UNIVERSIDADE ESTADUAL DA PARAÍBA
CENTRO DE CIÊNCIAS BIOLÓGICAS E SOCIAIS APLICADAS
PROGRAMA DE PÓS-GRADUAÇÃO EM RELAÇÕES INTERNACIONAIS
(PPGRI)

Ahmina Raiara Solsona Oliveira

O COMPROMETIMENTO ASIÁTICO COM O DESENVOLVIMENTO CIBERNÉTICO DA REGIÃO E A UTILIZAÇÃO SÍNICA DO CIBERESPAÇO COMO EXTENSÃO DE SUA ESTRATÉGIA TRADICIONAL

Orientador: Prof. Dr. Alexandre César Cunha Leite

João Pessoa - PB
2015

AHMINA RAIARA SOLSONA OLIVEIRA

O COMPROMETIMENTO ASIÁTICO COM O DESENVOLVIMENTO CIBERNÉTICO DA REGIÃO E A UTILIZAÇÃO SÍNICA DO CIBERESPAÇO COMO EXTENSÃO DE SUA ESTRATÉGIA TRADICIONAL

Dissertação apresentada ao Programa de Pós-Graduação em Relações Internacionais da Universidade Estadual da Paraíba, em cumprimento às exigências para obtenção do título de Mestre em Relações Internacionais.

Orientador: Prof. Dr. Alexandre César Cunha Leite

João Pessoa - PB
2015

O48c Oliveira, Ahmina Raiara Solsona
O comprometimento asiático com o desenvolvimento cibernético da região e a utilização sínica do ciberespaço como extensão de sua estratégia tradicional [manuscrito] / Ahmina Raiara Solsona Oliveira. - 2015.
91 p. : il.

Digitado.
Dissertação (Mestrado em Relações Internacionais) - Universidade Estadual da Paraíba, Centro de Ciências Biológicas e Sociais Aplicadas, 2015.
"Orientação: Prof. Dr. Alexandre César Cunha Leite, Departamento de Relações Internacionais".

1. Cibernético. 2. Segurança. 3. Desenvolvimento. 4. China. 5. Ásia-Pacífico. I. Título.

21. ed. CDD 303.483 3

AHMINA RAIARA SOLSONA OLIVEIRA

O COMPROMETIMENTO ASIÁTICO COM O DESENVOLVIMENTO CIBERNÉTICO DA REGIÃO E A UTILIZAÇÃO SÍNICA DO CIBERESPAÇO COMO EXTENSÃO DE SUA ESTRATÉGIA TRADICIONAL

Aprovada em 01 de Junho de 2015

BANCA EXAMINADORA

Prof. Dr. Alexandre César Cunha Leite
Orientador-PPGRI/UEPB

Prof. Dr. Paulo Roberto Loyolla Kuhlmann
PPGRI/UEPB

Prof. Dr. Augusto Teixeira Júnior
DRI-CCSA/UFPB

À minha família

William e Valéria – Meus Pais.

Ariadn – Minha Irmã.

Thiago – Meu Esposo.

Pelo amor e carinho,

Dedico

AGRADECIMENTOS

Inicio meus agradecimentos por Deus, que me dá força diariamente e abençoa meus caminhos. Em seguida agradeço à minha família: minha razão de ser e viver.

Por família eu compreendo meu esposo, Thiago Gouveia da Silva, companheiro de vida e amigo de todas as horas. Meu maior e melhor crítico. Meu complemento e minha metade. Obrigada pela paciência, compreensão, pelo incentivo e pela fé depositada.

Compreendo também os meus pais: William Coêlho de Oliveira e Valéria Gomes Solsona de Oliveira, pelos criadores, formadores e cuidadores que ainda são. Agradeço a vocês por todo amor, dedicação e incentivo, por compreender meus estresses e, principalmente, por acreditar em mim mesmo quando eu não acreditava.

Agradeço também à minha irmã, Ariadn Raílla Solsona Oliveira, minha amiga de colo nos momentos de estresse e companheira de alegrias e tristezas. Agraço também pela vida da minha sobrinha: Luna. Minha alegria. Meu presente.

Gostaria de agradecer a toda à equipe da Universidade Estadual da Paraíba e, em especial, às pessoas do Mestrado em Relações Internacionais, professores, amigos, companheiros de batalha e escudeiros fiéis.

Meu muito obrigada ao meu orientador, professor Alexandre César Cunha Leite, que foi de uma paciência inacreditável e me ensinou lições que levarei por toda a vida.

Agradeço aos professores Paulo Kuhlmann, Augusto Teixeira e Gills Lopes, que aceitaram participar da minha banca de defesa ou qualificação e que me ajudaram a organizar minhas ideias e, consequentemente, desenvolver meu trabalho.

Por fim, mas não menos importante, gostaria de agradecer aos meus amigos e familiares que, de uma forma ou de outra, se fizeram presentes nesta minha caminhada, me apoiando e torcendo para que eu terminasse logo de modo a voltar a participar dos encontros nos feriados.

RESUMO

A presença asiática se faz constante nos conflitos cibernéticos com seus países aparecendo como vítimas ou supostos responsáveis. O alto índice de participação em tais modelos de guerra, somado ao fato de países como Rússia, China, Índia, Japão, Paquistão e as Coreias serem considerados possuidores de exército cibernético pelo Pentágono, torna fatível a hipótese de forte envolvimento e compromisso asiático com o desenvolvimento das suas capacidades cibernéticas. Apesar da grande discrepância tecnológica entre os Estados do pacífico asiático, as ameaças comuns fomentaram a cooperação e uniram o continente em busca da sua segurança cibernética. Esta dissertação tem como objetivo explicitar o compromisso asiático com o desenvolvimento cibernético regional e a utilização sínica do espaço cibernético como extensão de seu pensamento estratégico nacional. A metodologia utilizada foi de natureza qualitativa, acrescida do método de estudo de caso aplicado à China. O trabalho está organizado em três capítulos, além de introdução e considerações finais. O primeiro capítulo traz conceitos e definições necessários à compreensão das discussões que circundam o termo cibernético. O segundo capítulo expõe alguns dos conflitos cibernéticos com participação asiática e evidencia três organizações asiáticas que trabalham em busca da segurança cibernética regional. O terceiro capítulo expressa a percepção sínica sobre a guerra cibernética, explica a utilização do espaço cibernético como ferramenta estratégica para seu desenvolvimento militar e econômico e revela suas ações de modo a se preparar para a Era Cibernética. Como resultado principal deste trabalho tem-se que a região pacífico asiática vem gradualmente se envolvendo em conflitos cibernéticos e se comprometendo com a cooperação por uma segurança cibernética comum – inclusive através da elaboração de instrumentos medidores de maturidade cibernética – e que a China vê na guerra cibernética a possibilidade de frustrar ações imperativas por parte de potências militarmente mais fortes e de, por meio da transferência tecnológica, alcançar nível militar similar ao das grandes potências.

Palavras-Chave:

Cibernético. Segurança. Desenvolvimento. China. Ásia-Pacífico.

ABSTRACT

The Asian presence is constant in cyber conflicts and theses countries are appearing as victims or alleged perpetrators. The high rate of participation in such models of war, added to the fact that countries like Russia, China, India, Japan, Pakistan and the Koreas are considered by the Pentagon as possessor of a cyber-army makes feasible the possibility of strong involvement and Asian commitment to the development of cyber capabilities in the region. Despite the strong technological gap between the states of the Asian Pacific, common threats fostered cooperation and united the continent in search for cybersecurity in the region. Therefore, this master's thesis aims to show the Asian commitment to the regional cyber development and the Chinese use of cyberspace as an extension of its national strategic thinking. The methodology is qualitative, with the case study method applied to China. This academic work is organized in three chapters, plus introduction and closing remarks. The first chapter has concepts and definitions we need to understand the discussions surrounding cyber terms. The second chapter sets out some of the cyber conflicts with Asian participation and highlights three Asian organizations working in pursuit of regional cybersecurity. The third chapter expresses the Chinese perception of cyber warfare, explains the use of cyberspace as a strategic tool for its military and economic development, and reveals their actions in order to prepare for the Cyber Age. The main result of this work has been that the Asian Pacific region is gradually getting involved in cyber conflicts and committing to cooperation for a common cyber security – including through the development of measuring tools for the cyber maturity – and that China sees in cyber warfare the possibility to block out impositions by militarily stronger powers and, through technology transfer, to achieve a military level similar to that of the great powers.

Keywords:

Cyber. Safety. Development. China. Asia Pacific.

LISTA DE ACRÔNIMOS

AD	Adido de Defesa
APCERT	Asian Pacific Computer Emergency Response Team
APEC	Asia-Pacific Economic Cooperation
APSIR	Asia Pacific Society for Impotence Research
ARPA	Advanced Research Projects Agency
ARPANET	Advanced Research Projects Agency Network
ASEAN	Association of Southeast Asian Nations
ASPI	Australian Strategic Policy Institute
CARICOM	The Caribbean Community
CERT	Computer Emergency Response Team
CIRTs	Computer Security Incident Response Team
CNE	Computer Network Explotation
DDoS	Distributed Denial of Service
DoS	Denial of Service
ELINT	Inteligência Eletrônica
GOP	Guardians of Peace
GPD	Departamento Político Geral
FBI	Federal Bureau of Investigation
HUMINT	Inteligência Militar Humana
ICPC	ASPI International Cyber Policy Centre
IMINT	Inteligência Militar de Imagens
IW	Information War
MERCOSUL	Mercado Comum do Sul
MIT	Massachusetts Institute of Technology

MPS	Ministério de Segurança Pública
MSS	Ministério de Segurança do Estado
OIs	Organizações Internacionais
ONU	Organização das Nações Unidas
OSINT	Inteligência de Fonte Aberta
OTAN	Organização do Tratado do Atlântico Norte
PLA	People's Liberation Army
PLAAF	PLA Air Force
PLAGF	PLA Ground Force
PLAN	PLA Navy
PLC	Programmable Logic Controllers
PSYOPS	Operações Psicológicas
RBN	Russian Bussiness Network
RMA	Revolution in Military Affairs
SAC	Second Artillery Corps
SIGINT	Inteligência de Sinais
TCP/IP	Transmission Control Protocol / Internet Protocol
TIC	Tecnologia da Informação e Comunicação
WAN	Wide Area Network
WWW	World Wide Web

LISTA DE FIGURAS E GRÁFICOS

Gráfico 1 - Proporção ocupada por cada membro da ASEAN 53

Gráfico 2 - Gráfico das áreas para a maturidade cibernética 61

Figura 1 - Estrutura sínica de poder 72

Figura 2 - Tráfego de dados relativos a ataques cibernéticos – Top 10 82

LISTA DE QUADROS E TABELAS

Quadro 1 - Alvos do poder cibernético 34

Tabela 1 - ASEAN: Penetração e Usuários da Internet 51

Quadro 2 - Centros de Operação da APCERT 55

Quadro 3 - Estrutura da Pesquisa 58

Tabela 2 - Ranking de maior maturidade cibernética da região 59

Tabela 3 - Pontuação dos países por categoria 60

Quadro 4 - Capacidade Cibernética dos Estados/Nações Asiáticos 77

SUMÁRIO

RESUMO 7
ABSTRACT 8
LISTA DE ACRÔNIMOS 9
LISTA DE FIGURAS E GRÁFICOS 11
LISTA DE QUADROS E TABELAS 12
SUMÁRIO 13
INTRODUÇÃO 14
CAPÍTULO 1. CONHECENDO O MUNDO CIBER 20
1.1 Breve histórico da Internet 20
1.2 *Cyber*: apresentando conceitos e definições 23
1.2.1 O termo cibernético e o ciberespaço 23
1.2.2 Compreendendo guerra tradicional e guerra cibernética 25
1.3 Porque investir em capacidade cibernética? 30
1.4 A Organização do Ciberespaço 32
CAPÍTULO 2. O ENVOLVIMENTO CIBERNÉTICO DA REGIÃO ASIÁTICA 36
2.1 Apresentando os ciberconflitos 36
2.1.1 Rússia contra Estônia – 2007 36
2.1.2 Rússia contra Geórgia – 2008 39
2.1.3 Stuxnet - 2010 41
2.1.4 Flame – 2012 42
2.1.5 Outubro Vermelho - 2012 44
2.1.6 A Coreia do Norte e o ataque à Sony – Novembro de 2014 45
2.2 Cooperação asiática pela segurança cibernética da região 46
2.2.1 APEC 47
2.2.2 ASEAN 49
2.2.3 ASPI 56
CAPÍTULO 3. UTILIZAÇÃO SÍNICA DO ESPAÇO CIBERNÉTICO 63
3.1 A situação da China 63
3.2 Conhecendo a China: Um breve histórico militar 65
3.3 Organização da estrutura sínica de poder/segurança 69
3.4 Vantagens da ciberguerra para o desenvolvimento da China 74
3.5 Ações da China 76
CONSIDERAÇÕES FINAIS 83
REFERÊNCIAS 86

INTRODUÇÃO

A Informação sempre foi um componente indispensável nas atividades humanas. Contudo, a globalização e a consequente maior integração entre os diversos atores sociais tornou-a insumo básico do processo decisório, sendo hoje classificada como artigo estratégico para Organizações Internacionais (OIs), *policy makers*, Estados, entre outros. No mundo globalizado, o advento da Internet possibilita acesso a grande quantidade de informação (incluindo informação confidencial), o que dificulta o gerenciamento deste espaço e cria certo desconforto quanto à veracidade e à proteção das informações. Nesse contexto, cada informação sigilosa alcançada oferece aos que a detém inquestionável vantagem no ambiente competitivo e nos contenciosos internacionais (CARVALHO, 2011; NYE, 2012; KREPINEVICH, 2012).

A busca pela informação e a dificuldade de gerenciamento da Internet promovem a sensação de vulnerabilidade diante da dificuldade em proteger informações (sejam documentos de Estado ou senhas de redes sociais e de cartões de crédito). Esse ambiente possibilita a criação dos termos com o prefixo "ciber"[1] (como ciberguerra, ciberpolítica, ciberativismo, ciberconflito, cibercultura, ciberespaço e demais) que estão no cerne das atuais discussões internacionais, e que, por conseguinte, auxiliam na promoção da insegurança. O que estes termos têm em comum, entretanto, é que todos acontecem no ciberespaço (ou espaço cibernético), que configura-se em um ambiente metafísico e torna sua definição de extrema importância para a compreensão dos demais termos.

