorque: PublicAfffairs, 2004).

60 Keegan, op. cit.

61 Nissenbaum, op. cit.; Hansen e Nissenbaum, op. cit.; Souza, "Reflexos da digitalização da guerra"; Suarez e Acácio, op. cit.

em Segurança da Informação. Logo, trata-se de um chamado para que mais estudiosos integrem diferentes abordagens teóricas visando a uma melhor explicação desses novos fenômenos da Segurança Internacional hodierna. Afinal, as teorias de RI têm muito a falar sobre o ciberespaço.

Teoria da Fronteira Cibernética: inquietações interdisciplinares

Walfredo Bento Ferreira Neto
Gills Vilar Lopes

Introdução

O trato do ciberespaço, sob os auspícios dos Estudos de Segurança Internacional, retoma uma problemática que, há muito tempo, parecia estar resolvida pelos demais campos que se debruçam sobre as relações de forças internacionais, qual seja: a noção de território e, portanto, de fronteira. Por exemplo, em Geopolítica, Direito Internacional Público (DIP) e Relações Internacionais (RI), o conceito de fronteira mostra-se imprescindível para delimitar o alcance soberano que um Estado exerce sobre um dado território. Não por menos, o conceito *weberiano* de Estado remonta à relação intrínseca entre poder e território: "[…]comunidade humana que pretende, com êxito, o monopólio do uso legítimo da força física *dentro de um determinado território*"[1]. Nessa mesma lógica, a Carta da Organização das Nações Unidas (ONU), em seu Art. 2º, eleva a máxima *weberiana* ao nível internacional, quando afirma que seus membros "[...]*deverão evitar em suas relações internacionais* a ameaça ou *o uso da força* contra a *integridade territorial* ou a dependência política de qualquer Estado[...]"[2].

1 Max Weber, "A política como vocação", in *Max Weber*, org. H. H. Gerth e C. Wright Mills (Rio de Janeiro: Livros Técnicos e Científicos, 1967), 56, grifo nosso.

2 Organização das Nações Unidas. "Carta das Nações Unidas e Estatuto da Corte Internacional de

Nesse sentido, o que caracteriza os espaços territoriais soberanos dos Estados é justamente o uso de demarcações fronteiriças, as quais têm delimitado também as questões de guerra e de paz entre as nações, ao longo de toda a história moderna. Todavia, o "espaço" cibernético tem ensejado conflitos interestatais – ainda que não declarados e/ou assumidos por uma das partes[3] – cuja responsabilização pelo dano fica prejudicada devido às questões do *situs* onde a controvérsia se origina ou se consuma. Nesse prisma, a utilização das chamadas redes zumbis (*botnets*) já se tornaram um exemplo desse tipo de falta de provas putativas, na recente história da Internet.

Assim, a questão territorial torna-se um dos elementos nevrálgicos tanto para o desenvolvimento de teorias geopolíticas[4], internacionalistas[5] e jurídicas[6] quanto para a legitimação do exercício de um poder estatal dentro de um dado espaço físico[7]. É por isso também que se diz que RI é um campo primordialmente centrado na territorialidade. Portanto, transpor essas questões para o ambiente cibernético torna-se um dos objetivos precípuos deste capítulo.

Análises centradas no Estado cuidam de conceitos ancorados

Justiça" (1945), 6, grifo nosso. http://unicrio.org.br/img/CartadaONU_VersoInternet.pdf, acessado em 29 dez. 2014.

3 Dois casos podem ilustrar tal assertiva: Estônia imputando, em 2007, à Rússia a responsabilidade por vultosos ataques cibernéticos que paralisaram suas estruturas estratégicas de informação e comunicação; e o imbróglio diplomático envolvendo Coreia do Norte e Estados Unidos da América (EUA), em 2014, por conta do lançamento de filme satirizando Kim Jong-un, cujas respostas foram materializadas em ataques cibernéticos à produtora da película – Sony –, bem como o subsequente "desligamento" da Internet no país asiático.

4 Ver os dois números especiais sobre o ciberespaço de uma das mais importantes revistas de Geografia e Geopolítica do mundo: Hérodote, http://www.herodote.org/spip.php?rubrique66, acessado em 3 jan. 2015.

5 C. Reus-Smit e D. Snidal, "Between Utopia and Reality", in *The Oxford handbook of International Relations*, ed. _____, 3-37 (Nova Iorque: OUP, 2008), 12. Ver também: T. J. Biersteker, "State, Sovereignty and Territory", in *Handbook of International Relations*, ed. W. Carlsnaes, T. Risse e B. A. Simmons, 157-176 (Londres: SAGE, 2002), 157.

6 F. Rezek, *Direito Internacional Público* (São Paulo: Saraiva, 2013).

7 J. Ruggie, "Territoriality and beyond: problematizing modernity in International Relations", *International Organization*, No. 47 (1998), 139-174.

em pressupostos físicos e geográficos, *i.e.*, da topologia "terra", que, por excelência e acepção da palavra, é também um espaço físico. Mas como ficam as relações de poder baseadas em uma nova topologia compreendida como um espaço virtual? A fim de responder a essa e a outras indagações, este texto lida com o ciberespaço, o qual, nos últimos anos, tem tornado-se um "território" para a inferência não só de ciências *outsider* aos olhos da Ciência da Computação, como a Sociologia e da Ciência da Informação, mas também da Geografia, RI e DIP.

Com o advento do ciberespaço, cujo carro-chefe é a Internet, e com as consequentes imersões das esferas pública e privada nele, surge a necessidade natural, por parte da primeira esfera, de projetar poder em tal ambiente. Dessa forma, o presente trabalho busca compreender os desafios teóricos que cercam a imersão estratégica dos Estados nesse novo espaço de interação entre humanos e máquinas.

O presente trabalho divide-se em quatro seções: a primeira é esta Introdução; a segunda contém um introito à teoria de fronteiras na visão dos seus autores clássicos; a terceira versa sobre prospecções estratégicas, internacionalistas e geopolíticas sobre o ciberespaço; e a quarta e última seção é composta por considerações finais, no intuito de defender uma nova abordagem que ponha em diálogo a relação Estado-poder-ciberespaço.

Teoria de fronteiras: um introito

Esta seção tem por objetivo apresentar o que se entende por *fronteira*, na visão de autores clássicos da Geopolítica. Justifica-se, assim, uma necessidade de conhecer seus conceitos e contextos históricos, a fim de que se possa pensar a questão da fronteira em um espaço em que a maioria de tais autores não viveu o suficiente para tomar ciência. Nossa maior preocupação aqui é pensar um esboço teórico razoavelmente aplicável ao ciberespaço, e não cometer anacronismos e

analogias frágeis; daí a importância de autores clássicos para ajudar a lançar luz sobre um ambiente tão aparentemente impreciso.

O tema *fronteira* desperta interesse sazonal ao longo da história, sobretudo da contemporaneidade. Por exemplo, em 1990, o general Carlos de Meira Mattos[8] analisa o processo de fixação de fronteiras e as implicações políticas daí advindas, realizando objetivamente uma síntese histórica sobre as fronteiras e os seus inúmeros significados históricos. Diz o general que os povos primitivos não tinham necessidade de estabelecer essa denominada limitação, tendo em vista que a população da Terra, à época, era ínfima e assaz esparsa. Portanto, não havia "pressões" no e pelo espaço natural.

Mattos ainda aponta que, durante as conquistas marítimas que envolviam sumérios, cartagineses, venezianos e romanos, o sentimento de posse/domínio do espaço fez-se pela conquista de cidades e portos, e pela submissão de governos locais. Dessa forma, não havia necessidade de se fixar linhas e faixas de fronteira naqueles tempos. Até mesmo no período feudal, quando houve extrema subdivisão do poder político – consubstanciada nos principados, grão-ducados, condados e feudos –, a fronteira despertou atenção analítica. Naquele tempo, o castelo com suas grossas muralhas e profundos fossos simbolizam o local a ser defendido pelo senhor e seus milicianos.

Acerca do Estado-nação e do uso da informação como fonte de centralização do poder, Anthony Giddens[9] menciona que, nos Estados tradicionais (formas pretéritas à do Estado-nação), não havia porque se falar em *fronteira*, mas sim em *limite*, uma vez que tratava-se de "uma área nas regiões periféricas de um Estado (não necessariamente contíguo a outro), no qual a autoridade política do centro é difusa ou fracamente disseminada".

8 C. de Meira Mattos, *Geopolítica e teoria de fronteiras* (Rio de Janeiro: Bibliex, 1990).

9 Anthony Giddens, *O Estado-nação e a violência* (São Paulo: Edusp, 2008), 76.

Contudo, tal realidade foi alterada – principalmente neste lado do mundo, ocupado pela chamada civilização ocidental, no âmbito daquilo que se compreende hoje como Europa. Aliás, esta última é um ingrediente essencial para se compreender a história das relações internacionais, sobretudo no período imediato à Revolução Francesa de 1789, na consolidação do conceito de fronteira, como o reconhecido atualmente. Assim, o território passa a possuir o chamado "espírito da fronteira" *lablachiano*, a inspirar e, até mesmo, a formar o sentimento de nacionalidade, ou seja, a emersão do Estado-nação na forma em que se mostra até hoje. Quanto a esse fenômeno, o general brasileiro escreve: "a posse do território nacional, sua defesa, passa a ser sagrado do cidadão.[...] A fronteira adquire importância excepcional – é o limite da soberania nacional"[10]. Já Giddens[11] segue semelhante entendimento: "as fronteiras, na minha visão, passam a existir somente com a emergência dos Estados-nação". Assim, Estado passa a ser a forma e a carapaça que envolve e protege – com todos os seus mecanismos eficazes de defesa, conforme acepções *weberianas* – uma nação.

A fronteira, naturalmente, possui um duplo viés: ao mesmo tempo em que serve de separação/delimitação de poder político, também inspira a interpenetração de culturas, interesses e objetivos difusos. Para garantir o funcionamento dessa duplicidade, faz-se necessário estabelecer, clara e precisamente, os limites fronteiriços, pois, somente assim, pode-se garantir a harmonia internacional; caso contrário, a fronteira passa a servir meramente como bloqueio e fonte de conflitos e preconceitos. Esse também era o pensamento de Mattos[12], ao afirmar que:

10 Mattos, *Geopolítica*, 1990, 15.

11 Giddens, *O Estado-nação*, 2008, 76.

12 Mattos, op. cit., 5.

> a História registra, em todas as épocas, o zelo inexcedível dos Estados na preservação e defesa de seus direitos territoriais. Este zelo impõe a delimitação clara dos territórios nacionais, a fim de que sejam evitadas as dúvidas perturbadoras e conflitivas[...]. Entramos, assim, no tema fronteira, linde que contorna o espaço geográfico de cada Estado, seja terrestre, marítimo ou aéreo.

Diferentemente das fronteiras de que fala Mattos – terrestre, marítima e aérea –, a novíssima fronteira do espaço cibernético ou ciberespaço tem postos desafiados teóricos e práticos ao Estado, devido a suas virtualidade, velocidade e volatilidade.

Os casos envolvendo os grupos *hacktivistas* Anônimos e LuzSec, o sítio virtual de vazamento de informações sigilosas Wikileaks, liderado por Julian Assange, e, mais recentemente, as revelações de espionagem internacional proferidas por Edward Snowden demonstram a elevada atenção dada ao ciberespaço por parte de Ministérios de Defesa e de Relações Exteriores e de serviços de Inteligência.

O fluxo que "trafega" pelo espaço cibernético não é tão perceptível, se comparado às topologias físicas. Eis que o que flui nessa rede de redes é, sobretudo, informação, por meio de caracteres simbólicos que, muitas vezes, fogem da imediata compreensão humana. A delimitação de poder e a imputabilidade de responsabilidades no espaço ou território cibernético torna-se a meta perseguida também pelo Estado, visando a garantia, sobretudo, da segurança, da harmonia e da paz internas e externas.

Nesse novo cenário, o conceito geográfico de rede – outrora estudado nos espaços terrestre, marítimo e aéreo – revela-se de suma importância igualmente no âmbito do território cibernético. Sua

aplicação guiou os Estados e os organismos internacionais, reguladores do DIP, na formulação dos limites e fronteiras cibernéticas, entre o final do século XX e o início do XXI.

Por exemplo, se já existiam formas de controle e monitoramento para as fronteiras físicas, nessa "nova" topologia, os contornos não se mostram muito claros ou precisos. Por enquanto, só se pode afirmar que o dever de delimitá-la e regulá-la, objetivando a garantia da paz – e do não transbordamento de conflitos virtuais para o físico –, é uma responsabilidade tanto de entes estatais quanto de não estatais.

É certo que essa "nova fronteira" não existe de hoje. A instalação e a operação da rede mundial de computadores – do inglês, *World Wide Web* (WWW) – em escala global e o aumento do número de internautas vêm ocasionando uma "pressão" político-social nesse espaço. Isso representa uma sequência bem próxima a da construção das fronteiras das outras dimensões ou topologias. O Quadro 1 ilustra resumidamente o histórico da evolução das fronteiras, a fim de que se tenha em mente uma possível construção do conceito de fronteiras cibernéticas.

QUADRO 1: Resumo histórico da evolução das fronteiras

FASE	ESTÁGIO	DESCRIÇÃO
1ª	vazios do ecúmeno	característicos do mundo antigo, pouco povoado, quando os núcleos geo-históricos eram separados por enormes vazios demográficos
2ª	largas zonas inocupadas ou fracamente ocupadas	não abrigavam nenhum poder político capaz de perturbar os interesses dos núcleos geo-históricos de que eram separadores
3ª	faixas relativamente estreitas (fronteiras-faixa)	áreas em que o povoamento dos países limítrofes não chega a pressionar um sobre o outro
4ª	fronteira linha, estabelecida sob vários critérios (natural, artificial, astronômico, étnico etc.)	áreas em que a densidade populacional colocou em contato permanente o *interesse* das partes

Fonte: Mattos, Geopolítica, 1990, 17 (com adaptação).

Resguardando as diferenças dos elementos em foco e tomando como base a forma de "pressão" por elas exercidas, identifica-se que, quanto ao fluxo de informações, a evolução do ciberespaço se dá geográfica e politicamente de forma bem parecida com a dos espaços tradicionais. Por exemplo, a fase ou estágio a que tal espaço se encontra atualmente é a última (fronteira-linha), na qual os *interesses* das partes (Estados e indivíduos) colocam-se em constante contato. Com tais pressões exercidas na nova dimensão cibernética, há a transformação do espaço em território, uma vez que, ali, o *poder* circula e é confrontado. Dessa maneira, o conceito de território proposto por Bertha Becker[13] vai ao encontro do objeto da Geopolítica: as relações entre poder e espaço geográfico.

Da mesma forma em que ocorre com os estágios e as fases mostradas no Quadro 1, a teoria de Mattos permitiu a elaboração de alguns conceitos fronteiriços e a classificação das fronteiras, segundo alguns critérios. Dentre esses, devido à temática ora abordada, destaca-se a fronteira do tipo antropogeográfica.

De acordo com Mattos[14], esse tipo de fronteira chega a ser fisicamente de impossível estabelecimento. Todavia, as fronteiras até então mais claramente delimitadas nem sempre o são fisicamente. Grande parte disso ocorre por acordos internacionais, sob a tutela do princípio da convencionalidade. Esse foi o caso inicial com as fronteiras terrestre, marítima, aérea e, de certa forma, sideral. No que se refere à aérea, a expectativa era a melhor possível em torno de uma paz perpétua e universal. Assim, tratados e convenções internacionais – considerados como a forma mais eficaz dentre as fontes do DIP[15] – exercem o importante papel de delimitar áreas de abrangência e/ou de

13 Bertha K. Becker, "Geopolítica da Amazônia", *Estudos Avançados*, Vol. 19, No. 53 (2005), 71-86.

14 Mattos, *Geopolítica*, 1990: 34.

15 Rezek, *Direito Internacional*, 2013.

atuação das Partes. Mesmo no âmbito cibernético, o DIP vê engendrar, em 2001, a Convenção de Budapeste sobre Crimes Cibernéticos. Porém, quanto aos "crimes de Guerra Cibernética", ainda persistem lacunas.

Assim, sob essa lente e utilizando-se de arcabouços teórico-normativos do DIP, das RI e da Geopolítica, este trabalho foca a fronteira cibernética enquanto limite territorial desafiador à tomada de decisões estratégicas para a salvaguarda da soberania nacional e da segurança internacional. Nessa visada, a próxima seção objetiva angariar embasamento para a proposição de uma Teoria da Fronteira Cibernética ancorada nesses três campos de estudo.

Pontos de partida para uma Teoria da Fronteira Cibernética

Nos últimos anos, o ciberespaço projetou-se, segundo alguns, como mais um domínio – ao lado dos já tradicionais mar, terra, ar e, em certa medida, espaço sideral – a ser compreendido e regulamentado pelo Estado. Dessa forma, como então identificar aspectos ciberespaciais que convirjam com os princípios básicos da Teoria Geral do Estado ou mesmo com a visão geopolítica clássica? Esse tipo de arguição se faz necessário devido à questão da *delimitação* de fronteiras. Assim como ocorre com os espaços tradicionais, é imprescindível haver também a *delimitação* de perspectivas políticas no ciberespaço – embora reconheçamos que seja algo bastante complexo –, a fim de que possíveis controvérsias possam ser solucionadas.

Os conceitos de *definição*, *delimitação* e, por fim, *demarcação* correspondem às fases formais exigidas pelo DIP para o estabelecimento de uma fronteira. De acordo com o geógrafo francês Raffestin[16], "a linha fronteiriça só é de fato estabelecida quando a *demarcação* se processa",

16 Claude Raffestin, *Por uma geografia do poder* (São Paulo: Ática, 1993), 167, grifo nosso.

ou seja, quando inexistir "[...]contestação por parte de um dos Estados que tivessem essa fronteira em comum. Pela *demarcação*, elimina-se não um conflito geral, mas um conflito do qual a fronteira pudesse ser o pretexto".

No caso do ciberespaço, essa *delimitação* é praticamente impossível de ser processada, embora seja altamente perseguida pelos Estados-nação. Todavia, vários autores, sob os mais diversificados ângulos e teorias, já tentaram identificar ou limitar as fronteiras do ciberespaço. Mas a literatura especializada em ciberespaço sugere que tal tarefa é assaz difícil, como se vê a partir de agora.

Por exemplo, para Wertheim[17], mensurar ou mesmo demarcar o ciberespaço é impossível, pois não se pode delimitar aquilo que não possui fronteiras. Assim, nesses termos, ela afirma metaforicamente que o domínio cibernético, por carecer de fronteiras e delimitações precisas, é a própria "[...]*nova fronteira* espacial" deste novo milênio[18].

Nesse ínterim, busca-se entender até que ponto a afirmação supracitada é verídica, ou, ao contrário, se é possível, ao menos, esboçar um princípio de delimitação ciberespacial. Para tanto, baseamo-nos em documentos oficiais e textos produzidos por órgãos governamentais, empresas especializadas em tecnologias de informação e comunicação (TICs) e membros ligados a setores-chave à pesquisa sobre a qual este trabalho se debruça.

Wertheim é inserida no debate para cobrir certos aspectos métricos concernentes à questão do ciberespaço. Outrossim, Joseph Nye[19] também é invocado, sob a intenção de direcionar nossas investigações acerca dos caminhos a serem percorridos pela busca

17 M. Wertheim, *Uma história do espaço de Dante à Internet* (Rio de Janeiro: Zahar, 2001).

18 Wertheim, op. cit., 162, grifo nosso.

19 J. S. Nye Jr., "Cyber Insecurity", *Project Syndicate* (10 dez. 2008), http://project-syndicate.org/commentary/cyber-insecurity>, acessado em 21 dez. 2014; _____, *The future of power* (Nova Iorque: PublicAffairs, 2011).

do poder neste raiar de novo milênio. Ao longo desta jornada, outros especialistas – das Ciências Militares, Exatas e Humanas – são trazidos com o fito de lançar luz sobre essa complexa e, aparentemente, paradoxal matéria.

A PROSPECÇÃO TEÓRICO-ESTRATÉGICA

A primeira década do século XXI marca a utilização militar das novas TICs nos conflitos interestatais[20], no âmbito da chamada Defesa Cibernética.

Nesse cenário, a Internet emerge como representação-mor do que a Terceira Revolução Industrial – ou Revolução da Informação – é capaz de proporcionar, em termos de inovação, oportunidade e desafio aos interesses estatais. Comportamento recente, os Estados passaram a vislumbrar sua imersão no ciberespaço[21] sob um viés também militar[22], refletindo, não obstante, em uma nova forma de se calcular o poder[23].

Consoante Mandarino Jr e Canongia[24], embora haja imprecisões quanto a conceitos como Guerra Cibernética, "finalmente, a segurança cibernética vem sendo tratada em nível estratégico pelas Nações[...]". Assim, o ciberespaço passa então a ser um dos campos de atenção das Forças Armadas da maioria dos países, uma vez que "a Segurança

20 Nye, "Cyber insecurity", 2008; Gills Lopes M. Souza, "A emergência do tema ciberguerra: contextualizando a criação do Centro de Defesa Cibernética à luz da Estratégia Nacional de Defesa", in *Artigos do* 6º *Seminário do Livro Branco de Defesa Nacional* (Brasília: Ministério da Defesa, 2011).

21 Mais especificamente na Internet, haja vista que a sua precursora, a ARPANET, já fora concebida com justificativas de segurança nacional inerentes à Guerra Fria

22 Souza, "A emergência do tema ciberguerra".

23 Walfredo B. Ferreira Neto, "Territorializando o novo e (re)territorializando os tradicionais: a cibernética como espaço e recurso de poder", *Coleção Meira Mattos - Revista das Ciências Militares*, Vol. 1, pp. 07-18 (2014).

24 R. Mandarino Jr e C. Canongia, *Livro verde: segurança cibernética no Brasil* (Brasília: GSIPR/SE/DSIC, 2010), 23.

Cibernética, desafio do século XXI, vem se destacando como função estratégica de Estado" [25].

Nessa linha de raciocínio, uma importante empresa especializada em antivírus aponta que, embora Guerras Cibernéticas *stricto sensu* não tenham ocorrido em 2009, vários Estados-nação estão definitivamente competindo entre si na área de Defesa Cibernética. Ao contexto que envolve essa espécie de corrida armamentista cibernética, McAfee[26] cunha de Guerra Fria Cibernética, conforme se apresenta no Mapa 1.

Fonte: McAfee, "Virtual Criminology Report", 13.

O fato de vários países estarem engendrando suas Políticas e Estratégias Nacionais de Segurança e/ou Defesa Cibernética pode ser entendido como um sinal de que novas percepções sobre Seguranças Nacional e Internacional, bem como de Doutrina e Estratégia Militares, estão se adaptando à nova realidade das ameaças assimétricas oriundas do ciberespaço.

25 Ibid., 13.

26 McAfee, "Virtual Criminology Report" (2009), http://www.mcafee.com/us/resources/reports/rp-virtual-criminology-report-2009.pdf, acessado em 17 dez. 2014.

Como lembra Nye[27], "há dezenas de definições para o termo ciberespaço, mas geralmente 'ciber' é um prefixo que representa atividades eletrônicas e informáticas". Nesse prisma, faz-se mister analisar alguns conceitos e definições engendrados, sobretudo, no âmbito da formulação de políticas nacionais acerca desse tema.

Por exemplo, a Estratégia de Segurança Cibernética do Canadá define o ciberespaço como "o mundo eletrônico criado por redes interconectadas de tecnologia da informação, bem como pela informação contidas nessas redes", e acrescenta que tal ambiente "é um patrimônio global, onde mais de 1,7 bilhão de pessoas estão ligadas entre si, com o intuito de trocar ideias, serviços e amizade"[28].

Em teor parecido, a Estratégia de Segurança Cibernética da Alemanha apregoa que o ciberespaço inclui todas as estruturas estratégicas de informação e comunicação acessíveis pela Internet e fora do alcance das fronteiras territoriais alemãs[29]. No mesmo sentido da estratégia canadense, a alemã também alça a Internet ao patamar de um patrimônio global, ao afirmar que:

O ciberespaço é o espaço virtual de todos os sistemas de TI vinculados ao nível dos dados em uma escala global. A base do ciberespaço é a Internet como uma conexão universal e publicamente acessível, bem como uma rede de transporte que pode ser complementada e expandida por qualquer número de redes de dados adicionais.[30]

De forma metafórica, porém não menos factual, a Estratégica de Defesa e Segurança Cibernéticas da França aponta o ciberespaço como *a nova Torre de Babel do século XXI*, ou seja, a França trata o ciberespaço como um mundo imaterial que apresenta uma nova roupagem à Batalha

27 Nye, *The future of power*, 122, tradução nossa.

28 Canadá, *Canada's Cyber Security Strategy* (Ottawa: Department of Public Safety, 2010), 2, tradução nossa.

29 Alemanha, *Cyber Security Strategy for Germany* (Berlim: Federal Ministry of the Interior, 2011), 2.

30 Ibid.: 14, tradução nossa.

das Termópilas[31]. Mas é sua definição técnica sobre o ciberespaço que nos interessa aqui: tal ambiente seria, para os franceses, o espaço de comunicação formado pela interconexão mundial de equipamentos automatizados de dados digitais[32]. É nesse sentido que a Estratégia afirma que, "ao contrário do mundo material, *as batalhas no ciberespaço não conhecem fronteiras*"[33].

Já para a Estratégia Nacional de Defesa (END) brasileira, o ambiente cibernético é visto como um dos três setores estratégicos – ao lado do nuclear e do espacial – e imprescindíveis para a salvaguarda da soberania nacional e do tão almejado desenvolvimento nacional independente[34]. Com tal viés desenvolvimentista, o Documento apregoa que não é independente quem não tem o domínio das tecnologias sensíveis, tanto para a defesa quanto para o desenvolvimento. E a cibernética, como já frisado, constitui-se como uma tecnologia sensível para o País.

Porquanto um documento que visa a apresentar, em linhas gerais, as principais idiossincrasias sobre a soberania nacional hodierna, a END não cita em nenhum momento a palavra "ciberespaço" nem "espaço cibernético", em seu escopo; se o fizesse, teria de definir tais conceitos, como ocorre nas Estratégias Nacionais de Segurança Cibernética da Alemanha, da França e do Canadá. Ao se referir a "setor cibernético", a END automaticamente engloba o ciberespaço, mas não limita o seu alcance geopolítico – apenas geográfico, *i.e.*, ao território nacional do Brasil –, alçando-o à categoria de imprescindível vetor de desenvolvimento e independência nacionais.

Com uma visão mais agressiva – em relação à visão brasileira,

31 França, *Défense et sécurité des systèmes d'information: stratégie de la France* (Paris: Agence nationale de la sécurité des systèmes d'information, 2011), 3.

32 Ibid., 21.

33 Ibid., 11, tradução nossa, grifo nosso.

34 Brasil, "Política Nacional de Defesa (PND) e Estratégia Nacional de Defesa (END). Brasília: Ministério da Defesa" (2012), http://www.defesa.gov.br/arquivos/estado_e_defesa/END-PND_Optimized.pdf, acessado em 2 dez. 2014.

por exemplo – sobre os perigos que advêm do ciberespaço, o general reformado da Força Aérea dos Estados Unidos (USAF), Norty A. Schwartz, lembra que o Departamento de Defesa estadunidense (DoD) reconhece o ciberespaço como "um novo domínio competitivo, onde o DoD irá operar e defender seus interesses mais vitais, de uma forma doutrinária similar àquela em que já opera nos domínios bélicos de ar, espaço, terra e mar"[35]. De forma semelhante também afirma o general Keith Alexander, o qual analisa que o ciberespaço vem sendo usado por militares e operado de dentro – ou através – dele para atacar pessoas, instalações ou equipamentos[36].

Contestando veementemente a analogia de que o ciberespaço é um campo de batalha a ser conquistado, Carr[37] aponta que tal consideração é um desafio conceitual hercúleo e que tentar classificá-lo como um domínio é frequentemente o primeiro erro que incorrem políticos, militares e analistas em geral. Ainda para esse autor, uma comparação mais precisa seria a dos *universos paralelos*, oriundos da ficção científica, os quais são "misteriosos reinos invisíveis existentes em paralelo ao mundo físico, mas capazes de influenciá-lo de inúmeras maneiras"[38].

Ainda em que pese essa percepção de que ciberespaço pode ser considerado um domínio ou topologia, Dutra[39] afirma que os mundos real e virtual se encontram interrelacionados, uma vez que as ações adotadas em um deles afetam o outro. Manjikian[40], por sua vez, corrobora tal

35 N. Schwartz, "The challenge of cyberspace", in *X National Symposium on Homeland Security and Defense* (2010), 5, tradução nossa, http://af.mil/shared/media/document/afd-101102-046.pdf, acessado em 3 dez. 2014.

36 Derek Reveron, ed., *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World* (Washington, DC: Georgetown University Press, 2012).

37 J. Carr, *Inside cyber warfare* (Sebastopol, CA: O'Reilly, 2009), 40.

38 Ibid., xiii, tradução nossa.

39 André M. C. Dutra, "Introdução à guerra cibernética", in *IX Simpósio de Guerra Eletrônica* (2007), http://sige.ita.br/IX_SIGE/aRTIGOS/ge_39.PDF, acessado em 4 abr. 2014.

40 Mary MacEvoy Manjikian, "From global village to virtual battlespace: the colonizing of the Internet and the extension of Realpolitik", *International Studies Quarterly,* Vol. 54, No. 2, pp. 381-401 (2010).

perspectiva, sustentando que há um novo tipo de território acarretando diferentes estratégias virtuais para alcançar os mesmos objetivos do mundo real. Em outras palavras, para este, os atores que buscam cada vez mais compreender o ciberespaço estariam buscando, no final das contas, projetar poder. Ademais, destaca-se, ainda nesse aspecto, a concreta possibilidade de nivelamento da assimetria entre os atores, *i.e.*, uma nova forma de interferir no balanço de poder. Um exemplo dessa ideia pode ser encontrado na entrevista do primeiro Comandante do antigo Centro de Defesa Cibernética do Exército Brasileiro (CDCiber) – agora, Comando de Defesa Cibernética do Ministério da Defesa – Gen José Carlos dos Santos[41], quando este cita a Coreia do Norte como grande possuidora de "um exército cibernético de cerca de 3 mil homens", salientando que ela, "por incrível que pareça, é menos vulnerável, porque tem poucas redes". O general ainda indaga: "como atacar uma rede que não existe?". Todavia, com os recentes desdobramentos do final de 2014, quando a conexão norte-coreana à Internet foi severamente prejudicada, pode-se dizer que a Coreia do Norte entra de vez nos estudos de Segurança e Defesa Cibernéticas, como um caso *sui generis*.

Da discussão acima, vê-se emergir, como pano de fundo, um verdadeiro embate entre adeptos de uma ontologia mais fundamentalista das relações internacionais – notadamente, teóricos das correntes Realista e Liberal –, em suas mais diversas variações e roupagens epistêmicas, como as "clássicas" e as "neo".

Para os mais jacobinos dos realistas – como Clarke e Knake[42] e Schwartz –, o ciberespaço possui sim fronteiras, haja vista que os problemas ocasionados no mundo virtual podem transbordar para o

41 L. Loyola, "General José Carlos dos Santos: 'Podemos recrutar hackers'". *Época*, 15 jul. 2011, http://revistaepoca.globo.com/Revista/Epoca/0,,EMI249428-15223,00-GENERAL+JOSE+CARLOS+DOS+SANTOS+PODEMOS+RECRUTAR+HACKERS.html, acessado em 3 fev. 2015.

42 Richard A. Clark e Robert K. Knake, *Cyber war: The Next Threat to National Security and What to Do About It*, 2. ed. (Nova Iorque: HarperCollins Publishers, 2012).

real, implicando, neste, *outputs* políticos e, até mesmo, militares. Trata-se, portanto, de um "novo" território ou domínio, que precisa apenas ser melhor identificado/delimitado.

Já os neoinstitucionalistas liberais – como Carr e Nye –, por sua vez, defendem, entre outros argumentos, que o ciberespaço é um espaço público e um local onde ocorrem trocas econômicas, comerciais, sociais, e que, portanto, deve ser entendido como um ambiente que não pode ser "dominado" pelo Estado.

Como se pode observar, no que tange a percepções ontológicas acerca do ciberespaço, os pensadores estratégicos tendem a divergir muito, apesar de todos eles concordam com a necessidade de haver uma espécie de cultura de Segurança Cibernética (*lato sensu*), seja para a burocracia estatal e a sociedade, seja para os fluxos comerciais e financeiros transnacionais.

Isso posto, cuida-se a seguir dos aspectos normativos que regem o ciberespaço.

A prospecção teórico-normativa

Criada em 2001 no âmbito do Conselho da Europa, a Convenção de Budapeste sobre Crimes Cibernéticos – tratado internacional ainda aberto para assinaturas de países não europeus – tenta preencher algumas lacunas deixadas no DIP acerca dos Crimes Cibernéticos, propondo tipificá-los e fomentar internacionalmente seu combate. Não abordando os diversos debates criados ao longo desses quase 15 anos que vinculam o precitado dispositivo legal à manutenção de alguns direitos individuais – como o direito à privacidade e ao sigilo das correspondências –, buscamos encontrar subsídios que permitam auferir onde se situam os marcos que delimitam o ciberespaço. Ao fazer isso, tem-se em mente que atos internacionais de conflito cibernético, como a Convenção de Budapeste, estão "intrinsecamente enredados

com Crime Cibernético, Segurança Cibernética, Ciberterrorismo e Espionagem Cibernética"[43].

Torna-se importante então destacar que a Convenção de Budapeste define *sistema informático* como "qualquer dispositivo isolado ou grupo de dispositivos relacionados ou interligados, em que um ou mais de um entre eles, desenvolve, em execução de um programa, o tratamento automatizado dos dados"[44]. Portanto, de pronto, a Convenção engloba dois tipos de sistemas: aqueles que estão *online* e os que estão *offline* à Internet. Entretanto, interessa-nos, aqui, a primeira categoria – *online* –, haja vista que "sistemas de tecnologia da informação em um espaço virtual isolado não fazem parte do ciberespaço"[45].

Continuando com a análise da Convenção, em seu corpo, afirma-se, *in verbis*, que:

> Cada [Estado-]Parte adoptará (*sic*) as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes para ordenar: a) A uma pessoa que se encontre *em seu território* que comunique os dados informáticos específicos, na sua posse ou sob o seu controlo [*sic*] e armazenados num sistema informático ou num outro suporte de armazenamento de dados informáticos.[46]

Desse modo, percebe-se que a Convenção parte do pressuposto de que a localização do indivíduo – neste caso, o criminoso cibernético

43 Carr, *Inside cyber warfare,* xiii, tradução nossa.

44 Conselho da Europa, "Convenção sobre o Cibercrime" (2001): 3, http://www.acidi.gov.pt/_cfn/529350b642306/live/+Conven%C3%A7%C3%A3o+sobre+o+Cibercrime, acessado em 9 dez. 2014.

45 Alemanha, *op. cit.,* 14, tradução nossa.

46 Conselho, "Convenção", 11, grifo nosso.

– é um fator *sine qua non* para tipificar o Crime Cibernético. Em outras palavras, verifica-se que a Convenção de Budapeste busca Combater Crimes cometidos *do* computador de quem ataca, e não *no* ambiente cibernético. E ao versar a competência sobre a infração cometida, o documento ainda elenca quatro possibilidades de isso ocorrer[47]: (i) no território da Parte; (ii) em um navio que detenha a bandeira da Parte; (iii) em uma aeronave da Parte; ou (iv) por um dos cidadãos da Parte, se a infração for punível criminalmente onde foi cometida ou se não for da competência de nenhum Estado[48]. Assim, a Convenção traz alguns indícios de regulamentação e tipificação internacional de "parte" do ciberespaço, uma vez que ela vincula a ideia tradicional de território com o Direito Penal e o Direito Processual Penal, consubstanciado no Princípio da Extraterritorialidade. Todavia, tal dispositivo legal não traz, ainda, informações acerca das especificidades fronteiriças do espaço cibernético.

Quanto à outra ideia que dificulta o desenvolvimento de uma teoria da fronteira cibernética e que está inserida na Convenção é a que se refere à localização por Endereço IP[49]. Se alguns defendem que o número IP seria uma espécie de registro de identidade virtual, Wertheim[50] vai informar que:

> O "lugar" exato onde estou quando entro no ciberespaço é uma questão ainda em aberto, mas claramente minha posição ["geocibernética", por assim dizer] não pode ser expressa em termos de uma localização matemática num espaço euclidiano

47 Cf. também o Art. 33 da Convenção sobre localização geográfica do sistema informático passível de contestação por uma Parte estrangeira.

48 Conselho, op. cit., 14.

49 Do inglês, *Internet Protocol (IP) address*, é uma sequência numérica que identifica um dispositivo conectado à rede mundial de computadores.

50 Wertheim, *Uma história do espaço*: 168.

> ou relativístico – nem com qualquer número de extensões do hiperespaço!