Assim, por se tratar de uma discussão relativamente recente que se popularizou e que, segundo Fernandes (2012: 53), vem se tornando moda, é possível constatar uma diversidade de definições. Não obstante – depois de explicar que a dificuldade em definir o ciberespaço não se encontra apenas em sua expansão ou na natureza global, mas também no fato de hoje ele estar quase irreconhecível quando comparado ao seu começo – após inúmeras tentativas, em 2008, o Pentágono definiu o ciberespaço como "*o domínio global dentro do ambiente de informação que consiste numa rede interdependente de infraestruturas de tecnologia da informação, incluindo a Internet, redes de telecomunicação, sistemas de computador, e*

[1] Do inglês *cyber*, redução de *cybernetics*, traduzido para o português como cibernético.

processadores e controladores embarcados" (SINGER e FRIEDMAN; 2014:13, tradução livre). Objetivando facilitar a compreensão, os autores afirmam que, em essência, o ciberespaço é o domínio das redes de computadores e os usuários por trás delas onde a informação é armazenada, compartilhada e comunicada *online*, e que ele é, sobretudo, um ambiente de informação.

Libicki (2009: 11) entende que o ciberespaço, por ser um espaço, é um meio de contenção como qualquer outro (terra, mar ou ar), mas que deveria ser apreciado por sua diferença: ser uma construção humana. Então ele o definiu como um meio virtual que é de longe bem menos tangível que qualquer outro. Um modo de entendê-lo em geral (e de entender os ciberataques, em particular) é vê-lo como consistente em três estruturas: a física, composta por fios e caixas; a sintática, que diz respeito às instruções dadas à máquina por seus designers ou usuários e protocolos de interação entre máquinas; e a semântica, condizente com informações contidas na máquina, o motivo da máquina existir. Assim, cabe ressaltar que o ataque cibernético acontece em qualquer uma destas camadas através de dano na estrutura física, modificação das instruções dadas às máquinas ou roubo e/ou modificação das informações contidas nas máquinas.

Desse modo, é possível observar que o espaço cibernético, assim como a Internet que se expandiu de uma rede inicialmente limitada para a comunidade científica a uma rede global que conta com mais de dois bilhões de usuários (KREPINEVICH, 2012), abarcou o comércio online e cresceu a ponto de incluir infraestruturas críticas que movem as civilizações modernas e controlam a distribuição de água, comida, energia, serviços bancários, assistência médica entre outros, aumentando os riscos (diante da possibilidade de um ataque às estruturas estratégicas gerar negação de serviço – *denial of service: DoS*) e a sensação de insegurança neste espaço.

Partindo destas discussões sobre conceituação – que serão abordadas no primeiro capítulo e servem de base para a compreensão dos capítulos seguintes – para observar atentamente os casos mais conhecidos de guerra cibernética, é possível perceber a constante participação de países asiáticos, estejam estes como supostos responsáveis ou como alvos dos ataques. Dentre os asiáticos o envolvimento de Rússia e China se sobressai aos demais com a primeira comparecendo, principalmente, ao se tratar do que Nye (2008) chamou de "*os primeiros ataques cibernéticos significativos acompanhados de conflitos armados*", enquanto a última faz-se presente nos casos mais recentes como provável responsável pelas agressões.

O grande número de participantes asiáticos em tais tipos de conflitos, além de países como Rússia, China, Índia, Israel, Japão, Paquistão e as Coreias serem apontados como possuidores de exército cibernético, torna fatível a hipótese de forte envolvimento e compromisso asiático com o investimento e desenvolvimento das capacidades cibernéticas da região, sendo a China, porém, o objeto do estudo de caso deste trabalho, já que além de ser possuidora de exército cibernético e ter papel principal em alguns conflitos deste tipo, tem no ciberespaço um plano para sua ascensão internacional. Desse modo, o problema explorado nesta pesquisa diz respeito ao modo como a região pacífico asiática vem se preparando para a Era Cibernética e quais as ações da China para, através do ciberespaço, elaborar seu plano estratégico de desenvolvimento. Por conseguinte, o objetivo geral deste trabalho é apresentar o compromisso regional de desenvolvimento cibernético e a utilização sínica da guerra cibernética como extensão de seu pensamento estratégico tradicional.

Como objetivos específicos estão: a identificação – através do estudo do caso chinês – da percepção sínica sobre a guerra cibernética, a exposição de suas ações de preparação para a chamada Era Cibernética e o uso do espaço cibernético como ferramenta estratégica para o desenvolvimento; a constatação do envolvimento asiático na construção de capacidades cibernéticas necessárias para a segurança regional; e a exposição de conceitos e definições que circundam o termo cibernético, visando melhor compreensão dos capítulos em específico e do tema de forma geral. Para tanto, faz-se necessária a assimilação de alguns conceitos chaves como espaço cibernético – já apresentado – e guerra cibernética entre outros a serem expostos no primeiro capítulo.

Seguindo esta lógica, o presente trabalho utiliza a ideia de guerra cibernética de Krepnevich (2012), que a entende como um conjunto de ações oriundas de atores tanto estatais quanto não estatais, que utilizam armas cibernéticas para invadir redes ou computadores com o objetivo de roubar, inserir, corromper, apagar e/ou falsificar dados; danificar computadores ou dispositivos de redes e/ou causar danos e/ou interrupções de sistemas de controle de computador. Da maneira exposta, o termo designa ataques, represálias ou intrusão ilícita em um computador ou rede. Ou seja, apresenta-se como uma forma alternativa de conflito de modo a possibilitar a obtenção de vantagens em um modelo de guerra assimétrica que permite vitória sem a imposição da morte.

A presente definição, no entanto, não anula a possibilidade de confronto real – já que ainda se trata de uma forma alternativa de guerra – mas minimiza o contato humano, tornando

possível a prática do que Liang e Xiangsui (1999) chamaram de "*humanização contemporânea*", a saber: a despeito da ocorrência de um conflito e de um eventual ataque, tem-se como premissa manter a garantia do direito à vida. Para esses últimos autores, o advento da guerra cibernética trouxe, além de uma nova concepção de guerra, mudanças na condução da guerra, uma vez que possibilita ações ofensivas de atores que não possuem capacidade militar para se envolver em um conflito tradicional contra grandes potências militares, como contra os Estados Unidos, por exemplo.

Em decorrência desta tendência observa-se o desenvolvimento de meios para desferir ataques diretos e, especificamente, visar ao centro nervoso do inimigo sem danificar outras áreas, de modo que atualmente é possível alcançar a vitória através de outros meios que não a imposição da morte, inclusive sem a necessidade de um exército físico, mas tornando essencial a existência de um "exército de controle" (LIANG e XIANGSUI, 1999). Essa nova forma de conflito permite a participação de um maior número de atores e pode promover as revanches que, muitas vezes só são possíveis neste modelo de guerra. Os ataques cibernéticos, no entanto, acontecem tanto em momentos de guerra quanto de paz.

Contrapondo a visão de humanização da guerra, autores como Clarke e Knake (2012) e Krepnevich (2012) defendem que o poder cibernético ainda não foi empregado com força total, uma vez que um ataque cibernético pode derrubar sistemas financeiros, elétricos e/ou governamentais de um país e consequentemente paralisá-lo. Por conseguinte, a busca grotiana por um modelo de guerra que não tivesse impacto sobre a sociedade civil (COKER, 2000: 11) ainda não foi alcançada. Embora a guerra cibernética abra espaço para uma prática criminosa sem crueldade, a utilização do poder cibernético de modo a atingir a população civil é tão real quanto em uma guerra tradicional. Contudo, se os resultados de um conflito cibernético irão ou não atingir níveis catastróficos dependerá única e exclusivamente das aspirações do atacante.

A incerteza (proveniente da vulnerabilidade da Internet e da criação de "exércitos de controle") é para Lewis (2009: 1) o aspecto mais importante da guerra cibernética, uma vez que o espaço cibernético permite ataques anônimos fazendo uso de identidades que podem ser facilmente fabricadas ou ocultadas. Essa qualidade, a título de exemplificação, possibilita que um oponente astuto construa provas forjadas para atribuir a outro(s) a responsabilidade pelas ações cometidas. Essa possibilidade levou alguns Estados a investir em tecnologia da informação e comunicação (TIC) tanto com o objetivo de criar um exército cibernético para

sua defesa e segurança nacional, quanto de penetrar e obter informações secretas e privilegiadas de organizações e instituições governamentais (LIBICK, 2009; SOUZA, 2010).

Sendo o espaço cibernético um ambiente de acesso mundial, ele atualmente facilita a comunicação entre diversos pontos do globo e para diferentes finalidades, tornando-se responsável por uma ampla parcela das relações sociais transnacionais. É também no espaço cibernético que grande parte da economia mundial se movimenta alcançando mais de 10 trilhões de dólares por ano (SINGER e FRIEDMAN, 2014: 15), gerando fluxo de capital e contribuindo para o Produto Interno Bruto (PIB) dos países. Há que se considerar também que em casos de vazamento de informação confidencial de grandes atores internacionais (Organizações, Estados entre outros), este pode gerar, além do desconforto no Cenário Internacional, retaliações generalizadas assim como influenciar comportamentos na política mundial. Do mesmo modo, faz-se mister considerar a importância do estudo da guerra cibernética como um novo modelo de guerra, que segundo Liang e Xiangsui (1999) e Nye (2012) é característico da Era da Informação.

Outro fator importante nesta discussão é que apesar de estar "virando moda", como comentou Fernandes (2012: 53), a discussão ainda é muito recente na área das Relações Internacionais, principalmente, no que tange ao envolvimento de Estados asiáticos, posto que grande parte dos estudos sobre o campo cibernético se concentra nas áreas de Tecnologia da Informação, Ciência da Computação e até do Direito, mas pouco se faz presente nas Relações Internacionais. Estes são os motivos que justificam a análise do espaço cibernético e das ações provenientes deste espaço, bem como de seu uso com fins estratégicos (aqui entendido como planejamento, implementações e ações políticas que visam à obtenção dos objetivos estipulados) e militares pela República Popular da China.

À vista disso, esta pesquisa se dá através da metodologia qualitativa, que se preocupa com o aprofundamento da compreensão e busca explicar o motivo dos fatos acontecerem. Na pesquisa qualitativa o objetivo é produzir informações aprofundadas e ilustrativas que sejam capazes de gerar novas informações (DESLAURIERS *apud* SILVEIRA e CÓRDOVA, 2009), o que se encaixa na proposta desta pesquisa ao possibilitar, mediante o instrumento documental bibliográfico, a revisão de bibliografia – seja através de livros, artigos científicos, documentos originais ou relatos – que serve de base para a compreensão do assunto e que possibilita a conexão entre os dois temas: ciberguerra e Ásia, dando origem a novas informações.

Esta pesquisa orienta-se pelo alcance descritivo e exploratório. O alcance descritivo pode ser percebido no capítulo dois com o relato do envolvimento asiático nas guerras cibernéticas, uma vez que esta modalidade de pesquisa se concentra na narração dos detalhes e proporciona novas visões sobre uma realidade já conhecida: a realidade dos conflitos cibernéticos. O alcance exploratório, por sua vez, busca a familiarização com um assunto pouco conhecido: a participação asiática em questões cibernéticas (GIL, 2008). Por fim, esta pesquisa utiliza o método do estudo de caso, que é uma modalidade de pesquisa consistente na exploração profunda e exaustiva de um caso particular (GIL, 2008), como acontece no terceiro capítulo, e trata-se de uma investigação para responder a questões específicas, onde nenhuma evidência é suficientemente válida, fazendo-se necessário o uso de múltiplas fontes de evidência (GILLHAM, 2000).

Para tanto, o trabalho está organizado em três capítulos, além de introdução e considerações finais. O primeiro capítulo dar-se-á de forma mais geral, de modo a apresentar o tema e explicar a utilização do ciberespaço como extensão da guerra, o que acontecerá através da exposição dos conceitos indispensáveis à compreensão da temática e da apresentação das discussões atuais que circundam a questão cibernética. O segundo capítulo trará a exposição do envolvimento cibernético do continente, que acontece tanto com relação à participação de alguns países asiáticos neste modelo de conflito, quanto à decisão conjunta de cooperação pela segurança cibernética da região. O terceiro capítulo será um estudo do caso da República Popular da China, objetivando, por intermédio da visão sínica, analisar a utilização do espaço cibernético como componente central na sua estratégia de ascensão internacional como instrumento de política de poder (afinal de contas, qualquer guerra ou conflito determina e visa obtenção de poder) e expor as ações de tal Estado de modo a se preparar na busca e manutenção da primazia cibernética.

1. CONHECENDO O MUNDO CIBER

Com o objetivo de facilitar a compreensão do tema, o presente capítulo inicia-se com um breve histórico sobre a criação e o desenvolvimento do espaço cibernético. Em seguida serão apresentadas as definições de guerra tradicional, guerra cibernética e ataque cibernético entre outros, que possibilitam a discussão sobre diferentes perspectivas. Para finalizar o capítulo, serão externadas algumas formas de organização desse espaço e os motivos que justificam investimento em capacidades cibernéticas.

1. Breve histórico da Internet

A informação – que sempre foi considerada elemento essencial na interação humana – gradualmente foi se transformando em diferencial estratégico até tornar-se insumo básico do processo decisório, fenômeno de grande relevância para os estudos de segurança internacional. Foi em busca de maior acesso à informação que no final dos anos 1950, durante a Guerra Fria, os Estados Unidos deram início à Agência de Projetos de Pesquisa Avançada (*Advanced Research Projects Agency* - ARPA), que foi um projeto de pesquisa militar em resposta ao lançamento do satélite Sputnik, posto em órbita pela antiga União Soviética (OLIVEIRA, 2007: 39; NYE, 2012: 161).

Inicialmente o projeto tinha como objetivo conectar ao Pentágono os mais importantes centros americanos de pesquisa, para permitir uma troca rápida e segura de informações importantes e para, com o uso da tecnologia, tornar os canais de comunicação do país resistentes a ponto de suportar uma guerra nuclear. A ideia surgiu da vulnerabilidade existente na comunicação militar – que se dava através da rede de telefone público – e como plano para a criação de uma única organização de defesa visando finalizar a disputa pelo orçamento de investigação do Pentágono, entre marinha, exército e aeronáutica (TANENBAUM e WETHERALL, 2011: 56).

Em agosto de 1962, Joseph Carl Robnett Licklider[2], pesquisador do Instituto de Tecnologia de Massachussetts (*Massachusetts Institute of Tecnology* - MIT), expressou pela primeira vez seu conceito de "Rede Galáctica", que ele vislumbrava como um conjunto de computadores globalmente conectados de modo que cada um pudesse acessar rapidamente informações e programas de qualquer site. Licklider foi o primeiro pesquisador do *computer*

[2] Conhecido como *J. C. R.* Licklider ou "Lick". Pesquisador do MIT (*Massachusetts Institute of Tecnology*), cientista da computação estadunidense considerado uma das figuras mais importantes da ciência da computação depois de ter contribuído para o desenvolvimento da Internet (SYSTEMS RESEARCH CENTER, 1990).

research program da ARPA. Dando continuidade a sua aspiração, em 1965 os pesquisadores Thomas Merrill (da ARPA) e Lawrence G. Roberts (do MIT) conectaram o computador TX-2 em Massachusetts ao Q-32 na Califórnia através de uma linha telefônica discada de baixa velocidade, dando origem à primeira rede de computador já construída (LEINER, 2009: 23).