Assim, a afirmação de que não existe nenhum marco legal sobre o que constitui, *de jure et de facto*, um Ato de Guerra Cibernética[51] não encontra subsídios favoráveis na Convenção de Budapeste. *A priori*, ela busca versar sobre o Crime Cibernético – compreendido dentro das esferas de atuação da Segurança Pública –, mas, *a posteriori*, não há imputação nenhuma ao ator estatal o *status* de ele ser também um transgressor de direitos no âmbito cibernético. Em outras palavras, responsabiliza-se apenas o indivíduo, mas não o Estado.

Ainda no que tange à definição do que seria um Ato Cibernético de Guerra – imprescindível para poder medir, em que seja minimamente, os contornos das fronteiras no ciberespaço –, esse fato, *per se*, não enseja nenhum tipo de falha legal nem vazio da lei (*vacuum legis*), uma vez que a Convenção de Budapeste busca tipificar e punir – como seu próprio nome já diz – o Crime Cibernético, não a Guerra Cibernética.

É nesses mesmos termos que Oppermann[52] indaga acerca da responsabilidade de quem comete, por assim dizer, um Crime de Guerra Cibernética. Por outro lado, uma parceria entre a Organização do Tratado do Atlântico Norte (OTAN) e Cambridge University lançou o chamado "Manual Tallinn"[53], o qual busca preencher a lacuna deixada nas relações internacionais, quanto à conceituação e à responsabilização em casos de Guerra Cibernética, a qual só deve ser entendida em um ambiente de conflito entre Estados[54]. Esse Manual se assemelha mais

51 Carr, *Inside cyber warfare*, 1.

52 Daniel Oppermann, "Virtual attacks and the problem of responsibility: the cases of China and Russia", *Carta Internacional*, Vol. 5, No. 2 (dez. 2010), 11-25.

53 Michael Schmitt, ed, *Tallinn Manual on the International Law applicable to cyber warfare* (Cambridge, UK: Cambridge University Press e CCDCOE/NATO, 2013).

54 Portanto, essa definição vai de encontro ao que Mandarino Jr e Canongia apregoam sobre a Guerra Cibernética fazer parte tanto da esfera militar quanto da civil.

a uma recomendação doutrinária do que uma fonte jurisprudencial, servindo apenas de sugestão para dirimir possíveis conflitos cibernéticos – uma espécie de *draft* de "Convenção sobre Guerra Cibernética" –, não tendo, portanto, força vinculante.

Sem dúvidas, dentre os fatores que colaboraram para a inexistência de uma convenção internacional sobre Guerra Cibernética, estão aqueles que perpassam pela questão da fronteira no ciberespaço, como já dito. Nesse quesito, é de se "chamar a atenção que o chamado espaço cibernético [...] não tem suas fronteiras ainda claramente definidas[...]"[55]. Talvez essa falta de demarcação fronteiriça se deva ao fato de que, ao realizar uma analogia com as topologias ou os domínios clássicos, o "ciberespaço seja um terreno eletrônico que não ocupa espaço físico, ainda que por meio dele flua quantidades cada vez maiores de dados que possam controlar processos físicos"[56].

Já Nye[57] lembra que o domínio cibernético, além de recente, é o único criado pelo ser humano e que por isso está sujeito às mais rápidas mudanças tecnológicas, se comparado aos domínios tradicionais. Ainda para ele, é nessa nova esfera de influência política que um novo tipo de poder emerge: o poder cibernético (*cyber power*). Na realidade, tal poder continua sendo o mesmo que foi perseguido por grandes estadistas e cuidado por filósofos políticos, ao longo, sobretudo, das Idades Moderna e Contemporânea. Todavia, a nova Revolução da Informação vem mudando o *modus operandi* de se obter poder, aumentando consequente e extraordinariamente sua difusão[58]. Assim, o poder cibernético torna-se "a capacidade de obter resultados preferidos por meio do uso dos recursos de informação eletronicamente interligados do domínio cibernético"[59].

55 Mandarino Jr e Canongia, *Livro verde*, 13.

56 Carr, *Inside cyber warfare*, 40, tradução nossa.

57 Nye, *The future of power*, 124.

58 Ibid., 114.

59 Ibid., 123, tradução nossa.

Seguindo a lógica diretamente proporcional de Nye, quanto mais o ciberespaço se expande, mais a difusão de poder também se estende entre os atores que utilizam esse ambiente. Mas, quando se fala em expansão e extensão, as noções de metragem físicas parecem não se enquadrar bem no ciberespaço, pois "o que cresce neste caso não é volume em um sentido estritamente geométrico; é, no entanto, uma *espécie* de volume"[60]. Wertheim ainda traz algumas tentativas de elucidações a essas questões abordadas:

> [...]esse novo espaço digital está "além" do espaço que a física descreve, pois o domínio cibernético não é feito de forças e partículas físicas, mas de *bits* e *bytes*. [...]Por não estar ontologicamente enraizado nesses fenômenos, o ciberespaço *não está sujeito às leis da física* e portanto não está preso pelas limitações dessas leis. [...]O próprio conceito de "espaço" assume aqui um sentido novo, e ainda muito pouco compreendido, mas certamente fora do alcance dos físicos.[61]

Considerações finais

Questões como território, espaço, jurisdição e poder no ciberespaço estão (e estarão, pelo menos, nos curto e médio prazos) bastante abertos a perquirições, por parte do Estado-nação, que é o defensor-mor da responsabilidade do Contrato Social originário e dos interesses de uma determinada sociedade, mesmo que tal Contrato seja assinado digitalmente e que a sociedade em questão seja, nos dizeres de Manuel Castells, a da Informação.

Na verdade, quanto às demais dimensões fronteiriças –

60 Wertheim, *Uma história do espaço*, 163, grifo nosso.

61 Ibid., 167, grifo nosso.

sobretudo, a terra e o mar –, não são poucos os casos de litígio ou de áreas de fricção entre atores estatais. Para uma breve noção da complexidade do tema *fronteira* no âmbito geopolítico, mesmo com os territórios perceptíveis aos sentidos humanos, no âmbito regional sul-americano tem-se a discussão entre Venezuela e Guiana (Essequibo), Venezuela e Colômbia (Maracaibo), Equador e Peru (Pacífico), Bolívia e Chile (Antofogasta), Argentina e Chile (Terra do Fogo); no Pacífico, persistem questões entre Japão e China, China e Rússia, China e Taiwan[62], *i.e.*, conversações inerentes a espaços e poder em ambientes tradicionais, tanto no terrestre quanto no marítimo e, consequentemente, no aéreo.

Apesar de o general Meira Mattos apontar a extrema dificuldade de se limitar fronteiras, quando essas não são caracterizadas por um acidente natural – por um rio ou um lago, por exemplo –, a utilização da fronteira do tipo artificial se faz necessária com base no DIP, isto é, *de jure*. Como demonstrado, no que tange aos Crimes Cibernéticos, já há uma legislação internacional, embora ainda restrita a poucos países e com muitas controvérsias.

Se se levar em consideração a tese de Giddens sobre a importância da informação e da comunicação para o papel e a utilização de recursos políticos, tem-se que, hoje, os meios de TIC tornam-se um grande instrumento de poder para as ações estatais, sobretudo no que concerne às relações internacionais. Alguns atores já se deram conta disso. No Brasil, principalmente após o impulso da END, esse tema vem ganhando cada vez mais destaque e, amiúde, acompanhado por institucionalizações militares.

Tendo em conta os diferentes pontos de vista inerentes às diversas abordagens teóricas e a forma com que a *política do poder* ocorre, o fato que destoa, quanto a Teorias da Fronteira Cibernética, é

62 B. Buzan e O. *Wæver, Regions and powers* (Cambridge: CUP, 2003): 91-182.

que, "embora destituído de fisicalidade, o ciberespaço é um lugar. *Eu estou lá* – seja qual for o significado final desta afirmação"[63].

Logo, continuando esse estado de coisas, no que concerne à imprecisão de localização no ciberespaço e à falta de responsabilização por um Ato de Guerra Cibernética, o teorizar sobre a fronteira cibernética continuará a ser uma tarefa hercúlea e, portanto, algo que diz respeito a diferentes tipos de pensadores e/ou cientistas, não encontrando ainda seu *local* nos Estudos Estratégicos e de Segurança Internacional.

63 Wertheim, *Uma história do espaço*, 169, grifo nosso.

Considerações sobre o ciberespaço e sua inserção nos Estudos Estratégicos

Eduardo Cesar Bohn
Maurício Reis Nothen

Introdução

O presente capítulo pretende contextualizar a inserção das análises sobre o ciberespaço no âmbito dos Estudos Estratégicos. Para tanto, lembra-se das origens e dos principais marcos teóricos relacionados a este campo, e apresentam-se as características dos demais espaços comuns, de forma a construir uma base com a qual se possa relacionar o espaço cibernético com as questões pertinente à segurança internacional e à defesa nacional.

Posteriormente, apresentam-se características mais específicas sobre o ciberespaço – muitas das quais ainda em debate –, a fim de se ter um ponto de partida para discussões mais aprofundadas no âmbito dos Estudos Estratégicos. Por entendermos que um dos fundamentos do presente debate é o de contribuir para o desenvolvimento brasileiro de uma área que toque a segurança internacional e o ciberespaço, não conseguimos evitar uma breve digressão no sentido de apontar como o tema tem sido tratado oficialmente no Brasil.

Por último, retoma-se uma discussão mais metodológica quanto ao enquadramento do estudo do ciberespaço como tema dos Estudos Estratégicos.

Os Estudos Estratégicos e os espaços comuns: preparando o terreno para o ciberespaço

Se os estudos sobre guerra cibernética tornam-se corriqueiros neste raiar de século, os sobre defesa e guerra, desde muito, preocupam e perpassam o imaginário de estadistas e acadêmicos.

Já a definição de um subcampo organizado de conhecimento de Estudos Estratégicos – ou de Segurança Internacional, como é conhecido fora do Velho Mundo – é relativamente recente, remontando à década de 1940. Tal campo se origina de um ambiente no qual o mundo confrontou-se com duas grandes guerras, e tornava-se imperativo o estudo mais aprofundado sobre a visceral relação entre a política, a guerra e o uso da força pelos Estados.

Apesar de os Estudos Estratégicos serem definidos estreitamente como o estudo do emprego dos meios de força estatais com propósitos politicamente determinados, este é um campo de estudos bastante diverso e essencialmente interdisciplinar. Isso ocorre porque o objeto de análise desse campo abrange disciplinas diversas, as quais se interseccionam no estudo do mesmo objeto, desde os aspectos humanos, sociais e políticos envolvidos na guerra, como também constrangimentos e escolhas tecnológicas que influenciam diretamente nas formas de aplicação de força.

Nesse sentido, diz-se que,

> Em termos específicos, os Estudos Estratégicos têm um objeto central que os caracteriza e distingue: a questão da segurança, expressa na avaliação, projeto, gerência e aperfeiçoamento de sistemas integrados de pessoas, equipamentos, materiais, procedimentos, e ambiente para o preparo, emprego, e aperfeiçoamento dos meios de força como instrumentos políticos,

> em nível local, regional, nacional internacional e, mesmo, planetário.[1]

O termo "estratégia" tem sua origem no exercício da guerra, cunhado como forma de expressar a arte do comando militar, ou a arte de fazer a guerra. Seu alargamento contemporâneo, de forma a expressar – especialmente no mundo dos negócios – basicamente qualquer coisa que determine o exercício de um método que vise um objetivo final, é de certa forma um risco aos Estudos Estratégicos. Isto porque o subcampo e a estratégia em si não comportam tal definição demasiada ampla que se tem conferido a mesma, atualmente. Deve-se ter claro, portanto, que, apesar de se utilizarem do mesmo vocábulo para definir suas formas de agir, os campos de conhecimento ligados à Administração, principalmente, não compõem o escopo dos Estudos Estratégicos, a não ser que digam respeito estreitamente a alguma forma de implementação política por meio da força. Com esse mesmo viés argumentativo, Hew Strachan apregoa que:

> A estratégia existe para que a guerra seja útil ao Estado, para que ele possa, se necessário, usar de força para atingir [seus] objetivos políticos. Uma das razões pelas quais estamos inseguros sobre o que é guerra é porque estamos inseguros sobre o que é ou não é estratégia. Não é política pública, não é política e nem diplomacia. Relaciona-se com elas, mas não as substitui.[2]

Fica evidenciado, desta forma, que existe uma latente preocupação no campo dos Estudos Estratégicos em relação à manutenção clara e bem definida do escopo de conhecimento de que o

1 Domício Proença Jr., Eugênio Diniz e Salvador Ghelfi Raza, *Guia de Estudos de Estratégia* (Rio de Janeiro: Jorge Zahar Editor, 1999), 21.

2 Hew Strachan, *Lost Meaning of Strategy* (Londres: Survival, 2005), 49-50, tradução nossa.

campo se reporta e estuda. Essa inquietação também se apresenta, mais adiante em nosso estudo, quando pesquisadores tentam associar ações estratégicas ciberespaciais à luz dos Estudos Estratégicos. Não obstante, Henry Eccles apresenta uma conceituação diversa da de Strachan, que, embora mais abrangente, é interessante para as nossas posteriores análises sobre ciberespaço, pois traz a noção de direcionamento do uso de poder. Assim, para o autor, estratégia se define como: "[...]o abrangente direcionamento de poder para controlar situações e áreas, de modo a obter objetivos"[3]. De qualquer modo, é crescente também a preocupação com a reafirmação constante do núcleo de conhecimento teórico dos Estudos Estratégicos, o qual é composto especialmente em torno da teoria da guerra e de seus desdobramentos nos diferentes domínios.

O estabelecimento de uma chamada *teoria da guerra* remonta ao século XIX e aos autores mais proeminentes que estabeleceram de certa forma a doutrina militar dos séculos XIX e XX, quais sejam: Jomini e Clausewitz. Essa teoria baliza em termos gerais os fatores que compõem o estudo da guerra e, por consequência, dos Estudos Estratégicos. Seu desenvolvimento foi basilar na definição e conceituação dos elementos e da gramática que compõem e circundam os Estudos Estratégicos até os dias de hoje. Tais autores divergiram na forma de propor suas análises acerca da guerra. Jomini, por um lado, busca construir um arcabouço de linguagem acessível, usando-se de exemplos históricos pinçados para propor uma espécie de receituário para o sucesso estratégico. Por outro lado, Clausewitz renegava a prescrição de métodos e fórmulas de sucesso, justamente por entender a guerra como um processo complexo, incerto e mutável com o tempo.

Coloca-se ainda que, dependendo das circunstâncias, as

3 Henry E. Eccles, *Military Concepts and Philosophy* (New Brunswick, NJ: Rutgers UP, 1965), 48, tradução nossa.

atividades logísticas podem estar diretamente envolvidas nas situações de confronto, sendo por vezes idênticas a ele. Desta forma, não há uma linha clara e definitiva que separe logística, tática e estratégia, e que a "arte" e a "conduta" – em dizeres clausewitzianos – da guerra estão em constante interação[4]. Não por menos, autores como Thomas Rid[5], defendem a ideia de que nenhuma guerra cibernética se encaixa na definição clausewitziana.

Dentre os diversos conceitos discutidos por Clausewitz, sobressaem-se alguns que tratam do entendimento dos domínios em que e como a guerra é travada. Assim, assinalamos:

- a definição de que a Guerra é um ato de força para compelir nosso inimigo a fazer a nossa vontade;
- o caráter político da guerra, de que a guerra é a continuação da política por outros meios;
- o objetivo da guerra para ambos os lados é desarmar o adversário;
- a definição da existência conceitual da guerra absoluta e da existência prática de guerras ilimitadas, limitadas, mas não absolutas;
- a trindade paradoxal da guerra constituída pelo governo, forças armadas e população; e
- o conceito de que a defesa é a forma mais forte da guerra[6].

4 Embora esta lógica seja derivada do conteúdo da obra de Clausewitz, o termo "logística" não é formalmente utilizado, constando esta contribuição em: Domício Proença Jr. e Érico Duarte, "The Concept of Logistics derived from Clausewitz: all that is required so that the fighting force can be taken as a given", *Journal of Strategic Studies*, Vol. 28, No. 4 (ago. 2005), 645-677.

5 Thomas Rid, "Cyberwar and Peace Hacking Can Reduce Real-World Violence", *Foreign Affairs*, nov.-dez. 2013, http://www.foreignaffairs.com/articles/140160/thomas-rid/cyberwar-and-peace, acessado em 28 jan. 2015.

6 Carl Von Clausewitz, *Da Guerra* (São Paulo: Martins Fontes, 2003).

Enfim, uma gama diversa de conceitos importantes, para só citar alguns, que são os alicerces da compreensão contemporânea da guerra e de sua gramática, e que, logicamente, têm de ser levados em conta nas análises estratégicas sobre o ciberespaço.

Ademais, deve-se ter em mente que a construção da Teoria da Guerra se baseia exclusivamente no domínio terrestre. Além de conveniente, esta proposta é lógica, uma vez que o território habitável dos Estados é o solo, e neste estão assentados seus principais ativos, sua população e geralmente seus principais meios de produção. Nesse contexto, Clausewitz e Jomini já identificavam o que posteriormente seria elaborado em mais detalhes por Biddle[7]: a influência da conformação geográfica do terreno para a estratégia.

Biddle afirma que a tecnologia somente pode alterar o sistema moderno se ela for capaz de tornar o terreno uma questão irrelevante, isto é, torná-lo transparente para a visão - radares e sensores – e ao fogo. Diante das tecnologias atuais, isto não está ainda vislumbrado em um horizonte próximo, o que reforça a Teoria da Guerra e adia a supremacia da tecnologia sobre esta. Logicamente, nem por isso, o avanço tecnológico é desprezado, levando-se sempre em conta a importância da evolução tecnológica para o desenvolvimento de táticas e operações específicas ou novas, como é o caso de algumas políticas e estratégias nacionais de Segurança Cibernética e Defesa Cibernética.

No entanto, é central perceber que, até o final do século XIX, não havia produção científica em Estratégia que ampliasse as perspectivas para os demais domínios, à época, unicamente o marítimo. Neste sentido, a produção acadêmica em estratégia marítima, entre o final do século XIX e início do XX, foi fundamental para a ampliação do conhecimento em Estratégia para os chamados *espaços comuns*.

7 Stephen Biddle, *Military Power: explaining victory and defeat in modern battle* (Princeton: Princeton University Press 2004).

Além disso, tal expansão auxiliou também com a definição dos conceitos aplicáveis ao cenário marítimo que seriam, posteriormente, extrapolados para compreender outros domínios, como é o caso do ciberespaço, no que tange à chamada *deep web*, cuja analogia destaca o papel da Internet que *está submersa* daquilo que os indexadores de conteúdo podem tocar.

No campo de teorização sobre Estratégia Marítima, tem-se Alfred Mahan como fundador do pensamento estratégico naval moderno, o qual, ao final do século XIX, escreve em um período de muita ênfase ao liberalismo inglês e às novas discussões de defesa de um mundo cada vez mais interligado, e particularmente receptivo (especialmente na Europa) às teorias gêmeas da Jeune École sobre defesa costeira e ataques à frota comercial, conhecidas como Guerra de Curso (*Guerre de Course*).

Na visão de Mahan, a verdadeira e única missão das forças navais deveria ser preponderar sobre as forças inimigas e, assim, controlar o mar. Para tanto, os navios e frotas inimigas são os únicos objetos a serem atacados em todas as ocasiões. Para que isso ocorra, a concentração de força é, na visão de Mahan, o princípio fundamental da guerra tanto terrestre quanto marítima. Como desdobramento, a divisão da frota para a proteção costeira é um erro na concepção do autor, uma vez que a armada visa combater outra armada e não proteger a costa; a proteção das costas deveria ser feita a partir de fortes e forças terrestres. O termo que definia a Marinha estadunidense como somente "defensiva" fora mal interpretado, na visão de Mahan, pois a questão da defesa, neste caso, está exposta no sentido político do termo, e não militar. O autor renegava a guerra de curso como opção viável de poder marítimo, somente dominando o mar com poder exorbitante, e expulsando as bandeiras inimigas dos mares, que se exerce a supremacia marítima; e isto

somente poderia ser executado por possantes marinhas[8]. No entanto, o autor não infere que marinhas menores são desprovidas de poder; pelo contrário, salienta que, quando bem posicionadas, elas podem causar um efeito muito superior, proporcionalmente ao seu tamanho[9].

Similarmente a Clausewitz, Corbett estrutura seu pensamento sobre a ideia de complementaridade entre as estratégias de ataque e defesa, considerando ainda a necessidade do uso de forças terrestres e marítimas harmonicamente em prol de um objetivo militar comum, especialmente porque o autor introduziu a percepção de que uma guerra dificilmente é decidida por meio da estratégia marítima isoladamente, exceto em casos extremamente limitados e específicos. Em analogia, essa parece ser outra discussão que emerge nos estudos estratégicos sobre o ciberespaço: a "defesa" de tal ambiente deve ser realizada por uma Força Singular nova, já existente ou pelo conjunto delas? Ao contrário do cenário terrestre, onde o território é fator predominante das ações, no cenário marítimo as linhas de comunicação constituem o principal objetivo estratégico. O ciberespaço, entretanto, parece aglutinar características tanto de front de batalha quanto comunicacional. Corbett salienta que a ruptura ou manutenção das linhas de comunicação marítimas são a base da interação marítima e a principal forma de obtenção de supremacia marítima e de influência no resultado da guerra[10]. A extrapolação do autor é especialmente relevante no cenário contemporâneo de interligação entre os domínios, no qual eventos diversos em cenários diferentes se relacionam e influenciam um ao outro, porém dificilmente se esgotam em si. Ou seja, deve-se refletir sobre a real possibilidade de uma guerra restrita aos domínios adjacentes, como o cibernético.

8 Sprout, op. cit., 1966.

9 Geoffrey Till, *Seapower: A Guide for the Twentieth First Century* (Nova Iorque: Routledge, 2004).

10 Julian S. Corbett, *Principles of Maritime Strategy* (Nova Iorque: Dover Publications, 2004).

O comando do mar significa a obtenção da primazia sobre os fluxos de comunicação, ou seja, a capacidade de operar livremente no mar e prevenir a operação das linhas de comunicação pelo inimigo. Tal comando é extremamente difícil de ser mantido em sua plenitude. É possível obter ou romper a supremacia localmente, mesmo com uma frota inferior, desde que concentre localmente força suficiente[11]. E quanto ao ciberespaço, o que estrategistas cibernéticos podem depreender do comando do mar? Embora o autor não toque nessa seara, depreende-se que, além de haver uma relação ontológica forte entre ciberespaço e mar[12], o "comando do ciberespaço" seria uma tarefa praticamente impossível de ser feita, haja vista a dinamicidade desse ambiente, bem como os diversos túneis de comunicação que poderiam ser facilmente criados, por meio de *chat*, *e-mail*, IRC, criação de protocolos de interconexão etc.

Neste ponto, Corbett aceita a importância do conceito de batalha decisiva de Mahan, mas concede maior ênfase à possibilidade de controle do oceano via manobra, enumerando diversas razões pelas quais a batalha decisiva pode ser evitada, realçando também o fato de que a supremacia total era ideal e que o amplo comando é custoso. Logo, as marinhas deveriam preocupar-se em maximizar seu poder de comando, por meio da manobra[13][14].

Geoffrey Till, por seu turno, defende que no mundo pós-Guerra Fria a globalização vem mudando o caráter das operações marítimas.

---

11 Corbett, op. cit, 2004.

12 "Ciber" advém da abreviação do verbo grego *kybernéo*, que significa pilotar um navio. Assim, "navegar na Internet" imprime uma ideia que vai além do que uma simples força de expressão.

13 Till, op. cit, 2004.

14 Ora, por ser mais flexível e, portanto, acomodar-se às vicissitudes ciberespaciais, a manobra se mostra como uma alternativa menos penosa que a da batalha decisiva. Todavia, como efusivamente advertimos ao leitor, estamos tratando de conceitos criados pré-Revolução da Informação, e qualquer teorização sem a devida reverberação empírica pode levar a um erro de anacronismo.

Além de estas estarem mais ligadas a áreas litorâneas, a constituição de frotas vem se adequando à posição dos Estados no sistema internacional. O autor defende ainda que países mais desenvolvidos tendem a constituir frotas "pós-modernas", qual sejam, com função de proteger, acima de si mesmos, o sistema internacional. Neste espectro, os Estados se dividiriam e comporiam marinhas complementares, com base industrial de defesa compartilhada, para operar em missões de controle dos mares, operações expedicionárias, manutenção da ordem e consenso no mar. No entanto, países que não alcançaram este grau de desenvolvimento e que ainda procuram se desenvolver desconfiam do sistema estabelecido e temem por sua segurança. Desta forma, tendem a manter suas marinhas sob um paradigma moderno, com frotas capazes de desenvolver todas as funções possíveis, indústria de defesa própria e baixa dependência externa[15]. Esta também demonstra ser uma tendência seguida por algumas forças armadas de países menos poderosos, como a Coreia do Norte: desenvolver suas próprias capacidades cibernéticas, de modo a evitar dependência externa.

Este apanhado de descrições da constituição de um corpo teórico acerca da estratégia marítima é relevante para se entender o ciberespaço a luz dos Estudos Estratégicos e no sentido de apresentar elementos particulares que podem ser observados de alguma forma em um ou mais domínios dos espaços comuns que se desenvolveram posteriormente, quais sejam, aéreo, espacial e por fim o cibernético.

Os espaços comuns, inaugurados com o domínio marítimo, carregam similaridades importantes, e por isso a reflexão e a inferência de um sobre o outro é possível e interessante aos objetivos deste texto. No cenário marítimo, por exemplo, têm-se bem definidas as características de comando e controle do mar e de linhas de comunicação, bem como

15 Till, op. cit., 2004.

o exercício ativo ou de *fleet-in-being*[16]. Estas são característica que podem ser transferidas e observadas, em parte, no domínio aéreo, por exemplo. Além do mais, vertentes de cooperação e disputa do espaço comum, bem como relacionamentos específicos entre ataque e defesa, podem ser identificados no domínio espacial. Entre outras características únicas de exercício de poder e estratégia, os quais têm similaridade com o buscado nos demais espaços comuns. Enfim, existe uma gama de reflexões afeitas à estratégia marítima que estão presentes nos demais domínios dos caracterizados espaços comuns.

Como forma de descrição dos supracitados espaços, afirma-se que existem quatro principais espaços comuns globais: o marítimo, o aéreo, o espacial e o ciberespacial. Cada um deles é fundamentalmente diferente dos demais. No entanto, é possível examiná-los em conjunto, caracterizando-os como "espaços comuns globais", uma vez que eles compartilham quatro características principais: (i) não são controlados ou de propriedade de qualquer entidade única; (ii) sua utilidade como um todo é maior do que se dividido em partes menores; (iii) Estados e atores não-estatais com as capacidades tecnológicas necessárias são capazes de acessá-los e usá-los para fins econômicos, políticos, científicos e culturais, bem como (iv) são capazes de usá-los como um meio para o movimento militar e como um teatro de conflito militar[17].

Os quatro espaços comuns, muito embora compartilhem características básicas, também contam com peculiaridades que os diferenciam entre si, como descrito no Quadro 1.

16 O Conceito de *Fleet-in-Being* está ligado ao poder emanado pela Marinha, em da sua própria existência. Em outros termos: ela evita o confronto direto, mas exerce seu poder e controle, mediante suas meras presença e ameaça.

17 Abraham M. Denmark e James Mulvenon, *Contested Commons: the future of American power in a multipolar world* (Washington, DC: Center for New American Studies, 2010).

Quadro 1: Comparação militar dos espaços comuns globais

	Marítimo	Aéreo	Espacial	Cibernético
Vantagens Estratégicas	Permite a projeção de poder global	Permite o ataque direto contra forças inimigas e centros de gravidade	Cria uma nova plataforma elevada; permite fazer imagens globais e telecomunicações	Permite a rápida transferência de informações; operações militares finamente ajustadas; multiplicador de força, especialmente para atores não estatais
Velocidade e Escopo de Operações	Trânsito lento por longas distâncias; permite ataques globais	Trânsito global rápido. Escopo depende da capacidade de saídas pra missão perto dos alvos	Permite a operação global contínua; C3ISR detalhado; ataque de precisão	Operação global extremamente rápida; automação de comando e controle
Exemplos de Características-chave	Linhas de comunicação marítimas, estreitos, canais, portos marítimos	Aeroportos; espaço aéreo; acesso à reabastecimento em bases e em pleno voo	Posições orbitais, pontos de Lagrange, Portos Espaciais	Físicos: cabos submarinos, estações de chegada, pontos de intercâmbio de internet, bancos de dados, nós de infraestrutura; Lógicos: padrão TCP/IP, nós *web* altamente conectados

Fonte: adaptado de Denmark e Mulvenon, op. cit., 15.

Podemos perceber, pelo Quadro 1, que os distintos espaços comuns globais têm distintas aplicações e implicações militares, além de sua importância para a economia mundial. Nesse viés, os espaços marítimo, aéreo e espacial têm similaridade em sua conceituação, no sentido de facilitar a cooperação em regimes comerciais e de defesa, que regulam o comportamento e o acesso aos mesmos. Os domínios marítimo e aéreo são os mais desenvolvidos, com maior estrutura e embasamento intelectual e institucional. O espacial é o menos maduro, contando com governança restrita. Já o espaço cibernético

é altamente anárquico, e os esforços de implementação de regimes, seja por Estados, seja por organizações intergovernamentais ou não-governamentais, tem tido sucesso tímido em sua regulação. Nesse sentido, independentemente de ser relacionado como um novo domínio estratégico ou somente um espaço comum, é inegável o crescente protagonismo do espaço cibernético. Provas empíricas disto são as políticas e estratégias nacionais de defesa cibernética adotadas pelas principais potencias mundiais, a exemplo de Estados Unidos, França, Reino Unido e Alemanha.

Mesmo que analisados à parte, não podemos desconsiderar que vivemos na era da informação e que as redes e os dados cada vez mais cumprirão um papel importante na estratégia. Assim, também é importante resguardar a crescente relevância do conceito atual de Guerra Centrada em Redes (GCR) ou *Network-Centric Warfare*, a qual

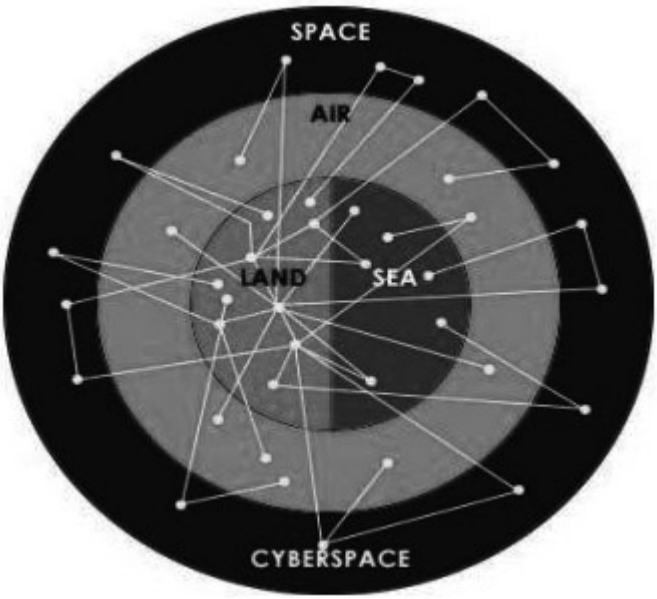
> [...]centra-se no poder de combate que podem ser gerados a partir da vinculação efetiva ou da interconexão do esforço de batalha. Caracteriza-se pela capacidade de forças dispersas geograficamente (consistindo-se em entidades) para criar um alto nível de consciência de batalha compartilhada que pode ser explorada através de auto-sincronização e outras operações centradas em rede para alcançar a intenção dos comandantes.[18]

Dessa forma, fica claro que a lógica compreendida no conceito de GCR pressupõe o uso extensivo de redes de informações e, por

18 Arthur K. Cebrowski e John J. Garstka, "Network Centric Warfare: its origins and future", *Proceedings*, U.S. Naval Institute, Vol. 124, No. 1, 1998, *apud* J. Boone Bartholomees Jr., *The US Army War College guide to National Security Issue*s, Vol. 1: theory of War and Strategy, 4ª Ed (Washington, DC: Strategic Studies Institute, 2010), 342.

conseguinte, do espaço comum cibernético como meio de ligação dos demais domínios para uma estratégia mais eficaz, inteligente e sincronizada. Neste aspecto, independente da caracterização do espaço cibernético como domínio, é possível entendê-lo como o espaço comum de inter-relação dos demais domínios, como mostrado na Figura 1.

Figura 1: Inter-relação do ciberespaço com os demais domínios



Fonte: adaptado de Paganini, 2013[19].

Por outro lado, existe uma série de peculiaridades próprias do ciberespaço que impõe a reflexão sobre sua inserção nos Estudos Estratégicos, a começar por suas características e classificação no subcampo de Estudos Estratégicos, bem como as lacunas metodológicas

19 Pierluigi Paganini, "Panetta is critical of the Security Level on NATO Networks", *Infosec Island*, 23 jan. 2013, http://infosecisland.com/blogview/22872-Panetta-is-Critical-of-the-Security-Level-on-NATO-Networks.html, acesso em 10 nov. 2014.

ainda presentes. Isto faz necessária uma análise mais objetiva do tema, como se vê adiante.

Ciberespaço: a Guerra Cibernética em um novo espaço?

Materializado de forma praticamente plena na década de 1980, o conceito de espaço cibernético ou ciberespaço foi inicialmente tratado como um ambiente eminentemente separado do mundo físico, onde portanto aconteceria a revelia das fronteiras nacionais e geográficas, e desta forma não submetido às restrições decorrente das noções de soberania e segurança nacional. Contudo, o espaço cibernético é baseado em estruturas físicas, derivadas da conexão de sistemas e redes controlados por protocolos submetidos às fronteiras do Estado-nação. Este ambiente tem como peculiaridade o fato de ter sido criado pelo homem, sendo desta forma extremamente mutável, embora não de forma absolutamente irrestrita. Tal maleabilidade demanda que os países desenvolvam também instituições e protocolos facilmente adaptáveis e passíveis de aprendizado ágil, uma vez que queiram usufruir de suas potencialidades da forma mais frutífera possível[20]. Podendo ser considerado um espaço comum, e dada a sua pertinência na sociedade moderna, o ciberespaço tende a ser mantido aberto, devido a esforços empreendidos pela comunidade internacional.

Complementarmente, Kuehl[21] descreve o espaço cibernético como sendo um domínio operacional cujo caráter particular e singular é enquadrado pelo uso de eletrônicos e do espectro eletromagnético

20 Greg Rattray, Chris Evans e Jason Healey, "American Security in the Cyber Commons", in *Contested Commons: the Future of American Power in a Multipolar World*, Abraham M. Denmark e James Mulvenon, eds (Washington, DC: Center for a New American Security, 2010), 139-175.

21 Daniel Kuehl, "From Cyberspace to Cyberpower: Defining the Problem", in *Cyberpower and National Security*, Franklin Kramer, Stuart Starr e Larry Wentz, eds (Washington, DC: National Defense University Press, 2009). Para conhecimento, nesta obra o autor demonstra a existência de uma serie de outras definições para o mesmo termo.

para criar, armazenar, modificar, trocar e explorar informações via sistemas baseados em tecnologias de informação e comunicação (TIC) e suas infraestruturas. Apesar da frequente associação imediata do espaço cibernético com a Internet, é de grande importância destacar que os termos não são de forma alguma intercambiáveis, sendo o primeiro muito mais complexo e heterogêneo que o primeiro.

A inserção formal do termo "*cyber*" (em "*cyberwar*", ou em "Guerra Cibernética") à terminologia dos Estudos Estratégicos deu-se pela obra de John Arquilla e David Ronfeldt[22] , que o entendiam como o melhor dentre as expressões existentes, como, por exemplo, o de "guerra de informação" ou, o mais amplo, de "operações de informação", para relacionar o campo da informação com o da Governança neste contexto. Os autores tinham como objetivo envolver duas facetas distintas desta relação, quais sejam, tanto a utilização de computadores e redes digitais[23] quanto os impactos organizacional e institucional de seus usos no recolhimento, processamento e compartilhamento de informação[24]. Neste sentido, a guerra cibernética estaria relacionada ao impacto do controle de processos dependentes de informação mediante o desenvolvimento de novas tecnologias e das subsequentes alterações processuais que estas acarretam.

O peso dado à chamada Revolução em Assuntos Militares (RAM), potencializa ainda mais a importância do entendimento desta questão. O termo cunhado no Pentágono, referia-se à interação entre os sistemas que coletam, processam, integram e comunicam informação e

22 John Arquilla e David Ronfeldt, *Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, CA: Rand Publishing, 1997).

23 Por "digitalização" entende-se o "processo pelo qual um determinado dado (imagem, som, texto) é convertido para o formato binário para ser processado por um computador", de acordo com: José Miguel Quedi Martins, *Digitalização e Guerra Local como Fatores do Equilíbrio Internacional* (Tese de doutorado, Universidade Federal do Rio Grande do Sul, 2008), 7.

24 Diego Canabarro e Thiago Borne, "Reflections on the Fog of (Cyber)War", *NCDG working paper*, No. 13-001 (2013).

aqueles que aplicam a força militar, com o objetivo de criar a "violência de precisão". A RAM se fundamenta na sinergia entre três elementos: (i) inteligência e capacidade de reconhecimento e vigilância no estado-da-arte; (ii) avançados ativos em comando, controle, comunicação, computadores e inteligência (C4I); e (iii) munição guiada de precisão[25]. Tendo isso em mente, não é de se estranhar que os EUA, país-berço desta "revolução", tratem o ciberespaço como um domínio próprio para a guerra. Como expressa a Estratégia de Defesa Nacional daquele país, "o ciberespaço é um novo teatro de operações", porém o mesmo documento lembra que "desenvolver operações de informação como uma competência militar fundamental demanda mudanças fundamentais em seus processos, políticas e cultura"[26]. Vemos, assim, que, mesmo quem mais aposta na tecnologia de ponta atrelada a fins militares, entende que lançar mão do ciberespaço vai muito mais além do que apenas desenvolver códigos-fontes.

Apesar de os efeitos deste fenômeno não serem consensuais na literatura especializada, como nos indicam tanto Biddle quanto Érico Duarte[27], a influência de muitos de seus adeptos e o impacto dos desdobres desta teoria são tão profundos que sua análise definitivamente não pode ser simplesmente ignorada. No mesmo sentido, embora com foco um pouco diferenciado, Canabarro e Borne também nos lembram que a grande parte dos conceitos utilizados nesta discussão são ainda controversos, e a interpretação dos mesmos repercutem de forma indelével na formulação de políticas a eles relativas.

De forma objetiva, tomemos um ponto levantado na obra

25 Geoffrey Parker, *Cambridge Illustrated History Warfare* (Nova Iorque: Cambridge University Press, 2009), 393.

26 Estados Unidos da América, *The National Defense Strategy* (Washington, DC: Department of Defense, 2005), 13, http://www.defense.gov/news/mar2005/d20050318nds1.pdf, acessado em 18 nov. 2014.

27 Érico Duarte, "Tecnologia Militar e Desenvolvimento Econômico: uma análise histórica", *Texto para Discussão*, No. 1748 (Rio de Janeiro: Ipea, 2012).

de Gills Lopes[28]: neste caso, o autor trata da diferença entre defesa cibernética e segurança cibernética, conceitos que "embora [...] soem, à primeira vista, semelhantes, ambos tratam de esferas de atuação político-institucional diferentes". Em outras palavras, se quer dizer que entender um ato como "hacktivismo", crime, terrorismo ou ato de guerra implica em desdobramentos bastante diferentes por parte de diferentes atores, e, portanto, as interpretações de cada ator tem de ser bastante claras e suficientemente debatidas.

Ainda para ilustrar essa problemática, Rattray e seus colaboradores[29] provocam-nos com uma analogia acerca da discussão, originada na década de 1940, sobre armas nucleares. Diz-se que era abertamente aceito que uma nova e significativa dimensão da guerra havia surgido com a era nuclear. Contudo, conceitos fundamentais como "*deterrence*" e "destruição mútua assegurada" ainda estavam por serem elaborados e consagrados. Desta forma, não nos parece improvável que estejamos, similarmente, aprendendo a nos adaptar às potencialidades do espaço cibernético.

Retomando o debate sobre o ciberespaço e a guerra cibernética, é pertinente destacar o impasse sobre a configuração ou não do espaço cibernético como um domínio próprio para a guerra. A partir de uma análise de caráter clausewitziana – baseada na caracterização da guerra apresentada anteriormente – tendemos a compartilhar da visão de Canabarro e Borne de que não parece ser apropriado descrever o espaço (comum) cibernético como um domínio próprio para a guerra. Contudo, esta é definitivamente uma questão sobre a qual ainda não existe consenso.

Em suma, os marcos teóricos que norteiam a utilização de desenvolvimento das atividades no espaço cibernético – e do próprio

28 Gills Lopes, "Análise sobre o Impacto das Novas Tecnologias de Informação e Comunicação nas Estratégias Nacionais de Defesa e Segurança Cibernéticas do Século XXI", *III Simpósio de Pós-Graduação em Relações Internacionais do Programa "San Tiago Dantas"* (nov. 2011).

29 Rattray et al., "American Security", 2010.

ambiente em si – ainda estão longe de serem cristalizados, sendo ainda necessário muita reflexão sobre tais temáticas. Mais uma vez, nas palavras de Rattray e seus colaboradores[30], "apesar de muito progresso ao se referir à segurança cibernética, governos e militares não conseguem nem mesmo concordar em como pensar o espaço cibernético, quanto mais em como defendê-lo e operar dentro dele".

Entendemos, ainda, ser necessária nesta discussão conceitual uma breve digressão no sentido de introduzir algumas das repercussões práticas no cenário brasileiro, e assim fundamentar a pertinência daquela. Para tanto, faremos a uma análise superficial dos principais documentos governamentais brasileiros acerca da segurança/defesa cibernética, com o intuito de realizar uma mera contextualização sobre o tema e sua implicância estratégica para o Brasil. Lançaremos mão da Política de Defesa Nacional (PDN)[31], de 2005, da Estratégia Nacional de Defesa (END)[32], do Livro Branco de Defesa Nacional (LBDN)[33] e do Livro Verde de Segurança Cibernética no Brasil[34].

Comparando-se tais documentos, pode-se notar uma marcante evolução no que tange à preocupação oficial do Estado brasileiro com a temática ora em tela, o que por si só já demonstra um indício positivo. Desde o documento de 2005, onde constam apenas duas linhas a ela destinadas, destacando a necessidade de se obter capacidades de defesa contra um possível ataque cibernético, até o Livro Verde, de 2010, destinado especificamente à segurança cibernética no âmbito da administração pública federal. Tais documentos tiveram também

30 Ibid., 139, tradução nossa.

31 Brasil, Política de Defesa Nacional (2005), http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Decreto/D5484.htm, acessado em 20 dez. 2014.

32 Idem, Estratégia Nacional de Defesa (2008), http://www.defesa.gov.br/projetosweb/estrategia/arquivos/estrategia_defesa_nacional_portugues.pdf, acessado em 20 dez. 2014.

33 Brasil, Livro Branco de Defesa Nacional (2012), http://www.defesa.gov.br/arquivos/2012/mes07/lbdn.pdf, acessado em 20 dez. 2014.

34 Idem, Livro verde: Segurança Cibernética no Brasil (2010) http://dsic.planalto.gov.br/documentos/publicacoes/1_Livro_Verde_SEG_CIBER.pdf, acessado em 20 dez. 2014.

um impacto institucional progressivo, dado que a partir deles foram indicadas as estruturações de órgãos cuja finalidade seria a de aumentar as capacidades nacionais no setor, nominalmente o Centro de Defesa Cibernética (CDCiber), decorrente do LBDN, por exemplo[35].

Contudo, há ainda muito a se evoluir, no que concerne ao tratamento oficial destas problemáticas. Canabarro e Borne nos lembram – embora contestem esta percepção – de que o Brasil trata a "cibernética" como um quinto domínio para a guerra[36]. Todavia, o País não descreve em nenhum dos documentos citados conceitos vitais como "espaço cibernético" ou "guerra cibernética", para citar apenas dois exemplos.

De forma ilustrativa, há outra iniciativa oficial referente ao ciberespaço, qual seja, o Marco Civil da Internet – Lei nº 12.965, de 23 de abril de 2014. Trata-se desta questão nesse momento como um exemplo de elementos com os quais deve ter cuidado ao se incluir o ciberespaço como tema dos Estudos Estratégicos. Embora por vezes esta seja tratada no contexto da "soberania digital", tal elemento apenas passa a ser sujeito do subcampo de estudos em questão no momento em que se possa relacionar de maneira estreita a forma de implementação política por meio da força.

Embora o Brasil o entenda o ciberespaço como um setor estratégico[37], reconhece que "o chamado espaço cibernético, não tem suas fronteiras ainda claramente definidas(...)"[38]. É notável ao longo desse documento uma consciência de que alguns dos termos centrais que o substanciam ainda têm suas definições porosas e incertas, conquanto se entenda que não por isso se deva dar menos atenção aos desafios com os quais a realidade confronta a atuação estratégica.

35 Canabarro e Borne, op. cit..

36 Lembramos que esta interpretação da posição brasileira não é consensual.

37 Brasil, "Estratégia Nacional de Defesa", 2008, *passim*.

38 Idem, "Livro Verde", 2010, 13.

A partir do entendimento de que a utilização do espaço cibernético se faz irreversivelmente presente, não há como se prescindir do estudo deste tema no âmbito dos Estudos Estratégicos. De forma proativa, criaram-se instituições militares e civis que endereçam este importante campo, porém baseadas em um debate ainda em andamento. De fato, esta questão não pode ser ignorada, sob o risco de se depositarem recursos e expectativas em organismos/instituições fundamentados em premissas equivocadas que apenas gerarão frustração.

Considerações Finais

Dado o exposto, nota-se que, por um lado, existe certo entusiasmo exacerbado em relação à abrangência do ciberespaço em relação às suas potencialidades, caracterização como domínio, e até mesmo a sobrevalorização de sua relevância em relação aos demais domínios de combate tradicionais. Por outro, o ceticismo em aceitar o ciberespaço como um fator relevante para os Estudos Estratégicos contemporâneos, pela dificuldade de enquadramento nos padrões analíticos consagrados do conhecimento em estratégia – como demonstrado na primeira parte deste texto –, representa uma negação imprudente da oportunidade de análise de um conjunto de fatores de relevância inegável em um cenário de combate contemporâneo centrado em redes e sistemas computadorizados.

A resistência à validação do espaço cibernético como domínio parece extrapolar a dificuldade de enquadramento de suas características enquanto espaço comum de combate, refletindo também o receio da academia com as devastadoras consequências que a assunção precipitada, e por vezes fantasiosa, conferida às potencialidades que a tecnologia pode causar ao campo dos Estudos Estratégicos. RAM é um exemplo sempre presente de que a extrapolação da capacidade de

obtenção de resultados providos por meio exclusivamente da tecnologia é insuficiente, quando aplicada em detrimento ao arcabouço conceitual estratégico desenvolvido[39].

Neste sentido, é possível traçar uma analogia ao programa de pesquisa lakatiano[40]. Na percepção do autor clássico, o conhecimento é estruturado em um núcleo duro de hipóteses teóricas que não pode ser alterado sem seu abandono por completo. Junto a esse núcleo, existe um cinturão protetor composto de hipóteses auxiliares que são dispensáveis ao programa de pesquisa e, dessa forma, funciona como uma gama de hipóteses que expande o programa de pesquisa e corrobora para validar o núcleo duro[41]. Ao incorporar o espaço cibernético como um domínio de combate, a aparente expansão teórica pode ser considerada regressiva, e não expansiva, quanto à capacidade explicativa do programa de pesquisa, transfigurada em uma metáfora: fragilizando o cinturão protetor do núcleo. Dessa forma, refutar a incorporação do ciberespaço como um domínio em estratégia pode ser compreendido como a manutenção do rigor metodológico para o reforço do programa de pesquisa. Por outro lado, negligenciar a relevância da agenda de pesquisa afeita ao espaço cibernético e suas implicações a operacionalização da guerra e à estratégia, em um cenário crescente de combate centrado em redes, tampouco parece sensato.

Diferentemente das teorizações clássicas sobre a guerra na

39 Michael O'Hanlon, *Technological Change and the Future of Warfare* (Washington, DC: Brookings Institution Press, 2000).

40 Acerca das implicações desse tema geopolítico nas análises cibernéticas e vice-versa, *vide* capítulo de Walfredo Ferreira Neto e Gills Vilar Lopes, neste mesmo volume.

41 Imre Lakatos e Alan Musgrave. *Criticism and the Growth of Knowledge: proceedings of the international colloquium in the philosophy of science*, Vol. 4 (Londres: Cambridge University Press, 1970).

terra e no mar, substanciadas por milhares de anos de observação[42], a reflexão sobre a utilização do espaço cibernético no contexto da guerra se dá de forma simultânea à sua gênese, de forma análoga ao ocorrido com a guerra no espaço aéreo. A primeira geração de pensadores da guerra neste domínio baseou-se mais em expectativas do que na experiência, sendo necessário mais tempo para que princípios fossem cristalizados. Parece-nos plausível que o mesmo esteja ocorrendo hoje com o espaço cibernético.

Independentemente de se caracterizar um domínio de combate ou um espaço comum, o espaço cibernético representa um cenário de interações crescentes entre atores estatais e não-estatais, capaz de influenciar no andamento e resultado das interações políticas e estratégicas entre os mesmos. Isso nos leva novamente à Clausewitz, pois o que é a guerra se não a continuação da política por outros meios? Dessa forma, a incorporação do estudo do espaço cibernético ao programa de pesquisa dos Estudos Estratégicos é prudente e pode caracterizar-se expansiva à medida que busca estender e aprofundar o entendimento de sua conformação, função, potencialidade e interação com os domínios tradicionais dos Estudos Estratégicos.

42 Proença Jr., Diniz e Raza, op. cit., 21.

PARTE 2

OPORTUNIDADES E DESAFIOS EMPÍRICOS

Guerra Virtual e eliminação da Fricção? O uso da cibernética em operações de contrainsurgência pelos EUA[1]

Alcides Eduardo dos Reis Peron

Introdução

> Bombardeio, fogo cerrado, fogo de barragem, gás, minas, tanques, metralhadoras, granadas de mão... são apenas palavras, mas encerram todo o horror do mundo [...] Vemos homens ainda vivos que não tem [*sic*] mais a cabeça; vemos soldados que tiveram os dois pés arrancados andarem [...]. O sol se põe, vem a noite, as granadas assobiam, a vida chega ao fim.[2]

> Selvagens, desprezíveis. Essas eram as figuras que enfrentávamos no Iraque. É por isso que muitas pessoas, inclusive eu, chamávamos os inimigos de "selvagens". [...] A primeira vez que você atira em alguém, você fica um tanto nervoso [...] Mas depois que você mata o seu inimigo, você vê que é ok. Você diz, legal! […] Eu amava o que fazia. E eu não estaria mentindo ou exagerando ao dizer que era divertido.[3]

1 Uma versão preliminar desse texto foi apresentada no Encontro Nacional da Associação Brasileira de Estudos de Defesa (ENABED 2014), em Brasília.

2 Erich Maria Remarque, *Nada de novo no front* (Porto Alegre: L&PM Pocket, 2011).

3 Chris Kyle, *American Sniper: The autobiography of the most lethal sniper in U.S. Military History* (Nova Iorque: William Morrow, 2012), 4-6, tradução nossa.

As duas passagens acima representam momentos distintos da arte da guerra, entre os séculos XX e XXI. Em um primeiro momento, tem-se a descrição humanística de Erich Maria Remarque sobre o horror e a carnificina na Primeira Guerra Mundial; em seguida, o relato indiferente, cínico, quase satírico do ato de matar, feito por Chris Kyle, um atirador de elite que fez parte da operação *Enduring Freedom* no Iraque.

Mais do que estilos literários diferentes, tais relatos retratam o movimento que marca a mudança no modo como a guerra vem sendo enfrentada, a saber: a renúncia ao combate direto por novos meios tecnológicos tem se manifestado como uma recente política estratégica das Forças Armadas estadunidenses.

A Revolução nos Assuntos Militares (RAM) nos anos 1980 e 1990 foi um divisor de águas no modo com que os Estados Unidos da América (EUA) conduziam suas operações militares e geriam o seu desenvolvimento tecnológico.

Buscando combater o terrorismo, a maioria das operações militares desde então tem sido categorizada enquanto ações "cirúrgicas", possibilitadas pelo uso de diversos tipos de tecnologias cibernéticas, sistemas informacionais, redes de comunicação via Internet e redes de telefonia móveis, bem como por interfaces de controle remoto, tais quais os chamados *drones* e as Armas Distanciadoras (*Stand-off Weapons*)[4].

Nesse contexto, é possível verificar vários estudos que buscam compreender tal processo bélico e militar, em que se destaca a perspectiva de James Der Derian[5], de que as operações militares estadunidenses têm se "virtualizado", ou seja, têm tornado-se um

4 Tais como os sistemas aéreos não tripulados (*Unmanned Aerial Systems* – UAS), e, em particular, os *drone*s.

5 James Der Derian, *Virtuous War: Mapping the Military-Industrial-Media-Entertainment Network* (Nova Iorque: Routledge, 2009).

processo pelo qual a mediação virtual das tecnologias militares resulta em uma reorganização no modo como a violência se atualiza, ao mesmo tempo em que há uma legitimação da forma como ela é lutada, supostamente "limpa" e precisa.

Outro *modus operandi* a serviço da arte da guerra diz respeito às operações denominadas Assassinato Seletivo (*Target Killing*), que consistem na "caçada" e eliminação de alvos específicos – como terroristas ou insurgentes –, em territórios estrangeiros em situação de guerra ou de paz[6].

Assim, esse capítulo tem como objetivo compreender de que modo as tecnologias empregadas nas operações de Assassinato Seletivo, ao promoverem a aniquilação do senso do real, contribuíram para um processo de banalização da violência ao mesmo tempo em que desenvolveram um senso de eliminação da Fricção no combate.

Para auxiliar nessa empreita, tem-se o marco teórico ancorado nos conceitos de simulacros e virtual, oriundos de Jean Baudrillard[7], e de *Virtuous War*[8], de Derian.

Em nossos indícios conclusivos, a consequência imediata que se vislumbra desse processo de virtualização da guerra é a progressiva eliminação do seu "princípio de realidade", em detrimento da emergência de um estado de "dissuasão global", como propõe o argumento de Baudrillard, em que a manutenção do potencial de dissuasão ativo – de vigilância e "brutalização" –, por meio da banalização da violência caracteriza-se como o principal fundamento

6 No último caso, pode ser caracterizada como uma modalidade de assassinato extrajudicial.

7 Jean Baudrillard, *Simulacra and Simulation* (University of Michigan Press, 1994).

8 Optamos por manter o termo *Virtuous War* em detrimento da sua tradução possível: guerra virtuosa ou, até mesmo, guerra virtual. Essa decisão se deve à percepção de que Der Derian intenciona manter tal duplo significado (conforme explicaremos mais adiante) em sua crítica de que uma guerra que constrói uma fantasiosa virtude a partir da virtualidade – seja no sentido que designa o fenômeno técnico dos sistemas informacionais, seja em seu sentido mais complexo, em que o virtual sobrepõe-se e elimina o real.

das novas práticas de guerra. Nesse sentido, tanto a ideia de cirúrgico e de eliminação da fricção no combate corporificam uma simulação de legitimidade da guerra, fundamental para a sua manutenção enquanto estado de dissuasão contínuo.

Hipótese e Caminho Argumentativo

Ancorado em um discurso de precisão cirúrgica e preservação da integridade física dos combatentes, permitido pelos novos tipos de Armas Distanciadoras, a RAM traz muito mais do que uma solução técnica ao contínuo desmantelamento do Complexo Militar Industrial (CMI) estadunidense. A RAM permite resolver a problemática do antagonismo público a longas campanhas militares com muitas mortes e destruição, que tanto categoriza a "Síndrome do Vietnã". Em verdade, evidencia-se um novo modelo de guerra que se associa perfeitamente aos ditames de uma prolongada "guerra irregular" ao terrorismo, em que as ameaças são atomizadas e a dinâmica de uma "guerra tradicional" se torna inviável.

No entanto, o constante emprego de *drone*s nessa modalidade de guerra irregular, principalmente após findas as operações em terra no Iraque, tem sido alvo de grande controvérsia, principalmente no que tange a suas legalidade e legitimidade.

Apesar de o Assassinato Seletivo ser uma prática "legal" em tempos de guerra, nos últimos dez anos, observa-se que esse tipo de operação vem ocorrendo em um contexto de profunda generalização do espaço de batalha, uma vez que se estende sobre territórios pacíficos que passam a ser determinados enquanto "Estados falidos", tais quais: Iêmen, Paquistão e Somália.

Assim, por traz do discurso de uma guerra enxuta (cujo uso cirúrgico da violência se torna "tolerável"), evolui um modo de guerra

extremamente brutal que tem, na ideia de redução da fricção[9], um dos de seus elementos mais contraditórios e problemáticos: precisão e distanciamento do *front*. Por um lado, o combatente é extirpado do campo de batalha, em que pese o fato de as tecnologias informacionais e cibernéticas supostamente confeririam precisão de ataque e maior conhecimento do teatro de guerra. Por outro, há um incremento estratégico significativo na indiferença do uso da força permitido pelo distanciamento, dado que o combatente, por meio de uma interface gráfica cibernética, não se expõe à totalidade das consequências de seu ato de violência.

Do mesmo modo, desenvolve-se uma complexa forma de administração da guerra a partir dos Centros de Comando totalmente informatizados, aproximando comandantes, oficiais e combatentes – estes últimos, em bases no território dos EUA –, observando e gerenciando o conflito em tempo real. Nesse caso, observaremos mais adiante, que o excesso de informações tem levado ao que chamaremos de uma intensificação da "névoa de guerra" pelos processos de ruptura digital (*digital divide*).

Nesse sentido, o objetivo principal das próximas seções é verificar como a adoção de sistemas cibernéticos para a mediação do combate a distância – sob a justificativa de se construir uma forma cirúrgica e certeira de conflito – tem conformado uma reorganização da fricção de guerra. Tudo isso à luz do debate entre Baudrillard e Derian acerca do processo de virtualização a que os conflitos armados estadunidenses desde a Guerra do Golfo estão sujeitos.

Para tanto, lança-se olhar sobre as operações de Assassinato Seletivo com o uso de *drone*s, as quais se caracterizam por um intenso processo de mediação técnica, a partir dos grandes sistemas tecnológicos de comunicação e processamento de dados desenvolvidos durante a

9 Cf. Carl von Clausewitz, *Da Guerra* (São Paulo: Martins Fontes, 2010).

RAM. Assim, as próximas seções brevemente abordam os problemas de ruptura digital e de desengajamento moral oriundos do emprego intensivo das tecnologias de informação e comunicação (TIC) e da cibernética nas guerras conduzidas a distância, como manifestações de uma *Virtuous War*.

Virtuous War: simulando a legitimidade e a guerra

Em períodos distintos, Baudrillard e Der Derian observam fenômenos muito próximos sobre o processo de mediação e midiatização da sociedade, e da mesma forma desenvolvem críticas bastante semelhantes sobre as campanhas militares estadunidenses.

A partir da compreensão de que os discursos e a prática de guerra se desassociam profundamente da "realidade" ou da "atualidade" de como as guerras ou as intervenções se manifestam, vislumbrando a construção de um espaço de ação moralmente justificável, ambos os autores denunciam a emergência de uma hiper-realidade ou virtualização da guerra. Sobre essa identidade com o pensamento de Baudrillard, Der Derian explica a identidade que busca construir entre os conceitos de hiper-real e virtual, e o processo de simulação como elementos capazes de lançar luzes sobre a discussão de uma guerra midiatizada, e mediatizada:

> [...]dispomos dos meios técnicos para se construir mapas e modelos que parecem tão reais quanto a realidade que eles simulam. Realidade "virtual" ou "artificial" é o que os cientistas da computação – e agora os cyber especialistas – começam a chamá-la. Baudrillard se referiu inicialmente a ela enquanto o reino da hiper-realidade, aonde as origens são esquecidas, referentes perdidos, e simulações começam a preceder e engendrar a realidade. Esse é

> o mundo da Destruição Mútua Assegurada, Guerra nas Estrelas e Tecnologia de Assalto, todas elas máquinas de deterrência que em grande medida "trabalham" persuasivamente no mundo hiper-real da simulação estratégica[10].

Essas categorias de análise escarnam um processo que se desenvolve desde as Guerras do Vietnã e do Golfo, atingindo seu apogeu nas intervenções no Iraque e no Afeganistão, *drone* o qual se fundamenta na criação de um discurso de terror e de emergência acerca do conflito, que legitime a intervenção diante às instancias multilaterais internacionais. Tal processo, que e se adensa na mediatização das informações do conflito se manifesta no distanciamento abrupto – e, muitas vezes, na total abdução – dos combatentes do campo de batalha, em detrimento do uso de poder aéreo.

Esses processos podem ser julgados enquanto *simulações* ou *virtualizações* da guerra, em que a criticidade está na profunda estetização de conflitos, que é inerente tanto do distanciamento mediado quanto do artificialismo das justificativas sobre as intervenções. Tais justificativas, por seu turno, não contribuem para a percepção do real estado de guerra, uma vez que, caso se imploda o princípio de realidade, o que resta é uma apreensão *in-vitro* do hiper-real, como afirma Baudrillard[11], ou como expõe Der Derian[12], faz com que a sociedade e os combatentes o percebam de forma banalizada, "*tragedy-free*".

Nesse sentido, apesar da distinção entre as tecnologias "analógicas" feitas por Baudrillard no início dos anos 1980, cujas propriedades são levemente distintas das "digitais" construtoras do ciberespaço (que servem de base crítica para Derian), ambos os autores

10 James Der Derian, "Simulation: The Highest stage of Capitalism?", in *Baudrillard: A Critical Reader*, org. Douglas Kellner (Oxford: Basil Blackwell, 1994), 194.

11 Jean Baudrillard, *La Guerra del Golfo no ha tenido lugar* (Barcelona: Editorial Anagrama, 1991), 16.

12 James Der Derian, *Virtuous War,* 121.

precedem da tradição teórica da Teoria Crítica, do modernismo e do pós-modernismo. Logo, concordam com o argumento de que a sociedade de consumo perpassa por um processo de mercantilização da realidade, algo muito próximo ao que Marx afirma ser o processo de abstração no capitalismo, em que as leis de equivalência dissolve todas as diferenças qualitativas em uma identidade quantitativa de valor[13]. Nesse processo de abstração, potencializado pelo advento dos *mass media* e das diversas mediações tecnológicas características da "cibercultura", ambos concordam com a ideia de uma ampla proliferação de imagens e signos, em que as distinções tradicionais entre ilusão e realidade, significado e significante, sujeito e objeto entram em colapso, e consequentemente não há mais um mundo social ou real ao qual se possa falar; apenas uma hiper-realidade "semioticamente" autorreferente[14].

Nesse contexto, Baudrillard afirma que o virtual expande-se às custas do real, uma vez que esta forma de comunicação potencializa a produção e a circulação de mensagens e anula o próprio processo de transmissão e absorção de conteúdo. Nesse processo de expansão das formas de comunicação virtual, em uma constante aniquilação dos significados pelos significantes, Baudrillard declara que o real desertifica-se, perdendo o seu sentido, e a consequência imediata disso é a nossa incapacidade de distinção entre o real e o imaginário. Esse processo, como afirma Derian, é parte do movimento da *Virtuous War*, no que tange à aproximação entre Forças Armadas e *mass media* no controle e divulgação de informações e narrativas oficiais sobre os conflitos aos quais os EUA têm participado desde então. Assim, a guerra contemporânea, para os autores, manifesta-se enquanto uma simulação, ou virtualização, em que a midiatização das campanhas e

13 Steven Best, "The Commodification of Reality and the Reality of Commodification: Baudrillard, Debord, and Postmodern Theory", in *Baudrillard: A Critical Reader*, org. Douglas Kellner (Oxford: Basil Blackwell, 1994), 41.

14 Ibid., 41.

das operações militares estadunidenses (principalmente após o Vietnã), e o desenvolvimento de novas tecnologias de apoio em sistemas informacionais (para o distanciamento do combate direto) buscam legitimar uma prática de operações militares brutal e ilegal.

Em Derian[15], a *Virtuous War* é entendida como a construção de um reino simbólico que projeta um tipo de inconsciência coletiva sobre os contemporâneos temas de segurança, de que a superioridade moral do combate concentra-se muito mais em seu potencial tecnológico e meticuloso para a promoção da violência, do que na brutalidade do martírio corpo a corpo. A guerra que se inicia como um processo de virtualização tecnológica dos instrumentos bélicos passa assim para o nível superior de uma *Virtuous War* ou "guerra virtuosa".

Nesse ponto, ao expor sua teoria do virtual, Der Derian[16] retoma a etimologia de "virtual", lembrando a origem latina da palavra, em seu duplo sentido: *virtuosos* e *virtualis*. Em seu primeiro sentido, designa inicialmente uma noção medieval de algo imbuído de virtude, por poder divino ou sobrenatural, mas incorpora também o senso de virtude greco-romano de propriedades e qualidades de conduta correta ou direita. Ainda, é possível compreender *virtualis* como um conjunto de qualidades inerentes que pode por vontade (*virtú*) ou potencialmente influenciar algo. O primeiro significado coexiste com o seu segundo uso, *i.e.*, o virtual como algo moralmente neutro, majoritariamente referente a fenômenos técnicos, no qual o novo modo de guerra oportunamente reconectaria com o significado *virtuoso*, de modo a legitimar suas práticas. Nesse sentido, a virtualidade tornou-se a "quinta dimensão" da hegemonia global dos EUA, ao desenvolver sua crítica sobre a *Virtuous War*.

15 James Der Derian, *Critical Practices in International Theory: Selected Essays* (Nova Iorque: Routledge, 2009), 244.

16 Ibid., 244-248.

> Usando informação em rede e tecnologias virtuais para trazer o "lá" até aqui, em tempo quase real e com quase total verossimilhança, a *virtuous war* exercita uma vantagem comparativa tanto quanto estratégica para os avanços digitais[17].

Portanto, ao tomarmos a afirmação, de Der Derian, de que a guerra é lutada da mesma forma que é representada (virtualmente, permeada por diversos aparatos técnicos e interfaces), e a associarmos às percepções de Baudrillard sobre as diversas retóricas concorrentes trazidas pela mídia sobre a Guerra do Golfo, que a caracterizariam enquanto um simulacro, podemos compreender o quanto as categorias de virtualização e simulação podem explicar o movimento de ruptura que caracteriza a "contemporaneidade" das campanhas militares estadunidenses no pós-RAM, particularmente nas missões comandadas pela Força Aérea (USAF) e pela Agência Central de Inteligência (CIA) estadunidenses no contexto de operações com *drones* para vigilância e eliminação de ameaças terroristas.

Revolução nos Assuntos Militares e ameaças assimétricas: a busca pela precisão pede auxílio à cibernética

Dizia-se que o advento de novas ameaças no cenário global e o surgimento de novas tecnologias informacionais contribuiriam para a "eficácia" da interoperabilidade entre as Forças Armadas estadunidenses, do nível decisório ao tático. A aplicação dessas tecnologias para o desenvolvimento de instrumentos de suporte às operações militares consubstanciaria o discurso de uma "guerra moderna", enxuta e cirúrgica em suas representações.

17 Ibid., 244.

Porém, observa-se, ao longo desta seção, que de fato há uma descontinuidade no modo como as operações militares estadunidense vinham sendo conduzidas, e isso se devia principalmente à adoção de novas tecnologias, doutrinas e táticas de combate pelos EUA. Contudo, de um lado, o "novo" das operações militares contemporâneas é muito mais tributário do caráter privilegiado que a gestão da informação, e, do outro, o distanciamento – senão a completa abdução do combatente da guerra – torna-se determinante para a condução de operações cirúrgicas e de alto risco físico e diplomático.

Dentre os entusiastas estadunidenses da RAM nesse período, destacam-se os generais Donn Starry e Donald Morelli (articuladores da ideia de guerra de "Terceira Onda"), além de Andrew Marshall, diretor do *Office of Net Assessment* do Pentágono, e do presidente do *Naval War College*, Vice Almirante Arthur Cebrowsky. No caso dos dois primeiros, foram profundamente influenciados pela ideia de Guerra de Terceira Onda de Alvin e Heidi Tofler na década de 1980, em que após a revolução da agricultura, e da revolução industrial, vivenciamos a conformação de um novo tipo de civilização, que reinventa sua própria economia, família, formas, mídia e política com base na informática[18]. Com a Revolução da Informação e a possibilidade de aproveitamento estratégico do ciberespaço, ao seu ver, a doutrina militar também deveria mudar: de força bruta para "cerebral". Desta forma, haveria maior interoperabilidade entre soldados e novas armas teleguiadas de precisão, orientando-se não em função do espaço (mobilização de tropas, deslocamento e posicionamento), mas sim em relação ao tempo (velocidade da Internet e dos *links* de comunicação, *feeds* em tempo real, velocidade de reação etc.)[19].

18 Alvin Toffler e Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (Londres: Little, Brown and Company, 1993).

19 Ibid., 11.

Assim, de acordo com Shimko[20], a RAM pode ser compreendida enquanto um conjunto de valores e percepções que evoluem, a partir de um distinto contexto politicoeconômico, e passam a constranger a agenda de política pública, no que tange desde a produção de novas tecnologias de guerra até o modo como ela deve ser conduzida e comandada.

O desenvolvimento da RAM se deve a uma sorte de fatores, desde econômicos, políticos ou sociais, dentre os quais se destacam os seguintes: a substantiva redução dos investimentos governamentais em pesquisa e desenvolvimento (P&D) militar, em detrimento da elevação dos da mesma ordem no setor civil[21]; o complexo desfecho da Guerra do Vietnã, em que as inúmeras mortes de combatentes foram responsáveis pelo desenvolvimento da aversão coletiva a um conflito de grandes proporções, reconhecida enquanto "síndrome do Vietnã"[22]; a profusão das TIC e da cibernética como novo paradigma de preceito tecnológico que, associadas a outros sistemas, provocam enormes transformações nas dimensões militares-culturais, nos princípios organizadores militares e nos seus sistemas tecnológicos; e, por fim, a substancial diversificação da natureza das ameaças à segurança nacional, que estimula a reordenação da política de defesa *drone* e, consequentemente, a reorganização de conceitos operacionais[23].

Logo, a RAM se estrutura, de um modo mais objetivo, como uma série de princípios organizacionais que se manifestam como uma correlação entre sistemas de gerenciamento de tecnologias, de defesa e de tecnologias de defesa, como expõe Matthews[24]. Por sua vez, o

20 Keith Shimko, *The Iraq Wars and America's Military Revolution* (Nova Iorque: Cambridge University Press, 2010), 2.

21 Fruto da percepção de que o núcleo dinâmico produtor de novas tecnologias segue o fluxo de "transbordamentos" do setor civil para o militar, e não o contrário, como observado no imediato pós-Grandes Guerras.

22 Ian Buchanan, "Treatise on Militarism", *in Simploke 14* (2006), 155.

23 Zbigniew Brzezinski, *American security in an interdependent world: a collection of papers presented at the Atlantic Council's 1987 Annual Conference* (University Press of America, 1989), 03-04.

24 Ron Matthews, "Introduction: Managing the Revolution", in *Managing the Revolution in Military*

Departamento de Defesa (DoD) dos EUA entende a RAM como uma série de modificações e combinações entre sistemas tecnológicos de armamentos e métodos operacionais que resultaram, a rigor, em uma nova forma de organização para a realização de operações militares e para a condução da guerra[25].

Dentre os sistemas tecnológicos de maior expressão desenvolvidos nesse período, destacam-se os de comunicação por satélite e transmissão ao vivo via satélite (destacando-se o *KU-band*), armas distanciadoras (particularmente, com o uso bélico dos veículos aéreos não tripulados – VANTs[26]), sistema sensorial para detecção e "*targeting*" para veículos terrestres não tripulados (VTNTs) e os próprios VANTs; sensores de "*countermine*", para detecção e detonação remota de minas terrestres; sensores e componentes para Simulação e modelos para treinamento; e, no que tange às atividades de P&D, sobressaem-se as investigações acerca da conjução eletro-óptica e infravermelho (EO/IR), além de sistemas de auxílio a reconhecimento e mira (ATR). Isso não apenas permitiu o desenvolvimento de sistemas de comando, controle, computação, comunicação, inteligência, vigilância e reconhecimento (C4IRS, em inglês)[27], como também conferiu às Forças Armadas estadunidenses o controle de todo o fluxo de informações acerca de uma dada guerra, materializando a dinâmica de "guerra centrada em rede" (GCR*)*, preconizada por Cerebrowsky[28].

Para Bellamy[29], a guerra centrada em rede se dividiria em três tipos de estratégia: (i) guerra de comando e controle (*C2 Warfare*), cuja

Affairs, org. Ron Matthews e John Treddenick (Nova Iorque: Palgrave, 2001).

25 Estados Unidos da América. Office of the Secretary of Defense, "Annual Report to the President and the Congress", 1999, http://fas.org/man/docs/adr_00/chap10.htm, acessado em 8 nov. 2014.

26 *Drone*, portanto, é o VANT projetado para disparar.

27 Os C4IRS otimizam as campanhas militares de dominação rápida (*shock and awe*).

28 Arthur Cerebrowsky, "Military Responses to the Informational Age", *The RUSI Journal* 145:5 (2000).

29 Christopher Bellamy, "What is information warfare?", in *Managing the revolution in military affairs,* org. Ron Matthews e John Treddenick (Nova Iorque: Palgrave, 2001), 56-75.

intenção é desenvolver operações com armas eletrônicas e sistemas de bombardeio cirúrgicos, capazes de destruir fisicamente ou inutilizar eletronicamente a infraestrutura de C2 do inimigo; (ii) a guerra de *softwares* (*Software Warfare*), um combate travado no campo de fluxo de dados computacionais, através de manipulação de códigos-fonte, acesso à dependência de *softwares* via Internet, com o objetivo de atingir as capacidades inimigas, neutralizando-as e, assim, alcançando uma supremacia no combate físico; e, por fim, (iii) a guerra informacional (*Information Warfare*), a qual prevê o uso dos "meios" de comunicação (mídia) como forma de estabelecer um controle sobre o fluxo informacional e, com isso, explicitar uma realidade específica do conflito, algo fundamental para estimular o apoio social e legitimar a campanha de guerra "prolongada".