Com o passar do tempo, foi criada uma rede WAN (*Wide Area Network*) que funcionava com uma linguagem muito complicada (utilizada nos computadores ligados em rede) e, portanto, mantinha-se restrita à comunidade científica que a utilizava (OLIVEIRA, 2007: 39). Em 1966, Roberts entrou para a ARPA, desenvolveu seu conceito de rede de computador e rapidamente começou a por em prática seu plano para a criação de uma rede para ARPA, a ARPANET (*Advanced Research Projects Agency Network*), projeto que rendeu um trabalho acadêmico publicado em 1967. Em 1969, na procura por redes de comunicação mais seguras para seus computadores, a ARPA deu vida à ARPANET, uma modesta conexão que veio a ser considerada a precursora da Internet moderna (LEINER, 2009: 23; SOUZA, 2011a: 3; NYE, 2012: 161).

Desde sua criação, a Internet tem sido percebida pelos Estados Unidos como ferramenta potencial de guerra. A ARPANET foi fortemente financiada pelos militares estadunidenses, com uma ênfase especial nos benefícios de colaboração de pesquisa e então, desde seu início, os estados Unidos enfatizam e investem no desenvolvimento da guerra centrada na rede (FRITZ, 2008: 40). Nos anos 1970, depois de resolvidas as complexidades da WAN, Roberts criou o primeiro programa de e-mail capaz de listar, ler seletivamente, arquivar, encaminhar e responder às mensagens. Esse se tornou o primeiro uso da Internet entre os pesquisadores – que podiam se comunicar facilmente e trocar informações entre as universidades – e modificou o padrão de autoria de trabalhos acadêmicos que passou a dispor de autores com visões compartilhadas, independente da proximidade de suas localizações. (OLIVEIRA, 2007: 39; LEINER, 2009: 23).

Em 1972 foi criado o TCP/IP (*Transmission Control Protocol / Internet Protocol*), que é um conjunto de protocolos responsável pela comunicação de computadores em rede, através de envios e recebimentos de pacotes de informação digital, sendo capaz de ler a informação recebida e de repassá-la ao destino determinado pelo usuário. Esses protocolos específicos são responsáveis pela distinção entre a Internet e os outros meios de comunicação. Nos anos 1980, a Internet ganha aplicação comercial com os primeiros provedores de serviço da

Internet e por volta de 1983 foram criados os primeiros vírus de computador. (NYE, 2012: 161; OLIVEIRA, 2007: 39; KREPNEVICH, 2012: II).

Com a criação do WWW (World Wide Web), em 1989, o número de servidores conectados aumentou consideravelmente e saltou de mais de cem mil no mesmo ano, para mais de um milhão em 1992. Em 1998 nasce o Google, o mais popular site de busca do mundo, e em 2001 é fundada a Wikipédia, maior enciclopédia de código aberto (NYE, 2012: 161; OLIVEIRA, 2007: 39). Diante de tais exemplos, é possível perceber que nas últimas décadas do século XX a Internet se expandiu em ritmo acelerado, tornando-se possuidora de mais de dois bilhões de usuários ao redor do globo e transformando-se em ferramenta essencial à sociedade moderna (KREPNEVICH, 2012: II).

A chave para esse rápido crescimento tem sido o acesso livre e aberto ao conhecimento e a facilidade de se compartilhar informação. Esses fatores fizeram a Internet crescer além do esperado – passando a abarcar atividades comerciais, transações financeiras, sistemas bancários e envolver redes de distribuição de água e energia, entre outros (LEINER, 2009: 29). A utilização da Internet para fins tão diferenciados aumentou as preocupações dos atores estatais e não estatais com relação à vulnerabilidade de suas informações e à possibilidade de sérios danos à população civil diante de invasões às redes e infraestruturas críticas.

Desse modo, é possível constatar que a Internet passou de uma rede simples – limitada à comunidade científica – a uma rede mundial que produz interação social, suscita a economia global e disponibiliza quantidade quase infinita de informação. A questão, no entanto, é que a grande quantidade de informação (incluindo informação confidencial) contida na rede dificulta seu gerenciamento e produz desconfiança quanto à confiabilidade das informações (SINGER e FRIEDMAN, 2014: 15). Segundo Krepnevich (2012:1), foi a união de tais fatores que deu origem ao crime cibernético, já que "o armazenamento de informações sensíveis, em redes, deu luz à espionagem cibernética contra os governos e à guerra econômica cibernética contra as empresas".

Vale observar que o projeto inicial de uma rede para compartilhamento de informação já tinha propósitos marciais, devido à Guerra Fria. Contudo, ele evoluiu daquela pequena rede de cientistas militares para uma rede global responsável por grande parte das estruturas estratégicas dos Estados e pela movimentação de mais de 10 trilhões de dólares por ano. A utilização da Internet para diferentes finalidades trouxe consigo, portanto, a preocupação com

a segurança das informações e deu início aos chamados crimes cibernéticos, a serem apresentados na próxima seção.

2. *Cyber*: apresentando conceitos e definições

Para melhor compreender as discussões sobre guerra cibernética e consequentemente entender os objetivos por trás das ações da China, faz-se necessário separar um espaço para a apresentação dos conceitos e definições que circundam esse tema, a começar pela explicação do termo cibernético.

1. O termo cibernético e o ciberespaço

O vocábulo cibernético(a), originário do inglês *cybernetic*, assim como os demais desta recente área de discussão, é possuidor de uma gama de definições produzidas por diferentes autores, contudo, cabe destacar a definição de Carvalho (2011:7) que afirma ser essa a definição aprovada pela literatura oficial do exército brasileiro. Assim, o autor apresenta cibernético(a) como "termo que se refere ao uso de redes de computadores e de comunicações e sua interação dentro de sistemas utilizados por instituições públicas e privadas, de cunho estratégico". Diante de tal conceituação torna-se imprescindível destacar o originário caráter crítico do termo.

Assim, as palavras acompanhadas do prefixo ciber – ou sufixo cibernético (a) – têm em sua natureza a característica tática fornecida pelos planos iniciais de sua concepção e são, por esse motivo, objetos de temor e desconfiança. São estes termos (ciberguerra, ciberespionagem, ciberespaço, ciberpolítica, ciberativismo, ciberconflito entre outros) os responsáveis pelo ambiente de desconfianças e incertezas, estando atualmente entre os assuntos mais discutidos da agenda internacional.

A criação desses termos se dá com base na relação entre as ações e o ambiente onde elas acontecem. Este, nomeado ciberespaço ou espaço cibernético, trata-se de um ambiente metafisico comum aos termos supracitados e que diz respeito ao interior das redes de computadores ou de comunicação. A definição de espaço cibernético faz-se importante para a absorção dos demais conceitos e, segundo Souza (2011b: 3), teve sua utilização pela primeira vez em 1984, quando o escritor William Gibson resolveu utilizá-lo em seu livro de ficção científica para descrever a interconexão entre os seres humanos através de computadores e da telecomunicação.

Por se tratar de uma discussão relativamente recente, Fernandes (2012: 53) afirma que, "como todo termo que se populariza tornando-se palavra da moda, [este] traz consigo uma utilização excessivamente livre e confusa". A popularização da discussão sobre o espaço cibernético e seus precedentes é, contudo, o que concede uma infinidade de definições e o que possibilitou que depois de inúmeras tentativas, em 2008, o Pentágono finalmente definisse o espaço cibernético como:

> "O domínio global dentro do ambiente de informação que consiste numa rede interdependente de infraestruturas de tecnologia da informação, incluindo a Internet, redes de telecomunicação, sistemas de computador, processadores e controladores embarcados". (SINGER e FRIEDMAN, 2014:13, tradução livre).

Pretendendo facilitar a compreensão, os autores explicam que, em síntese, o espaço cibernético é o domínio das redes de computadores e os usuários por trás delas, onde a informação é armazenada, compartilhada e comunicada *online*, e que ele é, sobretudo, um ambiente de informação (*ibidem*, 2014: 13).

Cole (2010: seção A1), corroborando a definição do Pentágono, afirmou ser o espaço cibernético "um domínio operacional formado pelo uso da eletrônica para [...] explorar informação via sistemas interconectados e sua infraestrutura associada", enquanto Nye (2012) resumiu ao explicar que o termo cibernético estava relacionado a atividades eletrônicas e ao computador. O último autor também afirma que o espaço cibernético não vai substituir o espaço geográfico nem abolir a soberania do Estado, mas que vai coexistir e complicar o conceito de Estado soberano ou de país poderoso no século XXI (NYE, 2012: 161).

Em sua definição, Cole (2010: seção A1) introduz termos que demonstram o caráter de ambiente a favorecer o ataque. Reforçando esse aspecto, Krepnevich (2012: 40) afirma que "A competição cibernética é uma competição dominantemente ofensiva, [pois] se ambos, atacante e defensor, possuírem recursos iguais, o atacante vai prevalecer". Essa característica se dá devido à rapidez com que os ataques são efetuados, à dificuldade de se descobrir a origem do ataque ou a identidade do agressor e à demora que pode existir entre o ataque e sua descoberta, uma vez que os ataques cibernéticos podem ser executados na velocidade da luz, enquanto seus efeitos podem levar anos até serem descobertos.

Assim, parece possível inferir que o espaço cibernético se refere a um ambiente onde há utilização de redes de computação ou de comunicação tanto com o objetivo de interconectar os seres humanos como de conectar, acessar e/ou compartilhar informações.

Uma vez compreendida a noção de ciberespaço, é fundamental seguir o curso das discussões e partir para as definições de guerra tradicional e de ciberguerra visando à assimilação das diferenças e similaridades entre os dois modelos de conflito.

2. Compreendendo guerra tradicional e guerra cibernética

A clássica definição de Clausewitz (1989:75, tradução livre) considera a guerra "um ato de uso da força para compelir o inimigo a fazer a nossa vontade" e chega a compará-la a um duelo em larga escala, cujos atores têm como objetivo principal a derrubada do adversário de modo a impossibilitar qualquer resistência. Para o autor, leis e costumes internacionais, embora tentem limitar o uso da força, só existem como apresentado na legislação do Estado, uma vez que a guerra seria um ato de força e que não existiria limite lógico que restringisse seu uso.

Embora algumas pessoas possam acreditar que haja maneira mais habilidosa para se derrotar e desarmar o inimigo, sem a necessidade de derramamento de sangue, esta seria uma falácia que o autor tentaria desfazer ao explicar que, sendo a guerra algo extremamente perigoso, os erros advindos da bondade são os piores, posto que se um dos lados utiliza força máxima sem remorso enquanto o outro se abstém de utilizá-la, então o primeiro estará em vantagem. Dessa forma, o "uso maximizado da força não é de modo algum incompatível com o uso simultâneo do intelecto" (CLAUSEWITZ, 1989:75, tradução livre).

Alguns autores estudiosos de Clausewitz explicam que ele vê a guerra como instrumento intencional para se atingir determinados fins. Ou seja, ela seria um dos tantos outros meios para a obtenção da vitória. Boniface (1997:165-166) esclarece que é dessa visão que surge a máxima clausewitziana de que "a guerra é meramente a continuação da política por outros meios" (CLAUSEWITZ, 1984:764). Por sua vez, Barbosa (2005:16), ao fornecer contraposições às visões de Clausewitz, oferece a percepção cataclísmica de Santos (2000:204-205) que defende a guerra como uma luta pela paz dos que almejam a vitória, sendo assim, uma catástrofe inevitável.

No clássico A Arte da Guerra, Sun Tzu (2012) mostra que na antiguidade já se pensava tal como a visão moderna de Clausewitz no que tange à guerra como instrumento para obtenção da vitória. Entretanto, diferentemente do moderno, que acredita no uso máximo da força como fator obrigatório para a conquista, a sabedoria dos antigos defende que a melhor vitória é aquela em que o oponente consegue alcançar seus objetivos sem precisar

entrar em guerra. O fato é que a função da guerra se modificou e seus novos princípios não estão mais relacionados ao uso da força armada de modo a obrigar o inimigo a sucumbir às nossas vontades; mas à utilização de todos os meios, inclusive das forças armadas ou não armadas e de meios letais ou não para compelir o inimigo a atender nossos interesses (LIANG e XIANGSUI, 1999:7).

A evolução da tecnologia e consequente modernização da guerra criaram novas ferramentas de conflito, aprimoraram algumas das existentes e permitiram que outras se mantivessem inutilizadas, como aconteceu com o caça russo SU-27, que antes de entrar em combate foi substituído pelo modelo mais moderno: o SU-35 Super-Flanker (LIANG e XIANGSUI, 1999: 9). 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 novas tecnologias, mas um novo modelo de relacionamento entre o homem, a tecnologia e a guerra.

Sun Tzu, embora tendo vivido há mais de 2.000 anos, traz em seus ensinamentos e táticas marciais uma percepção de guerra mais completa e atual que a de Clausewitz, de modo a se enquadrar perfeitamente tanto nos modelos tradicionais de conflito quanto na condução das guerras modernas, fato que torna a leitura de sua obra cada vez mais relevante no estudo dos conflitos contemporâneos. Apesar de 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 partir para um confronto real, ou seja: como sobrepujar o oponente de modo que o confronto físico não seja necessário.

Outros aspectos merecedores de atenção são a atuação, de modo a manipular o inimigo fazendo com que ele acredite que seus objetivos são uns quando, de fato, são outros, e a busca pelo conhecimento sobre o inimigo. Estes aspectos são pontos que migram da guerra tradicional para a virtual e fazem de sua obra uma leitura tão importante atualmente. Sun Tzu também dá destaque à importância dos espiões e os enxerga como elementos essenciais de um exército, dado que é deles que depende a capacidade de mobilidade dos soldados. O autor também ressalta o risco a que esses agentes estão expostos se descobertos infiltrados em território inimigo.

Outro autor a evidenciar o papel dos espiões é Libick (2009), que, trabalhando nos meios e classificações das invasões cibernéticas, defende a função dos agentes e/ou elementos infiltrados nas redes como de extrema importância para obtenção do acesso às redes e informações de sistemas mais seguros, cuja infiltração por meio de hackers e crackers talvez não fosse possível. Esses são mais fatores a corroborar com a semelhança entre a tradicional visão de guerra de Sun Tzu e a atual guerra cibernética, que Krepnevich (2012:8, tradução livre) 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 falsificar dados, interromper ou danificar computador ou dispositivo de rede; e/ou infligir danos e/ou interrupções dos sistemas de controle do computador".

Nesta definição percebe-se que a guerra cibernética, por acontecer em um ambiente virtual e ter como objetivo a penetração em sistemas de computador ou redes, é uma forma alternativa de guerra que, diferente da visão de Clausewitz, concede a conquista dos fins independente do uso da força, uma vez que consente a minimização do contato humano (LIANG e XIANGSUI, 1999).