Assim, tanto as perspectivas quanto as tecnologias oriundas da RAM e da guerra centrada em rede fundamentariam a conduta da guerra e de intervenções no novo horizonte político dos EUA, de combate ao terrorismo. Em grande medida, esse discurso dá conta de responder aos problemas de excessivas mortes de combatentes, ao mesmo tempo em que acresce a capacidade de se combater ameaças assimétricas em contextos de guerras irregulares, como, por exemplo, a guerra cibernética. No entanto, a noção de redução dos elementos friccionais de "névoa" – ou incerteza – do combate e do incremento da precisão é bastante controversa, haja vista que se apresentam problemas relativos tanto a um elevado número de mortes de civis, ao lado dos "inimigos" (problemas relativos ao "fogo amigo") quanto problemas de ordem tática, como a mencionada *ruptura digital*.

Apesar da maior aproximação e capacidade de gestão do conflito a partir da caserna, aproximando os generais da gestão tática em tempo real de suas batalhas, Shimko[30] afirma que teria sido um problema recorrente, na recente campanha do Iraque, o fato de que o comando da operação

30 Shimko, op. cit., 170.

tem mais conhecimento dos movimentos do campo do que os próprios combatentes em solo. Nesse período, o enorme aparato de vigilância, comunicação e processamento de dados, teriam sido incapazes de prover, às tropas em solo, informações valiosas sobre localização de forças amigas e inimigas. A *ruptura digital* fica evidente, quando Shimko[31] menciona que, durante as recentes operações militares americanas no Iraque, mais de 10% das fatalidades estadunidenses deveu-se a "fogo amigo", a partir de ataques aéreos de bombardeiros A-10. Em grande medida, esse tipo de erro se "justifica" pela incapacidade de os sistemas técnicos dos A-10 identificarem e distinguirem precisamente os veículos em solo por meio de: visão termal; frágil relação entre todos os elementos presentes nessa rede virtualmente construída (C4IRS, bombardeiros, tropas em solo etc.); e ao inconsistente *design* dos *softwares* usados em equipamentos pelas forças em solo (denominados *Blue Force Tracker*) para adquirir informações sobre o movimento do inimigo[32].

Casos como esses evidenciam uma ruptura digital da "guerra centrada em rede", causada tanto por uma insuficiência dos sistemas informacionais para integralmente reproduzir a situação do combate (*situational awarness*) quanto por sua sobre-estimação pelas Forças Armadas estadunidenses. É possível dizer que, nesse caso, a adoção de sistemas informacionais e dispositivos cibernéticos (não enquanto suporte, mas enquanto determinante para a organização das guerras contemporâneas) intensificam a possibilidade de erro àqueles que contemplam e administram os movimentos da batalha exclusivamente por meio da mediação técnica ou gráfica. Ao invés da precisão cirúrgica e da ampla compreensão do campo de batalha, a virtualização da guerra nos parece trazer novamente a *névoa* da incerteza e da imprevisibilidade dos conflitos, como mostra a próxima seção.

31 Ibid., 169.

32 Ibid., 169.

Drones e "Fricção" nas operações de Assassinato Seletivo

Como resultado direto dos avanços tecnológicos da RAM, os sistemas aéreos não tripulados (UAS, do inglês) passaram a ser empregados com maior regularidade nas campanhas e operações militares estadunidenses, principalmente a partir da intervenção no Kosovo, quando o *trade-off* entre a mobilização de tropas em larga escala e o uso de *drones* fica bastante evidente.

Desde 2001, o investimento do DoD com UAS tem aumentado substancialmente, passando de US$ 363 milhões em 2001 para US$ 2,9 bilhões em 2013, o que se manifesta em um expressivo incremento desse tipo de equipamento nos inventários estadunidenses: enquanto somente 5% das aeronaves, em 2005, eram não tripuladas, já em 2012 atinge-se 33% do total de aeronaves em operação, ao todo 7454[33].

Mais do que uma consequência de todo o *lobby* das empresas estadunidenses de material de defesa – as quais tiveram um aumento de 13% nas campanhas eleitorais de 2000 e 2002, e em torno de 30% entre 2006 e 2008[34] –, o aumento do emprego de *drone*s está relacionado a uma percepção de segurança em sentido amplo, em que as ameaças terroristas têm confundido as esferas civil e militar e os espaços soberanos ou não (como os Estados falidos), fazendo com que ataques supostamente cirúrgicos e pontuais tenham maior eficácia para prevenir futuros ataques[35].

Nesse sentido, ganha expressão o uso de *Drone*s como forma de aquisição de informações em contexto de risco e de eliminação de alvos pontuais, principalmente após as campanhas no Iraque e no

33 Abigail Hall e Christopher Coyne, "The political economy of *drone*s", *Defense and Peace Economics* (2013), 10.

34 Ibid., 18.

35 Chetan Bhatt, "Human Rights and the transformation of War", *Sociology 46* (2012), 818.

Afeganistão, ao se invocar uma prerrogativa de Estados falidos para nomear territórios que potencialmente poderiam abrigar pessoas relacionadas a atividades terroristas.

De acordo com a "*New America Foundation Drones Database*", no Paquistão, entre 2004 e 2007 houve nove ataques de *drones*; em 2008, 33; em 2009, 53; em 2010, 118; e, em 2011, 78. Abrindo a caixa preta desses ataques, o projeto "*Out of Sight, Out of Mind*"[36] revela que, entre 2004 e 2013, os ataques de *drones* no Paquistão:

- 3.213 pessoas morreram, sendo apenas 50 (1%) "*hight profile*" e pertencentes às chamadas "*kill lists*";
- 2.453 pessoas (76,3%) foram consideradas pelo governo estadunidense potenciais terroristas (militantes), até que se provasse o contrário[37]; e
- 536 (16,7%) eram comprovadamente civis e 175 (5,4%) eram comprovadamente crianças.[38]

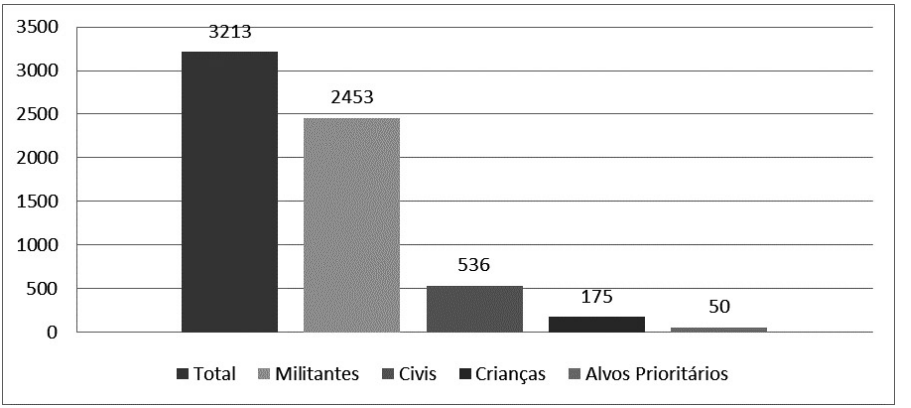
O Gráfico 1 apresenta e sumariza os dados contidos sobre os assassinatos provocados pelo uso desse tipo de VANT, no Paquistão.

36 Com base nos dados da "*New America Foundation*" e do relatório conjunto entre as Universidades de Stanford e de Nova Iorque denominado "*Living Under Drones*".

37 Uma categoria extremamente controversa, uma vez que não existe nenhum tipo de documentação ou critério divulgado pelos EUA que permita a categorização dessas vítimas enquanto militantes.

38 International Human Rights and Conflict Resolution Clinic at Stanford Law School e Global Justice Clinic at NYU School of Law. *Living under Drones: Death, Injury, and Trauma to Civilians from US Drone Practices in Pakistan* (2012), 35.

Gráfico 1: Vítimas dos Ataques de drones no Paquistão (2006-2014)



Fonte: elaboração própria.
Fonte dos dados: Stanford University e New York University[39].

O elevado número de alvos "não prioritários" eliminados contrasta profundamente com o 1% integrante aos alvos pertencentes às "*kill lists*", o que inicia uma profunda controvérsia acerca do discurso de "guerra cirúrgica" e de precisão atribuída às operações de Assassinato Seletivo.

Após o 11 de setembro, em que há uma profunda mudança em todo o aparato relacionado à política de segurança dos EUA, os discursos sobre *guerra global ao terror*, *guerra cirúrgica*, *guerra preventiva* e *caçada humana* ganham expressão enquanto justificativas recorrentes da então Administração nacional para a realização de intervenções em vários países desde então.

Desse modo, passadas as intervenções militares diretas, com mobilização ostensiva de contingente para alhures, verifica-se que as operações de Assassinato Seletivo ainda se mantêm ativas pela mesma prerrogativa do discurso de guerra global ao terror, qual seja

39 Ibid.

a eliminação de potenciais ameaças terroristas. Entretanto, os meios técnicos desenvolvidos ao longo da RAM permitiram que a eliminação de ameaças assimétricas pudessem se realizar de maneira remota e supostamente precisa, abrindo espaço para um discurso complementar de combates cirúrgicos. Nesse prisma, o conceito de *Virtuous War* elaborado por Der Derian poderia ser válido como uma forma de classificação dessas operações de caça e assassinato comandadas em conjunto pela USAF e CIA, uma vez que os meios técnicos de distanciamento e virtualização do combate corroboram para mascarar um contexto de controvérsia legal – como apontam O'Connell[40], Banta[41] e Bhatt[42] – em que a violência é banalizada em práticas descontinuadas, sem territorialidade e pretensamente racionalizadas a um discurso sobre uma prática supostamente cirúrgica e enxuta.

Como mostra Gregory[43], as operações de assassinato seletivo conduzidas em por USAF e CIA são realizadas a partir de uma intrincada rede de comando dispersada em diferentes níveis hierárquicos, mas principalmente em diferentes regiões do globo, e portanto em diferentes fuso-horários, denominada por eles mesmos de "Cadeia da Morte". Nessa cadeia, todos os participantes – sejam os operadores de *drone*, seja a equipe dos centros de comando – julgarão os inimigos a partir da identificação de padrões suspeitos de comportamento nas leituras de calor (*heat signatures*) produzidas pelo aparato. Apesar da distância geográfica entre a base e o teatro de operações e da submissão a uma mediação tecnológica de alta resolução gráfica, muitos (como Bhatt[44]

40 Mary E. O'Connell, "Seductive Drones: Learning from a Decade of Lethal Operations", *Journal of Law, Information & Science* (2011).

41 Benjamin Banta, "*Virtuous War* and the emergence of *jus post bellum*", *Review of International Studies 37* (2011), 277-299.

42 Chetan Bhatt, "Human Rights and the transformation of War", *Sociology 46* (2012).

43 Derek Gregory, "From a View to a Kill: Drones and Late Modern War", *Theory, Culture & Society*, 28, 188-215 (2011).

44 Bhatt, op. cit., 820.

e o oficial estadunidense da base de Creech, Mcloskey[45]) afirmam que o soldado operador de *drone* estaria próximo do ato de violência e portanto, perfeitamente consciente do emprego da violência.

Desse modo, considerando o excessivo número de mortes não justificadas na operação do Paquistão, e ainda as que tomam conta do Iémen (ao todo, 88 ataques entre 2002 e 2014, totalizando 945 mortos, sendo 134 civis mortos), podemos questionar essa perspectiva e advogar em função da ideia de que, embora haja uma proximidade da violência por meio de uma representação gráfica, tanto o espaço de combate simulado quanto a virtualização da guerra pela imagem – seguindo a lógica postulada por Baudrillard e Der Derian – eliminam o *princípio de realidade* de um conflito presencial e continuado, provocando uma espécie de "desprendimento moral" do "combatente de cubículo" em relação à violência empregada[46].

Nesse ponto, é possível considerarmos que tal desprendimento também se fundamenta enquanto um resultado da redução da "fricção de guerra", uma vez que imbui o emprego da violência pelo combatente de racionalidade e "certeza".

O termo fricção é explorado por Clausewitz enquanto um "fator invisível" que sempre governa as mudanças simplórias da teoria estratégica da guerra, para a complexidade do real[47].

De acordo com Clausewitz todos os perigos a que a guerra conduz, assim como os esforços físicos nela exigidos, contribuem para intensificar o *mal estar* da guerra, configurando-se portanto como o maior problema a ser enfrentado na marcha do conflito. Assim, os perigos e os desgastes físicos figuram como as principais variáveis "climáticas" que constrangem o ritmo e o desenvolvimento pleno do

45 Gregory, "From a View to a Kill", 200.

46 Làmber Royakkers e Rinie Van Est, "The Cubicle Warrior: The Marionette of Digitalized Warfare", *Ethics and Information Technology*, Vol. 12, No. 3 (2010), 293.

47 Clausewitz, *Da Guerra*, 83.

soldado na guerra. Desse modo, a noção de fricção clausewitziana compreende esse desgaste como elemento determinante para distinguir "a guerra real da que se pode ler nos livros"[48], reduzindo assim a previsibilidade e o mecanicismo da guerra.

A fricção seria então tudo aquilo que torna difícil o que parece fácil. Nesse âmbito, é notável que a experiência de guerra, o cotidiano do embate, o enfrentamento, as condições climáticas e o teatro de guerra, dentre outras "adversidades", são elementos que influenciam e constrangem o conflito e sua dinâmica, criando empecilhos e impedimentos para sua continuidade, ou mesmo para sua manutenção. A própria realidade da guerra, em suas particularidades brutais e nefastas, compromete a sua continuidade de modo uniforme e pleno.

À luz do debate que desenvolvemos até o momento, observamos que não é enganosa a correlação entre (i) a adoção de armamentos que primam pelo distanciamento do combatente do conflito (mediação técnica e automação dos instrumentos de combate), (ii) a intensificação da brutalidade e do poder de destruição da guerra, (iii) a intenção de eliminar a *névoa* que recobre a incerteza e a imprevisibilidade do campo de batalha e (iv) a manutenção "estratégica" da frieza e indiferença do combatente em relação ao horror inerente à batalha.

De súbito, é possível considerar que o imperativo do desenvolvimento das tecnologias aplicadas na guerra possibilitam, pelo distanciamento do conflito, uma maior capacidade de administração da percepção do combatente sobre a guerra. Isso se manifesta em uma "maximização" da eficácia na promoção da violência, em detrimento da maior previsibilidade do campo de batalha e da redução da aversão em relação à devastação que se processa.

No caso desses "combatentes de cubículo", sujeitos a um desprendimento moral, uma parcela bastante expressiva da fricção é

48 Ibid., 84.

eliminada: a de adversidades e de constrangimentos do contato com o campo de batalha e o medo de ser contra-alvejado. Um debate semelhante é preconizado por Grossman[49], é o de que o distanciamento em relação ao campo de batalha, e o consequente reordenamento sócio-técnico dos armamentos reduzem a inibição para matar, e isso, segundo Keagan[50], seria o movimento histórico do desenvolvimento de armamentos.

De certa forma, a redução da fricção pela virtualização produz um efeito favorável ao ato de matar, justamente pelo fato de despersonalizar a guerra, estando em consonância com a ideia de uma *Virtuous War*, em que a guerra lutada tende, da mesma forma que é representada, a eliminar todo o efeito trágico característico da guerra.

Isso ocorre porque (i) o corpo do combatente é extirpado do meio conflituoso e (ii) toda a relação com o ambiente de guerra é mediada por uma tela de computador[51], *joysticks* e uma série de técnicas e protocolos que ora provocam um "desprendimento moral" quanto ao uso da violência[52], ora tornam o ato de matar moral e politicamente tolerável, uma vez que são meios que se pretendem cirúrgicos, precisos, e que não colocam em risco a vida de soldados estadunidenses[53].

Considerações Finais

É notável que a busca por uma maior eficiência dos ataques[54] perpassa por uma maior gestão das informações sobre o *front*, a partir

49 Dave Grossman, *On Killing: The Psychological Cost of Learning to Kill in War and Society* (Nova Iorque: Back Bay Books, 2009).

50 John Keagan, *A History of Warfare* (London: Pimlico, 2004).

51 Em que a imagem do inimigo é reconstruída em um ambiente digital, enquanto um simulacro.

52 Royakkers e Van Est, "Cubicle Warrior", 23.

53 Ibid., 23.

54 Entendida não somente enquanto precisão dos armamentos, mas também como capacidade de realizar um combate rápido, pontual, logisticamente enxuto, e minimizar as consequências políticas dos ataques.

da retaguarda, ou dos centros de comando espalhados pela Terra e interligados pelo ciberespaço. Denominamos como *virtualização* esse movimento de constante informatização da guerra que busca maior eficiência, ao passo em que se constrói um argumento de *guerra cirúrgica* para legitimar moral e politicamente a guerra.

Apoiando no conceito de *virtuous war*, demonstramos que a introdução de novas formas e técnicas sob o epíteto "cirúrgico" intencionam, em última instância, esse processo, imbuindo virtudes e legitimidade a um modo de conflito perverso e de precisão moral e física questionável.

Observamos ainda que, ao longo do último decênio, as operações de assassinato seletivo tomam corpo a partir da reorientação estadunidense de políticas de segurança pós-11 de setembro, mas é outrossim tributária das percepções políticas e aplicações tecnológicas que se desenvolvem ao longo da RAM. Subordinadas ao discurso de combates cirúrgicos contra ameaças assimétricas, essas operações têm ocorrido mediante um constante emprego de *drone*s para eliminação de alvos pontuais envolvidos em atividades terroristas.

Apesar das implicações legais acerca dessa prática de assassinato, que conformam toda uma discussão no campo do Direito Internacional e Humanitário sobre a legitimidade da guerra preventiva, podemos destacar que o emprego de *drone*s tem sido uma prática militar moral e politicamente aceita. Isso ocorreria devido à proeminência do discurso de guerra cirúrgica, por parte da mídia e pelos discursos oficiais, os quais enaltecem as faculdades de precisão dos ataques e de proteção dos combatentes, em detrimento dos diversos erros cometidos a partir do uso de tais instrumentos.

Ademais, é levantada uma inquietação sobre a crença de que a virtualização tornaria a guerra mais racional e humana, pois, ao verificarmos que a substituição dos elementos friccionais próprios

da "experiência de campo" por uma nova subjetividade a partir da interação do combatente com o aparato de mediação do *drone*, pode induzir a um maior desengajamento moral dos combatentes (pilotos e operadores de sensores) em relação ao ato de matar.

Se, por um lado, a virtualização da guerra leva a problemas vistos como a ruptura digital e o aumento da névoa (incerteza e imprevisibilidade), por outro, como no caso dos *drones*, conduz-se a uma eliminação da *fricção*, no que concerne ao contato do combatente com as adversidades do campo de batalha – e consequentemente com os resultados da destruição que se causa.

Desse modo, as operações de assassinato seletivo poderiam ser compreendias enquanto *Virtuous War*, aos moldes propostos por Der Derian, uma vez que a virtualização da guerra elimina o combate real em detrimento de um espaço ciberneticamente simulado e, portanto, "toleráveis". A esse processo, contudo, enxergamos tão somente a banalização do uso da violência e a redução do combate à condição de um *simulacro* alienante e corruptivo que normaliza a condição da guerra ante a sociedade, ao ser imposto um discurso de manutenção e "perseverança" de uma guerra cirúrgica: limpa, moderada, e "*tragedy-free*"[55].

Logo, nem mesmo a cibernética pode ser utilizada como uma justificativa a esse meio tão comumente usado nas relações internacionais, que é a guerra.

55 Der Derian, *Critical Practices*, 241.

As Estratégias de Segurança e Defesa Cibernéticas na Argentina[1]

Sol Gastaldi
Candela Justribó

Introdução

A inovação acelerada e a contínua atualização das tecnologias de informação e comunicação (TICs) têm permeado os diversos campos da atividade humana, gerando crescente relevância e abrangência em diferentes áreas, tanto na agenda internacional quanto na doméstica, mesmo em questões como as relacionadas à Segurança Interna e à Defesa Nacional.

O ciberespaço, enquanto ambiente virtual criado pelo homem, não possui fronteiras físicas nem geográficas[2], não existem limites de tempo para sua utilização, e em seu interior podem-se gerar diferentes ações. Algumas delas chegam a ser hostis, como as ameaças ou os ataques virtuais que diferem apenas por sua natureza e motivação. Tais ações chegam muitas vezes a serem confundidas com outras modalidades de delito cibernético, podendo levar até mesmo ao emprego das Forças Armadas, dependendo da percepção que cada um desses ataques tenha no nível político (Segurança Cibernética), estratégico (Defesa

1 Tradução de Laura Ponessa.

2 Para mais detalhes sobre as questões de fronteira cibernética, ver capítulo 2 ("Teoria da Fronteira Cibernética: inquietações interdisciplinares", de Walfredo Bento Ferreira Neto e Gills Vilar Lopes) desta coletânea.

Cibernética) ou tático-operacional (Guerra Cibernética). Embora produzidas no ámbito virtual por excelência – o ciberespaço –, elas são resultado do intenso movimento de interesse dos Estados em produzir alterações no mundo físico[3]. O Esquema 1 apresenta esses níveis.

Esquema 1: Níveis decisórios argentinos em matéria de Segurança da Informação

Fonte: elaboração própria.

Esta situação resulta de um novo ambiente estratégico, no qual questões não só técnicas, mas também políticas surgem, tais quais: como será o processo de tomada de decisão? Como reagirão e atuarão os Estados para lidar com esses novos e emergentes desafios que são apresentados aos vários organismos estatais responsáveis pela Segurança e Defesa Nacionais?

Na República Argentina, a preocupação com a segurança dos sistemas de informação e comunicação vem gerando políticas,

3 Sergio G. Eissa, Sol Gastaldi, Iván Poczynok e Elina Z. Di Tullio. "El ciberespacio y sus implicancias para la defensa nacional", *Revista de Ciencias Sociales - Segunda Época*, No. 25 (out. 2014), 181-197, http://www.unq.edu.ar/advf/documentos/53e389d522b6b.pdf, acessado em 4 jan. 2015.

programas e distintos tipos de regras, há anos. O país, embora não não se encontre entre os principais alvos de vultosas operações cibernéticas, tem sido vítima, em varias ocasiões, de diferentes tipos de ataques cibernéticos contra *sites* de vários órgãos do governo[4]. A maioria destes eventos não ganhou notoriedade pública, pois isso tornaria evidente a existência de grandes vulnerabilidades nos sistemas e redes computacionais do governo. No entanto, urge-se a melhora nas medidas de Segurança da Informação, a fim de evitar quaisquer consequência indesejada que essas operações cibernéticas possam originar, tais como o dano à imagem da organização governamental afetada; o acesso não autorizado ou a alteração de dados pessoais contidos em bancos de dados; o possível envolvimento de recursos de usuário e as violações do direito à proteção dos dados pessoais dos cidadãos[5]. A este respeito, cabe destacar que a informação utilizada por qualquer tipo de organização pública ou privada exige *medidas de segurança* (defesa) para garantir a sua proteção, preservando assim, sua confidencialidade, integridade, autenticidade e disponibilidade.

Soma-se a isso a importância de proteger as chamadas estruturas estratégicas de informação, entendidas como aquelas instalações, redes, serviços e equipamentos físicos e de tecnologias da informação – *hardware* e *software* – cujo funcionamento é estrategicamente essencial para a prestação de serviços aos cidadãos e às instituições. Se tais estruturas forem vítimas de algum tipo de incidente, a prestação de serviços básicos, comunicacionais e de transportes poderiam, por exemplo, ser afetada, podendo chegar, nos casos mais graves, em ameaça à vida.

4 Cristian Borghello e Marcelo Temperini, "Seguridad o inseguridad informática. Ciberseguridad Nacional Argentina: Cracking de Servidores de la Administración Pública", in *13° Simposio Argentino de Informática y Derecho de las 42° Jornadas Argentinas de Informática*, Ciudad de Córdoba (16-20 set. 2013).

5 Ibid.

Para combater esses riscos, a *Oficina Nacional de Tecnologías de Información* (ONTI)[6] formulou em 2011 o *Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad* (ICIC), que poderíamos considerar como a semente da futura estratégia nacional de Segurança Cibernética do nosso país. Já o Sistema de Defesa Nacional argentino, por sua vez, contribui com tal Programa mediante o seu âmbito específico de competência. No entanto, encontra-se em desenvolvimento uma política de Defesa Cibernética que visa assegurar a defesa contra aqueles que pretendem impedir as operações militares das Forças Armadas argentinas, no cumprimento de sua missão principal, que é a de afastar e repelir qualquer agressão estatal militar externa contra os interesses vitais da Nação.

Defesa Cibernética, Segurança Cibernética e Guerra Cibernética como conceitos a definir e sua abordagem no quadro jurídico argentino

Uma peculiaridade da abordagem teórica desses novos fenômenos associados ao ambito do ciberespaço é a falta de consenso perante a literatura especializada. Assim, é necessário e essencial refletir, analisar e compreender os diferentes conceitos e expressões que traz este novo domínio – como Segurança Cibernética, Guerra Cibernética, Defesa Cibernética e Conflito Cibernético – e os vários debates sobre seu significado, considerando que não são categorias desprovidas de significado, enquanto intercedem diferentes interesses em sua definição e emprego.

Eissa e seus colaboradores[7] destacam, por exemplo, a tendência de "militarizar" o ciberespaço a partir de algumas perspectivas, tais

6 Por meio do Decreto nº 1.028/2003, outorgou-se à ONTI a responsabilidade de entender, asistir e supervisar os aspectos relativos à segurança e à privacidade da informação digital e electrônica do poder public argentino.

7 Eissa *et al.*, "El ciberespacio y la defensa nacional", 181-197.

como aqueles em vigor na Organização do Tratado do Atlântico Norte (OTAN) e nos Estados Unidos da América (EUA). Estas tendências são geralmente fundadas na ideia do ciberespaço como uma quinta dimensão operacional[8], a qual exige regras, meios e capacidades militares específicas. Neste sentido, a ausência de uma aprovação geral em torno das definições dos termos acima pode gerar confusão e falsas declarações em áreas como a Segurança Interna e a Defesa Nacional, podendo entrar em colisão com o quadro jurídico existente na Argentina no que tange a questões que tocam a essas duas áreas.

Em comparação com outros países da região, e referindo-se às áreas de Segurança e Defesa, a Argentina estabeleceu no seu quadro jurídico uma estrita separação entre ambas. Tal definição encontra-se disponível por meio da promulgação da Lei nº 23.554, que estabelece a base jurídica, organizacional e funcional para a preparação, execução e acompanhamento da Defesa Nacional.

Consoante se afirma no Livro Branco argentino, o próprio conceito de Segurança e defesa são modificados, ao longo das últimas décadas, haja vista que:

> a Lei de Defesa Nacional, de 1988, mudou essencialmente o conceito de Defesa prevalente no regulamento anterior emitido em outubro de 1966, que, inspirado na chamada Doutrina de Segurança Nacional, estabeleceu um escopo virtualmente abrangente de Segurança e baseou-se na noção de conflito total e permanente, próprio da Guerra Fria, prevendo a possibilidade de um inimigo ideológico interno.[9]

8 Javier López de Turiso y Sánchez, "La evaluación del conflicto hacía un nuevo escenario bélico", in *El ciberespacio: nuevo escenario de confrontación*, CESEDEN (Madrid: Ministerio de Defensa, 2012), 117-166.

9 República Argentina, *Libro Blanco de la Defensa* (Buenos Aires: Ministerio de Defensa de la

Em contrapartida, a Lei de Defesa Nacional (Lei nº 23.554) estabeleceu que a Defesa Nacional é "a integração e a ação coordenadas de todas as forças da ação para resolver esses conflitos que exigem o uso das Forças Armadas, de maneira disuasiva ou efetiva, para enfrentar as agressões de origem externas"[10]. Essa Lei também tem o objetivo de garantir os seguintes atributos e princípios da Nação Argentina: soberania permanente, independência nacional, integridade territorial, capacidade de autodeterminação e, por fim, da e a liberdade de seus habitantes. Ademais, esse dispositivo legal ainda estabelece que "a Defesa Nacional se concretiza em um conjunto de planos e ações de prevenção ou de superação dos conflitos geradores de tais ataques, tanto na paz quanto na guerra[…]"[11]. Além disso, seu art. 4º estabelece que, "para elucidar as questões relacionadas à defesa nacional, deve-se ter permanentemente em conta a diferença fundamental que separa Defesa Nacional e Segurança Interna"[12]. Esse artifício usado para a definição e a desambiguação dos termos "Segurança" e "Defesa", buscando sempre lancer luz da temática à sociedade, parece refletir também com a diferenciação entre "Segurança Cibernética" de "Defesa Cibernética". Ademais, mostra-se ser um movimento didático compartilhado pelas Forças Armadas do mundo todo, conforme se vê, a título de exemplo, na própria Estratégia Nacional de Defesa (END) brasileira[13].

Desde então, a separação entre Segurança Interna e Defesa Nacional tornou-se um dos princípios básicos sobre os quais se estrutura,

---

República Argentina, 2010), 72, tradução nossa. Note-se que o regulamento legal a que o Livro Branco se refere é a Lei Nº 16.970, de 1966.

10 Idem, *Lei n° 23.554* de Defensa Nacional (Buenos Aires: Honorable Congreso de la Nación Argentina, 1988), art. 2°, tradução nossa.

11 Ibid., art. 3°, tradução nossa.

12 Ibid., art. 4°, tradução nossa.

13 Brasil, *Política Nacional de Defesa (PND) e Estratégia Nacional de Defesa (END)* (Brasília: Ministério da Defesa, 2012), http://www.defesa.gov.br/arquivos/estado_e_defesa/END-PND_Optimized.pdf, acessado em 12 dez. 2014.

organiza e desenha a Política Nacional de Defesa argentina[14]. Em 1991, com a promulgação da Lei de Segurança Interna, estabeleceram-se os limites da ação do Ministerio da Defesa argentine e de seu instrumento militar, restringindo-lhe as ações de Segurança Interna, a menos que solicitadas pelo Comitê de Crise[15]. Assim, ela também acata a possibilidade de utilização "alternative" de elementos de combate das Forças Armadas, no restabelecimento da Segurança Interna da Argentina[16], nos casos excepcionais em que o sistema de Segurança Interna seja insuficiente, para cumprir os objetivos estabelecidos na Lei de Segurança Interna e, somente após isso é que poderá ocorrer a declaração do Estado de Sítio. Finalmente, o art. 32 determina que, por se tratar de uma forma excepcional de emprego militar desenvolvida apenas em situações de extrema gravidade, o Estado de Sítio não prejudica de forma alguma a doutrina, a organização, o equipamento e o treinamento das Forças Armadas, as quais terão as características derivadas da aplicação da Lei de Defesa Nacional.

Posteriormente, em 2006, a Lei de Defesa é regulamentada pelo Decreto nº 727, que permitiu normativamente definir o âmbito da definição de "Defesa Nacional" da lei homóloga, considerando o uso militar em resposta a agressões externas originadas e perpetradas por Forças Armadas pertencentes a outros Estados, conforme definido na Diretriz sobre Organização e Funcionamento das Forças Armadas (Decreto nº 1.691/06), sancionada alguns meses depois. Assim, a regulamentação da Lei afirma a separação entre a

14 Sergio Eissa, "Redefiniendo la defensa: posicionamiento estratégico defensivo regional", *Revista SAAP*, Vol. 7, Nº 1 (maio 2013), 41-64.

15 República Argentina, *Lei Nº 24.059 de Seguridad Interior* (Buenos Aires: Honorable Congreso de la Nación Argentina, 1991), art. 27.

16 De acordo com a Lei Nº 24.059, Segurança Interior é definida como "a situação está baseada no direito em se encontram resguardadas a liberdade, a vida e o patrimônio dos habitantes, seus direitos e garanteas, bem como a plena vigência das instituições do sistema representativo, republicano e federal que estabelece a Constituição Nacional" (Argentina, *Lei nº 24.059,* Art. 2º, tradução nossa).

Segurança Interna e a Defesa Nacional, defendida em 1988 e que foi redesenhada entre as décadas de 1990 e 2000 a partir de vários setores, visando levar as Forças Armadas à luta contra "novas ameaças" e em combate contra a insegurança[17]. Com efeito, o Decreto nº 727/2006 prevê que:

> O sistema de Defesa deve orientar-se estrutural e organizacionalmente para evitar agressão externa perpetrada pelas Forças Armadas de outro Estado, em plena conformidade com as disposições da Resolução 3314 (1974) da Organização das Nações Unidas (ONU), deixando fora da órbita do mesmo, ou seja, em seus aspectos doutrinários, de planejamento e de treinamento, bem como a produção de Inteligência, toda questão que se refira à Segurança Interna.[18]

Em suma, o Sistema de Segurança Interna e o Sistema Nacional de Defesa da República Argentina possuem princípios de distinta natureza e se excluem mutuamente em sua aplicação. Por exemplo, o Sistema de Segurança Interna é direcionado principalmente para a prevenção, repressão e punição de conteúdos ilegais contrários ao Código Penal e leis especiais. Por seu turno, o Sistema Nacional de Defesa argentino se direciona a evitar e repelir agressões militares estatais externas, incompatíveis com as disposições e Resoluções da ONU, preservando os interesses vitais da nação[19].

17 Marcelo Sain, "Las 'nuevas amenazas' y las Fuerzas Armadas en la Argentina de los 90", in *XXIII International Congress Latin American Studies Association (LASA),* Washington, DC (6-8 set. 2001).

18 República Argentina, "Decreto nº 727/06 (2006), http://www.resdal.org/Archivo/decreto-reglamentario-arg.htm, 3 jan. 2015.

19 Nicolás Dapena, "La diferencia entre seguridad interior y defensa nacional: conceptos, competencias, facultades, límites, prohibiciones e interacciones en el sistema legal argentino", *Revista de la Defensa*

Esses critérios políticos e jurídicos, específicos do quadro legal argentine, também devem ser preservados no ciberespaço. A dificuldade em compreender este âmbito gerará novos desafios, dado a virtualidade das relações que transitam por ele e pelo fato de ele ser considerado um "âmbito global" em que é quase impossível identificar o autor de uma operação cibernética.

Nesse sentido, partindo da Lei de Defesa Nacional, Héctor Flores considera que a Guerra Cibernética é:

> Toda agressão externa das Forças Armadas de um Estado, que utilizando o ciberespaço, ataca os sistemas de decisão e de gestão, infraestrutura e/ou sistema de Defesa, afetando a capacidade de garantir permanentemente as soberania, independência, integridade territorial e capacidade de autodeterminação e de proteção à vida e à liberdade dos seus cidadãos.[20]

Portanto, de acordo com este ponto de vista, deve-se levar em conta o ator que comete a ação ofensiva e o que realmente ela afeta para, então, determinar quais as agências estatais (civis ou militares) devem agir no contra-ataque.

Nesse sentido, diante da possibilidade de sofrer danos por causa das ameaças que advêm do ciberespaço, os Estados começaram a desenvolver capacidades em Defesa Cibernética, as quais são constituídas por ações ofensivas ou defensivas que consideraram importantes para a proteção das estruturas estratégicas de informação.

Nacional, Nº 1 (2007), 28- 49.

20 Héctor Flores, "Los ámbitos no terrestres en la guerra futura: ciberespacio", in *Los ámbitos no terrestres de la guerra futura: ciberespacio*-aeroespacio, org. _____ (Buenos Aires: Gabinete de Estrategia Militar del Estado Mayor Conjunto de las Fuerzas Armadas, 2011), 26, tradução nossa.

Nas palavras de Miguel Ángel Barrios, trata-se de "uma iniciativa desenhada para ampliar os sistemas de defesa dos Estados e protegê-los de novos riscos emergentes na Sociedade da Informação"[21]. Dada esta conceituação de Defesa Cibernética, é importante esclarecer a diferença que existe entre tal conceito e Segurança Cibernética, a qual, por seu turno, é entendida como "a disciplina que se relaciona com várias técnicas, aplicações e dispositivos responsáveis por garantir a integridade e a privacidade de informações em um sistema de computador, bem como de seus usuarios"[22].

Paralelamente, não se deve deixar de mencionar que, por meio do ciberespaço, desenvolvem-se também outras dinâmicas de natureza criminal que afetam a liberdade, a vida e os bens dos cidadãos, assim como seus direitos e garantias. Estamos tratando daquelas atividades maliciosas contidas na categorização dos Crimes Cibernéticos ou Computacionais, que correspondem a várias espécies de delitos (roubo de dados pessoais, assédio virtual, crime financeiro e fraude, dentre outros) e que são da alçada das Forças de Segurança Pública (polícias repressivas e investigativas federais e estaduais, bem como a atuação destas no âmbito internacional, mediante articulação e coordenação da Interpol).