É primordial destacar que, por tratar-se de guerra, há possibilidade de esta ser utilizada tanto em conjunto com o confronto real (como aconteceu nos conflitos entre Rússia x Estônia e Rússia x Geórgia – a serem apresentados no segundo capítulo) quanto como meio de desferir ataques a infraestruturas críticas podendo paralisar o Estado e massacrar sua população civil. Compartilhando desse pensamento, o antigo Vice Chefe do Estado-Maior russo, Alexander Burutin, falou sobre como a guerra cibernética está mudando a paisagem do combate moderno e defendeu 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 a estabilidade de controle da economia e das Forças Armadas do Estado". (KREPNEVICH, 2012:3, tradução livre).

Para Liang e Xiangsui (1999:26-27), essa tendência é a constatação de que a humanidade alcançou alto nível de belicosidade de modo a temer sua destruição (como se faz possível através da utilização de armamento nuclear). Os autores defendem que "a invenção da arma nuclear mergulhou a humanidade em uma armadilha existencial de sua própria autoria", posto que sua utilização não destruiria apenas o inimigo, mas suas futuras gerações,

e poderia significar a destruição do planeta. Os autores explicam que diante dos perigos da arma nuclear nasce uma nova abordagem científica que privilegia o aprimoramento do controle de poder.

Nesse sentido, a utilização de armas cibernéticas, que Liang e Xiangsui (1999:26-30) chamaram de "armas suaves" – classificação que não está relacionada ao poder letal que essas armas possuem, mas à sua capacidade de ataque ao centro nervoso do inimigo sem a necessidade de um resultado catastrófico – representa uma mudança na formação cultural da humanidade quanto às expectativas da guerra, diante da possibilidade de se alcançar a vitória através do controle do poder em vez da morte.

Entretanto, com a gradativa utilização do ataque cibernético como modo de atingir o centro nervoso do inimigo evitando o comprometimento de outras áreas – o que produz novas opções para obtenção da vitória e desfaz a crença de que a melhor forma de obtê-la é através de um maior exército físico, quando na verdade, pode-se obter resultado através da existência de um maior "*exército de controle*" e não através da imposição da morte (LIANG e XIANGSUI, 1999) – um maior número de governos e grupos aliados utiliza o ciberespaço para a prática de espionagem e ataques às infraestruturas críticas de outros países (Relatório de Criminologia Virtual da McAfee *apud* SHAH e RAVI, 2012: 56).

O ataque cibernético, segundo Caplan (2012: 94), pode ser definido como conjunto de "ações determinadas a alterar, interromper, enganar, degradar ou destruir sistemas ou redes de computador, ou a informação e os programas que neles residem ou por eles transitam". Embora esses ataques possam ser executados na velocidade da luz, seus efeitos podem demorar anos até serem percebidos. Assim, ataques cibernéticos direcionados a infraestruturas críticas, apesar de considerados meios menos violentos de se fazer a guerra, são capazes de provocar grandes estragos. Apesar de alguns pesquisadores optarem por ignorar essa possibilidade, é fato que as armas cibernéticas possuem alcance maior que quaisquer outras (com exceção dos mísseis balísticos) (KREPNEVICH, 2012: 4).

Krepnevich (2012), por exemplo, compara os efeitos de um ataque cibernético ao de um ataque nuclear, deixando claro, entretanto, que o poder do primeiro estaria muito aquém do segundo. O autor explica que a comparação só é possível caso o termo "catastrófico" possua definição abrangente. Ele apresenta o ex-diretor da Agência Nacional estadunidense,

almirante Mike McConnell e o ex-presidente da *Joint Chiefs of Staff*[3], general James Cartwright, que corroboram sua crença de que os resultados de um ataque cibernético às estruturas estratégicas de um Estado podem alcançar a proporção das armas de destruição em massa (KREPNEVICH, 2012: 3).

Quanto à comparação entre os efeitos da guerra cibernética e da guerra nuclear, alguns pesquisadores discutem a possibilidade de resultados cibernéticos catastróficos serem acompanhados do elemento surpresa, considerando que para atingir tal classificação é preciso gerar, no inimigo, a visualização do inesperado. Lawrence Freedman explica que embora fatível, o poder de catástrofe dificilmente acontece mais de uma vez, considerando que depois da surpresa o inimigo costuma se preparar para outras possibilidades (KREPNEVICH, 2012: 12-15).

Outros autores defendem que, independente da utilização do elemento surpresa, o domínio cibernético atual é capaz de produzir efeitos catastróficos e que se isso ainda não aconteceu é simplesmente porque ainda não tiveram interesse. Essa afirmação, de certa forma, corrobora Liang e Xiangsui (1999) ao cogitar a hipótese de que, embora haja condição para o uso do nível mais alto de dano, os ataques cibernéticos da atualidade não estão seguindo essa linha. Contudo, há que se destacar a preocupação de que ataques terroristas possam atingir tal nível de destruição em operações contra os Estados Unidos, maior alvo em potencial.

Kelth B. Alexander, ex-diretor da Agência de Segurança Nacional americana comparou o domínio cibernético com o domínio aéreo e comentou: “O domínio cibernético é, de algum modo, como o domínio aéreo, ao ser uma esfera que não tinha relevância para o planejamento militar até que, de repente, uma nova tecnologia lhe ofereceu acesso”. Ora, a evolução que ocorreu no domínio aéreo ocorre diariamente no domínio cibernético que, aos poucos, vem sendo construído de acordo com o objetivo de cada usuário (KREPNEVICH, 2012:12-15, tradução livre).

CLARCK e KNAKE, 2012 observam que na primeira Guerra do Golfo guerreiros cibernéticos estadunidenses tinham o plano de usar armas cibernéticas visando derrubar o sistema de defesa aérea do Iraque. Isso inspirou a criação da primeira turma de oficiais da Universidade de Defesa Nacional, em 1995: treinados para conduzir campanhas de guerra cibernética. Isto mostra a relevância que o espaço cibernético galgou no domínio militar.

[3] Optou-se pela não tradução do termo por receio de não fazê-la de modo fidedigno.

Dando sequência a este fato, agentes da inteligência observaram a expansão da Internet como um ambiente de prosperidade para a espionagem eletrônica. Em princípio eles temiam que ao passar para a unidade de guerra a Internet estivesse tornando possível um novo tipo de conflito, pelo qual pudessem perder o controle do espaço cibernético para os soldados. Por outro lado, a oportunidade que o ciberespaço estava oferendo – para, de um modo relativamente fácil, causar expressivos danos a um inimigo – era boa demais para ser ignorada (CLARCK e KNAKE, 2012).

À vista do exposto, compreende-se que a ciberguerra, acompanhada por ciberataques, é considerada por alguns autores um modelo menos violento de se guerrear, posto que evita o contato físico e conta com várias alternativas para obtenção da vitória por meio dos exércitos de controle. Embora haja a possibilidade de seus danos atingirem níveis catastróficos, os pesquisadores a concordar com essa assertiva também alegam que se isso ainda não aconteceu foi porque não houve interesse.

Essa alegação reforça a crença de que esse modelo de conflito só poderia ter surgido na Era da Informação e das discussões sobre Direitos Humanos e sobre questões ambientais. Contudo, por se tratar de um tipo de guerra que se faz mais vantajoso àqueles com objetivo agressivo, cada vez mais países se preparam e participam deste tipo de conflito. Tzu (2012), por exemplo, explica que para impossibilitar a derrota é preciso investir em táticas defensivas, mas que, para garantir a obtenção da vitória, faz-se necessário o investimento em capacidade agressiva.

3. Porque investir em capacidade cibernética?

Observou-se que a quantidade de infraestruturas críticas vem crescendo gradativamente com o passar do tempo e, unida à dependência dos sistemas de informação e ao grande acesso à Internet, vem colocando os Estados em posição cada vez mais vulnerável. Essa vulnerabilidade, porém, é fruto das incertezas do ambiente cibernético e justifica o interesse dos Estados em se antecipar a essas guerras.

Lewis (2009: 1) defende que a incerteza é o aspecto mais importante do conflito cibernético, uma vez que o ciberespaço permite ataques anônimos e identidades são facilmente ocultadas ou fabricadas. Essa qualidade permite, a título de exemplificação, que um inimigo inteligente possa atribuir a outrem a responsabilidade pelos ataques auferidos. Essa possibilidade faz com que cada vez mais Estados procurem investir em tecnologia da

informação e comunicação (TIC) tanto com o objetivo de criar um exército cibernético para sua defesa e segurança nacional, quanto de penetrar e obter informações secretas e privilegiadas de organizações e instituições governamentais.

Diante da velocidade do ataque cibernético e da dificuldade de se descobrir sua origem – sendo o espaço cibernético um ambiente que favorece o ataque no lugar da defesa, incentivando as ações ofensivas e fomentando as revanches, muitas vezes só possíveis neste espaço – Hjortdal (2011: 3) explica que os maiores interessados em capacidades cibernéticas agressivas são os Estados que não possuem forte capacidade militar, tecnológica ou econômica, devido à espionagem no ciberespaço poder ser utilizada como meio para alcançar tais capacidades.

Outros motivos que o autor apresenta como justificativa para o investimento em tais capacidades são: i) a acessibilidade e fácil manuseio das ferramentas para *hackers*; ii) a possibilidade de detenção de infiltração de outros Estados em suas infraestruturas críticas; iii) o aumento do conhecimento específico através da espionagem para desenvolvimento militar, por exemplo; iv) a obtenção de ganhos econômicos onde o progresso tecnológico tenha sido alcançado, através da espionagem industrial; e v) a capacidade de atacar e paralisar tanto a capacidade militar do adversário quanto a capacidade que o adversário teria, de paralisar e controlar suas forças (HJORTDAL, 2011: 3).

Embora sejam muitos os motivos para que os Estados invistam em tecnologia cibernética, o recrutamento e capacitação de recurso humano ainda é a parte mais importante do processo, uma vez que qualquer um pode causar dano no espaço cibernético (NYE, 2012: 173). Embora haja chance real de qualquer ator produzir atos danosos, diferentes atores possuem diferentes níveis de recurso, o que permite que Estados maiores ainda possuam maiores recursos. No entanto, o modelo de guerra cibernética tem como material mais importante a capacidade humana de se superar intelectualmente.

De acordo com a Escola Asiática de Leis Cibernéticas (*Asian School of Cyber Laws*) o mundo gasta cerca de 45 milhões de dólares por ano no combate ao crime cibernético e seus efeitos, motivo de muitos países procurarem se antecipar. Como afirmaram Clarck e Knake (2010), a guerra cibernética começou e, para se antecipar às hostilidades, cada nação está preparando seu campo de batalha para o mais novo modelo de guerra cuja evolução acontece diariamente.

Visando facilitar a compreensão sobre o modo como os ataques cibernéticos acontecem e consequentemente propiciar melhor investimento e utilização do espaço cibernético é preciso saber como se dá a organização deste espaço e a classificação dos ataques cibernéticos, tanto com relação à sua origem quanto à sua forma.

4. A Organização do Ciberespaço

Libick (2009: 12) divide o espaço cibernético em três camadas: a física, a sintática e a semântica. A camada física é responsável por todo o sistema de informação, sendo composta por caixas e fios, e se fazendo essencial à existência do sistema, uma vez que nenhum sistema sobrevive sem estrutura física. A camada sintática é responsável pelo armazenamento de instruções e protocolos que possibilitam interação entre as máquinas, formatação de documentos, manipulação de banco de dados, entre outros. Este é o nível em que a maioria dos ataques costuma acontecer. Por fim, é no nível semântico que as informações contidas nas máquinas (como tabelas de pesquisa, que apesar de sintáticas no propósito seriam semânticas na origem) se encontram, ou seja: o motivo do computador existir.

Embora o ataque cibernético possa acontecer em quaisquer destas camadas, apenas no nível semântico é possível modificar informações a ponto de coagir o computador a agir de modo oposto ao esperado para a obtenção do objetivo. Como exemplo tem-se o caso de um computador que aumenta a temperatura quando recebe comando para resfriar um ambiente. Porém, há que se explicar que a introdução de informações falsas no nível semântico só é possível se no nível sintático elas também tiverem sofrido modificações. É igualmente importante informar que os ciberataques, além de acontecer em quaisquer dos três níveis, também se classificam quanto à sua origem, que pode vir de fora da rede, por meio de *hackers;* ou de dentro da rede, por meio de agentes e/ou elementos infiltrados (LIBICK, 2009: 13; NYE, 2012: 166).

Os *hackers* são os responsáveis por ataques externos. Eles utilizam várias táticas para invadir um sistema de computador: podem burlar a segurança da camada sintática e roubar informações desta e podem emitir comandos atribuindo ao computador funções antes inexistentes ou possivelmente opostas às existentes. Há também o roubo de informação por e entre Estados, conhecido como exploração de rede de computador (*computer network exploitation* - CNE), por empresas, que na maioria das vezes busca roubo de propriedade intelectual, e por indivíduos, fator que dificulta a atribuição dos ataques a agências estatais.

Para a existência do ataque interno é necessário o recrutamento de membros que tenham acesso aos computadores - chamados *insiders*, (o que normalmente acontece em sistemas verdadeiramente fechados) ou que alterações sejam feitas na rede de abastecimento, que serão usadas na construção dos sistemas. Assim, faz-se mister informar que no caso dos *insiders* um erro dificilmente se repete, já que a descoberta de um espião mantém o ambiente em alerta e dificulta a existência de outros. Já no uso dos *hackers*, a descoberta da façanha apenas indica a seus administradores que algo não está correto.

Há ainda duas outras classificações quanto ao modo como o computador é atingido e podem ser identificadas de acordo com as respostas da máquina. São estas: interrupção e corrupção. A interrupção corrompe os sistemas e pode ser identificada ao causar o desligamento do computador, forçá-lo a trabalhar com uma fração de sua capacidade e permitir que erros bobos sejam cometidos. A corrupção altera dados ou algoritmos e tem efeitos sutis, dificultando sua percepção. Em regra geral, os efeitos da interrupção são drásticos, imediatos e claros, enquanto os da corrupção são lentos, sutis e podem permanecer ou sumir com o tempo (LIBICK, 2012: 16).

Diante das explanações, Libick (2009: 17) afirma que não é possível forçar a entrada no espaço cibernético. A entrada só acontece se a máquina permitir. Desse modo, em teoria, a infiltração de qualquer *malware*[4] em um computador é culpa do sistema do computador, embora todos os sistemas sejam passíveis de erro. O autor afirma que quanto mais complexos os sistemas, mais brechas existem onde os erros podem se esconder.

Outro autor a se preocupar com a organização das ações cibernéticas é o Nye (2012: 166), que separa o poder cibernético em brando e duro. Assim como nas Relações Internacionais, o poder brando corresponde às ações leves e que de algum modo vão persuadir ou atrair a atenção do alvo para onde os possuidores do poder desejam, enquanto o poder duro é aquele capaz de gerar maiores danos, além de ser mais facilmente percebido.

Quanto às ações de controle, estas também se dividem de acordo com sua localização, tratando-se do intraespaço e do extraespaço cibernético. O intraespaço está relacionado ao que ocorre no domínio da Internet, ou seja, dentro da rede; enquanto o extraespaço é o que acontece fora deste domínio, podendo acontecer nas estruturas físicas ou longe das redes e computadores (NYE, 2012:166-167).

---

[4] Termo do inglês entendido como *software* malicioso, porém, por tratar-se de um jargão da área de Segurança da Informação, optou-se por não traduzi-lo.

Por fim, há a qualificação dos instrumentos utilizados para o controle do poder cibernético. Estes se dividem em físicos (aqueles ocorrentes nas estruturas físicas e que podem servir de alvo dos ataques) ou de informação (aqueles que são comandados pelo computador). Para facilitar a compreensão da organização definida por Nye (2012) e acima apresentada é interessante a visualização dos exemplos do Quadro 1:

Quadro 1 - Alvos do poder cibernético

	Intraespaço cibernético	**Extraespaço cibernético**
Instrumentos de informação	**Duro**: Ataques de negação de serviço **Brando**: determinação de normas e padrões	**Duro**: ataque em sistemas Scada[5] **Brando**: campanha de diplomacia pública para influenciar a opinião pública
Instrumentos físicos	**Duro**: controle das companhias por parte do governo **Brando**: software para ajudar ativistas dos direitos humanos	**Duro**: roteadores de bomba ou corte de cabos **Brando**: protestos para denunciar os provedores cibernéticos

Fonte: Nye (2012: 166).

Como apresentado no Quadro 1, o autor demonstra que tanto no intraespaço quanto no extraespaço cibernético os ataques podem ocorrer de forma dura ou branda e através de instrumentos físicos ou de informação, ou seja, não há grau de dependência entre os modos de ataque. Ainda sobre o poder cibernético, o autor afirma existirem três faces que ele não nomeou, mas apresentou. A primeira é quando por meio da computação ou da comunicação um ator é convencido a agir diferente do delineado em seu planejamento anterior. Na segunda face, a estratégia do inimigo é eliminada, impedindo que suas escolhas se mantenham, enquanto na última as preferências de um ator são moldadas de modo a garantir que algumas estratégias jamais sejam consideradas (NYE, 2012: 169-171).

Thévenet (2006: 7) classificou os ataques em físicos, eletrônicos e informáticos. Os ataques físicos envolvem armas convencionais e são aqueles que acontecem contra centros de informação ou conjuntos de cabos que fornecem *links*, como bem explicou Libick. Os

[5] Primeiro pacote de software para controle e aquisição de dados (PENIN, 2007:25).

eletrônicos utilizam energia eletromagnética como arma. Alguns exemplos são: o uso de um pulso eletromagnético para sobrecarregar os circuitos de computadores, ou, de modo menos violento, a inserção de um fluxo de códigos maliciosos nas transmissões de micro-ondas do inimigo. Por fim, o ataque informático implica na inserção de códigos maliciosos que, como uma arma para infectar computadores, vão procurar explorar as falhas do *software*.

Face ao exposto percebe-se a existência de uma variedade de formas e meios para desferir ataques cibernéticos. Por se tratar de uma área relativamente recente ainda há muito a ser descoberto e, consequentemente, organizado, porém, os trabalhos supracitados já possibilitam compreensão do grau de periculosidade e da importância do investimento cibernético como forma de se preparar para tais ataques. Assim, o próximo capítulo tem como objetivo apresentar o modo como se dá a participação asiática e como o espaço cibernético vem sendo utilizado por esses atores. Para tanto, serão expostos alguns dos conflitos cibernéticos mais relevantes nas discussões internacionais de modo a constatar a frequente participação de países asiáticos, seja como vítimas ou possíveis agressores.

2. O ENVOLVIMENTO CIBERNÉTICO DA REGIÃO ASIÁTICA

O envolvimento asiático nos conflitos cibernéticos tornou-se muito frequente, com seus países aparecendo algumas vezes como vítima e em outras como agressor. O destaque dado à Rússia, China, Índia, Japão, Paquistão e às Coreias, considerados pelo Pentágono como países possuidores de exército cibernético, também é fator a evidenciar um poder cibernético preponderante no continente asiático. Logo, visando facilitar a visualização de tal capacidade, o segundo capítulo será iniciado com a exposição de alguns conflitos com participação asiática e seguirá para a busca por uma maturidade cibernética[6] na Ásia-Pacífico.

1. Apresentando os ciberconflitos

Considerando que as definições de guerra cibernética e ataque cibernético muitas vezes se confundem – como acontece com as definições de Krepnevich (2012:8) e Caplan (2012:94), apresentadas no primeiro capítulo – a presente seção tratará da exposição de alguns ataques e conflitos cibernéticos envolvendo países asiáticos. A apresentação de tais casos visa ao conhecimento das capacidades cibernéticas asiáticas e do modo como essas capacidades vêm sendo utilizadas pelos países da região. Os eventos serão apresentados em sequência cronológica começando com os iniciados pela Rússia, em 2007, contra a Estônia e no ano seguinte contra a Geórgia, e seguirão até o caso mais recente de ataque à Sony, supostamente provocado pela Coreia do Norte, ocorrido em novembro de 2014. Diante da pequena quantidade de artigos científicos e acadêmicos, dado que alguns destes conflitos ainda são considerados recentes, a presente seção dar-se-á através da utilização de fontes acadêmicas e jornalísticas.

1. Rússia contra Estônia – 2007

O primeiro caso de ataque cibernético a ser exposto foi iniciado pela Rússia, em 2007, contra a Estônia[7]. O conflito foi desencadeado depois que a estátua de bronze de um soldado soviético, assim como seus restos mortais enterrados sob a estátua, foi realocada do centro de Tallinn, a capital estoniana, para o cemitério militar. Embora para a população estoniana a

[6] O termo maturidade cibernética foi elaborado pelo Instituto Australiano de Política Estratégica (*Australian Strategic Policy Institute* - ASPI) e diz respeito à presença, à implementação e à operação efetiva de estruturas, políticas, legislação e organizações relacionadas à área cibernética (ASPI:2014:5).

[7] A Estônia é um país pequeno e de alta tecnologia. Foi um dos pioneiros na utilização de meios eletrônicos para uso do governo e é dependente de redes de computadores, tendo na Internet a estrutura vital de seu Estado. Por tais motivos, é considerado altamente vulnerável aos ataques cibernéticos. (THE ECONOMIST, 2007; THE GUARDIAN, 2007).

ação tenha significado o abandono ao símbolo da odiosa ocupação estrangeira, os estonianos de descendência russa e imigrantes russos (cerca de 30% da população estoniana) entenderam o ato como desrespeito às lembranças contidas no memorial soviético da Segunda Guerra Mundial e, movidos por esse sentimento, mobilizaram-se e organizaram uma onda de protestos (BBC BRASIL, 2007).

O governo russo se opôs à retirada do monumento, considerando-a uma afronta à memória daqueles que morreram para salvar do perigo nazista a região. Em represália, o Estado russo chamou o ato de blasfêmia e anunciou que as relações diplomáticas entre os países seriam afetadas, como pode ser constatado no discurso do líder do senado russo, Sergei Mironov.

> "Posso estar abusando de minha autoridade, mas proponho que consideremos a sugestão ao presidente russo de que ele corte as relações com a Estônia [...] Já é hora de eles (estonianos) pararem de zombar dos mortos, é hora de eles pararem de zombar da memória de uma grande vitória. Isto já foi longe demais!" (BBC BRASIL, 2007).

A Rússia também chegou a pedir a renúncia do governo estoniano. O principal motivo de sua inconformidade deu-se, em especial, pelo fato de a transferência da estátua acontecer no dia 8 de maio, véspera do feriado sagrado em comemoração à vitória russa sobre a Alemanha nazista (BBC BRASIL, 2007). O fato é que a polêmica em torno da remoção da estátua mobilizou ciberativistas por todo o globo, mas principalmente de origem russa, que espalharam instruções no idioma russo sobre como atacar os sites das instituições estonianas. Os ataques ficaram conhecidos como o primeiro incidente direcionado a um Estado (THE GUARDIAN, 2007) e ameaçavam cortar a comunicação dos sites do país com o resto do mundo.

Os *hackers* desativaram o servidor de e-mail parlamentar e as capacidades de tecnologia da informação e comunicação (TIC) de vários ministérios do governo, impossibilitando que o Estado pudesse responder de forma eficaz. Eles também elaboraram uma estratégia que Herzog (2011: 52) chamou de estratégia "enxame" de ataque de negação de serviço distribuída (*Distributed Denial of Service Attack - DDoS*), pela qual sites de bancos e agências do governo, que costumavam receber mil acessos diários, de repente, estavam recebendo 2 mil acessos por segundo. Para o ex-assessor de segurança da Casa Branca, Howard Schmidt, "*a Estônia tem construído seu futuro na busca por um governo e uma economia de alta tecnologia, e estes, basicamente, estão de joelhos por causa desses ataques*" (HERZOG, 2011:52, tradução livre).

A frase do ex-assessor de segurança diz respeito ao nível tecnológico da Estônia, que é altamente informatizada e é considerada um dos países pioneiros no investimento em "governo eletrônico" (CASTRO, 2007:1). O alto nível de informatização do país produziu maior vulnerabilidade e permitiu que os ataques de negação de serviço, iniciados em 27 de abril, permanecessem por várias semanas. De acordo com Fritz (2008:66), os ataques estonianos demonstraram capacidade de duração de um mês. Em meio a tanta movimentação, um grupo juvenil de apoio ao governo russo atacou a embaixada estoniana em Moscou. Essa ação deu origem a protestos em vários outros países e por parte do governo dos Estados Unidos, da União Européia e da Organização do Tratado do Atlântico Norte (OTAN).

Com o forte apoio que o ocidente ofereceu à Estônia, a Rússia foi acusada de desencadear guerra cibernética para desativar a Estônia (THE GUARDIAN, 2007; THE ECONOMIST, 2007). Embora a maioria dos ataques iniciais seja proveniente de endereços russos, principalmente de instituições estatais do Estado, Castro (2007:2) defende ser impossível alegar que os ataques eram realmente provenientes do governo russo, já que os endereços utilizados podem ter sido trocados ou falsificados com o objetivo de conferir aos russos tais realizações.

A Organização do Tratado do Atlântico Norte (OTAN), que tem a Estônia como membro, enviou especialistas em terrorismo virtual para investigar a situação do país, que foi considerada uma séria questão de segurança tanto para a Estônia quanto para a OTAN. A União Europeia seguiu o exemplo da OTAN e resolveu se envolver, porém de modo mais severo. Enquanto a OTAN interveio sem atribuir culpa a qualquer ator, o então presidente da Comissão Européia, José Manuel Barroso, em reunião com o presidente russo, Vladmir Putin, em 18 de maio de 2007, anunciou que qualquer ataque a um membro da comunidade europeia seria considerado um ataque ao todo (CASTRO, 2007:2-3).

Como explicado por Herzog (2011: 50), as respostas multinacionais sobre os ataques terroristas da Estônia demonstram um crescente interesse dos Estados e organizações na defesa da soberania nacional no domínio cibernético. Esse interesse pode oferecer a base para uma discussão mais aprofundada sobre os casos e possíveis resoluções para os problemas cibernéticos e para a construção de uma cooperação para a segurança cibernética. Outro caso com participação russa, motivação étnica e envolvimento externo foi o conflito envolvendo a Geórgia, apresentado no próximo tópico.

2. Rússia contra Geórgia – 2008

O segundo caso, e que também possui participação russa, é o conflito entre Rússia e Geórgia, ocorrido em 12 de agosto de 2008. Depois de períodos de guerra entre Geórgia e Ossétia do Sul, a Rússia entrou na região como mediadora do conflito, levando consigo as Operações de Paz. Horas depois do Estado russo entrar no conflito, *hackers* localizados na Rússia criaram um *site* – stopgeorgia.ru – onde expuseram uma lista com sites da Geórgia a serem alvos, mostrando quais sites tinham sido abatidos com sucesso e disponibilizando um programa simples que depois de baixado permitiria que o computador com o programa participasse do ataque (FRITZ, 2008:61).

De acordo com Fritz (2008:61), as invasões incluíram ataques de DDoS de seis *botnets*[8] diferentes contra o governo e *sites* de notícia, invasões de páginas da rede, *spam*, distribuição de endereços de *e-mail* dos funcionários georgianos e a distribuição de uma lista de *sites* do governo georgiano com conhecidas falhas de segurança. *Hackers* que se comunicavam em russo tentaram impossibilitar qualquer resposta por parte da comunidade *hacker* georgiana, derrubando, em seu ataque inicial, os dois sites de hackers com maior destaque na Geórgia: *hacker.ge* e *warez.ge*. Ainda segundo o autor, o nível de sofisticação destes ataques foi superior aos da Estônia, mostrando que a utilização das capacidades cibernéticas está sendo continuamente aprimorada.

De acordo com a versão eletrônica do *The New York Times*, de 12 de agosto de 2008, especialistas americanos convidados para analisar a situação afirmaram que os ataques às infraestruturas críticas estonianas começaram em 20 de julho. O mesmo grupo que rastreou a atividade maliciosa na rede informou que o *site* do presidente georgiano, Mikheil Saakashvili, ficou inoperável por 24 horas depois dos incalculáveis ataques de DDoS. Conforme cresciam as tensões do conflito armado, os ataques de negação de serviço se espalhavam por toda a Estônia, atingindo também as empresas de transporte e comunicação (THE NEW YORK TIMES, 2008).

Mais uma vez a autoria do ataque cibernético recai sobre a Rússia, quando oficiais georgianos alegam que as forças armadas do Estado russo estavam por trás dos ataques. Novamente a informação careceu de comprovação, mas abriu os olhos da comunidade

[8] *Botnet* significa rede de robôs (do inglês: *robot network*) e diz respeito a uma série de comando ou um programa projetado para desempenhar funções de comando, podendo enviar vírus ou *spam* para outros computadores conectados à Internet. Não é necessariamente malicioso ou prejudicial, mas ultimamente vem sendo utilizado por cibercriminosos no roubo de informações confidenciais, introdução de *malware* em arquivos de código fonte, interrupção do acesso ou do serviço e roubo de informação de identidades (BU et al., 2010:3).

internacional para a possibilidade de conflitos patrióticos envolverem a união da guerra tradicional à guerra cibernética e provou que ataques cibernéticos patrióticos podem prejudicar o *soft power* dos Estados e iniciar ataques nocivos de retaliação (FRITZ, 2008:62).