Assim, cabe destacar a contribuição de Bonnie Adkins, que desenvolve uma escala de conflitos cibernéticos, onde vários fenômenos podem ser identificados pelas seguintes variáveis: tipo de ataque, atores intencionais ou não intencionais, local do ataque e agência estatal responsável por identificar e tomar medidas contra o autor das ameaças e/ou dos ataques. A partir dessas distinções, a autora diferencia entre

21 Miguel Ángel Barrios, *Diccionario Latinoamericano de Seguridad y Geopolítica* (Buenos Aires: Editorial Biblos, 2009), 104, tradução nossa.

22 Silvina Chaves, "Guerra cibernética: el nuevo paradigma de Seguridad Informática (2012), http://argentinainvestiga.edu.ar/noticia.php?titulo=guerra_cibernetica:_el_nuevo_paradigma_en_seguridad_informatica&id=1645, acessado em 9 set. 2014.

cinco conflitos que podem ocorrer dentro do espaço virtual, os quais são os que se seguem: Crime Cibernético, Hacktivismo, Terrorismo Cibernético, Espionagem Cibernética e Guerra Cibernética[23].

A última categoria proposta por Adkins define Guerra Cibernética como a utilização de técnicas virtuais para intrusão na infraestrutura de informação de outro Estado para provocar intencionalmente qualquer tipo de dano, no que se refere à Segurança Nacional. Ela também acrescenta que o instrumento militar só deveria agir se houver um ataque grave que provenha de atores que estão fora do país onde o ato ocorreu.

Vinculando o conceito de ciberespaço com o uso do poder militar, Richard Clarke e Robert Knake definem Guerra Cibernética como o conjunto de ações por parte de um Estado-nação para penetrar em computadores ou redes de outra nação com a intenção de causar danos ou interrupções no sistema. Além disso, eles argumentam que aqueles Estados que desenvolvem cada vez mais as suas capacidades cibernéticas e não se preocupam com a tecnologia de estrutura estratégica tornam-se mais vulneráveis a possíveis ataques cibernéticos e intrusões na rede, particularmente no contexto de uma Guerra Cibernética[24].

Hector Flores, por sua vez, estabelece de maneira semelhante uma diferenciação de conflitos, como faz também Adkins. Com a exceção do Hacktivismo e da Espionagem Cibernética, coloca-se os outros três casos na mesma categoria, identificando, assim, dois atores: criminosos e Forças Armadas[25]. A partir da ideia anterior, podemos descrever, de um lado, como fenômenos do Crime Cibernético, o Hacktivismo e o Terrorismo Cibernético, enquanto que, do outro lado, a Espionagem

23 Bonnie Adkins, *The spectrum of Cyberconflict: from hacking to information warfare. What is law enforcement´s role* (2001), http://www.dtic.mil/dtic/tr/fulltext/u2/a406949.pdf, acessado em 4 set. 2014.

24 Richard A. Clarke e Robert K. Knake, *Cyber war: the next threat to national security and what to do about it* (Nova Iorque: Harper Collins, 2010).

25 Adkins, op. cit.

Cibernética e a Guerra Cibernética são dois fenômenos característicos das Forças Armadas[26].

Para concluir, e continuando com a distinção entre as esferas de Segurança e Defesa que transmite o Sistema de Defesa Nacional argentino, é essencial que comecemos a refletir sobre a necessidade de se chegar a um mínimo aceitável de consenso político e acadêmico sobre os conceitos que envolvem a Defesa Cibernética. Isso será importante para a implementação de marcos legais e de medidas que possibilitem proteger as estruturas estratégicas do país, mediante suas agências estatais criadas para tal fim.

A globalização que tanto caracteriza o ciberespaço não deve ofuscar o fato de que as operações nesse ambiente têm consequências também no plano físico e, portanto, não é totalmente estranho aos limites territoriais que ajudam dar, literalmente, forma aos Estados-nação. Além disso, essas operações cibernéticas podem ser geradas por agentes estatais, não estatais ou por indivíduos com fins políticos, criminais ou de outra natureza. Definir o ator e o objeto da dita operação e sua natureza constitui um dilema para a elaboração de políticas nacionais de Segurança e de Defesa Cibernéticas.

A Política de Segurança Cibernética argentina

A fim de detalhar os antecedentes da atual Política de Segurança Cibernética da República Argentina, podemos citar que, em setembro de 2003, a ONTI iniciou um trabalho de diagnóstico com especialistas em Segurança da Informação de várias agências governamentais destinado a desenvolver uma Estratégia e os procedimentos de segurança a serem adotados por cada órgão da Administração Pública Nacional da Argentina.

26 Flores, "Guerra futura: ciberespacio".

Por meio da Decisão Administrativa nº 669/2004 da Chefia de Gabinete de Ministros, estabeleceu-se a adoção do "Modelo de Política de Segurança", por parte dos organismos do Setor Público Nacional, e a criação de um Comitê de Segurança da Informação. Um ano depois, é aprovado o "Modelo de Política da Segurança da Informação", graças à Disposição nº 6/2005 da ONTI.

Dado o aumento em quantidade, variedade e sofisticação das ameaças e vulnerabilidades que podem afetar os ativos de informação – como os *softwares* maliciosos (*malwares*) e os ataques de negação de service (DoS) –, o "Modelo de Política de Segurança" é ajustado pela Disposição ONTI nº 3/2013, a fim de manter sua validade e seu nível de eficiência.

Enquanto isso, em julho de 2011, a Argentina lança seu Programa Nacional de Infraestruturas Críticas de Informação e Segurança Cibernética (ICIC)[27], com o objetivo principal de desenvolver políticas e regulamentos relacionados à proteção das estruturas estratégicas de informação da Argentina. Assim como ocorre com algumas políticas nacionais de Segurança Cibernética, mundo à fora, a exemplo da canadense, o ICIC também aceita adesão de participação organismos civis e privados.

De acordo com o Diretor desse Programa, Pedro Janices, o ICIC surgiu

> […]da necessidade que todo governo argentine tem de responder a situações críticas que afetam o desenvolvimento normal dos sistemas essenciais para as ações diárias dos cidadãos. Dentre eles estão as redes de comunicação informatizadas e seus dados, que desempenham um papel essencial atualmente. Referindo-se especificamente ao digital, o ICIC

27 República argentin, *Resolución Nº 580/2011* (Buenos Aires: Jefatura de Gabinete de Ministros, 2011).

cumpre a tarefa de prevenir todos os atos que tentam violar os sistemas do Estado ou a seus cidadãos.[28]

Para realizar esse processo, o ICIC formou quatro grupos de trabalho, a saber:

- Equipe de Resposta a Emergências Teleinformáticas (CERT): fornece assistência e assessoria na análise dos incidentes, bem como formula recomendações para sanar tais males;
- Grupo de Ação Preventiva (GAP): analisa possíveis falhas de segurança e age preventivamente para possibilitar a redução de incidentes de segurança computacional, além de desenvolver as "Políticas de Segurança" e de dar assessoria para sua implementação;
- INTERNET SÃ: programa educacional concebido para proporcionar a conscientização e treinamento em Segurança Cibernética, especialmente entre crianças e jovens; e
- Grupo de Infraestruturas Críticas da Informação (GICI): levanta, identifica e classifica informações estratégicas e críticas, monitora serviços que o Setor Público Nacional fornece através da Internet e coordena exercícios de resposta a tentativas de violação dessas estruturas estratégicas.

Por fim, resta mencionar que, a partir dos esforços realizados no momento e da ampla participação dos diferentes setores da esfera

28 Christopher Holloway, "El Plan Argentino para su ciberseguridad", *América Economía* (2001), http://tecno.americaeconomia.com/noticias/el-plan-argentino-para-su-ciberseguridad, acessado em 4 set. 2014.

pública, a Argentina está avançando no desenvolvimento de uma Estratégia Nacional de Segurança Cibernética.

A Política de Defesa Cibernética argentina

A atual Política de Defesa Cibernética da Republica Argentina parte do reconhecimento do ciberespaço como uma área estratégica em duas dimensões: por um lado, relacionada com o desenvolvimento tecnológico; por outro, por sua importância para a Defesa Nacional.

No primeiro caso, e dado que a política de defesa é concebida como contribuinte para a estratégia nacional de desenvolvimento, o Livro Branco da Defesa argentino, assim como o do Brasil, identificou como suas áreas estratégicas, as tecnologias nuclear, aeroespacial e cibernética. Particularmente, as duas últimas são consideradas "contribuições críticas para viabilizar os efeitos pretendidos no marco de uma estratégia para fins defensivos"[29], uma vez que contribuem decisivamente para as capacidades de alerta estratégico precoce e à condução das operações militares contra uma eventual agressão militar externa ao Estado. Portanto, a estratégia de defesa argentina considera as tecnologias associadas com o ciberespaço[30] como sendo pertencentes a um "Programa Transversal Sistêmico" a ser priorizado pelo sistema de pesquisa e desenvolvimento (P&D) para a área de Defesa.

No segundo caso, o Livro Branco mensura a importância do ciberespaço para a Defesa Nacional, ao afirmar que:

> O seu domínio não só é essencial para o exercício de comando e controle e para o funcionamento em rede do sistema, como também para repelir e afastar as

29 Argentina, *Libro Blanco*, 48, tradução nossa.

30 Isto é, aquelas destinadas a assegurar as confidencialidade, integridade, autenticidade e disponibilidade da informação imprescindível para o exercício das operações militares.

> ameaças militares estatais externas que possam ser criadas utilizando o chamado ciberespaço como um meio de execução ou tendo-o como objetivo.[31]

Considerando o ciberespaço como uma "nova dimensão operacional"[32], o Livro Branco da Defesa conclui sobre a necessidade de se desenvolver um "núcleo orgânico-funcional, com uma doutrina específica"[33] a fim de garantir "o uso e o controle do ciberespaço que seja próprio dos componentes do Sistema de Defesa Nacional e das áreas de interesse estratégico, frente às agressões externas contra o ciberespaço nacional (Guerra Cibernética)"[34].

A partir desse ponto de vista e, ainda, considerando o advento da crescente importância e complexidade da questão que se aporta nas novas TICs, o Ministério da Defesa argentino decidiu elaborar uma política nacional de Defesa Cibernética que refletisse o conjunto de Resoluções assinadas nos últimos tempos.

A primeira delas foi a Resolução do Ministério da Defesa nº 364, de 2006, que estabelece a criação do Comitê de Segurança da Informação na área do Ministério da Defesa, composto pelos presidentes das várias agências pertencentes à jurisdição argentina. Sua origem se dá pela Decisão Administrativa nº 669/2004, anteriormente mencionada.

Em segundo lugar, a resolução da Secretaria de Estratégia e Assuntos Militares nº 8, de 2010, que cria um grupo de trabalho para analisar e avaliar a relevância e as implicações do ciberespaço na agenda do Sistema de Defesa Nacional.

Por outro lado, a Resolução nº 385/2013 estabelece, no âmbito do Gabinete de Assessores do Ministério da Defesa, a Unidade de

31 Argentina, op. cit., 48, tradução nossa.

32 Ibid., 277, tradução nossa.

33 Ibid., 48, tradução nossa.

34 Ibid., 277, tradução nossa.

Coordenação de Defesa Cibernética e define as funções e integração desse órgão, reunindo, em uma única agência, a coordenação da política de Defesa Cibernética com o intuit de gerar mecanismos de resposta integrados para a tomada de decisões. As responsabilidades dessa Unidade são as seguintes: coordenar as políticas e o desempenho dos atores ligados à Defesa Cibernética, o que inclui empresas e organismos descentralizados; fazer e manter atualizado um levantamento exaustivo das infraestruturas, redes, recursos humanos, processos e atividades em Defesa Cibernética na Argentina; compreender a concepção, o planejamento estratégico e a implementação de políticas da jurisdição e impulsionar o desenvolvimento doutrinário na matéria; analisar permanentemente a evolução jurídica na área e sua relação com o quadro jurídico de Defesa; intervir na implementação da Resolução JGM nº 580/2011; desenvolver intercâmbio e cooperação com as áreas acadêmica e científica; fomentar políticas de editais e de formação de recursos humanos; e promover a adoção de procedimentos e protocolos comuns.

Posteriormente, a partir da aprovação da Resolução MD nº 343/2014, inicia-se a inclusão do Instrumento Militar do Sistema de Defesa Nacional na montagem da estratégia defensive ciberespacial, criando o Comando Conjunto de Defesa Cibernética, ligado ao Estado-Maior Conjunto das Forças Armadas da Argentina. Essa Resolução estabelece como missão a condução permanente das operações de Defesa Cibernética com a finalidade de garantir as operações militares do Instrumento Militar da Defesa Nacional.

Finalmente, não se pode esquecer que estas medidas também são acompanhados pelo compromisso da República Argentina de articular a política de Defesa Cibernética com os outros países da União de Nações Sul-Americanas (UNASUL). Tais ações convergem positivamente a favor do objetivo da Política de Defesa argentina, no sentido de avançar progressivamente na direção de um sistema de Defesa sub-regional. Em

2013, foi assinada a Declaração de Buenos Aires, entre o Ministro da Defesa argentino e seu homólogo brasileiro, que decidiram impulsionar a cooperação em Defesa Cibernética, criando um grupo de trabalho bilateral (que se reuniram dois meses mais tarde em Brasília) e definindo uma agenda de trabalho orientada para as áreas de treinamento, métodos e sistemas tecnológicos, desenvolvimento do ensino combinado, pesquisa científica e intercâmbio entre os respectivos CERTs.

Defesa Cibernética e Planejamento Estratégico

O Planejamento Estratégico é um instrumento de gestao pública essencial para o alcance das metas institucionais. Como uma ferramenta da Política de Defesa Nacional, ele indicará o modo de utilização dos recursos disponíveis na jurisdição para garantir a defesa da Nação e o uso efetivo do emprego das Forças Armadas em todas as missões estabelecidas pelo Nível Estratégico Nacional.

A República Argentina adotou o planejamento baseado em capacidades como metodologia de planejamento para a Defesa. Isso significa que ela renunciou a estruturar o seu instrumento militar com base nas hipóteses de conflito. Ao contrário do que aconteceu no passado, a projeção de forças não é realizada em função de um potencial agressor, mas a partir da consideração dasa capacidades militares necessárias para responder a um agressor genérico que, sob o atual cenário de incerteza estratégica, proporciona flexibilidade para antecipar ameaças que não são definidas *a priori*. Assim, esse modelo de planejamento é baseado em uma relação defeito-efeito, ou seja, concentra-se na minimização das próprias vulnerabilidades (defeito) mediante a identificação e o desenvolvimento das capacidades militares (efeito) para poder, enfim, enfrentar com sucesso as agressões militares genéricas.

Na Argentina, o Ciclo de Planejamento da Defesa Nacional (CPDN), criado pelo Decreto nº 1.729 de 2007, tem início com a emissão

de uma Diretriz de Política de Defesa Nacional (DPDN), feita pela mais alta autoridade política. Por intermédio da DPDN, o Poder Executivo define os parâmetros e as diretrizes segundo o desenho de suas Forças Armadas, bem como a orientação de suas capacidades, levando em consideração a avaliação estratégica da situação internacional, regional e local. Com base nesse documento, realiza-se o planejamento estratégico militar, elaborado pelo Estado-Maior Conjunto das Forças Armadas, sob permanente supervisão ministerial, com cada uma das Forças contribuindo com o planejamento operacional. O CPDN se conclui com a preparação, também do Nível Estratégico Nacional, do Plano de Capacidades Militares (PLANCAMIL) que determinará o modelo de evolução do Instrumento Militar possível e necessário para o médio prazo. Neste contexto, o primeiro CPDN (2009-2011) identificou, entre as diferentes capacidades a incorporar, melhorar ou recuperar, a criação de uma Agência de Defesa Cibernética no Nível Estratégico Militar – que veio a se tornar o atual Comando Conjunto de Defesa Cibernética argentino.

A adoção e a implementação desse método de planejamento é consistente com as definições políticas adotadas em matéria de política externa e de postura estratégica defensiva. Como se sabe, a República Argentina

> Apoia um modelo de defesa de caráter defensivo, de repúdio e oposição a políticas, atitudes e capacidades ofensivas de projeção de poder frente a terceiros Estados, no qual o conceito e a disposição estratégica, a política de defesa e militar, o desenho das Forças e o emprego e a evolução do instrumento militar se encontram estruturados segundo o princípio de legítima defesa[…].

> Nesse sentido, em um mundo crescentemente interligado e interdependente, a Argentina concebe sua defesa em dupla dimensão "autônoma" e "cooperativa", ou seja, a Política de Defesa Nacional, seu desenho de Forças e suas capacidades não ofensivas frente a terceiros Estados vinculam o conceito e o posicionamento estratégico argentino com a dimensão e os compromissos multilaterais nos níveis subregional, regional e global.[35]

De acordo com o modelo argentino de Planejamento da Defesa, "uma capacidade resulta de um conjunto de fatores [...]empregados com base em princípios e processos doutrinários e orientados a conseguir um determinado efeito militar"[36].

Portanto, é com esse posicionamento estratégico estritamente defensivo e com o modelo de planejamenteo baseado em capacidades que a Política de Defesa Cibernética argentina será orientada. Assim, o desenvolvimento das capacidades em matéria de Defesa Cibernética deverá dotar tanto o Comando Conjunto de Defesa Cibernática quanto seus demais organismos correlatos de capacidades necessárias para garantir o desenvolvimento das operações militares contra qualquer ataque cibernético, assim como parar e repelir qualquer operação cibernética contra os objetos de valor estratégico da Argentina. Em seus posicionamento e atitude estratégicos, a Estratégia de Defesa Cibernética terá características defensivas, dirigidas principalmente às prevenção, detecção, reação e persistência frente a ataques cibernéticos e intrusões contra as redes e os sistemas de informação da jurisdição, assim como da análise forense. As capacidades necessárias para

35 República Argentina. *Decreto nº 1.714/09*, versando sobre a Diretriz de Política de Defesa Nacional (Buenos Aires: Ministerio de Defensa, 2009), tradução nossa.

36 Idem, *Libro Blanco de la Defensa*, 241, tradução nossa.

tanto estão definidas nos anteriormente mencionados fatores de planejamento.

Por último, embora a postura estratégica argentina seja defensiva, não se deve abandonar a capacidade ofensiva no Nível Tático, caso o país seja agredido militarmente por outro Estado. Nesse cenário de enfrentamento bélico, as capacidades de defesa indireta do ciberespaço aparecem como de relevância crucial. Por exemplo, ter liberdade de ação na dimensão do ciberespaço, usar e negar o ciberespaço próprio ao inimigo e ter capacidade de resposta. Tal abordagem não implica em tratar o ciberespaço como uma quinta dimensão que exija a aplicação de um ambiente operacional específico: o atual desenvolvimento das TICs e sua previsível evolução para todas as operações militares (terrestres, marítimas e aeroespaciais) estão vinculadas com tecnologias cibernéticas com maior ou menor grau de dependência. Assegurar o desenvolvimento de tais operações de forma permanete e independente será a questão-chave da Política de Defesa Cibernética argentina.

Considerações finais

Como apresentado previamente, nos últimos anos, teêm-se feito inúmeros esforços na Argentina para começar a reforçar a Segurança da Informação e a Defesa Cibernética do país. No entanto, é necessário continuar esse processo e incluir o debate acadêmico em torno da Segurança e da Defesa Cibernéticas. Assim, afigura-se relevante para o futuro da Estratégia Nacional de Segurança Cibernética a capacidade de se vincular pluralmente as demandas dos setores governamentais e dos poderes legislativos e judiciais com as do setor privado e universitário, bem como das organizações não governamentais.

Pode-se detectar uma emergente estratégia nacional, tanto em termos de Segurança Cibernética quanto de Defesa Cibernética,

embora ainda exista um longo caminho a ser percorrido, especialmente nas concepção e obtenção das capacidades de Defesa Cibernética para equipar as Forças Armadas argentinas com condições necessárias para o desenvolvimento das operações militares ligadas a sua missão principal.

Neste sentido, preservar estruturas estratégicas de informação é um grande desafio à República Argentina, pois ela tem de garantir – na esfera de atuação de seu Sistema de Defesa Nacional – os sistemas de comando, controle, comunicações, computadores e guerra eletrônica (C3IGE) das Forças Armadas perante qualquer incidente cibernético que possa afetar o desenvolvimento das operações militares.

Ao mesmo tempo, ela deve articular o campo da Defesa Cibernética com a Política Nacional de Segurança Cibernética, levando em conta que os sistemas de computação e de comunicação militares devem ser considerados "estruturas estratégicas" com a particularidade de estarem sempre operacionais.

Mais desafiante ainda é a preservação das informações contidas ou transmitidas através desses sistemas, dispositivos e redes interconectados ciberneticamente com o fito de manterem sua confidencialidade, integridade, autenticidade e disponibilidade, assegurando eficazmente a Defesa da Argentina e de seus interesses vitais contra qualquer agressão militar externa. Isto implica desenvolver a coordenação de políticas (Nível Político) e mecanismos (Níveis Estrtaégico, Tático e Operacional) de Defesa Cibernética com os países do seu imediato entorno regional, a fim de preservar não só a própria Argentina, mas também a América do Sul como uma zona de paz, inclusive no ciberespaço.

A condição da China como potência cibernética

Ahmina Raiara Solsona Oliveira
Alexandre Cesar Cunha Leite

Introdução

Os países asiáticos apresentam-se como figura de destaque quando o assunto é conflitos cibernéticos, chegando a ser difícil citar algum caso de guerra cibernética que não envolva um país deste continente[1].

A China, especificamente, é um dos países mais acusados por atos criminosos neste espaço, embora, pelas próprias condições do ambiente cibernético, não seja fácil obter comprovações a respeito da participação de uma nação. Tal questão se deve, dentre outras possibilidades analíticas, à origem do ataque, ou seja, aparece como oriundo de uma nação, mas, na realidade, não necessariamente tem origem naquele Estado, e sim em um ator isolado.

Não se pode negar que o tema Segurança Cibernética tenha se tornado um tópico relevante e central a ser debatido entre várias nações, no âmbito de suas relações internacionais. Por exemplo, a China e os Estados Unidos da América (EUA) têm iniciado um diálogo entre si para reduzir tensões e estabelecer uma cooperação na questão da Segurança Cibernética. Contudo, o governo chinês ainda parece reticente quanto a isso. Muito dessa hesitação deve-se, do lado chinês,

1 Uma forma de acompanhar o ritmo dos ataques pode ser vislumbrada em: http://map.ipviking.com.

aos "*mistaken U.S. practices*", que terminaram por causar certa rejeição nas tratativas[2], embora, no final de 2014, ambos os lados tenham reunido-se e considerado a existência de avanços nas negociações[3].
Não obstante, ataques cibernéticos passam a compor a pauta da agenda de segurança nacional e internacional. Isso se deve, em muito, à rápida expansão e ao contínuo aprofundamento e tecnologicamente sofisticado presentes nos denominados sistemas-base utilizados tanto pelos aparatos governamentais quanto pela sociedade. Sistemas de armazenamento de informações, comunicações, operações econômicas, militares, entre outras, dependem hoje de uma macroestrutura e, principalmente, de infraestruturas baseadas no ciberespaço.

Ainda, não somente em relação à corriqueira participação em conflitos internacionais, como também ao fato de enxergar o espaço cibernético como extensão de seu pensamento estratégico tradicional, bem como de o utilizar como elemento decisivo para sua ascensão no Sistema Internacional, a China é também apontada, por EUA e outros países, como *potência cibernética*. Torna-se também visível, no discurso oficial chinês, o fato de que a questão cibernética é estrategicamente levada em conta para a transposição daquele país como potência regional e postulante à condição de potência global, como se pode perceber nos pronunciamentos do presidente chinês Xi Jinping[4].

É possível atribuir essa ascensão chinesa à posição de expoente mundial na área cibernética ao fato de o conceito de Inteligência

2 Benjamin Kang Lim, "China says it's hard to resume cyber security talks with U.S.", *Reuters*, 19 out. 2014, http://reuters.com/article/2014/10/19/us-china-usa-cybersecurity-idUSKCN0I80GU20141019, acessado em 30 jan. 2015.

3 Cory Bennett, "US, China see little progress on cybersecurity", *The Hill*, 12 nov. 2014, http://thehill.com/policy/cybersecurity/223865-us-china-see-little-progress-on-cybersecurity, acessado em 30 jan. 2015.

4 Ver Paul Carsten e Michael Martina, "Forças armadas da China incentivam cibersegurança e softwares chineses, diz mídia estatal", *Reuters*, 8 out. 2014, http://br.reuters.com/article/internetNews/idBRKCN0HX1MR20141008, acessado em 30 jan. 2015; Magnus Hjortdal, "China's Use of Cyber Warfare: espionage meets strategic deterrence", *Journal of Strategic Security* 4, No. 2 (2011), 1-24.

de Estado[5] estar bem enraizado na cultura chinesa e datar de antes mesmo dos Reinos Combatentes, como mencionado por Sun Tzu[6]. Uma forma de analisar a importância que a China confere às áreas de Segurança Cibernética e de Defesa Cibernética pode ser feita por meio da compreensão da perspectiva que o país possui sobre os conceitos de guerra e guerra cibernética.

Neste contexto, o presente trabalho tem como objetivo fomentar a discussão acerca da emersão da China ao *status* de potência cibernética. Para tanto, a organização do trabalho se dá por intermédio de duas seções: a primeira discute os conceitos de guerra e guerra cibernética vista pela perspectiva chinesa; e a segunda expõe ações tomadas pela República Popular da China, de modo a se preparar para a chamada Era Cibernética.

Diante do exposto, finalizamos com a percepção de que a China, embora invista sistematicamente em capacidades cibernéticas agressivas, visualiza a guerra cibernética como uma modalidade menos agressiva para a obtenção de ganhos e para a derrota do inimigo.

Guerra, guerra cibernética e a perspectiva chinesa

Nesta seção, com o objetivo de aprofundar a compreensão acerca da perspectiva chinesa sobre o que vem a ser a guerra cibernética, iremos usar como ponto de partida a definição de guerra, passando por sua humanização, para chegar ao conceito de guerra cibernética. Postos esses conceitos, tentaremos discuti-los segundo a ótica sínica, evidenciando, assim, os motivos que a levam a investir de forma estratégica e militar no ciberespaço.

5 Entendida como o conjunto de ações que, por meio da espionagem, traça planos para o acesso a dados negados que substanciam a tomada de decisão no mais alto nível político.

6 Sun Tzu, *A arte da guerra: os treze capítulos originais*, trad. Henrique Amat Rêgo Monteiro (São Paulo: Clio Editora, 2012).

Clausewitz[7] considera a guerra "um ato de violência para levar o inimigo a fazer a nossa vontade" e explica que ela não é nada além de um duelo em larga escala cujo objetivo principal é derrubar o adversário e torná-lo incapaz de qualquer resistência. O autor esclarece que "pessoas de bom coração podem acreditar que havia maneira engenhosa para desarmar ou derrotar um inimigo sem muito derramamento de sangue e podem imaginar que este é o verdadeiro objetivo da arte da guerra", mas essa é, na verdade, uma falácia que deve ser exposta, pois a guerra é algo tão perigoso, que os erros advindos da bondade são os piores. Nesse viés, o uso maximizado da força não seria incompatível com o concomitante uso do intelecto, posto que, se um dos lados utiliza força máxima sem remorso e o outro se abstém de utilizá-la, então o primeiro estará em vantagem.

Boniface[8] explica que Clausewitz vê a guerra como instrumento intencional para se atingir determinados fins, ou seja, ela seria um dos possíveis meios para obtenção da vitória. É dessa visão que surge a máxima clausewitziana de que "a guerra é meramente a continuação da política por outros meios"[9]. Por seu turno, Barbosa[10], ao oferecer visões opostas à de Clausewitz, apresenta a concepção cataclísmica de Santos[11], que acredita na guerra como uma catástrofe inevitável. Sua concepção visualiza a guerra como modo de se alcançar um nível superior na vivência humana, pois a entende como um momento de busca pela paz dos que almejam a vitória.

A evolução da tecnologia e a consequente modernização da

7 Carl Von Clausewitz, *On War* (Princeton, NJ: Princeton University Press, 1989), 79.

8 Pascal Boniface, *Dicionário das Relações Internacionais* (Lisboa: Plátano Edições Técnicas, 1997), 165-166.

9 Clausewitz, op. cit., 764.

10 Tânia Isabel Lopes Barbosa, "A ajuda internacional e as guerras civis: uma relação perversa?" (*Dissertação de Mestrado*, Universidade Técnica de Lisboa, 2005), 16, https://repository.utl.pt/bitstream/10400.5/646/2/Tese%20de%20Mestrado%20DCI.pdf, acessado em 5 out. 2014.

11 José Loureiro Santos "Reflexões sobre Estratégia", *Temas de Segurança e Defesa*, (Lisboa: Publicações Europa-América, 2000), 204-205.

guerra fizeram com que não só novas ferramentas de conflito fossem criadas, mas também que algumas existentes fossem aprimoradas, permitindo, ainda, que outras se mantivessem inutilizadas. Este último caso foi o que aconteceu, por exemplo, com o caça russo SU-27, que, antes de entrar em combate, foi substituído pelo modelo mais moderno, o SU-35 Super-Flanker[12]. Dentre as novas ferramentas de conflito, os autores citam a tecnologia cibernética como a mais importante revolução na história da tecnologia e como uma novidade benéfica para a civilização, posto que seu poder agregador permite não apenas o desenvolvimento de outras novas tecnologias, mas também um novo modelo de relacionamento entre o homem, a tecnologia e a guerra.

A utilização da tecnologia cibernética para a prática de conflitos deu início às chamadas armas cibernéticas, que Liang e Xiangsui[13] chamam de "armas suaves". Essa classificação não está relacionada ao grau letal que essas armas possuem, mas à capacidade de ataque ao centro nervoso do inimigo[14] ou que possa significar a destruição da humanidade como um todo, como é o caso das armas nucleares. Os autores explicam que os perigos da utilização maciça de armas nucleares fazem nascer uma nova abordagem científica que privilegia o aprimoramento do controle de poder estatal.

Embora a união dos termos "armas" e "suaves" pareça contrassenso, a possibilidade de se obter dados ou causar danos às estruturas estratégicas do inimigo, sem a existência do conflito armado ou do prejuízo físico, é fator importante que permitiu que

12 Qiao Liang e Wang Xiangsui, *Conjecturas sobre a Guerra e a tática na era da Globalização* (Pequim: Pla Literature and Arts Publishing House, 1999), 9.

13 Ambos são coronéis da nova geração de Oficiais do Exército de Libertação do Povo e autores da obra "A guerra além dos limites: conjecturas sobre a guerra e a tática na era da globalização", publicada na China em 1999, propondo atitudes e procedimentos que transcendem as táticas militares, para serem implementadas por países em desenvolvimento, como a China, em particular, visando compensar sua inferioridade militar em relação aos EUA, em um conflito envolvendo meios de alta tecnologia.

14 Sem a necessidade de um resultado catastrófico, que não apenas o destrua, como também o faça a suas futuras gerações.

as armas cibernéticas trouxessem a discussão sobre a possibilidade de humanização da guerra, a saber: a despeito da ocorrência de um conflito e de um eventual ataque, tem-se como premissa a manutenção da garantia do direito à vida. Esse é o resultado da introdução dos valores internacionais de direitos humanos que norteiam as novas concepções de guerras, envolvem forças políticas e sociais, fortalecem as preocupações com o meio ambiente e criando uma nova ética na condução da guerra[15].

Como complementa Perrin[16], há um debate atual em relação ao rótulo mais apropriado para se descrever a regularização internacional da guerra e a proteção de suas vítimas. Nesta busca, foram criados os termos "lei da guerra", "lei humanitária internacional", "lei humanitária de conflitos armados" e "lei de conflitos armados".

Há, contudo, uma divergência quanto ao foco desse conjunto de normas; se, por exemplo, esse deveria ser a proteção dos interesses individuais fundamentais ou a reconciliação da promoção eficaz da guerra com considerações elementares de humanidade. O fato é que tais discussões promoveram mudanças no modo de se fazer guerra, uma vez que tais aspectos passaram a ser também considerados. Embora alguns autores com um viés mais realista defendam que, nos períodos de guerra, esses acordos sejam desrespeitados, a possibilidade de ganhos sem a imposição da morte pode ser percebida na própria compreensão de guerra cibernética. É o que Krepnevich define como:

> ações por Estados e atores não estatais que empregam armas cibernéticas para penetrar computadores ou redes com finalidade de inserir, corromper e/ou

15 Liang e Xiangsui, op. cit.

16 Benjamin Perrin, *Modern Warfare: Armed Groups, Private Militaries, Humanitarian Organizations and the Law* (Washington, DC: University of Washington Press, 2012), 18.

> falsificar dados, interromper ou danificar computador ou dispositivo de rede; e/ou infligir danos e/ou interrupções dos sistemas de controle de computador[17].

Nesta definição é possível perceber que, por acontecer em um ambiente virtual e ter como objetivo a intrusão em sistemas ou redes de computador, a guerra cibernética é uma forma alternativa de guerra que concede a existência de conflitos sem mortes. É primordial destacar que, por se tratar de guerra, há a possibilidade de esta ser utilizada tanto em conjunto com o confronto real (como aconteceu nos conflitos entre Rússia e Estônia em 2007 e Rússia e Geórgia em 2008) quanto com o propósito de causar danos físicos e/ou levar à morte, como pode acontecer no caso de uma invasão às estruturas estratégicas.

Liang e Xiangsui embora tenham origem militar, apresentam a guerra cibernética como uma alternativa à belicosidade, isto é, uma forma mais inteligente de se obter ganhos por meios mais "humanos", ou seja: sem a imposição da morte ou o estado de guerra declarada. Compartilhando-se desse pensamento, o antigo Vice-Chefe do Estado-Maior russo, Alexander Burutin, fala como a guerra cibernética está mudando a paisagem do combate moderno e defende que:

> Em um futuro próximo, os objetivos finais em guerras e confrontos serão alcançados não pela destruição de forças e tropas de grupos inimigos, mas através da supressão de seu Estado e de seus sistemas de controle militar, navegação e sistemas de comunicação, e também por influenciar outros serviços cruciais de informação das quais dependem

17 Andrew F. Krepnevich, *Cyber warfare: a "nuclear option"?* (Washington, DC: Center for Strategic and Budgetary Assessment, 2012), 8.

> a estabilidade de controle da economia e das Forças Armadas do Estado.[18]

Embora Sun Tzu tenha vivido há mais de 2.000 anos, seus ensinamentos parecem atemporais e suas táticas para a vitória podem se encaixar perfeitamente nas guerras modernas. Apesar de ter pensado nos aspectos da guerra tradicional, Sun Tzu é leitura cada vez mais relevante nos estudos sobre modernização da guerra e dos aspectos necessários para a obtenção da vitória neste espaço, como comentado por McNeilly[19] e Wilcoxon[20].

Ainda que intitulada "A Arte da Guerra", em vez de se prender aos aspectos da guerra propriamente dita, a obra se dedica às práticas que buscam alcançar a vitória sobre o inimigo. Grande parte da obra explica como travar batalhas sem efetivamente confrontar o oponente no *front*, isto é: como superar o oponente de modo que o confronto físico não seja necessário. Esse aspecto é um dos pontos que migram da guerra tradicional para a virtual e fazem de sua obra uma leitura tão importante atualmente.

Sun Tzu também dá importância aos espiões e explica que eles são os elementos mais importantes de um exército, dado que é deles que depende a capacidade de mobilidade de soldados. Assim o estrategista chinês, Libick[21] lembra dos ataques cibernéticos como ocasiões em que, de um lado, *hackers* e *crackers* invadem sistemas mesmo estando fora da rede, enquanto que, do outro, agentes e/ou elementos já infiltrados na rede (como *softwares* espiões) ajudam a conseguir acesso de dentro dela, Outro aspecto interessante diz respeito à atuação e ao conhecimento

18 Krepnevich, op. cit., 3.

19 Mark McNelly, *Sun Tzu and the Art of Modern Warfare* (Oxord: Oxford University Press, 2001).

20 Gregory L. Wilcoxon, *Sun Tzu: theorist for the twenty-first century* (Washington, DC: U.S. Army War College, 2010).

21 Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Mônica, CA: Rand Corporation, 2009), 12-13.

sobre o inimigo, fatores que permitem que um adversário astuto possa enganar seu oponente, fazendo-o acreditar que seus interesses são uns, quando, de fato, são outros.

Tzu também explica que, para impossibilitar a derrota, é preciso investir em táticas defensivas, mas que, para garantir a obtenção da vitória, faz-se necessário investimento em capacidade agressiva, ponto que corrobora com as ações e com a atual capacidade cibernética chinesa. Deste modo, é possível perceber que a percepção chinesa do conflito cibernético é, assim como na época de Sun Tzu, um elemento para a conquista de objetivos estratégicos. Ela, porém, não é o único meio, mas atualmente tem sido bem utilizada com eficácia, principalmente diante da dificuldade de se descobrir a origem de um ataque cibernético e da possibilidade de implantar provas que atribuam a outrem os ataques cometidos[22].