De acordo com Nye (2008), este é o conflito que "representa os primeiros ataques cibernéticos significativos acompanhados de conflito armado". Nichol (2009:11) explica que além do enorme dano causado pelos ataques às infraestruturas críticas do país, centenas de civis e militares foram deslocados e inseridos nas listas para ações humanitárias. Entre 1500 e 2000 pessoas morreram neste conflito. Desse modo, o ataque cibernético à Geórgia, que evoluiu para um conflito armado, terminou com a intervenção norte americana por meio do Conselho de Segurança da Organização das Nações Unidas (ONU) (SOUZA, 2010: 52-55).

Segundo o *The New York Times*, de 12 de agosto de 2008, pesquisadores americanos de segurança da computação, cujos nomes não foram mencionados, rastrearam programas maliciosos conhecidos como *botnet* e afirmaram ter evidência da participação de uma gangue criminosa com base em St. Petersburg, conhecida como *Russian Business Network*, ou RBN. "*Os atacantes estão usando as mesmas ferramentas e comandos de ataque usados pela RBN*", afirmou Don Jackson, diretor de inteligência de ameaças da *SecureWorks*, empresa de segurança da computação, sob responsabilidade da Dell. Apesar da suposta conexão, por questões próprias à natureza do espaço cibernético, nem a origem dos ataques, nem a conexão entre a RBN e o Estado Russo podem ser comprovadas (THE NEW YORK TIMES, 2008).

Contudo, faz-se necessário considerar a longa história de conflitos étnicos entre Rússia, Estônia e Geórgia, além dos demais países da extinta União Soviética, como possível motivação para os ataques cibernéticos nas mais variadas situações. Cabe destacar que a participação russa em um grande número de conflitos regionais deu-se depois que, em 1992, o país abriu um processo de candidatura à cidadania russa. O processo contou com muitos pedidos das regiões vizinhas e concedeu ao estado russo o poder de, através do direito à intervenção para a proteção de sua população, participar das diversas negociações (AFCEA, 2012: 2-3).

Assim deu-se o primeiro conflito cibernético a unir a guerra virtual à guerra tradicional, que só não obteve resultados mais drásticos porque, diferentemente da Estônia, a Geórgia não é dependente da alta tecnologia. No final, a Geórgia, com uma população de apenas 4,6 milhões de habitantes e um considerável atraso em relação à Internet, sentiu pouco efeito além da inacessibilidade de muitos dos seus *sites* do governo e da limitação na capacidade do governo espalhar sua mensagem *on-line* e de se conectar com o mundo durante

o conflito (THE NEW YORK TIMES, 2008), enquanto a Rússia, que busca melhor desempenho na "guerra de informação", se prepara por meio de participação externa (GILES, 2011:56). Ademais, também há casos de uso da tecnologia cibernética para fins de roubo, destruição e/ou modificação de dados, expostos a seguir.

3. Stuxnet - 2010

Outros casos de ataque cibernético demostram a utilização da tecnologia como meio exclusivo para se alcançar simples objetivos ilícitos, como obtenção de informação secreta, roubo de identidade, destruição e/ou modificação de dados e de programas virtuais. Um bom exemplo desse tipo de utilização é o vírus Stuxnet – considerado a primeira "ciberarma" de uma guerra cibernética – que em 2010 invadiu o sistema iraniano e danificou suas ogivas, atrasando seu programa nuclear. O Stuxnet é um vírus sofisticado, projetado para atacar específicos sistemas SCADA (de controle industrial) e ter sua detecção dificultada pelo antivírus, uma vez que se apresenta como um programa de software legítimo e com certificado digital (MUELLER, YADEGARI, 2012: 1).

Descoberto em junho de 2010, o vírus teve sua primeira versão no ano anterior. Possuidor de uma função muito especial, o Stuxnet visava ao ataque específico ao programa iraniano de enriquecimento de urânio (MUELLER; YADEGARI, 2012:1-3). O vírus aparentemente infectou mais de 60 mil computadores com mais da metade estando localizada no Iran, apesar de também ter alcançado computadores na Índia, China, Indonésia, Azerbaijão, Coreia do Sul, Malásia, Estados Unidos, Reino Unido, Finlândia e Alemanha. O especialista alemão, Ralph Lagner, descreve o Stuxnet como "um míssil cibernético de nível militar, utilizado para lançar uma 'greve geral' contra o programa nuclear iraniano" (FAREL; ROHOZINSKI, 2011:23, tradução livre).

O vírus, julgado o mais sofisticado e inusitado pedaço de *software* já criado (*ibidem*) e uma das mais complexas ameaças de que se tem conhecimento (FALLIERE et al., 2011:1), recebeu muita atenção por parte de investigadores e meios de comunicação. Por tratar-se de um *malware* tão sofisticado, a investigação sobre seu funcionamento e seus objetivos tem tomado muito tempo dos laboratórios. Apesar do trabalho sobre o vírus ainda não estar completo, algumas suposições vem sendo polemizadas.

Se o objetivo do vírus era acabar com o programa nuclear iraniano, por exemplo, ele falhou quando destruiu cerca de mil centrífugas, que correspondem a apenas 11% do total. Embora essa diminuição seja significativa, não foi suficiente para acabar com o programa. O

vírus, que usou técnicas avançadas para se esconder de usuários e antivírus, também era capaz de se atualizar automaticamente de modo a atualizar as versões antigas de si mesmo para as versões mais recentes disponíveis numa rede local. Apesar de se espalhar facilmente, o Stuxnet possuía limites de propagação: cada unidade infectada poderia infectar mais três computadores no prazo de até 24 de junho de 2012 (MUELLER; YADEGARI, 2012:5).

Dado que o destino final do Stuxnet era os computadores que controlavam as centrífugas, chamados de Controladores Lógicos Programáveis (*Programmable Logic Controllers* - PLCs), considerados computadores de uso especial, controlados e monitorados por outros computadores e, normalmente, não conectados à Internet, Falliere (et al.,011:3) acredita que se fazia extremamente necessária a utilização de *insiders*, os quais possuem papel fundamental no alcance de informações que exige elementos e/ou pessoas infiltradas. Outros autores levantam a hipótese de que os dispositivos USB infectados devem ter sido introduzidos nos computadores de controle via empresas externas que trabalham na fábrica, ou seja, por meio de alterações na rede de abastecimento (MUELLER; YADEGARI, 2012: 5; FAREL; ROHOZINSKI, 2011: 24-25).

Para Singer (2012), estes ataques cada vez mais sofisticados foram secretamente ordenados pelo presidente Obama que decidiu acelerar os ataques iniciados no governo Bush (de codinome Jogos Olímpicos), porém de tipo e sofisticação completamente diferentes dos primeiros ataques. O supervisor do Symantec Security Response, Liam O Murchu, cuja empresa emitiu um relatório detalhado sobre o seu funcionamento, declarou: "Nós definitivamente nunca vimos nada como isso antes" (FAREL; ROHOZINSKI, 2011:23, tradução livre).

Dessa forma, pode-se constatar que as invasões cibernéticas seguem evoluindo em ritmo acelerado, admitindo que cada nova arma cibernética se faz muito superior à última. Outro caso de infiltração, porém objetivando o roubo de informação, é o vírus Flame, que envolveu países do Oriente Médio. Ele foi descoberto dois anos depois do caso Stuxnet e será retratado no próximo tópico.

4. Flame – 2012

Por tratar-se do *malware* mais sofisticado já encontrado até a finalização da pesquisa, muitos dos pesquisadores a trabalhar no estudos dos conflitos cibernéticos tinham como objetivo o estudo completo das funções e aplicações do vírus. Com isso, a maioria dos artigos acadêmicos sobre o Flame trata especificamente de seus sistemas, técnicas e algoritmos

utilizados para a captura de informação, aspectos que não estão relacionados ao presente trabalho e que justificam o breve comentário.

O vírus Flame é um caso de "ciberespionagem", descoberto em maio de 2012, mas que, segundo Rohr (2012), já agia há dois anos roubando dados dos governos do Irã (com o maior número de vítimas), Israel e Palestina, Sudão, Síria, Líbano, Arábia Saudita e Egito. Esse vírus se sobressai por sua capacidade de se camuflar e enganar os *softwares* – uma vez que não foi identificado por nenhum sistema antivírus – e sua complexa estrutura, que segundo a Kaspersky, empresa de segurança *online*, deve levar anos para ser analisado adequadamente (ROHR, 2012).

Ainda de acordo com a Kaspersky, o Flame é um programa malicioso altamente sofisticado, projetado para realizar espionagem cibernética e capaz de roubar informações valiosas incluindo, mas não se limitando, a dados contidos nas telas dos computadores e conversas de áudio. Naquele período ele considerado a maior arma cibernética descoberta, uma vez que foi projetada de modo a tornar seu rastreamento quase impossível. O programa ainda infectou computadores utilizando técnicas sofisticadas antes utilizadas apenas pelo Stuxnet. Apesar de descoberto em 28 de maio de 2012, o Kaspersky Lab afirma que o vírus estava em ativa desde março de 2010 (KASPERSKY LAB, 2012).

Os vírus Flame e Stuxnet possuem propósitos e composições diferentes e parecem ser originários de programadores diferentes. Porém, a complexidade e a localização geográfica de suas infecções, além de seus comportamentos, indicam que estes são frutos de ações de um Estado e não de cibercriminosos comuns. Patrascu (2013:2) acredita que o Flame seja parte de um projeto paralelo criado por trabalhadores contratados pela mesma equipe do Estado por trás do Stuxnet e dos *malwares* relacionados.

Entre muitos módulos do vírus Flame há um com a função de ligar o microfone interno de uma máquina infectada para gravar secretamente conversas que ocorrem tanto através do Skype quanto nas proximidades do computador. Há ainda um módulo que transforma em um farol os computadores habilitados para *Bluetooth*. E também há um módulo *Bluetooth* que agarra e armazena *screenshots* frequentes de atividade da máquina, tais como de mensagens instantâneas e comunicações por *e-mail* e envia-os através de um canal SSL secreto para os servidores de comando e controle dos agressores (*ibidem*:3).

Segundo Morton e Grace (2012), o Flame, também conhecido como w32, foi projetado para roubar diferentes bancos de dados. Uma funcionalidade distinta usada por um

vírus é a "Áudio espionagem" que pode gravar áudio, imagens e pode monitorar as atividades do teclado e o tráfego da rede. O *malware* também tem um componente que pode digitalizar toda a informação de uma máquina infectada e coletar nomes de usuários e senhas transmitidas através da rede. Os atacantes parecem utilizar esse componente para roubar contas administrativas e ganhar privilégios de alto nível em outras máquinas e outras partes da rede. Apesar de usar vários métodos para se replicar, os mais interessantes são o uso do serviço de Atualização do Microsoft Windows e através de dispositivo Bluetooth (PATRASCU, 2013:5).

5. Outubro Vermelho - 2012

O caso descoberto em outubro de 2012 é o do vírus batizado de Outubro Vermelho. Este, que existe há pelo menos cinco anos, atacou organizações em aproximadamente setenta países, incluindo o Brasil – apesar de os principais alvos serem os países do Leste Europeu, ex-repúblicas soviéticas e países da Ásia Central. A empresa russa Kaspersky afirma ainda que o vírus foi desenvolvido para roubar arquivos de instituições como embaixadas, centros de pesquisa nuclear e institutos ligados a setores como gás e petróleo.

Teti (2013:63-64) explica que o código malicioso assumiu o papel de caçador, pois, como tal, manteve-se silencioso e agressivo e os ataques se espalharam da Ásia para os Estados Unidos, principalmente contra estruturas institucionais, governos e principalmente embaixadas. A missão principal dos criminosos cibernéticos era a coleta de informações referentes aos tipos de sistemas de informação que foram objeto dos ataques aos dispositivos móveis conectados a eles (*notebooks, netbooks, smartphones, iPads* etc.), às diferentes variedades de aparelhos roteador e às bases de dados armazenados na memória dos sistemas de computador.

Técnicos da Kaspersky afirmam que mais de três mil dispositivos foram derrubados pelo Outubro Vermelho e que documentos altamente confidenciais foram roubados da memória do computador. Os especialistas também defendem que o vírus é capaz de decifrar mensagens e documentos criptografados (TETI, 2013:65). O vírus é capaz de penetrar nos computadores e retirar todas as informações armazenadas e também detectar todos os dispositivos ligados ao controlador através de interfaces de conexão diferente – como USB, *wireless* e *Bluetooth* – dos computadores violados.

Kamlyuk, componente da unidade espacial da Kaspersky, ao ser entrevistado por Teti (2013) sobre as capacidades do Outubro Vermelho, afirmou: "Nunca antes vimos um ataque

realizado com tal precisão cirúrgica". Outubro Vermelho pode ser considerado o primeiro programa autêntico desenvolvido para realizar ações de espionagem em rede (TETI, 2013:73). Segundo a empresa McAfee (2013), o Outubro Vermelho é uma rede de ataque e espionagem cibernética que tinha como alvo agências diplomáticas e governamentais. As ameaças que foram utilizadas nessa campanha de ataques têm sido conhecidas por estarem na ativa desde 2009. Esse ataque teve como alvo escritórios diplomáticos e ministérios, incluindo a embaixada da Rússia.

Quanto ao suposto culpado, as suspeitas caem sobre os chineses e russos, pois, segundo relata a Kaspersky, o código do programa inclui termos no inglês mal escrito e uma gíria russa que não é usada em nenhuma outra língua. Já os chineses estão sendo acusados de envolvimento em muitos outros ataques por possuírem um "exército" cibernético. Apesar da evidência, esta palavra pode ter sido propositadamente posta no programa para gerar suspeitas contra os russos, embora na verdade não haja nenhuma prova (KASPERSKY, 2013). Mais um exemplo de guerra cibernética envolvendo ataques entre Ocidente e Oriente é o caso da agressão à empresa Sony, explanado a seguir.

6. A Coreia do Norte e o ataque à Sony – Novembro de 2014

Em 24 de novembro de 2014, dados confidenciais pertencentes à *Sony Pictures Entertainment* foram divulgados. Entre informações pessoais de funcionários, *e-mails* e dados financeiros da empresa, havia também cópias prévias de filmes inéditos. Os *hackers* que se intitularam guardiões da paz (*Guardians of Peace* - GOP) reivindicaram o cancelamento do lançamento do filme 'A Entrevista', uma comédia sobre um complô para assassinar o líder norte-coreano Kim Jong Un. Depois de avaliar o software, técnicas e fontes de redes utilizadas na ação, o FBI (*Federal Bureau of Investigation*) divulgou que o ataque era de origem norte coreana. Alguns especialistas em segurança cibernética duvidarem das provas e sugeriram participação de *insiders* trabalhando na Sony.

Apesar das novas suposições, a Sony decidiu suspender o lançamento do filme. Em nota, o presidente americano afirmou ser um erro permitir que estranhos se manifestassem contra a liberdade americana e defendeu:

> Não podemos ter uma sociedade na qual algum ditador de algum lugar pode começar a impor a censura aqui nos Estados Unidos" e concluiu explicando que "se alguém é capaz de intimidar as pessoas para não liberar um filme satírico, imagine o que eles começarão a fazer quando virem um documentário que eles não gostam ou notícias de algo que eles não gostam (THE WASHINGTON POST, 2014, tradução livre).

O discurso do presidente estadunidense reacendeu o nacionalismo americano e deu suporte à decisão da Sony de manter a exibição do filme, embora em uma menor quantidade de salas. Esse e os demais conflitos ou ataques aqui expostos constatam que desde o primeiro ato de guerra cibernética há forte participação de países asiáticos. O envolvimento de Estados da região em tais modelos de conflito tem promovido inseguranças e aumentado os riscos de atos cibernéticos com resultados catastróficos.

Apesar da grande disparidade tecnológica entre as nações da região asiática, que possuem os países de maior e menor índice de conexão à Internet, a percepção comum que vem afligindo todos os Estados da região foi responsável pela união e organização de ações necessárias para a construção da segurança cibernética da região e pela idealização de uma maturidade cibernética na Ásia-Pacífico, como evidenciadas a seguir com o objetivo de fornecer visão e ações continentais possibilitando melhor compreensão das intensões e objetivos sínicos.

2. Cooperação asiática pela segurança cibernética da região

O espaço cibernético, unido às tecnologias de informação e comunicação (TIC), tem servido de ferramenta responsável por grande crescimento econômico, transformação política e mudança social na região da Ásia-Pacífico. Como resultado, os países da região passaram a investir cada vez mais em tecnologias conectadas à rede visando melhor organização e aproveitamento de seu capital. Embora a adesão a esta tecnologia tenha verdadeiramente facilitado a distribuição de recursos essenciais à sociedade civil, (como água e energia entre outros), e alavancado o comércio *online*, também trouxe novas vulnerabilidades e expôs os países às ameaças cibernéticas (THOMAS, 2009: 3; ASPI, 2014: 5).

Sabe-se que o espaço cibernético é um ambiente originalmente "desenhado para ser livre, anárquico, descentralizado e autoexpansível" (SOUZA, 2012: 13), cujas identidades podem ser facilmente fabricadas. Nele os ataques acontecem dentro e fora das fronteiras nacionais e têm vantagem sobre a defesa (LEWIS, 2009:1). A natureza transnacional dos conflitos inviabiliza ações governamentais de securitização das ameaças cibernéticas, já que ações unilaterais permitem apenas a execução de leis limitadas a um território específico, não possuindo alcance global (ASPI, 2014:5).

Diante da dificuldade de se garantir uma segurança cibernética em âmbito nacional – uma vez que ações no âmbito doméstico não produzem resultado em outros territórios, motivo pelo qual se tornam insuficientes para o controle de um espaço sem fronteiras – os Estados

asiáticos cogitaram uma integração regional visando à proteção de seus interesses comuns e à implementação de uma segurança cibernética coletiva, que, segundo Thomas (2009:14), depende de ações nas camadas doméstica, regional e internacional. Por ser uma região com forte participação nos casos de ataques cibernéticos, as preocupações da região vêm envolvendo todos os países e instituições regionais que passaram a disponibilizar maior tempo e recurso para as questões que tanto afligem os países do continente (THOMAS, 2009:4) e resolveram se unir na busca pela segurança cibernética coletiva da região pacífico-asiática.

Para tanto, Thomas (2009:3-4) afirma ser necessário recorrer às práticas utilizadas para assegurar a integração em outros setores e reproduzi-las no campo cibernético. Cabe ressaltar que o continente asiático possui inúmeros casos de rivalidade histórica ainda não superada sendo, portanto, um ambiente de hostilidade e desconfiança, fatores que dificultam o processo de integração regional, principalmente no que diz respeito a questões de segurança.

À vista disso, serão apresentadas as tentativas de cooperação e segurança cibernética desenvolvidas na APEC (Asia-Pacific Economic Cooperation), ASEAN+3 (Association of Southeast Asian Nations), assim como na ASPI (Australian Strategic Policy Institute), que apesar de instituto australiano, é responsável por galgar a "maturidade cibernética" da região Ásia-Pacífico. As organizações não serão apresentadas por disposição cronológica, mas por critério crescente de importância no tocante aos ganhos obtidos para a segurança cibernética coletiva da região.

1. APEC

A despeito da APEC (*Asia-Pacific Economic Cooperation*) tratar-se de uma organização para integração econômica da região Ásia-Pacífico, o presente trabalho busca apresentar suas atitudes no tocante à segurança regional e segurança cibernética, assim como explicar sua influência nas ações futuras de Estados e demais entidades da região.

A APEC, que foi construída para ser uma instituição econômica regional intragovernamental, idealizada pelos governos australiano e japonês e originada em 1989, com sua primeira reunião em Canberra (TERADA, 1999: 36), é hoje uma importante organização que conta com Austrália, Brunei, Canadá, Chile, Cingapura, Coreia do Sul, China, Estados Unidos, Filipinas, Hong Kong, Indonésia, Japão, Malásia, México, Nova Zelândia, Papua Nova Guiné, Peru, Rússia, Tailândia, Taiwan e Vietnã. A participação de países pertencentes a outras instituições regionais, como CARICOM (*The Caribbean Community*) e MERCOSUL (Mercado Comum do Sul), concede a exposição dos ideais de

segurança da APEC e a coloca em duas das camadas que Thomas (2009: 11-16) considera necessárias para a execução de uma segurança cibernética coletiva: a regional e a inter-regional ou internacional.

Embora os interesses da APEC estejam obviamente relacionados a questões comerciais, depois dos ataques de 11 de Setembro de 2001, assim como outras organizações regionais, a APEC, em 21 de outubro de 2001, considerou fundamental a inclusão de questões de segurança regional em suas agendas políticas. Depois de inúmeros desafios ao tentar proteger das ameaças cibernéticas os seus membros, seu foco encontrou-se nas áreas de comércio eletrônico e roubo de identidades e um grande aumento de recursos foi direcionado ao combate do crime regional e dos ataques cibernéticos terroristas, mudanças que foram responsáveis pela modificação do nome do Grupo de Tarefas de Autenticação Eletrônica para Grupo de Tarefas de Segurança Eletrônica (THOMAS, 2009: 11-15; APEC, 2002: 2-5).

Outras ações foram a inclusão da segurança às tecnologias de informação e comunicação e à proteção das infraestruturas de informação. As reuniões de 2001 e 2003 se concentraram em torno da proteção às infraestruturas críticas, especialmente de informação e comunicação, e resultaram, em 2001, na adoção da Estratégia de Segurança Cibernética (*Cybersecurity Strategy*), cujo documento continha recomendações que deveriam ser seguidas pelos Estados membros, incluindo a adoção de instrumentos legais para garantir a aplicação da segurança cibernética. A criação de tal documento foi fator importante na união de esforços para a construção de respostas domésticas e regionais para as ameaças cibernéticas (THOMAS, 2009: 13; APEC, 2002: 2-3).

No mesmo ano, em Moscou, a APEC formulou mais um quadro de recomendações extremamente importante para o desenvolvimento de ações necessárias para a segurança cibernética. Tal documento, entre outras coisas, conta com a afirmação de que a cibersegurança depende dos Estados-nacionais contarem com três pontos legais: 1) leis que criminalizem ataques às redes; 2) leis processuais garantindo que os agentes da lei possuam autoridade necessária para investigar e processar delitos facilitados pela tecnologia; v e 3) leis e políticas que permitam a cooperação internacional com outras partes na luta contra a criminalidade informática (APEC, 2002: 3).

Como consequência, alguns dos Estados que não possuíam leis para crimes cibernéticos passaram a elaborar sua legislação cibernética, enquanto outros acabaram reformulando as já existentes. No caso de Índia, Japão e Singapura houve tanto a atualização das políticas nacionais de cibersegurança já existentes quanto a formulação de outras leis

nessa área. Papua Nova Guiné e Camboja são exemplos de países que estão desenvolvendo novas leis para punição de delitos cibernéticos e a Austrália construiu, em 2014, o Centro Australiano de Segurança Cibernética (*Australian Cyber Security Centre*) (ASPI, 2014: 6). Todas essas iniciativas são positivas para o desenvolvimento da segurança cibernética da região e devem servir de modelo para outros países e regiões.

Ainda que a APEC seja uma instituição de natureza econômica ela tem servido de base para as ações dos Estados e de outras organizações da região. É relevante destacar que essa organização, por possuir membros de outras regiões e contar com Taiwan e Hong Kong, que não fazem parte da ASIAN, conseguiu vantagens, no que tange ao âmbito cibernético, superiores às conquistas da ASIAN (que trata especificamente de questões de segurança), além de ter sido precursora na criação de leis e doutrinas a orientar o comportamento dos Estados e a desenvolver a percepção da necessidade das três camadas (doméstica, regional e internacional) para a realização de uma segurança cibernética efetiva.

Ademais, a elaboração de diretrizes para a segurança cibernética serviu de base para o desenvolvimento de políticas e ferramentas nos três âmbito: doméstico, regional e internacional. Elas puderam ser adotadas por outras instituições, incluindo a Organização das Nações Unidas (ONU), que só em 2003 elaborou um quadro para a criação de um regime de segurança cibernética global através da proteção de infraestruturas críticas, apesar de vir discutindo o impacto das tecnologias da informação e comunicação na segurança internacional desde 1998 (THOMAS, 2009: 14-15; APEC, 2002: 1-6). Além da APEC, a região pacífico asiática detém ao menos mais duas instituições de cunho específico cujo intuito é de proporcionar fortes avanços à cooperação cibernética da região: ASEAN e ASPI.

2. ASEAN

A Associação de Nações do Sudeste Asiático (*Association of Southeast Asian Nations* - ASEAN) foi criada em 1967 por Indonésia, Malásia, Filipinas, Singapura e Tailândia com o objetivo de promover cooperação política, econômica e estabilidade regional. Atualmente é uma organização política, econômica e sociocultural formada por dez países que são os cinco iniciais mais a participação de Brunei, Camboja, Laos, Mianmar e Vietnã (U. S. DEPARTMENT OF STATE, 2015). A ASEAN possui suas variações que contam com a participação de mais países em situações específicas. Com foco na segurança cibernética, o presente trabalho se concentra na ASEAN + 3, que conta também com as presenças de Japão, China e Coreia do Sul.

Segundo Thomas (2009:3), todas as nações da ASEAN + 3 estão comprometidas com a criação de uma comunidade regional do Leste asiático. Desde a criação do Fórum Regional da ASEAN, em 1994, essas nações têm discutido formas de diminuir a insegurança regional e aumentar o nível de integração. Com o atentado de 11 de Setembro de 2001 nasce a era das ameaças cibernéticas, dada a produção de novos temores e o aumenta do interesse pela superação das deficiências cibernéticas assim como a construção de maior união entre os Estados, dentro das organizações, visando suavizar os desafios impostos pelas ameaças cibernéticas.

Nesse contexto a ASEAN vem trabalhando de duas formas: uma mais específica, de modo a tentar proteger o espaço cibernético de ameaças externas e principalmente do que pode ser ação de organismos terroristas; e uma mais geral, que busca a melhoria das capacidades regionais através do processo e-ASEAN (THOMAS, 2009:11). Este é um acordo entre seus Estados membros, pensado em 1999 e que tem entre seus objetivos o crescimento do comércio eletrônico, a promoção da cooperação para diminuição da exclusão digital e a construção de uma comunidade eletrônica que promova a consciência, os conhecimentos gerais e a valorização das TICs (e-ASEAN FRAMEWORK AGREEMENT, 2015).

Em suma, os Estados decidiram, através do plano e-ASEAN, utilizar estratégicas eletrônicas para aprofundar a integração e a interconexão entre as nações do bloco, promover a investigação coletiva de métodos para a superação da desigualdade digital do continente e criar oportunidades para através dos cursos de formação em TICs, promovidos pelos Estados mais avançados para os menos avançados, melhorar as economias dos países. Desde 2000, quando o quadro foi assinado, a cooperação entre os membros da ASEAN vem se expandindo e se aprofundando, principalmente no que tange aos campos de tecnologia da informação e comunicação e comércio eletrônico (THOMAS, 2009: 11-12).

Também pensado em 1999, em complemento ao projeto, nasce a Força Tarefa da e-ASEAN (e-ASEAN *Task Force*), único órgão consultivo da ASEAN que possui representantes dos setores público e privado de seus países membros e fornece conselhos políticos aos países do Leste asiático de modo a apresentar os meios mais apropriados para a construção de um ambiente propício ao desenvolvimento de infraestruturas de informação. Seu resultado mais visível está relacionado à criação do acordo sobre produtos, serviços e investimentos em TIC (*Framework Agreement on Information and Communications Technology Products, Services and Investiment*) (e-ASEAN TASK FORCE, 2015).

O acordo, assinado pelos chefes dos Estados membros da organização, representa um passo decisivo nos esforços de se criar uma estratégia coordenada para o desenvolvimento das TICs na região e estabelece o compromisso político de tomar as medidas necessárias para se alcançar as metas estipuladas na ASEAN. Como objetivo inicial, a Força Tarefa visa à utilização das TICs de modo a mostrar que a Revolução da Informação pode apresentar benefícios à sociedade civil (e-ASEAN TASK FORCE, 2015). Hoje, contudo, sabemos que além do desenvolvimento dos Estados e da interconexão entre eles, as tecnologias da informação e comunicação também promovem vulnerabilidades e podem causar sérios danos a suas populações e estruturas estratégicas.

Pensando nisso, a ASEAN vem desenvolvendo projetos de política conjunta - desenhados para aumentar a capacidade regulatória da região – e construindo uma rede de centros de treinamento de TIC para dar assistência a empresas de pequeno e médio porte. Como a ASEAN tem procurado aprofundar as conexões e capacidades cibernéticas regionais tornou-se primordial contar com a colaboração da China, que, considerada a maior potência cibernética da região, conduziria a formação de novas redes de TIC para tecnologia e desenvolvimento de aplicação, avanço de recursos humanos e a construção de redes de segurança capazes de resistir à exploração por organizações regionais cibercriminosas (THOMAS, 2009:12-13).

Ainda que o interesse inicial por investimentos em TIC estivesse relacionado à efetivação do comércio eletrônico, hoje a região percebe a necessidade de fortalecer e prevenir seus sistemas das ameaças e ataques cibernéticos. Essa preocupação tem por base o forte envolvimento de países da região em conflitos cibernéticos e a porcentagem de penetração sofrida pelos países membros da ASEAN. Embora a organização represente apenas 6% dos usuários da Internet, tem o índice de 20% de penetração[9], com Brunei, Singapura e Malásia sendo os países com maior porcentagem de participação na Internet, e Indonésia, Filipinas e Vietnã possuindo o maior número de usuários da Internet (KHANISA, 2013: 41-43), como apresentado na Tabela 1.