Ações chinesas de investimento cibernético

Como exposto anteriormente, a República Popular da China vem sendo considerada uma das principais potências cibernéticas, fato este que se dá principalmente por sua corriqueira participação nessa modalidade de conflito, seja como alvo, seja como suposta agressora.

Ainda, deve-se ter em mente que o comportamento chinês, no que concerne à sua política externa, incluindo aí sua gestão de atividade cibernética, é conduzida prioritariamente pelos seus princípios domésticos de proteção e desenvolvimento de suas autonomia e soberania.

Amy Chang[23], em texto publicado pelo *Center of New American Security*, sustenta que a prioridade da gestão pública chinesa é composta

22 James A. Lewis, "The 'Korean' Cyber Attacks and Their Implications for Cyber Conflict" (2009), http://dspace.africaportal.org/jspui/bitstream/123456789/26510/1/The%20Korean%20Cyber%20Attacks%20and%20Their%20Implications%20for%20Cyber%20Conflict.pdf, acessado em 13 ago. 2013.

23 Amy Chang, "Warring State: China's Cybersecurity Strategy" (2014), http://cnas.org/sites/default/files/publications-pdf/CNAS_WarringState_Chang.pdf, acessado em 13 jan. 2015.

por objetivos internos que transbordam para o ambiente internacional. Logo, os objetivos de garantir a estabilidade interna[24], a integridade territorial, a modernização produtiva, o maior acesso a mercados externos e o crescimento econômico (também associado à melhoria e à manutenção do bem-estar social), bem como, simultaneamente, preparando-se para a possibilidade de ocorrência de um conflito cibernético militarizado no futuro. Segundo Chang[25], são todos esses objetivos que direta ou indiretamente sustentam a governabilidade do Partido Comunista Chinês[26].

Ainda segundo a contribuição de Chang, quanto à forma de tratamento dada por Beijing à questão da Segurança Cibernética, observam-se três pilares que norteiam o processo decisório do dragão asiático, a saber: o econômico, o político e o militar. Segundo Chang, para a manutenção do crescimento econômico (e a autora associa o crescimento ao desempenho industrial), deve-se levar em consideração o fator da espionagem cibernética[27]. Portanto, na proteção de informações confidenciais do Estado chinês, há que se levar em conta o ciberespaço. Dentre outras, estas são motivações que tornam o tema tão relevante para o mundo contemporâneo, e a China faz parte dele como protagonista nessa seara.

Outro fator importante diz respeito aos investimentos da China e ao modo como ela enxerga o espaço cibernético. Hjortdal[28] faz coro

24 Estabilidade interna compreende objetivo de sentido amplo, que passa pela segurança alimentar, pela elevação ao acesso a bens públicos e básicos e até mesmo pela segurança da sociedade ante ameaças externas.

25 Chang, op. cit., 07.

26 Além da referência ao texto da Amy Chang, publicado em 2014, para uma versão divulgada na imprensa sobre o mesmo tema, cf. Edward Wong, "For China, Cybersecurity Is Part of Strategy for Protecting the Communist Party", *The New York Times*, 3 dez. 2014, http://sinosphere.blogs.nytimes.com/2014/12/03/for-china-cybersecurity-is-part-of-strategy-for-protecting-the-communist-party, acessado em 4 jan. 2015.

27 Chang, op. cit., 08-17.

28 Hjortdal, op. cit., 3.

ao argumento de Chang, ao defender que o espaço cibernético é um elemento decisivo na estratégia chinesa de ascensão no sistema internacional. Ele afirma ainda que o interesse da China na utilização de capacidade ofensiva para o ciberespaço é maior que o de qualquer outra nação. Embora todos os Estados tenham pelo menos três motivos reais para investir em capacidade cibernética[29], o autor explica que a possibilidade de ganhos é ainda maior para os que continuam buscando desenvolvimentos econômico e militar.

Considerando esses motivos, sustentados em duas abordagens distintas, porém de trajetória e resultado semelhantes, constatamos que Estados já econômica e militarmente desenvolvidos não precisam do espaço cibernético para deter outros Estados, uma vez que conseguem fazê-lo militarmente. Com o exemplo dos Estados Unidos, é possível perceber que, desde que a tecnologia militar estadunidense tornou-se inigualável, a espionagem visando conhecimento da tecnologia militar de outros Estados tem sido desnecessária. Da mesma forma, ao se encontrar entre os níveis industriais e tecnológicos mais avançados do mundo, a espionagem industrial visando vantagens econômicas tem menos importância para os EUA do que para países com economia ainda em desenvolvimento. Contudo, cabe ressaltar que o fator cibernético não deve ser considerado como um instrumento de contenção, mas sim como um mecanismo de ação em um cenário internacional integrado, sobretudo, pelas tecnologias de informação e comunicação (TICs).

Como explana Inkster[30]: "há muita [informação] que a China deseja roubar do Ocidente, mas relativamente pouca que o Ocidente

29 São eles: (i) deter infiltração em suas estruturas estratégicas; (ii) obter conhecimento estrategicomilitar, mediante espionagem tecnológica militar (cibernética); e (iii) obter ganhos econômicos onde o processo tecnológico tem sido alcançado, por meio de espionagem industrial cibernética.

30 Nigel Inkster, "Chinese Intelligence in the Cyber Age" *Survival Global, Politics and Strategy*, Vol. 55, No. 1 (fev.-mar. 2013), 62.

precise roubar da China". Esse comentário nos leva novamente a Hjortald, o qual afirma que a China potencialmente é o país que mais se beneficiaria com os ataques cibernéticos, enquanto que os Estados Unidos seriam o maior alvo de tais tipos de ataque.

Para uma melhor clareza da atual capacidade cibernética chinesa – que, embora seja a mais extensa e mais praticada da Ásia, é inversamente proporcional ao seu nível de conhecimento técnico[31], como pode ser percebido no Quadro 1 –, é fundamental acompanhar a construção dessa capacidade, que parece ter nascido com o novo Ministério de Segurança do Estado, o qual, em 1983, combinou a coleta de funções externas com as da contrainteligência e da contraespionagem[32].

Quadro 1: Capacidade cibernética dos Estados/nações asiáticos

	China	Índia	Iran	Coréia do Norte	Paquistão	Rússia
Doutrina oficial de Guerra Cibernética	X	X			Provável	X
Treinamento em Guerra Cibernética	X	X	X		X	
Exercícios e Simulações de Guerra Cibernética	X	X				
Colaboração com a indústria de TI e/ou com Universidades Tecnológicas	X	X	X		X	X
IT Roadmap[1]	Provável	X				
Unidades de Guerra Cibernética	X	X		X		
Histórico de Ataques Cibernéticos a Outras nações	X					X

Fonte: adaptado de Billo e Chang[33].

31 Desmond Ball, "China's Cyber Warfare Capabilities", *Security Challenges*, Vol. 7, No. 2, pp. 81-103 (Winter 2011), 81.

32 Inkster, op. cit., 48.

33 Charles Billo e Welton Chang, *Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States* (Hanover, NH: Institute for Security Technology Studies, 2004).

Embora o Quadro 1 seja de 2004, ele apresenta os dados mais recentes em nível de comparação entre os Estados da região asiática com relação à capacidade cibernética, além de corroborar com a visão de Ball – de que a China é possuidora da capacidade cibernética mais extensa deste continente – e demonstrar que os investimentos cibernéticos chineses têm levado a China à posição de destaque no cenário internacional, no que tange a este assunto. Outro a ratificar o mesmo ponto de vista é o Major-General Wang Pufeng[34], que afirma:

> Em resumo, nossos métodos de guerra devem se adaptar às necessidades da guerra da informação. Nós devemos utilizar todos os tipos, formas e métodos de força e, especialmente, fazer mais uso da guerra não linear e muitos tipos de métodos de guerra da informação que combinam elementos nativos e Ocidentais para usar nossa força com o objetivo de atacar as fraquezas dos adversários, evitar ser reativos, e lutar para ser ativos. Deste modo, será inteiramente possível para China conquistar a vitória global sobre o inimigo, mesmo sob condições de inferioridade em relação à Tecnologia da Informação..[35]

Pufeng também expressa a possibilidade de obtenção de ganhos através do espaço cibernético, mesmo diante de sua inferioridade tecnológica, como já exposto anteriormente. Vale ressaltar, contudo, que o investimento na área cibernética tem sido parte importante da história chinesa especificamente desde 1985, como se apresenta a seguir.

---

34 O Major General Wang Pufeng é um antigo Diretor do Departamento de Estratégia da Academia de Ciência Militar de Beijing, na China.

35 Wang Pufeng, "The Challenge of Information Warfare", *China Military Science* (Spring 1995), http://www.fas.org/irp/world/china/docs/iw_mg_wang.htm, acessado em 7 out. 2014.

Em 1985, Shen Weiguang, soldado de uma unidade de campo chinês, começou a escrever sobre a Guerra da Informação (*Information War* – IW) e publicou um livro de mesmo nome que mais tarde foi publicado como artigo no Diário do Exército de Libertação da China. A doutrina da Guerra da Informação, entretanto, só obteve atenção, por parte das autoridades e estrategistas competentes, depois da Guerra do Golfo (1990 a 1991) e da crença de que ela teria um papel importante na vitória dos Estados Unidos, bem como de que a próxima guerra seria parecida com a Guerra do Golfo[36].

Em 1986, as exigências dos serviços de inteligência externa chinesa nas áreas de ciência e tecnologia (C&T) determinaram, aos olhos externos, que esta seria a chave para o desenvolvimento econômico do gigante asiático. O que ocorria na verdade era o desenvolvimento de um programa proposto por um grupo de cientistas de armas nucleares que primeiro focou o lado militar, mas que rapidamente envolveu projetos mais gerais que visavam eliminar a dependência chinesa de tecnologia estrangeira em áreas consideradas estratégicas[37], como a ciberespacial.

Nos anos 1990, o Exército de Libertação do Povo dá início aos exercícios militares que envolviam alguns aspectos da Guerra da Informação. Em 1995, a China implementa o plano de Guerra da Informação. Em 1997, um corpo de elite com 100 membros é criado pela Comissão Militar Central da China para elaborar meios de implantar vírus de computador incapacitantes, em sistemas estadunidenses e de outros países do ocidente, além do fato de a China começar a conduzir numerosos exércitos com a função de utilizar vírus de computador para interromper comunicações militares e sistemas públicos de radiodifusão[38].

---

36 James C. Mulvenon, "The PLA and Information Warfare", in *The People's Liberation Army in the Information Age*, ed J. C. Mulvenon e Richard H. Yang, eds, 175-186 (Washington, DC: RAND, 1999), 179.

37 Inckster, op. cit., 50.

38 Ball, op. cit., 81.

Em 1998, os coronéis Liang e Xiangsui escreveram um livro, publicado em fevereiro de 1999, no qual descreveram a dependência militar dos Estados Unidos nos sistemas de redes de TICs como a maior vulnerabilidade que a China poderia explorar na busca por vantagens assimétricas[39].

A partir desse momento, as unidades militares chinesas de guerra cibernética parecem trabalhar de maneira mais veloz, embora seja bastante difícil descobrir se ações agressivas no espaço cibernético são oriundas de agências oficiais – como as chinesas –ou simplesmente de internautas. O fato é que, desde 1999, ataques a *sites* oficiais de Taiwan, Japão e Estados Unidos têm sido constantes e têm tipicamente envolvido penetrações muito básicas, permitindo que *websites* sejam modificados (pixação) ou que servidores-*web* sejam atacados por programas de "negação de serviço" (DoS, do inglês *Denial of Service*). Em 2000, a China estabelece sua unidade estratégica de Guerra da Informação, que os observadores estadunidenses chamaram de *Força Net*, projetada para combater a redistribuição de informação através de redes de computadores, e para manipular sistemas de informação inimigas. Neste mesmo ano, as unidades de Guerra da Informação do Exército de Libertação do Povo dão início ao desenvolvimento de procedimentos detalhados para se guerrear na Internet, incluindo a criação de *softwares* para exploração de redes, obtenção de senhas, quebra de códigos-fonte, roubo de informação, criação de *softwares* para efetivas contramedidas, dentre outros[40].

Ainda em 2000, em um exercício de guerra cibernética na província de Hubei, 500 soldados chineses simularam ataques cibernéticos contra Taiwan, Índia, Japão e Coreia do Sul. Em outro exercício, em Xian, 10 missões de ataque cibernético foram praticadas,

39 Liang e Xiangsui, op. cit.

40 Ball, op. cit., 84.

incluindo implantação de minas de desinformação, condução de reconhecimento de informação, modificação de dados nas redes, liberação de bombas de informação, clonagem de informação, organização de defesa da informação e estabelecimento de estações de redes espiãs[41].

Em outubro de 2000, um exercício organizado pelo Chefe de Equipe do Exército de Libertação do Povo simula ataques cibernéticos e guerra eletrônica com países ao sul e ao oeste do Deserto de Gobi. Em 2001, 40 especialistas do exército chinês ficam responsáveis pela criação de métodos de tomada de controle das redes de comunicação de Taiwan, Índia, Japão e Coreia do Sul. Em 2002, uma versão mais aprimorada de um *malware* do tipo Cavalo de Troia é usada para invadir a rede do computador do Dalai Lama, e, mais recentemente, disfarçado de documentos do Microsoft Word e PowerPoint, este programa é encontrado inserido em computadores de escritórios de vários governos ao redor do mundo[42].

Há também uma versão desse Cavalo de Troia considerada "em hibernação", cuja ativação é estimada para períodos de paz. Como se vê, esse programa, depois de instalado, pode levar anos até ser ativado e receber comandos. Depois de ativado, ele pode danificar ou destruir sistemas, além de enviar informações confidenciais de volta à Pequim[43]. São exemplos de *malware* com esse viés estratégico os *worms* Downadup e Conficker que infectam sistemas operacionais da Microsoft, e que podem permanecer imperceptíveis até que os comandos sejam enviados[44].

Em 2004, durante um exercício na região militar de Pequim, sua

41 Ibid.

42 Ibid., 82.

43 Discos rígidos portáteis de grande capacidade, muitas vezes utilizados por agências governamentais, foram encontrados transportando cavalos de Troia que enviavam aos *websites* de Pequim tudo o que o usuário do computador infectado salvava no disco rígido (Ibid.).

44 Dave Piscitello, *Conficker Summary and Review* (ICANN, 2010).

Força Azul informatizada atacou a rede da Força Vermelha para tomar o controle de sua rede de comando, poucos minutos após o início do exercício que tinha como objetivo a prática da invasão aos centros de comando e controle dos sistemas de informação inimigos. No mesmo ano, *hackers* chineses atacaram *sites* do Ministério da Defesa de Taiwan na tentativa de interromper o Han Kuang-20, exercício anual de defesa daquele país[45].

Até 2005, o Exército de Libertação do Povo conduziu mais de 100 exercícios militares envolvendo aspectos da guerra cibernética. Em julho de 2006, o Ministério da Defesa Nacional de Taiwan resolveu incluir sua primeira ferramenta *anti-hacker* no exercício do Han Kuang-22, como um modo de aumentar a consciência quanto ao perigo de vazamentos descuidados de informações privilegiadas, através das redes de computadores internas e externas[46].

Em maio de 2007, o Secretário de Defesa dos Estados Unidos informa ao Congresso estadunidense que o Exército de Libertação do Povo chinês tinha as operações de redes de computadores como fundamentais para alcançar o domínio eletromagnético ainda no início de um conflito. O Secretário resolveu, então, seguir o exemplo chinês e incorporou as operações ofensivas de redes de computadores em seus exercícios, principalmente como primeiro ataque às redes inimigas[47].

Em 2008, a culpa sobre o lançamento de um vírus anti-japonês recaiu sobre a China. O vírus lê as chaves de registro do computador, julga o tipo de sistema operacional usado e, ao perceber que a língua utilizada é a japonesa, destrói o disco rígido, preenchendo os dados com lixo, reiniciando o sistema e, por fim, paralisando o computador por completo. Depois de tal descoberta, o Pentágono proibiu o uso de

45 Ball, op. cit., 87.

46 Ibid.

47 Ibid.

dispositivos de armazenamento com entrada USB, cartões de memória, *pen drives* e cartões de câmeras fotográficas em todos os departamentos militares dos Estados Unidos.

Em abril de 2009, *hackers*, que se acredita serem apoiados pelo regime comunista chinês, penetraram nos computadores críticos para o funcionamento de redes de energia elétrica dos Estados Unidos e instalaram um *malware* que permitia interromper o serviço quando comandado. Em julho de 2009, *websites* do Gabinete da Presidência e do Ministério da Defesa da Coreia do Sul foram atacados. No mesmo ano, pesquisadores da China e do Japão se uniram para discutir a possibilidade de pesquisarem sobre a Hegemonia na Era da Internet[48]. O *website* do Escritório de Segurança Nacional de Taiwan foi supostamente atacado pela China cerca de 590 mil vezes no período de janeiro a outubro de 2010, ou uma média de cerca de 2000 vezes por dia[49]. No mesmo ano, autoridades da Coreia do Sul disseram que o país tinha sido vítima de ataques no mesmo estilo dos ocorridos no ano anterior. As instruções envolveram ataques de negação de serviço (DoS), que foram lançados a partir de 120 endereços de IP originários da China. Os *websites* teriam fornecido informações sobre serviços administrativos e políticas de governo sul-coreano. Em 20 de julho de 2010, o Exército de Libertação do Povo anunciou que tinha estabelecido uma Base de Proteção da Informação sob o Departamento de Equipe Geral, que é uma espécie de centro de operações de segurança do computador.

Em março de 2011, o Centro Nacional de Segurança Cibernética da Coreia do Sul afirmou que cerca de 40 *websites* governamentais e privados haviam sido atacados no dia anterior, incluindo os do

48 Li Zhang, "A Chinese Perspective on Cyber War", *International Review of Red Cross*, Vol. 94, Issue 886, pp 801-807 (jun. 2012), 802, http://journals.cambridge.org/abstract_S1816383112000823, acessado 18 ago. 2014.

49 Ball, op. cit., 87.

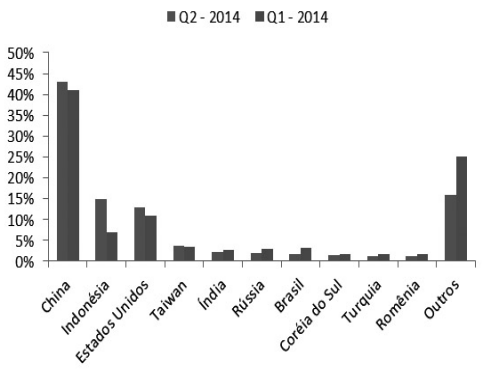
Gabinete Presidencial, do Ministério das Relações Exteriores, do Serviço Nacional de Inteligência, das Forças dos EUA na Coreia e de instituições financeiras. Todas as agressões eram originárias da China. Os ataques envolveram uma forma mais sofisticada de operação de negação de serviço, na qual dois *websites* de compartilhamento de arquivos foram inicialmente infectados com um vírus a partir do qual até 11 mil computadores foram tomados e usados nos ataques[50].

Ainda sobre as ações de participação chinesa, a empresa Akamai[51] apresenta, em seu relatório trimestral de 2014 sobre o estado da Internet, os dados mais recentes referentes ao primeiro e ao segundo trimestre do ano de 2014. A partir dele, ofertamos o Gráfico 1, que expõe as porcentagens do tráfego de dados de ataque cibernético mundial e aponta a China como provável responsável pelo maior número de ataques cibernéticos no mundo.

Gráfico 1: Top 10 do tráfego de dados relativos à ataques cibernéticos (2º trim. 2014)

	País	Q2 - 2014	Q1 - 2014
1	China	43%	41%
2	Indonésia	15%	6,8%
3	Estados Unidos	13%	11%
4	Taiwan	3,7%	3,4%
5	Índia	2,1%	2,6%
6	Rússia	2,0%	2,9%
7	Brasil	1,7%	3,2%
8	Coréia do Sul	1,4%	1,6%
9	Turquia	1,2%	1,7%
10	Romênia	1%	1,6%
-	Outros	16%	25,0%

Porcentagem do tráfego total de dados de ataque.



Fonte: elaboração própria.

Fonte dos dados: Akamai.

50 Ibid., 86-87.

51 Akamai, "State of the Internet Report" (segundo trim. 2014), http://www.akamai.com/dl/akamai/akamai-soti-q214.pdf, acessado em 31 jan. 2015.

Os dados do Gráfico 1 refletem uma tendência do comportamento chinês nos últimos anos. Levando em consideração as informações citadas ao longo deste capítulo, a ilustração ainda nos permite inferir que a questão cibernética é tratada como estratégica e prioritária no planejamento estatal chinês. Contudo, a informação não nos possibilita afirmar que toda ação de obtenção de dado negado ou de dano técnico via ciberespaço tem origem ou é coordenada pelo Estado chinês. Muitos ataques realizados são individuais, o que não nos licencia a tomá-los como de responsabilidade pública, ainda mais chinesa.

Considerações finais

Diante das discussões apresentadas até aqui, é possível concluir que, embora baseada na ideia tradicional de guerra, a perspectiva chinesa sobre a guerra cibernética considera que se trata de uma ferramenta para a obtenção de vantagens em um modelo de guerra assimétrica que possibilita a vitória sem a imposição da morte. Ainda que haja a possibilidade de resultados com efeitos catastróficos (ao se considerar principalmente os danos que um ataque cibernético pode causar a estruturas estratégicas) e a China seja possuidora de capacidade cibernética agressiva (inclusive permitindo a alguns países lhe darem a denominação de potência "cibernética"), suas ações condizem com a defesa de uma postura menos belicosa em um espaço onde os objetivos podem ser alcançados sem a imposição da morte. Há que se ressaltar que existem objetivos maiores por trás das ações chinesas que norteiam a ação do Estado na busca de suas metas políticas internas, como se pode observar com as contribuições de Chang e Hjortdal.

Como observado na segunda seção deste capítulo, a China é considerada uma potência cibernética por parte de países como Estados Unidos, Austrália, França, Reino Unido, Índia, Japão, Alemanha e Coreias[52], e é, por eles, acusada de atos cibernéticos contra suas redes

52 Ball, op. cit.,

e sistemas informacionais de governo. Destarte, seu conhecimento técnico não está no mesmo nível de sua capacidade cibernética agressiva, considerada a mais extensa e mais praticada da Ásia. Com isso, faz-se mister compreender que a China utiliza muito o ciberespaço como meio para espionagem visando a obtenção do conhecimento econômico e tecnológico de seus oponentes e a destruição de dados e capacidades inimigas.

Para corroborar com esses argumentos, é possível observar que a China vem promovendo treinamentos para testar suas táticas de guerra cibernética e implantar seus *softwares* maliciosos, como aconteceu em 1997, quando a China criou um vírus incapacitante e resolveu instalá-lo nos Estados Unidos e em outros países ocidentais.

Além das simulações de ataques cibernéticos contra Taiwan, Índia, Japão e Coreia do Sul, outros exemplos são também os incidentes envolvendo a invasão de redes de computadores do Dalai Lama e de agências governamentais de vários países, bem como a criação de um vírus anti-japonês. Por fim, é importante comentar o uso das capacidades cibernéticas chinesas em ataques a estruturas estratégicas, como os *blackouts* que aconteceram nos Estados Unidos em abril de 2009 e que, acredita-se, terem sido resultado de ações de *hackers* apoiados pelo regime comunista chinês.

Logo, é importante ressaltar que, apesar do grande número de acusações em direção à China, o que é possível comprovar é a origem do endereço de IP deixado como rastro por quem estava atacando. Todavia, dificilmente poderá estabelecer um forte conexão com órgão oficiais do governo chinês. Assim, o dragão asiático parece mostrar-se não só uma potencia emergente no mundo real, mas também uma cibernética.

A Estratégia Interamericana para Combater Ameaças Cibernéticas: consequências e desafios

Lucas Ribeiro de Belmont Fonseca
Tiago Medeiros Delgado

Introdução

O presente capítulo oferece uma reflexão sobre a construção de uma cultura de Segurança Cibernética latino-americana, destacando o papel da Organização dos Estados Americanos (OEA) nesse processo. Considerando a ausência de fronteiras no ciberespaço e o crescimento exponencial do número de usuários da rede mundial de computadores nas Américas, a preocupação dos governos americanos com a regulação da Internet e com a promoção da segurança na rede é crescente.

Desde o início dos anos 2000, a OEA, em conjunto com agências especializadas em Segurança da Informação, tem concentrado vários esforços no sentido de estabelecer mecanismos de cooperação regional em assuntos relativos ao ciberespaço. Diante de números assustadores que retratam o crescimento da ocorrência de crimes cibernéticos nas Américas, parece haver uma preocupação hemisférica comum em não apenas fortalecer a proteção cibernética de Tecnologias da Informação e Comunicação (TICs) utilizadas em estruturas estratégicas, mas também criar dispositivos legais que criminalizem ações danosas cometidas no ciberespaço, treinar juízes e promotores para lidar com esses casos e fomentar a criação de uma

tão desejada cultura de Segurança Cibernética, em consonância com a iniciativa privada e a sociedade civil.

O ambiente da OEA parece ser bastante propício às discussões sobre Segurança Cibernética, diante das iniciativas já em curso e da presença, entre seus membros, tanto de Estados com amplo desenvolvimento tecnológico e experiência jurídica em questões cibernéticas quanto daqueles que ainda buscam sua efetiva inserção na interconectividade global da Era da Informação. Dessa forma, abrem-se grandes possibilidades para a cooperação triangular, o compartilhamento de boas práticas, a assistência legislativa e outras formas de cooperação internacional em matéria de Segurança Cibernética.

Reconhece-se a importância do trabalho desenvolvido até o momento pela OEA, assim como destacam-se as responsabilidades das diferentes entidades envolvidas, entre as quais se incluem não apenas a referida organização regional, mas também governos, iniciativa privada, sociedade civil e agências especializadas. Objetiva-se, portanto, explanar sobre quais desafios são enfrentados no âmbito cibernético continental e quais medidas estão sendo tomadas pela OEA e demais interlocutores da discussão.

Ao mesmo tempo em que se exaltam os sucessos das iniciativas já implementadas, o presente capítulo revela – com base em uma metodologia fundamentada na leitura de bibliografia especializada e de documentos produzidos pela própria organização intergovernamental e por demais organismos internacionais – os principais desafios para as próximas décadas, entre os quais se incluem a harmonização das legislações nacionais, a adoção de regulações internacionais e o fortalecimento da cooperação regional.

Dessa forma, este capítulo se divide em duas partes, estando a primeira distribuída em três subtópicos, em que se faz a apresentação

de um panorama sobre a conjuntura hodierna, seguida de uma análise dos procedimentos e iniciativas atualmente em vigor, com uma perspectiva crítica acerca da efetividade desses mecanismos, e, já na segunda e última seção, expõem-se as carências que ainda precisam ser supridas.

A problemática da criminalidade cibernética nas Américas

A semiubiquidade e a disseminação do uso das TICs, bem como as ameaças – tanto existentes quanto potenciais – no âmbito da Segurança da Informação, impõem mundialmente sérios desafios aos legisladores e tomadores de decisão. Há uma preocupação crescente com as maneiras pelas quais pessoas e grupos – incluindo-se aí organizações criminosas e terroristas –, podem utilizar-se do ciberespaço para promover atividades ilegais ou irregulares que põem em xeque a proteção das sociedades.

Observa-se uma dependência tecnológica e informacional sem precedentes como resultado do crescimento do mercado de produtos e serviços cada vez mais revolucionários e baseados em TICs, o que oferece tanto vantagens e comodidades quanto ameaças à segurança. É necessário perceber que a amplitude de informações que seguem o desenvolvimento das TICs é bastante atrativa para criminosos cibernéticos, uma vez que possibilita ações que variam desde a danificação gravosa de estruturas estratégicas até o roubo de dados confidenciais[1].

Apesar do considerável avanço no campo da Segurança Cibernética, ainda há muito o que ser feito. O progresso tecnológico com foco no desenvolvimento de sistemas de segurança em redes

1 Organization of American States e Trend Micro, "Brazil: Cybersecurity Challenges Faced by a Fast Growing Market Economy" (2013), 8, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-brazil.pdf, acessado em 30 jan. 2015.

de computadores e a criação de normas internacionais e acordos de cooperação, por exemplo, foram iniciados há pouco. O caráter inerentemente dual – ou seja, o de servir concomitantemente a propósitos militares e a civis – das TICs, a ausência de fronteiras claramente delimitadas no ciberespaço, os interesses conflitantes entre diferentes entidades e distintas percepções entre os países sobre o que se constituem reais ameaças cibernéticas são vistos como grandes desafios, quando se tenta lidar com os problemas concernentes à temática ora em tela[2].

Por exemplo, a Convenção de Budapeste, firmada no âmbito do Conselho da Europa, em 2001, pode ser citada como um passo importante para a regulação dos crimes cibernéticos, visto que ele constitui um dos poucos instrumentos internacionais vinculantes nesse âmbito. Todavia, não há instrumento semelhante nas Américas, cuja materialização seria importante, na medida em que tal mecanismo poderia ser adaptado às particularidades e necessidades regionais, já que muitos países criticam a natureza eurocêntrica do conteúdo da supracitada Convenção. Tal instrumento interamericano seria mais que um mero dispositivo legal; ele ajudaria, entre outros, a criar entendimentos comuns sobre crime cibernético, fortalecer a cooperação regional e futuramente global, bem como orientar o desenvolvimento das legislações nacionais quanto a essa matéria.

A interconectividade global torna bastante difícil que um Estado lide sozinho com o melhoramento de sua Segurança Cibernética em nível estrategicamente nacional. Nesse sentido, a ampliação da cooperação entre Estados, iniciativa privada e sociedade civil organizada é essencial para se atingir uma necessária e complexa

2 Götz Neuneck, "Assesment of International and Regional Organizations and Activities", in *Cyber Index*, org. Instituto das Nações Unidas para a Investigação sobre o Desarmamento (Genebra: ONU, 2013), 91-107.

regulação efetiva do ciberespaço, bem como prevenir e combater o crime cibernético.

O compartilhamento de boas práticas em Segurança Cibernética, o intercâmbio de informações e a construção de infraestruturas que fortaleçam a segurança da informação são também ações que se mostram imprescindíveis para a região. Nas Américas, a OEA seria a organização internacional responsável por coordenar os avanços desse processo.

É importante destacar que a OEA busca desempenhar um papel ativo ante o fortalecimento da Segurança Cibernética no continente americano. Ela é responsável, por exemplo, por promover iniciativas e políticas governamentais que visem à cooperação internacional, à harmonização de legislações domésticas e à aplicação de leis contra os crimes cibernéticos nas Américas[3].

Além da existência de uma organização intergovernamental que possa vir a colaborar com matérias de Segurança Cibernética na região interamericana, há que se mencionar também o crescente número de seus usuários de Internet, constituindo-se como um dos maiores do mundo. Isso claramente reforça a necessidade de se fomentar a criação de uma cultura de Segurança Cibernética e de combate a uma parcela ínfima de internautas que maliciosamente usam sistemas e redes computadorizadas.

Assim, a consequência macropolítica desejável, diante do cenário de insegurança cibernética no mundo e, consequentemente, na região americana, é o desenvolvimento de redes de informação confiáveis e seguras e de centros de tratamento e respostas a incidentes cibernéticos, os chamados CERTs[4]. Nesse processo, para que haja a criação de tal cultura,

3 Michael Portnoy e Seymour Goodman, *Global initiatives to secure cyberspace: an emerging landscape* (Nova Iorque: Springer, 2009).

4 Brian Sullivan, *Regional efforts to strengthen cybersecurity in Americas* (Porto de Espanha: Internet Governance Forum, 2011).

deve haver, a nosso ver, demandas cada vez mais ativas por parte do setor privado, de organizações não governamentais (ONGs) e de setores pontuais da sociedade civil, visto que elas podem contribuir fortemente com os governos para a conscientização e o fortalecimento da segurança no ciberespaço, principalmente em países em desenvolvimento. É nesse viés de chamamento participativo e plural que o "Livro Azul das Políticas de Telecomunicações das Américas" apregoa que:

> devemos estar conscientes de que a responsabilidade de cada Estado de elaborar políticas para o setor, ao que deve seguir seu desenvolvimento, e de promover o crescimento econômico com equidade, inquestionavelmente inclui o reconhecimento do papel da iniciativa privada, do investimento público e privado em pesquisa e desenvolvimento, regulação, novas tecnologias e segurança em rede, comércio de equipamentos e serviços de telecomunicação, e estratégias a nível regional e global para o desenvolvimento e uso das TIC.[5]

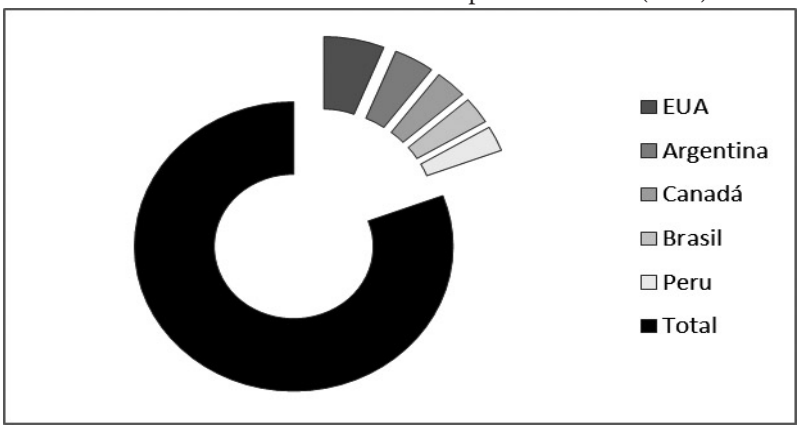
Como já mencionado, uma das tendências nos últimos anos é o crescimento do número de incidentes cibernéticos. Nas Américas, não é diferente: as diversas formas de criminalidade têm frequentemente utilizado especificamente a Internet para cometer delitos e até mesmo propagar terror, incluindo lavagem de dinheiro e rompimento de estruturas estratégicas que estão interligadas entre si ou a redes informacionais.

De acordo com um relatório emitido pela OEA e pelo Trend Micro, as perdas econômicas provocadas sobretudo por *crackers*, apesar

5 Comissão Interamericana de Telecomunicações e União Internacional de Telecomunicações, *The Blue Book: Telecommunication Policies for the Americas* ([s.l.].: UIT, 2005), 2, tradução nossa.

de não poderem ser definidas com precisão, certamente são maiores que aquelas provocadas por qualquer outro tipo de crime, inclusive o tráfico de drogas que tanto marca as relações interamericanas. Além disso, cinco Estados-membro da OEA figuram em uma lista das 10 maiores fontes de *spam* do mundo, conforme se apresenta no Gráfico 1.

Gráfico 1: As 10 maiores fontes de spam do mundo (2013)



Fonte: elaboração própria.

Fonte dos dados: Symantec, "Intelligence Report", 2013[6].

Dessa forma, o uso do ciberespaço por grupos criminosos tem-se tornado um problema sério na América Latina, uma vez que a "narcoeconomia" regional e os grupos associados a ela "se utilizam do ciberespaço para organizar e propagar suas atividades, recrutar membros, intimidar autoridades e cidadãos, extorquir dinheiro e contratar assassinos"[7]. Some-se a isso também o fato de eles realizarem lavagem de dinheiro, por meio da compra de serviços *online* e de

6 Symantec Corporation, "Symantec Intelligence Report" (dez. 2013), 21, http://symantec.com/content/en/us/enterprise/other_resources/b-intelligence_report_12-2013.en-us.pdf, acessado em 3 set. 2014.

7 Open Empowerment Initiative, *Cyberspace & Open Empowerment in Latin America* (Rio de Janeiro: Instituto Igarapé; Ottawa: The SecDev Foundation, 2013), tradução nossa.

transferência monetária: eis aí a transnacionalização do crime sob a égide de um ambiente sem fronteiras.

Além da fraude de cartões de crédito e falsificação de identidades, há também outras modalidades criminosas avulsas: narco-cartéis e traficantes de drogas, membros de gangues, traficantes de pessoas, entre outros, todos eles se utilizam do poder da *web* para organizar suas operações, intimidar competidores, recrutar aliciandos, fugir do controle estatal, extorquir dinheiro e vender seus produtos[8]. Tudo isso sendo feito de maneira mascarada devido à insegurança que caracteriza a Internet desde seus primórdios tempos de ARPANET.

Não surpreende, portanto, que governos americanos tenham grande preocupação em combater o cibercrime. O grande problema, a nosso ver, é que cada Estado americano, utilizando-se logicamente de sua prerrogativa de ator soberano e independente, tem proposto sua própria visão de combate aos delitos cibernéticos, fazendo com que a cooperação entre eles, quando existente, não seja total e legalmente articulável. Daí, a necessidade de um elo institucional maior entre eles, que, no caso interamericano, poderia ser levado a cabo pela OEA.

O aumento da criminalidade no âmbito do ciberespaço nas Américas e globalmente pode ser explicado não apenas pelo já mencionado crescimento exponencial de usuários de Internet, mas também porque a origem da ação criminosa e a identidade dos perpetradores são difíceis de serem precisadas. A semiubiquidade do ciberespaço, propiciada pelos avanços das TICs[9], permite que praticamente qualquer pessoa possa promover operações cibernéticas maliciosas, bastando apenas comprar um *kit* pré-configurado com *software* malicioso (*malware*). Considerando também a dificuldade de se delimitarem fronteiras no ciberespaço, os

8 Ibid.

9 A massificação da *web* também pode ser apontada como causa de tal aumento de criminalidade virtual, pois o amplo acesso ao ciberespaço – notadamente, Internet e redes de telefonia móvel – faz com que quantitativamente aumente o número de crimes lá.

internautas podem não só acessar e disseminar informações produtivas, como também podem cometer crimes cibernéticos, partindo de e dirigidos a qualquer parte do globo. Destarte, os Direitos Nacional e Internacional encontram dificuldades em acompanhar o avanço das TICs e da sofisticação das ações maliciosas.

Logo, a cooperação interestatal nessa seara, aportada também em uma cultura pluralista de Segurança Cibernética, mostra-se crucial para se lidar com riscos não só à segurança ciberespacial propriamente dita, mas também à segurança nacional. Responder rapidamente a incidentes cibernéticos e promover a efetiva aplicação da lei – daí a importância do aparato policial em se atualizar frente às novas TICs – são desafios idiossincráticos dos Estados neste novo milênio. É por isso que repetimos que governos, iniciativa privada e sociedade civil devem trabalhar conjuntamente para fomentar esforços nacionais e respostas internacionais a presentes e futuras ameaças cibernéticas. Desta forma, o desenvolvimento da "Estratégia Interamericana para Combater Ameaças à Segurança Cibernética" se coloca como uma das medidas mais importantes que a OEA adota para satisfazer essas necessidades.

A importância da Estratégia Interamericana de Segurança Cibernética

Organizações intergovernamentais regionais são geralmente conhecidas por promover a cooperação internacional de maneira improvável de ser alcançada a nível global, respeitando as características de cada região. Normalmente, isso se deve ao fato de que acordos regionais envolvem um número menor de Estados, aumentando as probabilidades de que estes possuam interesses e necessidades semelhantes, com a devida atenção às particularidades regionais. Assim, "o acordo e a implementação de medidas específicas são mais fáceis de ocorrer a nível regional do que a global, principalmente em regiões em que já existem

acordos de cooperação desenvolvidos e complexos"[10].

Dessa forma, a OEA seria a organização intergovernamental regional responsável pela promoção de iniciativas que visem políticas para as áreas de segurança cibernética, cooperação regional, harmonização de legislações nacionais, resposta a incidentes cibernéticos e aplicação da lei contra crimes cibernéticos[11].

Em 2003, a Assembleia Geral da OEA destacou a necessidade de se desenvolver uma Estratégia de âmbito interamericano para lidar com os problemas concernentes à segurança no ciberespaço. Tal propositura ocorreu por meio da Resolução nº 1939. Nesse documento, decide-se dar início ao desenvolvimento de um projeto integral de Estratégia que pudesse lidar com o caráter multidimensional e multidisciplinar por trás da Segurança Cibernética. E isso ocorreu, de fato, durante a Conferência sobre Segurança Cibernética da OEA, em Buenos Aires, em julho de 2003[12].

Nesse mesmo ano, o Encontro do Grupo de Especialistas Governamentais em Cibercrime da Reunião de Ministros da Justiça ou de Outros Ministros ou Procuradores-Gerais das Américas (REMJA), no âmbito da OEA, publicou o documento OEA/Ser. K/XXXIV, que contém uma série de recomendações quanto aos esforços hemisféricos para o combate ao crime cibernético. Esse Grupo de Especialistas chama a atenção primeiramente para a importância de haver unidades específicas para o trato com os incidentes virtuais, com os necessários recursos humanos, financeiros e técnicos, que possuam a responsabilidade de investigar e processar diferentes modalidades desse tipo de crime.

Quanto ao trato dos incidentes no ciberespaço, nos últimos anos, vários países montaram seus Centro de Estudos, Resposta e

10 Neuneck, "Assesment of Organizations".

11 Portnoy e Goodman, *Global initiatives to secure cyberspace*.

12 Organization of American States, *AG/RES. 1939 (XXXIII-O/03)*, assinada em 10 jun. 2003.

Tratamento de Incidentes de Segurança da Informação (CERTs)[13]. Essas equipes de segurança da informação possuem a atribuição de responder a incidentes de computador e, assim, reduzir o dano quando houver ataques a sistemas conectados em rede. Ademais, elas também devem prover informações sobre possíveis ameaças virtuais[14].

Os benefícios de se ter um CERT, todavia, não são limitados a ações que visem ao mero reporte ou encaminhamento de incidentes; ele também pode oferecer: centralização coordenada das atividades de segurança relacionadas a TICs; suporte e assistência especializados contra incidentes; apoio a usuários para se recuperarem de incidentes cibernéticos; habilidade jurídica para lidar com questões legais; preservação de evidências dos crimes; manutenção de informações atualizadas sobre o *status* da Segurança Cibernética nacional; e ajuda para a conscientização sobre os problemas relativos à segurança no ciberespaço[15].

O documento do Grupo de Especialistas da OEA ainda reitera que os sistemas legais intraestatais devem estar "apropriados" para combater crimes cibernéticos, por meio da criminalização de suas diferentes modalidades, bem como devem estar adaptados para possibilitar a coleta e a preservação de evidências eletrônicas. Para assegurar a prevenção, investigação e processo de crimes cibernéticos, os Estados devem rever seus códigos penais e atualizar suas respectivas leis para se moldarem à nova realidade virtual[16].

De forma geral, pode-se dizer que a propositura da OEA

13 Sullivan, *Regional efforts*.

14 União Internacional de Telecomunicações, *Cybersecurity: The role and Responsibilities of an Effective Regulator* (Beirute: UIT, 2009), http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR-background-paper-on-cybersecurity-2009.pdf, acessado em: 3 jan. 2015.

15 Agência Europeia para a Segurança das Redes e da Informação (ENISA), "Abordagem Gradual de Criação de uma CSIRT" (2006), https://www.enisa.europa.eu/activities/cert/support/guide/files/csirt-setting-up-guide-in-portugese/at_download/fullReport, acessado em 3 jan. 2015.

16 UIT, *Cybersecurity*.

se assemelha ao disposto na Convenção de Budapeste. Esta afirmação se torna ainda mais forte quando se assevera que "toda nação tem a responsabilidade de incluir os crimes cibernéticos em sua legislação criminal substantiva"[17]. Devido à atual interconectividade global e o fato de que criminosos cibernéticos não são barrados por fronteiras, tal medida busca principalmente evitar a existência de "paraísos cibernéticos", assim como promover o desencorajamento do uso malicioso das TIC.

Ainda, o desenvolvimento exponencial de ferramentas cibernéticas no mundo digital dificulta a regulação dos tipos de leis nacionais[18]. Desse modo, um nível adequado de flexibilidade se faz necessário para evitar que a legislação fique prematuramente obsoleta, em face ao progresso tecnológico. Isso se torna possível graças ao estabelecimento de princípios gerais aplicáveis a novas e variadas circunstâncias que surgem com o contexto da cibernética[19]. Tal flexibilidade, todavia, não deve redundar em vagueza de termos ou expressões, o que dificultaria a tipificação criminal ou a tornaria excessivamente ampla. Não apenas consultorias técnicas, mas também o Direito Comparado e a assistência legal mútua devem ser utilizados de maneira a facilitar o desenvolvimento de legislações nacionais efetivas e harmônicas.

Deve-se destacar também que um esforço efetivo contra crimes cibernéticos também requer o treinamento específico de procuradores e juízes, como já mencionado. Esse processo exige ampla cooperação internacional e compartilhamento de boas práticas nos temas aqui versados. A falta de legislações adequadas e de políticas

17 Filipe D. C. Alves, "EU Law and Internet Traffic Control Lost Between Privacy Rights and Freedom of Individual and Corporate Enterprise", in *Proceedings of the 11th European Conference on Information Warfare and Security* (Reading: API, 2012).

18 Eneken Tikk, *Ten rules for cybersecurity* (Tallinn, NATO CCDCOE, 2011), 14.

19 Comissão Interamericana de Telecomunicações e UIT, *The Blue Book*, 8.

nacionais de segurança cibernética, nesse sentido, tem trazido enormes dificuldades para que vários Estados possam processar criminosos por seus atos cometidos no ou do ciberespaço[20].

Por um lado, o fato de as investigações no ciberespaço serem bastante difíceis de ocorrer decorre não apenas do anonimato oferecido sobretudo pela Internet e de sua natureza inerentemente aberta, mas também porque os criminosos cibernéticos, conscientes de que podem deixar pistas, tentam esconder informações e evidências por meio de técnicas antiforenses cada vez mais sofisticadas. Por outro lado, "técnicas antiforenses são raras, visto que a maioria dos usuários não necessita de esconder informações além das suas senhas; então, qualquer evidência de seu uso é uma pista que pode valer a pena uma inspeção mais minuciosa"[21].

Finalmente, o relatório da OEA urge por maior cooperação internacional, inclusive entre diferentes organizações internacionais, e demonstra a necessidade de haver encontros periódicos do Grupo de Especialistas da REMJA, de maneira a fazer recomendações para combater os diferentes tipos de delitos informacionais e para prevenir o surgimento dos já mencionados "paraísos cibernéticos".

Em 2004, a Assembleia Geral da OEA aprovou uma Resolução intitulada de "Adoção de uma Estratégia Interamericana para Combater Ameaças à Segurança Cibernética: uma abordagem multilateral e multidisciplinar para a criação de uma cultura de segurança cibernética", doravante chamada de "Estratégia Interamericana de Segurança Cibernética". Esse documento solicita aos Estados-membro que: adotem a Estratégia Interamericana, descrita em seu Anexo A; estabeleçam a criação de CERTs nacionais; coordenem esforços entre si; e implementem

20 OEA e Trend Micro, "Tendencias en la Seguridad, 19.

21 Neil Rowe e Simson Garfinkel, "Finding Suspicious Activity on Computer Systems", in *Proceedings of the 11th European Conference on Information Warfare and Security* (Reading: API, 2012), tradução nossa.

as recomendações do Grupo de Especialista Governamentais da REMJA, "como uma forma de criar uma estrutura para a implementação de leis que protejam sistemas de informação, previnam o uso de computadores para facilitar atividades ilegais e punam cibercrimes"[22].

Tal documento é fruto dos esforços conjuntos dos Estados-Membro da OEA e do conhecimento técnico oriundo de três órgãos, a saber: Comitê Interamericano contra o Terrorismo (CICTE), Comissão Interamericana de Telecomunicações (CITEL) e Grupo de Especialistas da REMJA. Desde sua criação, a Estratégia Interamericana de Segurança Cibernética tem buscado ser uma peça orientadora das políticas nacionais de Segurança Cibernética nas Américas, as quais, de fato, têm se mostrado bastante limitadas[23].

A Estratégia ora em apreço possui os seguintes objetivos: despertar a conscientização social, criar uma cultura de Segurança Cibernética, identificar ou estabelecer CERTs nacionais e fortalecer a cooperação hemisférica para lidar com problemas relativos à sua temática-mor. A Resolução que a cria ainda reconhece que a efetividade de uma estrutura para proteção de sistemas de informação depende da conscientização de usuários e operadores da Internet acerca de preceitos e pressupostos, tais como: segurança e vulnerabilidades, promoção de parcerias público-privadas (PPP), adoção de legislações e políticas de combate ao crime cibernético, assim como identificar, avaliar e estimular a adoção de padrões técnicos e de boas práticas. Em outras palavras, é praticamente a repetição dos considerandos que geralmente aparecem em documentos dessa temática, como, por exemplo, os da Convenção de Budapeste e de outras políticas e estratégias nacionais de segurança cibernética.

Por seu turno, para se tornar evidentemente efetiva,

22 Portnoy e Goodman, *Global initiatives*.

23 Organização dos Estados Americanos, *AG/RES.2004 (XXXIV-0/04)*, assinada em 2004.

a Estratégia Interamericana deve identificar e avaliar os riscos e ameaças potenciais que afligem os Estados-membro da OEA. Ela deve estabelecer metas relacionadas à Segurança Cibernética, entre as quais se incluem acordos de cooperação, criação de mecanismos institucionais para compartilhamento de boas práticas, assistência mútua em processos legislativos e criação de instrumentos para frear o crescimento da criminalidade virtual. Também cabe à Estratégia Interamericana definir as funções e responsabilidades dos participantes em redes e sistemas de informação, o que inclui, notadamente, não apenas governos nacionais e agências internacionais, mas também a esfera privada.

Antes de discutir esses grupos, é importante reforçar a ideia de que as organizações internacionais possuem um amplo escopo de trabalho, que vai desde o estabelecimento ou fortalecimento de normas e princípios para prevenir o uso de *malware*, até mesmo a promoção nacional de prevenção, preparação, resposta e recuperação de incidentes cibernéticos, como é o caso, por exemplo, do CERT brasileiro. Desse ponto de vista, as organizações internacionais são capazes de unir seus diferentes e relevantes atores ciberespaciais para adentrarem nas discussões[24].

Um ano antes da publicação da Estratégia Interamericana, foi aprovada a "Declaração sobre Segurança nas Américas". Tal dispositivo apregoa a necessidade de haver um novo conceito multidimensional de segurança hemisférica capaz de proporcionar o combate tanto de ameaças tradicionais quanto das novas. Ela reconhece que tais ameaças requerem respostas multifacetadas por parte das diferentes entidades envolvidas, incluindo o setor privado e a sociedade civil. Finalmente, a Declaração destaca o mesmo comprometimento da Estratégia Interamericana de desenvolver uma cultura de Segurança Cibernética

24 Neuneck, "Assesment of Organizations".

nas Américas e de implementar uma estratégia integral de Segurança Cibernética no âmbito da OEA.

O papel da OEA no combate aos crimes cibernéticos

Primeiramente, é preciso enfatizar que os governos abordam a Segurança Cibernética de diferentes maneiras. Alguns desses atores consideram a Segurança Cibernética como um tópico de segurança e defesa nacionais; já outros acreditam que ela tem um impacto maior no desenvolvimento econômico e na segurança pública. Um terceiro grupo a toma como um elemento-chave da educação, da interação social e da governança cidadã, ainda que a maioria deles leve em consideração todos esses aspectos nos seus regimes de Segurança Cibernética[25].

Embora os Estados-membro da OEA estejam apenas começando a desenvolver normas e princípios voltados à Governança da Internet – a exemplo do pioneiro Marco Civil da Internet, no Brasil –, a Estratégia Interamericana parece ser um primeiro passo que pode levar a possíveis, ainda que tímidas, reformas nos ordenamentos jurídicos de seus membros. A despeito disso, trabalhar na criação de uma Convenção semelhante à Convenção de Budapeste sobre Crime Cibernético é uma medida importante para harmonizar legislações nacionais e adaptar regulações aos interesses e às necessidades regionais. Todavia, como já frisado, apenas a modificação jurídica não resolve o problema; é necessário que haja, dentre outros elementos, uma cultura interamericana de Segurança Cibernética.

De acordo com a Comissão Interamericana de Telecomunicações e a UIT[26], esforços jurídicos devem levar em consideração, entre outros princípios, a proteção dos usuários, a promoção de infraestrutura,

25 Comissão Interamericana de Telecomunicações e UIT, *Blue Book*.

26 Sullivan, *Regional efforts*, 2011.

de P&D tecnológico, o acesso de todos os cidadãos à Sociedade da Informação e o uso das telecomunicações, para facilitar a integração de países e o crescimento de mercados regionais.

Já o CICTE tem como principal objetivo promover e desenvolver a cooperação entre os Estados-membro da OEA, bem como prevenir, combater e eliminar o terrorismo[27]. A respeito da Segurança Cibernética, o CICTE dá suporte aos membros na criação de CERTs e promove uma rede hemisférica desses centros, com o fito de compartilhar e coordenar informações entre os países-parte. Ele também busca nutrir a tão almejada cultura de Segurança Cibernética, com o fito de desencorajar o mau uso da Internet e dos sistemas computacionais e de fomentar o desenvolvimento de redes de informação que sejam confiáveis.

Em 2004, o CICTE aprovou a Declaração de Montevidéu, em que reconheceu a criação de uma Rede de Pontos de Contato Nacionais, para facilitar e aperfeiçoar a troca de informações e o compartilhamento das melhores técnicas de cooperação hemisférica em contraterrorismo. Ao mesmo tempo, ele busca intensificar essa troca de conhecimentos entre as autoridades competentes, a fim de facilitar o fluxo rápido e seguro de informações a respeito de prevenção, punição e eliminação do terrorismo. Finalmente, esse instrumento internacional reconhece os prenúncios relativos à segurança cibernética como uma ameaça terrorista emergente, expressando o compromisso dos Estados-membro em lhes identificar e combater.

Em 2012, o CICTE aprovou uma Declaração, reiterando conquistas prévias, assim como a abordagem multidimensional e multidisciplinar sobre Segurança Cibernética estabelecida pela Estratégia Interamericana, e a necessidade de fortalecer parcerias entre todas as partes interessadas nessa temática.

27 Portnoy e Goodman, *Global initiatives to secure cyberspace*.

Não obstante, a CITEL objetiva facilitar e promover o desenvolvimento contínuo das telecomunicações no continente[28]. Consequentemente, ela é responsável por combater o uso das TIC para fins criminosos, além de criar uma cultura de segurança cibernética. No que tange às atribuições feitas pela Estratégica Interamericana, o principal papel da CITEL é identificar e adotar normas técnicas, a fim de obter uma arquitetura segura da Internet, em um processo de múltiplas fases. Ela deve também identificar obstáculos que podem impedir a aplicação dessas normas em redes regionais.

A CITEL deve também procurar estabelecer PPPs e fomentar a cooperação com outras organizações internacionais, como a UIT, cuja parceria resultou em importantes publicações, como o Livro Azul de Segurança Cibernética para as Américas.

No que concerne às REMJA, sua principal responsabilidade é assegurar que os Estados-membro da OEA adotem as legislações necessárias para combater as ameaças ciberespaciais e proteger os internautas. Isso é feito por meio de assistência técnica para a criação de leis apropriadas contra o crime cibernético, de medidas de capacitação e de seminários e de conferências. As REMJA também podem facilitar a cooperação entre os corpos judiciários e policiais nacionais, a fim de melhor investigar e processar criminosos do ciberespaço localizados além-mar.

De acordo com a Estratégia Interamericana, todos os membros da OEA devem estabelecer proibições legais e processuais para os ataques contra a confidencialidade, a integridade e a segurança dos sistemas informáticos. Além disso, todos os países devem adotar procedimentos claros de acordo com normas internacionais para o acesso governamental às comunicações e aos dados armazenados, quando necessário para a investigação de um delito cometido no ciberespaço.

28 OEA e Trend Micro, "Tendencias en la Seguridad Cibernética", 2013, 19

A atuação conjunta da CITEL, CICTE e REMJA tem provocado impactos positivos na promoção da Segurança Cibernética nas Américas. Nesse processo, cabe destacar o crescimento surpreendente do número de CERTs na região e a realização de treinamentos periódicos, em diversos países, de juízes e promotores, assim como assistência legal em processos legislativos.

Todavia, é necessário lembrar que, com o progresso tecnológico, surgem novas ameaças e vulnerabilidades a todo instante. Apesar de as iniciativas tomadas até então trazerem perspectivas otimistas de cooperação internacional, reitera-se a necessidade de existir esforços contínuos, de maneira a lidar com ataques cada vez mais sofisticados e com o aumento da criminalidade no ciberespaço.

O crescimento vertiginoso de usuários da Internet nas Américas, juntamente com a criação de novos e sofisticados instrumentos invasivos e potencialmente danosos, podem ser um fator que contribua para uma tendência de aumento no número de delitos ciberespaciais no continente. Entretanto, essa tendência não reflete, necessariamente, um fracasso da Estratégia Interamericana, mas lhe confere ainda mais importância.

Apenas as iniciativas governamentais não são suficientes para conter a criminalidade no ciberespaço. Por isso, o foco da Estratégia Interamericana na criação de uma cultura de Segurança Cibernética pode ser essencial, haja vista que essa inclui os papéis respectivos da sociedade civil, da iniciativa privada e das agências especializadas em TICs, bem como busca pela criação de mecanismos que possibilitam a cada indivíduo contribuir para a promoção da Segurança Cibernética no continente. Além disso, a conscientização de indivíduos e empresas acerca da importância desse tema[29] são outras etapas importantes

29 De como se proteger, e, com a criação de CERTs e CSIRTs, de como reportar crimes e violações ocorridos no ciberespaço.

incluídas na Estratégia Interamericana, as quais podem ter impactos positivos a médio e longo prazos. Portanto, apesar da amplitude e importância das iniciativas tomadas até então, são inúmeros os desafios para a construção de um continente ciberneticamente mais seguro.

Considerações finais: os desafios cibernéticos futuros nas Américas

Dadas as características inerentes ao ciberespaço, a cooperação internacional se mostra como uma grande oportunidade de superar as barreiras impostas pela insegurança cibernética, no mundo e especificamente nas Américas.

Em um nível global, os Estados enfrentam grandes problemas, e um novo padrão de comportamento precisa ser adotado, a fim de finalmente alcançar o que se poderia chamar de paz cibernética.

Um relatório da UIT[30] demonstra que o problema fundamental da insegurança cibernética é a falta de métodos de desenho e de análise que sejam cientificamente comprovados para lidar com a enorme complexidade dos sistemas digitais interconectados futuros, especialmente a respeito da confiabilidade, da funcionalidade e da segurança dos dados trafegados e armazenados.

Por isso, também é necessário que a cooperação internacional seja encorajada nos vários domínios de ação, como nos centros nodais nacionais da Internet, no diálogo com os provedores globais de serviço e CERTs, no campo de gerenciamento e resposta a incidentes, na proteção de estruturas estratégicas, no compartilhamento de melhores práticas, no contínuo processo de conscientização de ameaças cibernéticas, na adoção de normas legais aceitáveis e na coordenação entre departamentos policiais.

30 Axel Lehmann, Vladimir Briktov e Jacques Bus, "Technology Trends and Threats", in *The Quest for Cyber Peace*, ed. Hamadoun Touré (Genebra: UIT, 2011), 31-52.

É notório que os países desenvolvidos, sobretudo os chamados de potências cibernéticas – como Estados Unidos da América, Rússia e China[31] –, têm visões diferentes da natureza da Segurança Cibernética. Isso faz com que acordos consensuais sejam dificilmente alcançados, especialmente quando a ideia de um tratado vinculante é posta na mesa de negociações.

A fim de prevenir que as divergências entre as nações impeçam o progresso das negociações relativas à governança da Internet, alguns princípios devem estar presentes. É o caso, por exemplo, da proteção da liberdade de expressão, mesmo que ela torne o anonimato muito mais fácil. Os formuladores de políticas americanos também precisam estar cientes de que nem toda resposta adequada pode ser dada sem o suporte do setor privado. O relacionamento entre os governos e as empresas privadas tem de ser transparente, confiável, estruturado e constante. Daí a importância de uma Estratégia Interamericana que fomente uma cultura de Segurança Cibernética.

Como é sabido que desconfiança e percepções errôneas são comuns na discussão sobre governança no ciberespaço, as organizações internacionais podem apresentar um importante caminho para solucionar esse problema em particular. Nesse sentido, a própria natureza da Estratégia Interamericana de Segurança Cibernética se põe como uma alternativa valiosa, uma vez que seu planejamento visionário e seus objetivos têm uma abordagem multidisciplinar, deveras necessária para o trato com os incidentes cibernéticos.

Em primeiro lugar, a Estratégia em questão tem uma estrutura baseada em três pilares, dividida entre o CICTE, a CITEL e as REMJA. Desse modo, todos os temas fundamentais que ameaçam a Segurança Cibernética continental são abordados pela Estratégia sob as

31 Sobre a China enquanto potência cibernética, conferir capítulo escrito por Ahmina Raiara Solsona Oliveira e Alexandre César Cunha Leite, neste mesmo livro.

perspectivas legal, técnico, militar, social e econômica. Em um segundo aspecto, a Estratégia cientifica que, por meio da coordenação entre nações e instituições, bem como da adoção de legislações nacionais apropriadas que regulem crimes cibernéticos, será possível aprimorar a segurança informacional nas Américas.

Não obstante, o aumento do acesso à Internet na América Latina é responsável por muitas e permanentes mudanças em diferentes aspectos do cotidiano da região, tais como política, educação, cultura e economia. Por isso, a OEA enfrenta algumas implicações que precisam ser abordadas por intermédio de seu corpo multilateral e de frequente revisão da Estratégia Interamericana de Segurança Cibernética, a fim de que ela não se torne obsoleta em um curto período de tempo. Um modo de se fazer isso é alargar o escopo tomado pela OEA, "considerando os modos multifacetados pelos quais o ciberespaço está gerando formas positivas e negativas de obtenção de poder"[32]. Em outro prisma: se, por um lado, a esfera cibernética é responsável por uma maior eficiência tanto no setor público quanto no privado, por outro, ela também permite que criminosos ajam anonimamente, com uma grande perspectiva de ganhos a custos baixos. Por último, incorporado pela Estratégia Interamericana de Segurança Cibernética, a OEA precisa fomentar uma próxima e contínua coordenação entre Estados, o setor privado e a sociedade civil[33] cujo caminho parece ser o melhor para lidar com os desafios postos pelos avanços tecnológicos digitais.

Também deve ser dada importância às respectivas atribuições dos Estados, das companhias e, sobretudo, dos cidadãos, pois eles são os usuários finais da tecnologia informática e, ao mesmo tempo, as principais vítimas de crimes cibernéticos. O rumo que deve ser seguido

32 Open Empowerment Initiative, *Cyberspace*, tradução nossa.

33 Ibid.

pelos Estados ao redor do mundo – e como já frisado sobremaneira neste capítulo – é a criação de uma cultura de Segurança Cibernética, a qual só pode ser alcançada com trocas de informação constantes entre os participantes da esfera cibernética das Américas.

Para se ter ideia da importância de tal busca, a Assembleia Geral das Nações Unidas aprovou uma Resolução com os seguintes princípios norteadores de uma cultura global de Segurança Cibernética: conscientização, responsabilidade, resposta, ética, democracia, gerenciamento de riscos, desenho, implementação e gerenciamento de segurança. E a OEA parece fazer a sua parte também: esses princípios estão arrolados na Estratégia Interamericana de Segurança Cibernética e são particularmente atribuídos aos órgãos que compõem a estrutura fundamentada nos três pilares supramencionados.

Todavia, é preciso notar que os princípios defendidos pela Resolução da ONU precisam ser constantemente revisados e postos em prática, colocando um desafio para a OEA e seus membros: eles serão capazes de exercer sustentavelmente a Estratégia Interamericana de Segurança Cibernética? Em outras palavras, eles estarão prontos para se adequarem às rápidas mudanças do cenário da Segurança Cibernética? Terão capacidade tecnológica e vontade política para tal? Contarão com a disposição, no longo prazo, para a cooperação e para o entendimento não só de governos de países vizinhos, mas outrossim do amplo escopo de atores que participam da governança cibernética – órgãos especializados, empresas, usuários e técnicos?

No futuro, é preciso iluminar algumas discrepâncias legais que caracterizam as atuais legislações cibernéticas nacionais. Esse é o papel que as REMJAs vêm desempenhando na Estratégia Interamericana. Entretanto, a cooperação legal e processual presente nas *Recomendações do Grupo de Especialistas*, de 2003, não é suficiente para abordar o problema da criminalidade que cruza as fronteiras

físicas e muros virtuais. Na verdade, deve-se ter em mente que, no âmbito da OEA, os aspectos de cooperação legal presentes em sua Estratégia Interamericana são apenas o começo de uma jornada rumo a um acordo nos moldes da Convenção de Budapeste.

A responsabilidade do CICTE também enfrenta alguns obstáculos, haja vista que cooperação e desenvolvimento técnico não são isoladamente suficientes para atingir as metas propostas. Para tanto, uma infraestrutura delicada e consistente precisa ser criada nas Américas, a fim de que os Estados-membro – por meio especialmente de seus CERTs – possam se comunicar de forma segura e rápida entre eles. Para esse propósito, os governos das Américas precisarão educar suas sociedades, informando como os usuários podem proteger seus computadores e redes e a quem chamar, quando um incidente ocorrer. Do contrário, dada a dependência em estruturas críticas ligadas a TICs que podem ser danificadas por ataques cibernéticos, a falta de confiança pode ser responsável pela erosão social e pela instabilidade internacional.

O caso particular da América Latina é um bom exemplo que pode lançar luz sobre como a OEA pode ajudar seus membros a lidar com problemas relativos à Segurança Cibernética, com o incentivo para criar CERTs e corpos policiais especializados, bem como adotar molduras legais apropriadas. Contudo, a OEA precisa encontrar uma maneira para que o setor privado, a sociedade civil e os governos americanos possam caminhar juntos em direção a um ambiente de cooperação estreita e de paz cibernética sob a égide de uma cultura comum de Segurança Cibernética. Nesses termos, a Estratégia Interamericana é apenas a ponta do *iceberg*.

PARTE 3

OPORTUNIDADES E DESAFIOS METODOLÓGICOS

Glossário de termos aplicados a CiberRI

Arma cibernética: qualquer *software* malicioso (*malware*) produzido por um Estado com o intuito de provocar dano moral, material ou virtual a uma estrutura cibernética de outro Estado. O caso mais impactante de arma cibernética, em CiberRI, é o Stuxnet, que foi descoberto em 2010 e projetado para sabotar as os sistemas informacionais e operacionais das centrífugas de enriquecimento de urânio do programa nuclear iraniano; desde então, esse verme de computador (*worm*) é conhecido, pela literatura especializada, como a primeira e mais poderosa arma cibernética de que se tem notícia. <<Cf. Introdução e Capítulos 1 e 6>>

Bit: acrônimo diminuto de *binary digit* (dígito binátio), representa a menor unidade de informação a ser armazenada ou transmitida em meios computacionais, sendo valorada em 0 ou 1 de acordo com a variação da carga elétrica, abaixo ou acima de um nível padrão, respectivamente, em cada um dos capacitores dentro de um dispositivo de armazenamento/transmissão. <<Cf. Capítulo 2>>

Bot: abreviatura da palavra *robot* (robô), é um *software* implementado para simular ações humanas em outro *software*, repetidas vezes e de forma padronizada, similar a como faria um robô físico em relação às

ações mecânicas do ser humano. Nesse sentido, uma *botnet* é o conjunto de *bots* conectados em rede com o propósito de trabalharem de maneira conjunta e distribuída, amplificando o alcance de suas ações e ataques. <<Cf. Capítulo 2>>

CERT: sigla de *Computer Emergency Response Team*. Tais centros existem por todo o mundo para tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet. <<Cf. Capítulos 5 e 7>>

Ciberespaço | espaço cibernético: ambiente virtual por excelência, ou seja, que não necessita da presença física ("real") para haver trocas comunicacionais e informacionais. O termo surgiu pela primeira vez em 1984 no livro "*Neromancer*", de William Gibson. No âmbito de CiberRI, ele pode exprimir diversas concepções de espaço cibernético. Por exemplo, para a caserna estadunidense, trata-se de um novo domínio (como ar, mar, terra e espaço sideral) a ser dominado militarmente; já para o Ministério da Defesa, refere-se a um setor estratégico para o desenvolvimento e a defesa nacionais. <<Cf. todos os Capítulos>>

CiberRI: acrônimo para Relações Internacionais Cibernéticas, que exprime o conjunto de pressupostos ontológicos, epistemológicos e metodológicos – geralmente oriundos de Ciências Sociais e da Computação, em especial Relações Internacionais e Redes de Computadores – aplicados com o intuito de explicar, descrever, prescrever ou prever um acontecimento internacional. <<Cf. Introdução>>

Código-fonte: conjunto de símbolos e instruções inteligíveis por um ser humano, escritos na sintaxe de uma linguagem de programação existente, com o objetivo de resolver, de maneira lógica e ordenada, um determinado problema computacional. É a forma original de um

programa de computador em um estágio antes de ser traduzido em linguagem de máquina ou de programação. <<Cf. Capítulos 3, 4, 5, 6>>

Cracker: indivíduo que "quebra" códigos-fonte e sistemas informáticos de detecção de intrusos, a fim de obter qualquer tipo de vantagem. Geralmente confundido com a figura do *hacker*. <<Cf. Capítulos 6 e 7>>

Crime Cibernético | Cibercrime: infração ou ato ilegal praticado a partir de – ou em – um dispositivo computacional (PC, *smartphone*, *notebook* etc.) contra sistemas e dados informáticos. No âmbito do Conselho da Europa, existe a famosa Convenção de Budapeste sobre Cibercrimes, de 2001. <<Cf. Introdução e Capítulos 2, 5, 6 e 7>>

(D)DoS: sigla para designar o tipo de ataque cibernético identificado pela causação da negação de serviço (*denial of service*), que se constitui de inúmeras tentativas sucessivas para forçar a sobrecarga de um computador – geralmente, um servidor-*web* –, fazendo com que seus serviços fiquem inutilizados para seus usuários externos e/ou mantenedores internos. Fala-se também do ataque distribuído de negação de serviço (DDoS), um tipo de ataque cibernético que tem o mesmo fito do ataque DoS, mas que, por meio de um único computador-mestre, consegue "escravizar" as demais máquinas "zumbis", as quais direcionam os ataques em um único alvo. Nesse sentido, uma única pessoa pode ser responsável por vários ataques originados de um DDoS. É o que a literatura de CiberRI tem dito sobre as características dos ataques sofridos pela Estônia em 2007, a mando supostamente pelo governo russo. <<Cf. Capítulos 5 e 6>>

Defesa Cibernética | Ciberdefesa: conjunto de ações estrategicomilitares tomadas e executadas no ciberespaço. Assim como ocorre com os

conceitos de Segura e Defesa, há certa confusão, na literatura de CiberRI, entre os conceitos de Segurança Cibernética e Defesa Cibernética. Todavia, a analogia entre Segurança e Defesa parece ser a que mais se adequa: para a segurança (fim) de um Estado, mecanismos defensivos (meio) são necessários; para a consecução da Segurança Cibernética, mecanismos de Defesa Cibernética (como armas cibernéticas, *firewalls*, antivírus, guerreiros cibernéticos, centros de defesa cibernética etc.) são necessários. Nesse prisma, esta está contida naquela. <<Cf. Introdução e Capítulos 1, 2, 3, 5 e 6>>

Drone: veículo aéreo não tripulado (VANT) com o objetivo estratégico de identificar alvos e, em alguns casos, realizar disparos de projéteis bélicos. Pode-se dizer que, no que concerne aos estudos de CiberRI, as operações militares dos Estados Unidos para desmantelar a Al-Qaeda no Paquistão são consideradas o *leading case* para se discutir os limites do uso de tal instrumento tecnológico. <<Cf. Capítulo 4>>

Endereço IP | número IP: identificação numérica exclusiva – em sua sexta versão conhecida como IPv6 – de um equipamento conectado a uma rede de computadores. <<Cf. Capítulo 2>>

Estrutura estratégica (nacional): designação, que está dando lugar às chamadas infraestruturas críticas, para um sistema ou serviço essencial para um determinado Estado, tais como: hidrelétrica, usina nuclear, serviços de emergência, sistemas bancário, telecomunicacional, de transporte aéreo, de defesa, policial etc. <<Cf. Capítulos 1, 2, 5, 6 e 7>>

Governança da Internet: processo de discussão de medidas técnicas e, sobretudo, políticas sobre o desenvolvimento da Internet, que está

sendo levado a cabo pelos três setores (governo, empresas privadas e sociedade civil) de vários países isoladamente e no âmbito das Nações Unidas, por meio do seu Fórum de Governança da Internet (IGF). No âmbito das CiberRI brasileiras, o próprio Itamaraty possui uma obra específica sobre o assunto. <<Cf. Introdução e Capítulo 7>>

Guerra Cibernética | Ciberguerra: modalidade conflituosa entre dois ou mais Estados, com o objetivo estratégico de acessar o dado negado e/ou causar dano (material, moral ou virtual) a determinada estrutura estratégia nacional, utilizando, para tal, o ambiente cibernético. Apesar de um termo ser usado, *lato sensu*, para designar qualquer ataques cibernético – principalmente o da intrusão –, pode-se dizer que, até o momento, não houve nenhuma guerra cibernética *stricto sensu*. Todavia, o caso dos ataques cibernéticos russos a estruturas estratégicas de TIC da Estônia antes da invasão por tanques, em 2008, demonstra a importância que o tema tem despertado nos âmbitos civis e militares. <<Cf. Introdução e Capítulos 1, 2, 3, 4, 5 e 6 >>

Hacker: pessoa geralmente autodidata em assuntos ligados à Ciência da Computação e que compartilha seus feitos na Internet, a fim de obter satisfação própria por seus feitos. Não se pode dizer que um *hacker* faz suas descobertas apenas por prazer, pois já se tornaram corriqueiras as competições patrocinadas por empresas e governos que gratificam o *hacker* por suas descobertas na área de Segurança da Informação. <<Cf. Capítulo 6>>

Hacktivismo: prática de *hackear* ou invadir sistemas e dispositivos informáticos, alegando motivação política e/ou social. São exemplos de grandes eventos sociopolíticos que tiveram participação importante

de hacktivistas: o chamado Protestos de Junho, em 2013 no Brasil, e a Primavera Árabe, que ocorre desde 2010 nos Oriente Médio e na África setentrional. <<Cf. Introdução, Capítulos 2, 3 e 5>>

Internet: principal sistema de interconexão de redes de computadores do mundo, que, utilizando-se da e pilha de protocolos TCP/IP. Também conhecida como a Rede das Redes e *Web*. <<Cf. Introdução e todos os Capítulos>>

Interpol: abreviatura da *International Criminal Police Organization*, uma organização internacional responsável pela cooperação entre polícias de países diferentes. Dentre suas várias frente de atuação, destaca-se a de combate a Crimes Cibernéticos, por meio do seu *Cyber Fusion Centre* e do *Digital Forensic Laboratory*.<<Cf. Introdução e Capítulo 5>>

Malware: conurbação de "*software* malicioso" que se refere a uma praga virtual projetada para se infiltrar ilicitamente em um sistema ou dispositivo computacional alheio com o intuito de causar danos e/ou de obter o dado negado ou a informação ocultada. <<Cf. Capítulos 5, 6 e 7>>

Segurança Cibernética | Cibersegurança: conjunto de medidas oriundas da Segurança da Informação – daí que os atributos de confidencialidade, integridade e disponibilidade são tidos como os mais importantes, dentre aqueles imprescindíveis para a salvaguarda da informação – adotadas para o combate e a prevenção dos denominados crimes cibernéticos. No âmbito do poder público, tal conjunto é tomado no nível político; na iniciativa privada, pode ser implementada por qualquer indivíduo, grupo ou empresa. Todavia, seu uso em CiberRI parece se voltar mais para uma metáfora em que os elementos "segurança" (sensação de

proteção de uma sociedade que necessita de mecanismos de Segurança e Defesa) e "cibernética" se unem sob um forte viés "securitizatório". <<Cf. Introdução e Capítulos 1, 2, 3, 5, 6 e 7>>

Segurança da Informação: conjunto de medidas que visam a manter as autenticidade, confidencialidade, disponibilidade e integridade da informação. No âmbito nacional, é utilizada tanto por profissionais que trabalham diretamente com a manutenção de serviços e dispositivos relacionados às tecnologias da informação e comunicação (TIC), como também por peritos forenses e profissional dos serviços de Inteligência militares e civis. <<Cf. Introdução e Capítulos 1, 5 e 7>>

TCP/IP: sigla para Protocolo de Controle de Transmissão sobre Protocolo de Internet (*Transmission Control Protocol/Internet Protocol*), é, na realidade, uma pilha de protocolos que permite que os mais diversos e diferentes dispositivos (computadores, *smartphones*, impressoras etc.) conectem-se entre si e consigam "falar" a mesma língua, independentemente do meio (fio, cabo etc.) ou do fabricante. <<Cf. Capítulo 3>>

TIC: sigla para tecnologias de informação e comunicação, que designa o conjunto de tecnologias consideradas novas, pois se baseiam nas principais descobertas provenientes da Revolução da Informação – ou Terceira Revolução Industrial – que garantiu, dentre outros, maior poder de processamento e diminuição de tamanho aos *microchips*. Por meio delas, é possível haver instantaneamente nos dias atuais a comunicação de e o acesso a dados. <<Cf. Introdução e todos os Capítulos>>

Vírus: *malware* que possui a característica de infectar um programa hospedeiro, de quem necessita para se replicar e se espalhar para

outros computadores, utilizando-se de diversos meios possíveis. <<Cf. Capítulos 1 e 6>>

Worm: *malware* independente e autorreplicante que não necessita de uma máquina ou sistema hospedeiro para executar suas próprias ações. O caso mais emblemático, para a literatura de CiberRI, de utilização dessa praga virtual é o Stuxnet. <<Cf. Capítulos 1 e 6>>

WWW: sigla de *World Wide Web* ou Rede Mundial de Computadores, é um sistema de arquivos de hipermídia – áudio, vídeo, imagem, texto e hipertexto – interligados, que é executado na Internet e consumido pelos usuários finais por intermédio de um programa de computador (*software*) chamado navegador-*web* (*browser*). <<Cf. Capítulo 2>>

Referências de estudo em CiberRI

Abaixo, algumas sugestões de leitura são listadas para o leitor que deseja se aprofundar mais nos estudos que cercam as Relações Internacionais Cibernéticas (CiberRI). Antes, porém, algumas observações.

A listagem *infra* é meramente exemplificativa, fazendo, consequentemente, com que outras obras fiquem de fora.[1]

São elencadas referências voltadas mais aos Estudos Estratégicos e de Segurança Internacional englobados pelo amplo espectro de CiberRI. Portanto, não estão incluídas as inúmeras referências possíveis ao estudo no âmbito da CiberRI, tais como: ciberespaço-Economia, ciberespaço-Sociologia, ciberespaço-Direito etc.

As referências estão separadas alfabeticamente pela primeira letra do nome do(s) autor(es), e, dentre elas, em negrito, aquelas que têm merecido maior destaque na literatura analisada.

Todos os *links* foram acessados em 8 fev. 2015.

A

1. Abigail Hall e Christopher Coyne, "The political economy of *drones*", *Defense and Peace Economics* (2013).

1 Uma lista complementar pode ser obtida em: https://staff.washington.edu/dittrich/cyberwarfare.html.

2. Agência Europeia para a Segurança das Redes e da Informação (ENISA), "Abordagem Gradual de Criação de uma CSIRT" (2006), https://www.enisa.europa.eu/activities/cert/support/guide/files/csirt-setting-up-guide-in-portugese/at_download/fullReport.
3. Akamai, "State of the Internet Report" (2º trim. 2014), http://www.akamai.com/dl/akamai/akamai-soti-q214.pdf.
4. Alemanha, *Cyber Security Strategy for Germany* (Berlim: Federal Ministry of the Interior, 2011).
5. Alexandre César Cunha Leite e Ahmina Raiara Solsona Oliveira, "Conflitos Cibernéticos: um overview sobre a participação asiática recente", *Meridiano 47*, Vol. 15, N. 144, 3-9 (jul.-ago. 2014), http://periodicos.unb.br/index.php/MED/article/view/10273/8391.
6. Aloísio Mercadante, "As razões do diálogo com os hackers", *Folha de São Paulo*, São Paulo, 11 ago. 2011, p. 3.
7. Amy Chang, "Warring State: China's Cybersecurity Strategy" (2014), http://cnas.org/sites/default/files/publications-pdf/CNAS_WarringState_Chang.pdf.
8. André M. C. Dutra, "Introdução à guerra cibernética", in *IX Simpósio de Guerra Eletrônica* (2007), http://www.sige.ita.br/anais/IXSIGE/Artigos/GE_39.pdf.
9. Andrew F. Krepnevich, *Cyber warfare: a "nuclear option"?* (Washington, DC: Center for Strategic and Budgetary Assessment, 2012).
10. Arne Schönbohm, *Germany's security: cyber crime and cyber war* ([s.l.]: Verlagshaus Monsenstein und Vannerdat OHG, 2012).
11. Arthur Cerebrowsky, "Military Responses to the Informational Age", *The RUSI Journal*, Vol. 145, No. 5 (2000).
12. Arthur K. Cebrowski e John J. Garstka, "Network Centric Warfare: its origins and future", *Proceedings,* U.S. Naval Institute,

Vol. 124, No. 1, 1998.
13. Assis Medeiros, *Hackers: entre a ética e a criminalização* (Florianópolis: Visual Books, 2002).
14. Axel Lehmann, Vladimir Briktov e Jacques Bus, "Technology Trends and Threats", in *The Quest for Cyber Peace*, ed. Hamadoun Touré (Genebra: UIT, 2011).

B

15. Benjamin Kang Lim, "China says it's hard to resume cyber security talks with U.S.", *Reuters*, 19 out. 2014, http://reuters.com/article/2014/10/19/us-china-usa-cybersecurity-idUSKCN0I80GU20141019.
16. Benjamin Sutherland, ed, *Modern warfare, intelligence and deterrence: the technologies that are transforming them* (Nova Jérsei: Wiley e The Economist, 2012).
17. Boldizsár Bencsáth, Gábor Pék, Levente Buttyán e Márk Félegyház, *Duqu: a Stuxnet-like malware found in the wild* (Budapeste: CrySyS at the Budapest University of Technology and Economics, 2011).
18. Bonnie Adkins, "The spectrum of Cyberconflict: from hacking to information warfare. What is law enforcement's role" (2001), http://www.dtic.mil/dtic/tr/fulltext/u2/a406949.pdf.
19. Boone Bartholomees Jr., *The US Army War College guide to National Security Issue*s, Vol. 1, 4ª Ed (Washington, DC: Strategic Studies Institute, 2010).
20. Brasil, Instrução Normativa GSI Nº 1, de 13 de junho de 2008. Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências (Brasília: Gabinete de Segurança Institucional da Presidência da República, 18 jun. 2008).

21. Brasil, "Laboratório de Defesa Cibernética do IME", http://defesacibernetica.ime.eb.br.
22. Brasil, Portaria Nº 3.389/MD, de 21 de dezembro de 2012. Dispõe sobre a Política Cibernética de Defesa. *Diário Oficial [da] República Federativa do Brasil*, Poder Executivo, Brasília, DF, 27 dez. 2012. Seção 1, p. 11-12.
23. Brasil, *Política Nacional de Defesa (PND) e Estratégia Nacional de Defesa (END)* (Brasília: Ministério da Defesa, 2012), http://www.defesa.gov.br/arquivos/estado_e_defesa/END-PND_Optimized.pdf.
24. Brian Sullivan, *Regional efforts to strengthen cybersecurity in Americas* (Porto de Espanha: Internet Governance Forum, 2011).
25. Bruno Lupion, "Exército se arma para defender o espaço cibernético brasileiro", Estadão.com.br, São Paulo, 8 jun. 2011, http://www.estadao.com.br/noticias/nacional,exercito-se-arma-para-defender-o-espaco-cibernetico-brasileiro,729291,0.htm.

C

26. Canadá, *Canada's Cyber Security Strategy* (Ottawa: Department of Public Safety, 2010).
27. _____, *Un cadre de sécurité civile pour le Canada*, 10ª Ed. (Ottawa: Sécurité publique Canada, jan. 2011).
28. Carlos A. Afonso, org, *Governança da Internet: contexto, impasses e caminhos* (São Paulo: Peirópolis; Rio de Janeiro: RITS, 2005).
29. Catherine Hart, "Mobilizing the Cyberspace Race: the Securitization of the Internet and its Implications for Civil Liberties", *Cyber-Surveillance in Everyday Life: an International Workshop* (Toronto: Universidade de Toronto, 2011).
30. Charles Billo e Welton Chang, *Cyber Warfare: An Analysis of*

the Means and Motivations of Selected Nation States (Hanover: Institute for Security Technology Studies, 2004).

31. Christopher Bellamy, "What is information warfare?", in *Managing the revolution in military affairs,* org. Ron Matthews e John Treddenick (Nova Iorque: Palgrave, 2001), 56-75.
32. Christopher Holloway, "El Plan Argentino para su ciberseguridad", *América Economía*, 26 set. 2011, http://tecno.americaeconomia.com/articulos/el-plan-argentino-para-su-ciberseguridad.
33. **Colin S. Gray, *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling* (Washington, DC: US Army, 2013), http://www.strategicstudiesinstitute.army.mil/pubs/download.cfm?q=1147.**
34. **Conselho da Europa, "Convenção sobre o Cibercrime" (2001), http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_Portugese.pdf.**
35. Cory Bennett, "US, China see little progress on cybersecurity", *The Hill*, 12 nov. 2014, http://thehill.com/policy/cybersecurity/223865-us-china-see-little-progress-on-cybersecurity.
36. Cristian Borghello e Marcelo Temperini, "Seguridad o inseguridad informática. Ciberseguridad Nacional Argentina: Cracking de Servidores de la Administración Pública", in *13° Simposio Argentino de Informática y Derecho de las 42° Jornadas Argentinas de Informática*, Ciudad de Córdoba (16-20 set. 2013).
37. Cristina Tavares e Milton Seligman, *Informática: a batalha do século XXI* (Rio de Janeiro: Paz e Terra, 1984).

D

38. Daniel Kuehl, "From Cyberspace to Cyberpower: Defining the Problem", in *Cyberpower and National Security*, ed. Franklin

Kramer, Stuart Starr e Larry Wentz (Washington, DC: National Defense University Press, 2009).
39. Daniel Oppermann, "Virtual attacks and the problem of responsibility: the cases of China and Russia", *Carta Internacional*, Vol. 5, No. 2 (dez. 2010), 11-25.
40. David E. Sanger, *Confront and conceal: Obama's secret wars and surprising use of American power* (Nova Iorque: Crown: 2012).
41. _____. "Obama order sped up wave of cyberattacks against Iran", *The New York Times*, 1 jun. 2012, http://nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.
42. DefesaNet, "Cyberwar", http://www.defesanet.com.br/cyberwar.
43. Fernando A. Demeterco, "Segurança das infraestruturas críticas", in *X Ciclo de Estudos Estratégicos* (Rio de Janeiro: Escola de Comando e Estado-Maior do Exército – ECEME, 2011), http://eceme.ensino.eb.br/meiramattos/index.php/RMM/article/viewFile/197/166.
44. Derek Gregory, "From a View to a Kill: Drones and Late Modern War", *Theory, Culture & Society*, No. 28, 188-215 (2011).
45. Derek Reveron, ed, *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World* (Washington, DC: Georgetown University Press, 2012).
46. Desmond Ball, "China's Cyber Warfare Capabilities", *Security Challenges*, Vol. 7, No. 2, 81-103 (Winter 2011).
47. Edward Wong, "For China, Cybersecurity Is Part of Strategy for Protecting the Communist Party", *The New York Times*, 3 dez. 2014, http://sinosphere.blogs.nytimes.com/2014/12/03/for-china-cybersecurity-is-part-of-strategy-for-protecting-the-communist-party.

E

48. Eneken Tikk, *Ten rules for cybersecurity* (Tallinn, NATO CCDCOE, 2011).
49. Érico Duarte, "Conduta da guerra na era digital e suas implicações para o Brasil: uma análise de conceitos, políticas e práticas de defesa", *Texto para discussão*, Rio de Janeiro, n. 1760, IPEA, ago. 2012.
50. Espanha, *El ciberespacio: nuevo escenario de confrontación* (Madri: Ministerio de Defensa, 2012).
51. Estados Unidos da América, *International Strategy for Cyberspace: prosperity, security, and opennessin a networked world* (Washington, DC: The White House, maio 2011), http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.
52. _____, *National Strategy to Secure Cyberspace* (Washington, DC: Department of Defense, 2003), https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.
53. _____, *Strategy for Operating in Cyberspace* (Washington, DC: Department of Defense, 2011), http://defense.gov/news/d20110714cyber.pdf.
54. _____, *The National Defense Strategy* (Washington, DC: Department of Defense, 2005), http://www.defense.gov/news/mar2005/d20050318nds1.pdf.
55. Everton Lucero, *Governança da Internet: aspectos da formação de um regime global e oportunidades para a ação diplomatica* (Brasília: FUNAG, 2011).

F

56. Filipe D. C. Alves, "EU Law and Internet Traffic Control Lost Between Privacy Rights and Freedom of Individual and Corporate Enterprise", in *Proceedings of the 11th European Conference on Information Warfare and Security* (Reading: API, 2012).

57. França, *Défense et sécurité des systèmes d'information: stratégie de la France* (Paris: Agence nationale de la sécurité des systèmes d'information, 2011).

G

58. Geórgia, "Russian invasion of Georgia: Russian cyberwar on Georgia" (2008), http://www.mfa.gov.ge/files/556_10535_798405_Annex87_CyberAttacks.pdf.
59. Gills Lopes, "Análise sobre o Impacto das Novas Tecnologias de Informação e Comunicação nas Estratégias Nacionais de Defesa e Segurança Cibernéticas do Século XXI", *III Simpósio de Pós-Graduação em Relações Internacionais do Programa "San Tiago Dantas"* (nov. 2011).
60. _____, "A cibersociedade anárquica: análise do uso das Tecnologias de Informação e Comunicação nos conflitos internacionais do século XXI à luz da Escola Inglesa de Relações Internacionais" (*Monografia do Curso de Relações Internacionais*, Universidade Estadual da Paraíba, 2010).
61. _____, "A emergência do tema ciberguerra: contextualizando a criação do Centro de Defesa Cibernética à luz da Estratégia Nacional de Defesa", in *Artigos do* 6º *Seminário do Livro Branco de Defesa Nacional* (Brasília: Ministério da Defesa, 2011).
62. **_____, "Reflexos da digitalização da guerra na política internacional do século XXI: uma análise exploratória da securitização do ciberespaço nos Estados Unidos, Brasil e Canadá", (*Dissertação de Mestrado em Ciência Política*, Universidade Federal de Pernambuco, 2013).**
63. **_____ e Dalliana Vilar Pereira, "A Convenção de Budapeste e as leis brasileiras", in *Seminário Cibercrime e Cooperação Penal Internacional* (João Pessoa, CCJ-UFPB, 2009), http://www.**

mpam.mp.br/centros-de-apoio-sp-947110907/combate-ao-crime-organizado/doutrina/574-a-convencao-de-budapeste-e-as-leis-brasileiras.

64. Gills Lopes e Marcelo de A. Medeiros, "Da cibersegurança à ciberdefesa Americana: a Diplomacia da Internet como instrumento de proteção e de integração dos estados da OEA", in *3° Encontro Nacional ABRI* (São Paulo, ABRI, 2011), http://www.proceedings.scielo.br/scielo.php?script=sci_arttext&pid=MSC0000000122011000200017.
65. Greg Rattray, Chris Evans e Jason Healey, "American Security in the Cyber Commons", in *Contested Commons: the Future of American Power in a Multipolar World*, Abraham M. Denmark e James Mulvenon, eds (Washington, DC: Center for a New American Security, 2010), 139-175.

H

66. Héctor Flores, org, *Los ámbitos no terrestres de la guerra futura: ciberespacio*-aeroespacio (Buenos Aires: Gabinete de Estrategia Militar del Estado Mayor Conjunto de las Fuerzas Armadas, 2011).
67. Helen Nissenbaum, "Where Computer Security Meets National Security", *Ethics and Information Technology,* No. 7 (2005), 61-73.
68. Hérodote, "Cyberespace: enjeux géopolitiques" (1º-2º semest. 2014), http://www.herodote.org/spip.php?rubrique66.

I

69. I Seminário de Relações Internacionais Cibernéticas – CiberRI-UFPB, João Pessoa (2014), http://www.ccsa.ufpb.br/dri/CiberRI.
70. Igor D. P. Acácio, "Segurança Cibernética: Análise sobre a Política de Defesa Brasileira (2000-2011)", (*Monografia de Relações*

Internacionais, Niterói: Universidade Federal Fluminense, 2011).
71. Igor D. P. Acácio e Gills Lopes, "Segurança internacional no século XXI: o que as teorias de Relações Internacionais têm a falar sobre o ciberespaço?", *Anais do 36º Encontro Anual da ANPOCS* (Caxambu: ANPOCS, 2012), http://www.anpocs.org/portal/index.php?option=com_docman&task=doc_details&gid=8169&Itemid=76.
72. Instituto das Nações Unidas para a Investigação sobre o Desarmamento, *Cyber Index* (Genebra: ONU, 2013).
73. International Human Rights and Conflict Resolution Clinic at Stanford Law School e Global Justice Clinic at NYU School of Law. *Living under Drones: Death, Injury, and Trauma to Civilians from US Drone Practices in Pakistan* (2012).
74. Irã, "Iran calls for IAEA to detect Stuxnet agents", *Iranian Student's News Agency*, Teerã, 13 Jun. 2011, http://isna.ir/en/news/9003-14857/Iran-calls-for-IAEA-to-detect-Stuxnet-agents.
75. International Organization for Standardization e International Electrotechnical Commission, *ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security management* (Suíça: ISO/IEC, 2005).

J

76. James A. Lewis, "The 'Korean' Cyber Attacks and Their Implications for Cyber Conflict" (2009), http://dspace.africaportal.org/jspui/bitstream/123456789/26510/1/The%20Korean%20Cyber%20Attacks%20and%20Their%20Implications%20for%20Cyber%20Conflict.pdf.
77. James C. Mulvenon, "The PLA and Information Warfare", in *The People's Liberation Army in the Information Age*, ed J. C. Mulvenon e Richard H. Yang, eds, 175-186 (Washington, DC: RAND, 1999).

78. Jan-Frederik Kremer e Benedikt Müller, eds, *Cyberspace and International Relations* (Berlin: Springer, 2014).
79. Jason Andress e Steve Winterfeld, *Cyber warfare: techniques, tactics and tools for security practitioners* (Boston: Syngress/ Elsevier, 2011).
80. Jeffrey Carr, *Inside cyber warfare* (Sebastopol, CA: O'Reilly, 2009).
81. Jessica Ramirez, "All is not quiet on the digital front", *Newsweek*, 20 abr. 2010, http://www.newsweek.com/2010/04/20/all-is-not-quiet-on-the-digital-dront.html.
82. Johan Eriksson e Giampiero Giacomello, "International Relations, Cybersecurity, and Content Analysis: a Constructivist approach", in *The Global Politics of Science and Technology - Vol. 2*, ed. Maximilian Mayer, Mariana Carpes e Ruth Knoblich (Berlim: Springer, 2014), 205-219. d.o.i.: 10.1007/978-3-642-55010-2_12.
83. John Arquilla e David Ronfeldt, "Cyberwar is coming!", *Comparative Strategy*, Vol. 12, No. 2, p. 141-165 (Spring 1993).
84. John Arquilla e David Ronfeldt, eds, *Athena's Camp: preparing for conflict in the information age* (Santa Monica, CA: RAND Corporation, 1997).
85. Jorge Bessa, *O escândalo da espionagem no Brasil: o caso Snowden* (Brasília: Thesaurus, 2014).
86. José Miguel Quedi Martins, *Digitalização e Guerra Local como Fatores do Equilíbrio Internacional* (Tese de doutorado, Universidade Federal do Rio Grande do Sul, 2008).
87. Joseph S. Nye Jr., "Cyber Insecurity", *Project Syndicate* (10 dez. 2008), http://project-syndicate.org/commentary/cyber-insecurity.
88. _____, "Foreword", in *Securing cyberspace: a new domain for national Security*, ed. Nicholas Burns e Brent Scowcroft (Washington, DC: Aspen Institute, 2012), 11-13.

89. _____, "Nuclear lessons for cyber security?", Strategic Studies Quarterly, Vol. 5, No. 4, 18-37 (2011).
90. _____, *The future of power* (Nova Iorque: PublicAffairs, 2011), Cap. 5.
91. Julian Assange, *Cyberpunks: Liberdade e o Futuro da Internet* (São Paulo: Boitempo Editorial, 2013).

K

92. K. Saalbach, *Cyber war: methods and practice* (Osnabrück: Universität Osnabrück, 2012, Version 9.0, 17 jun. 2014), http://www.dirk-koentopp.com/downloads/saalbach-cyberwar-methods-and-practice.pdf.
93. Kai E. Lehmann, "Unfinished Transformation: the three phases of complexity's emergence into International Relations and foreign policy", *Cooperation and Conflict*, Vol. 47, No. 3, 404-413 (2012).
94. Keith Shimko, *The Iraq Wars and America's Military Revolution* (Nova Iorque: Cambridge University Press, 2010).
95. Kevin Newmeyer, "The challenge of Cybersecurity for the Caribbean: what are the policy options?, Security and Defense Studies Review, Vol. 15 (2014), 60-77.
96. Konrand Adenauer Stiftung e CEBRI, *International Security: a European-South American dialogue* (Rio de Janeiro: Konrand Adenauer, 2014), 95-126, 167-181, 229-242, 255-267.

L

97. Làmber Royakkers e Rinie Van Est, "The Cubicle Warrior: The Marionette of Digitalized Warfare", *Ethics and Information Technology*, Vol. 12, No. 3 (2010).
98. Leandro Loyola, "General José Carlos dos Santos: 'Podemos recrutar hackers'". *Época*, 15 jul. 2011, http://revistaepoca.globo.com/Revista/Epoca/0,,EMI249428-15223,00-GENERAL+JOSE

+CARLOS+DOS+SANTOS+PODEMOS+RECRUTAR+HACKERS.html.

99. Lene Hansen e Helen Nissenbaum, "Digital disaster, cyber security and the Copenhagen School", *International Studies Quarterly*, No. 53 (2009), 1555-1575.

100. Leonard Kleinrock, "History of the Internet and its flexible future", *IEEE Wireless Communications* (2008), 8-18.

101. Lewis University, "The History of cyber warfare" (2010), http://online.lewisu.edu/images/the-history-of-cyber-warfare-infographic.jpg.

102. Li Zhang, "A Chinese Perspective on Cyber War", *International Review of Red Cross*, Vol. 94, Issue 886, pp 801-807 (jun. 2012), http://journals.cambridge.org/abstract_S1816383112000823.

M

103. Magnus Hjortdal, "China's Use of Cyber Warfare: espionage meets strategic deterrence", *Journal of Strategic Security* 4, No. 2 (2011), 1-24.

104. Marcelo Bezerra, "Artigo sobre Guerra Cibernética 'Cyberwar'", DSIC/DSI-PR, 2009, http://dsic.planalto.gov.br/artigos/71-artigo-sobre-guerra-cibernetica-qcyberwarq.

105. Marcelo de A. Medeiros e Gills Vilar Lopes, "O Ciberespaço na Agenda da Segurança Internacional Contemporânea", in Relações internacionais contemporâneas: teorias e desafios, org Thales Castro, 139-152 (Curitiba: Íthala, 2014).

106. Marcelo Ninio, "A internet é um barril de pólvora", *Folha de S. Paulo*, 29 jul. 2012, http://www1.folha.uol.com.br/ilustrissima/1127046-a-internet-e-um-barril-de-polvora.shtml.

107. Margaret Wertheim, *Uma história do espaço de Dante à Internet* (Rio de Janeiro: Zahar, 2001).

108. Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Mônica, CA: Rand Corporation, 2009).
109. Mary E. O'Connell, "Seductive Drones: Learning from a Decade of Lethal Operations", *Journal of Law, Information & Science* (2011), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1912635.
110. Mary MacEvoy Manjikian, "From global village to virtual battlespace: the colonizing of the Internet and the extension of Realpolitik", *International Studies Quarterly,* Vol. 54, No. 2, 381-401 (2010).
111. Maximilian Mayer, Mariana Carpes e Ruth Knoblich, eds., *The Global Politics of Science and Technology - Vol. 2* (Berlim: Springer, 2014).
112. McAfee, "Virtual Criminology Report" (2009), http://www.mcafee.com/us/resources/reports/rp-virtual-criminology-report-2009.pdf.
113. Michael Benedikt, ed, *Cyberspace: first steps* (Cambridge, MA: MIT Press, 1991).
114. Michael O'Hanlon, *Technological Change and the Future of Warfare* (Washington, DC: Brookings Institution Press, 2000).
115. Michael Portnoy e Seymour Goodman, *Global initiatives to secure cyberspace: an emerging landscape* (Nova Iorque: Springer, 2009).
116. Michael Schmitt, ed, *Tallinn Manual on the International Law applicable to cyber warfare* (Cambridge, UK: Cambridge University Press e CCDCOE/NATO, 2013).
117. Myrian D. Cavelty, "Cyberwar: concept, status quo and limitations", *CSS Analysis in Security Policy*, Issue 71, 2010.
118. _____, V. Mauer e S.F. Krishna-Hensel, eds, *Power and Security in the Information Age* (Hampshire: Ashgate, 2007).

N

119. N. Schwartz, "The challenge of cyberspace", in *X National Symposium on Homeland Security and Defense* (2010), http://af.mil/shared/media/document/afd-101102-046.pdf.
120. Neil Rowe e Simson Garfinkel, "Finding Suspicious Activity on Computer Systems", in *Proceedings of the 11th European Conference on Information Warfare and Security* (Reading: API, 2012).
121. Nicholas Burns e Brent Scowcroft, eds, *Securing cyberspace: a new domain for national Security* (Washington, DC: Aspen Institute, 2012).
122. Nick Hopkins, "Stuxnet attack forced Britain to rethink the cyber war", *The Guardian*, Londres, 30 maio 2011, http://www.guardian.co.uk/politics/2011/may/30/stuxnet-attack-cyber-war-iran.
123. _____, "UK developing cyber-weapons programme to counter cyber war threat", *The Guardian*, Londres, 30 maio 2011, http://www.guardian.co.uk/uk/2011/may/30/military-cyberwar-offensive?intcmp=239.
124. Nicolas Falliere et al., *W32.Stuxnet Dossier* (Cupertino, CA: Symantec Corporation, 2011).
125. Nigel Inkster, "Chinese Intelligence in the Cyber Age", *Survival Global, Politics and Strategy*, Vol. 55, No. 1 (fev.-mar. 2013).

O

126. O Debatedouro, Vol. 1, No. 84, maio 2014, http://odebatedouro.com.
127. Open Empowerment Initiative, *Cyberspace & Open Empowerment in Latin America* (Rio de Janeiro: Instituto Igarapé; Ottawa: The SecDev Foundation, 2013).
128. Organization of American States e Trend Micro, "Brazil: Cybersecurity Challenges Faced by a Fast Growing Market Economy" (2013), http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-brazil.pdf.

129. Oscar Medeiros Filho, Walfredo B. Ferreira Neto e Selma L. de M. Gonzales, orgs, *Segurança e Defesa Cibernética: das fronteiras físicas aos muros virtuais* (Recife: Editora UFPE, 2014).

130. Otávio Santana R. Barros, Ulisses de M. Gomes, Whitney L. de Freitas, orgs, *Desafios estratégicos para a Segurança e Defesa Cibernética* (Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011), http://www.sae.gov.br/site/wp-content/uploads/Seguranca_Cibernetica_web.pdf.

P

131. Paul Carsten e Michael Martina, "Forças armadas da China incentivam cibersegurança e softwares chineses, diz mídia estatal", *Reuters*, 8 out. 2014, http://br.reuters.com/article/internetNews/idBRKCN0HX1MR20141008.

132. Paulo S. M. de Carvalho, "A defesa cibernética e as infraestruturas críticas nacionais", *Apresentações do X Ciclo de Estudos Estratégicos*, Rio de Janeiro (2011).

133. Peter W. Singer, *Wired for war: the robotics revolution and conflict in the 21st century* (Nova Iorque: Penguin, 2010).

134. Pierluigi Paganini, "Panetta is critical of the Security Level on NATO Networks", *Infosec Island*, 23 jan. 2013, http://infosecisland.com/blogview/22872-Panetta-is-Critical-of-the-Security-Level-on-NATO-Networks.html.

Q

135. Qiao Liang e Wang Xiangsui, *Conjecturas sobre a Guerra e a tática na era da Globalização* (Pequim: Pla Literature and Arts Publishing House, 1999).

R

136. Raphael Mandarino Jr, *Um estudo sobre a segurança e a defesa do espaço cibernético*, Monografia de Especialização em Ciência da Computação (Brasília: UnB, 2009), http://dsic.planalto.gov.br/documentos/cegsic/monografias_1_turma/raphael_mandarino.pdf.

137. Raphael Mandarino Jr e Claudia Canongia, *Livro verde: segurança cibernética no Brasil* (Brasília: GSIPR/SE/DSIC, 2010), http://dsic.planalto.gov.br/documentos/publicacoes/1_Livro_Verde_SEG_CIBER.pdf.

138. Richard A. Clark e Robert K. Knake, *Cyber war: The Next Threat to National Security and What to Do About It*, 2. ed. (Nova Iorque: HarperCollins Publishers, 2012).

139. Robert Muggah e Misha Glenny, "Why Brazil Put Its Military In Charge of Cyber Security", *DefenseOne*, 13 jan. 2015, http://defenseone.com/technology/2015/01/why-brazil-put-its-military-charge-cyber-security/102756.

140. Ron Deibert, *Distributed security as cyber strategy: outlining a comprehensive approach for Canada in cyberspace* (Calgary: Canadian Defence & Foreign Affairs Institute – CDFAI, 2012), http://www.cdfai.org/PDF/Distributed%20Security%20as%20Cyber%20Strategy.pdf.

S

141. Sergio G. Eissa, Sol Gastaldi, Iván Poczynok e Elina Z. Di Tullio. "El ciberespacio y sus implicancias para la defensa nacional", *Revista de Ciencias Sociales – Segunda Época*, No. 25 (out. 2014), 181-197, http://www.unq.edu.ar/advf/documentos/53e389d522b6b.pdf.

142. Silvina Chaves, "Guerra cibernética: el nuevo paradigma de Seguridad Informática (2012), http://argentinainvestiga.edu.ar/noticia.php?titulo=guerra_cibernetica:_el_nuevo_paradigma_en_seguridad_informatica&id=1645.
143. Siobhan Gorman e Julian E. Barnes, "Cyber combat: act of war – Pentagon sets stage for U.S. to respond to computer sabotage with military force", *The Wall Street Journal*, 30 maio 2011, http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html.
144. Stanilaw Calandreli, "A batalha russa no ciberespaço" (2011), http://jornalggn.com.br/blog/luisnassif/a-batalha-russa-no-ciberespaco.
145. Stéphane Leman-Langlois, ed, *Technocrime: technology, crime and social control* (Londres : Willan Publishing, 2008).
146. Symantec Corporation, "Symantec Intelligence Report" (dez. 2013), http://symantec.com/content/en/us/enterprise/other_resources/b-intelligence_report_12-2013.en-us.pdf.

T

147. Thomas Rid, "Cyberwar and Peace Hacking Can Reduce Real-World Violence", *Foreign Affairs*, nov.-dez. 2013, http://www.foreignaffairs.com/articles/140160/thomas-rid/cyberwar-and-peace.

U

148. União Europeia, *National cyber security strategies: setting the course for national efforts to strengthen security in cyberspace* (Heraklion: European Network and Information Security Agency – ENISA, 2012).
149. União Internacional de Telecomunicações, *Cybersecurity: The role and Responsibilities of an Effective Regulator* (Beirute: UIT,

2009), http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR-background-paper-on-cybersecurity-2009.pdf.

V

150. Vytautas Butrimas, "National Security and International Policy Challenges in a Post Stuxnet World", *Lithuanian Annual Strategic Review*, Vol. 12, Issue 1 (dez. 2014), 11-31, http://www.degruyter.com/view/j/lasr.2014.12.issue-1/lasr-2014-0001/lasr-2014-0001.xml.

W

151. Walfredo B. Ferreira Neto, "Territorializando o novo e (re) territorializando os tradicionais: a cibernética como espaço e recurso de poder", *Coleção Meira Mattos - Revista das Ciências Militares*, Vol. 1, 07-18 (2014).

152. Wang Pufeng, "The Challenge of Information Warfare", *China Military Science* (Spring 1995), http://www.fas.org/irp/world/china/docs/iw_mg_wang.htm.

153. William J. Broad, John Markoff e David E. Sanger, "Israeli test on worm called crucial in Iran nuclear delay", *The New York Times*, 15 jan. 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all.

154. Wladimir D'Andrade, "Mercadante quer trabalhar com hackers que atacaram sites do governo", *Estadão.com.br*, São Paulo, 27 jun. 2011, http://www.estadao.com.br/noticias/nacional,mercadante-quer-trabalhar-com-hackers-que-atacaram-sites-do-governo,737600,0.htm.

155. William J. Lynn III, "The Pentagon's Cyberstrategy, one year later: defending against the next cyberattack", *Foreign Affairs*, 28 set. 2011, http://www.foreignaffairs.com/articles/68305/william-j-lynn-iii/the-pentagons-cyberstrategy-one-year-later.

Título Relações Internacionais Cibernéticas
Projeto Gráfico Ildembergue Leite
Capa Ildembergue Leite
Revisão de Texto Ana Maria

formato 15,5 x 22,0 cm
fontes Exo, Minion Pro
papel Offset 75 g/m² (*miolo*)
Triplex 250 g/m² (*capa*)

tiragem 200 exemplares - Janeiro 2016
Impressão e Acabamento Oficina Gráfica | EdUFPE
Rua Acadêmico Hélio Ramos, 20, Várzea
Recife, PE | CEP: 50.740-530
Fone: (0xx81) 2126.8397 | Fax: (0xx81) 2126.8395
www.ufpe.br/edufpe | livraria@edufpe.com.br

Ahmina Raiara Solsona Oliveira
Alcides Eduardo dos Reis Peron
Alexandre Cesar Cunha Leite
Candela Justribó
Eduardo Cesar Bohn
Gills Vilar Lopes
Igor Daniel Palhares Acácio
Joanisval Brito Gonçalves
Lucas Ribeiro de Belmont Fonseca
Marcos Aurélio Guedes de Oliveira
Maurício Reis Nothen
Ricardo Borges Gama Neto
Sol Gastaldi
Tiago Medeiros Delgado
Walfredo Bento Ferreira Neto

UNIVERSIDADE FEDERAL DE PERNAMBUCO

ISBN 978-85-415-0633-5