Tabela 1 - ASEAN: Penetração e Usuários da Internet

País	Penetração da Internet	Usuários de Internet	População
Brunei Darussalam	81%	318.900	395.027

[9] Traduzido do inglês, *penetration*, o termo está relacionado à porcentagem de pessoas com acesso à Internet, não à quantidade de infiltrações sofridas pelos Estados.

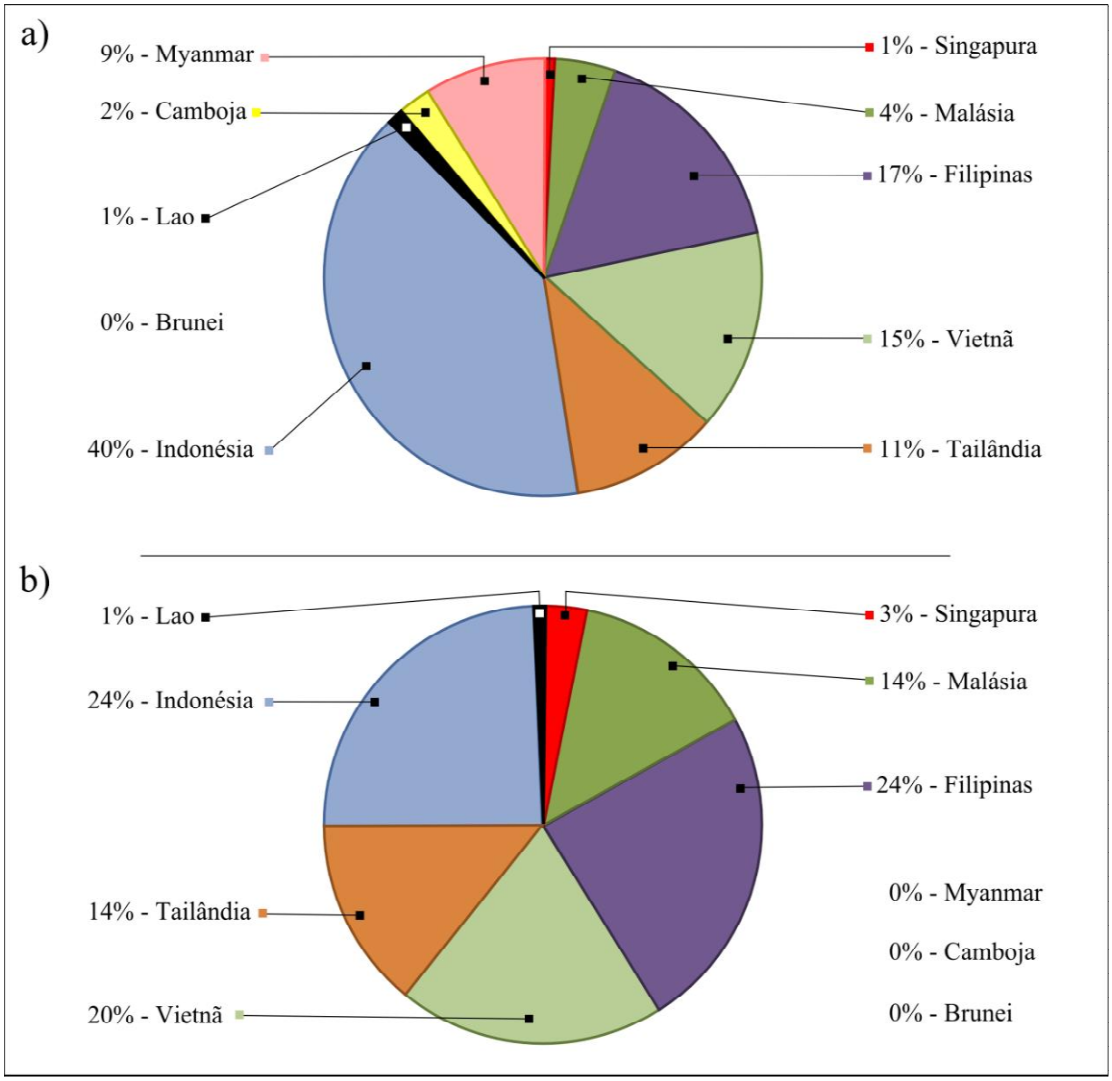
Singapura	78%	3.658.400	4.701.069
Malásia	65%	16.902.600	26.160.256
Filipinas	30%	29.700.000	99.900.177
Vietnã	27%	24.269.083	89.571.130
Tailândia	26%	17.486.400	66.404.688
Indonésia	16%	30.000.000	242.968.342
R.P.D. Lao	8%	527.400	6.993.767
Camboja	1,3%	173.675	13.800.000
Mianmar	0,2%	110.000	53.414.374
ASEAN	**20%**	**123.146.458**	**604.308.830**

Fonte: Adaptada de ASEAN E-Commerce Database Project (2010)

Outro modo de visualizar a proporção entre a população e o número de usuários da Internet dos países integrantes da ASEAN é através dos gráficos apresentados em Gráfico 1, o qual expõe as porcentagens que cada país representa na organização como um todo. Isso significa dizer que enquanto a Tabela 1 apresenta a porcentagem de acesso à Internet de cada país com base no cálculo entre sua população e quantidade de usuários da Internet, o Gráfico 1 apresenta, em porcentagem, a representação do espaço ocupado por cada Estado membro da ASEAN na própria organização. Observe.

Gráfico 1 - Proporção ocupada por cada membro da ASEAN

Em relação a: (a) População e (b) Usuários de Internet



Fonte: Baseada nas informações da ASEAN E-Commerce Database Project (2010).

Para melhor compreensão da diferença entre a Tabela 1 e o Gráfico 1, como exemplo, é dado destaque à população da Indonésia. Depois de observar ambas as fontes de informação é possível constatar que embora apenas 16% de sua população possua acesso à rede, de acordo com o exposto na Tabela 1, a população total da Indonésia corresponde a 40% da população da ASEAN e representa 24% dos usuários de Internet desta instituição. Desse modo, faz-se mister perceber que tanto a Tabela 1 quanto o Gráfico 1 consistem num complemento às informações já fornecidas, tornando-se necessárias para uma compreensão maior sobre o desenvolvimento cibernético da região.

Ainda que o espaço cibernético possua papel importante na região, a discrepância entre os poderes cibernéticos de cada Estado do continente é enorme. A despeito dos gráficos

corresponderem às informações sobre os países da ASEAN, e não da ASEAN + 3, Japão e Coreia do Sul, assim como Singapura, são os países tecnologicamente mais avançados do continente, com 84,1% da Coreia do Sul e 79,1% do Japão conectados à rede, enquanto China, Indonésia, Malásia, Filipinas e Tailândia são países de menor poder tecnológico, mas ainda muito expressivos se comparados à Brunei, Camboja, Laos, Mianmar e Vietnã (ASPI, 2014: 5).

As discrepâncias econômicas, sociais, políticas e principalmente tecnológicas da região Pacífico asiática dificultam a relação entre as nações do continente, principalmente, no que tange a questões de segurança, posto que Estados de maior poder econômico também são possuidores de maior recurso para investimento e, consequentemente, maior capacidade (NYE, 2012: 173-175). Contudo, diante do contexto cooperativo pela construção de uma segurança cibernética regional, o compartilhamento de informações e o trabalho conjunto dos atores regionais por meio da implementação de medidas comuns nas camadas doméstica, regional e internacional têm fortalecido a região e permitido que os Estados asiáticos se desenvolvam.

Outro fator a corroborar com a consolidação da segurança cibernética da Ásia-Pacífico é a criação de centros nacionais de estudo, resposta e tratamentos de incidentes de segurança da informação: do inglês, *Computer Emergency Response Team* – CERT (CERT BRASIL, 2015). Para os países da região asiática há a variação APCERT (*Asian Pacific Computer Emergency Response Team*), formada em 2002, que conta com vinte e sete centros em vinte economias e promove reuniões anuais chamadas de Conferência APSIR (*Asia Pacific Society for Impotence Research*), cuja primeira Conferência ocorreu em 2002, na capital do Japão (GLOBAL CYBER SECURITY CAPACITY CENTRE, 2014: 14; ITO, 2005: 3).

A APCERT, que, assim como as CERTs, parece ser fruto do comprometimento da ASEAN, tem a missão de melhorar a consciência e competência regional em relação à segurança da informação; desenvolver medidas que viabilizem lidar com incidentes em grande escala; facilitar a partilha de informação e troca de tecnologia entre seus membros, principalmente nos campos da segurança da informação, vírus e códigos maliciosos; promover a colaboração em investigações; auxiliar outras CERTs e CSIRTs (*Computer Security Incident Response Team*) a realizar respostas mais eficientes além das fronteiras regionais; e fornecer insumos e/ou recomendações para resolução de questões jurídicas de segurança da informação.

No APCERT, assim como na APEC, há a participação de países e regiões que não fazem parte da ASEAN ou de suas variações, o que demonstra maior alcance e consequentemente, maior poder de transformação e de produção de resposta eficaz por meio destes centros. Assim, somadas às ações de comprometimento da APEC e da ASEAN, Estados de todos os continentes têm se rendido à construção de unidades de Operação da CERT. No caso asiático, muitos são os países a participar da iniciativa e alguns com mais de uma unidade, como observado no Quadro 2:

Quadro 2 - Centros de Operação da APCERT

Centro	Nome Oficial do Centro	País
AusCERT	*Australian Computer Emergency Response Team*	Austrália
bdCERT	*Bangladesh Computer Emergency Response Team*	Bangladesh
BruCERT	*Brunei Computer Emergency Response Team*	Brunei Darussalam
CCERT	*CERNET Computer Emergency Response Team*	China
CERT Australia	*CERT Australia*	Austrália
CERT-In	*Indian Computer Emergency Response Team*	Índia
CNCERT/CC	*National Computer network Emergency Response technical Team / Coordination Center of China*	China
EC-CERT	*Taiwan E-Commerce Computer Emergency Response Team*	Taiwan
HK CERT	*Hong Kong Computer Emergency Response Team Coordination Centre*	Hong Kong
ID-CERT	*Indonesia Computer Emergency Response Team*	Indonésia
ID-SIRTII/CC	*Indonesia Security Incident Response Team on Internet Infrastructure Coordination Center*	Indonésia
JPCERT/CC	*Japan Computer Emergency Response Team Coordination Center*	Japão
KrCERT/CC	*Korea Internet Security Center*	Coréia
LaoCERT	*Lao Computer Emergency Response Team*	Laos
mmCERT	*Myanmar Computer Emergency Response Team*	Myanmar
MNCERT/CC	*Mongolia Cyber Emergency Response Team/Coordination Center*	Mongólia
MOCERT	*Macau Computer Emergency Response Team Coordination Centre*	Macau
MonCIRT	*Mongolian Cyber Incident Response Team*	Mongólia
MyCERT	*Malaysian Computer Emergency Response Team*	Malásia
NCSC	*New Zealand National Cyber Security Centre*	Nova Zelândia

SingCERT	*Singapore Computer Emergency Response Team*	Singapura
SriLanka CERT/CC	*Sri Lanka Computer Emergency Readiness Team Coordination Centre*	Sri Lanka
TechCERT	*TechCERT*	Sri Lanka
ThaiCERT	*Thailand Computer Emergency Response Team*	Tailândia
TWCERT/CC	*Taiwan Computer Emergency Response Team / Coordination Center*	Taiwan
TWNCERT	*Taiwan National Computer Emergency Response Team*	Taiwan
VNCERT	*Vietnam Computer Emergency Response Team*	Vietnã

Fonte: Adaptada de APCERT (2015)

Alguns países, participando ou não da ASEAN, possuem mais de um centro de operação do APCERT. Considerando que a ASEAN é possuidora de 9% da população mundial e 6% de todos os usuários da Internet (KHANISA, 2013: 41-43), os países da ASEAN + 3 unidos a outros países da região Pacífico Asiática passaram a construir seus organismos nacionais de suporte de emergência aos computadores (*Computer Emergency Response Team* - CERT) em resposta insegurança cibernética identificada no continente, dando origem ao APCERT.

Outra organização a se concentrar no desenvolvimento cibernético da região e na construção de uma maturidade cibernética conjunta capaz de prover segurança ao continente, além da elaboração de métodos medidores de capacidade cibernética e do nível de preparação de cada país para as ameaças cibernéticas, é o ASPI (*Australian Strategic Policy Institute*), cuja instituição, objetivos, método de trabalho e resultados também merecem apreciação.

3. ASPI

Antes de entrar diretamente na apresentação do ASPI e de seus objetivos de integração cibernética para a região Ásia-Pacífico faz-se imprescindível destacar que por se referir à construção de um ideal regional recente, relatado em um documento intitulado *Maturidade Cibernética na região Ásia-Pacífico 2014*, essa seção dar-se-á em torno do trabalho de análise e divulgação dos objetivos, métodos e resultados apresentados em tal relatório, de modo a começar pela instituição e desenvolver-se para o plano de cooperação cibernética regional.

O Instituto Australiano de Política Estratégica (*Australian Strategic Policy Institute* – ASPI) foi criado em 2001 como um grupo de estudos independentes e não partidário, cujo foco encontrava-se nas questões de defesa, segurança e políticas estratégicas da Austrália.

Hoje, o Centro de Política Cibernética Internacional do ASPI (ASPI *International Cyber Policy Centre* – ICPC), une os vários departamentos do governo australiano (responsáveis pelas questões cibernéticas), o setor privado e pensadores criativos para ajudar a Austrália a elaborar políticas cibernéticas construtivas nos âmbitos nacional e internacional (ASPI, 2014: 2).

Visando à integração entre governo, setor privado e academia de toda a região Pacífico Asiática para aumentar o diálogo nas questões cibernéticas e criar um entendimento comum sobre possíveis soluções para as questões no ciberespaço, o instituto australiano passou a vislumbrar a integração regional no setor cibernético de modo que a construção de instrumentos necessários a esta integração fosse praticada por todos os Estados da região e em todas as esferas necessárias. O grande obstáculo dessa proposta está na disparidade tecnológica do continente, que possui os países de maior e menor porcentagem de conexão à rede, sendo Coreia do Sul e Mianmar, com respectivamente 84,1% e 1,1% do país conectados (ASPI, 2014: 5).

No entanto, o grande crescimento econômico, político e social atribuídos à TIC e à conexão em rede mobilizaram os Estados em busca de maiores investimentos no setor cibernético. As vulnerabilidades provenientes desse espaço alimentaram a busca por meios garantidores da segurança cibernética nacional, e o fato de vários Estados se encontrarem na mesma posição possibilitou que unissem forças e compartilhassem soluções para o problema comum. Assim, o objetivo comum se fortalece e a proposta australiana para criação de uma "maturidade[10] cibernética" regional ganha força.

A maioria dos Estados da região começou a priorizar os setores cibernéticos como preocupação cerne na formulação de políticas. Embora cada nação sinta e responda de modo diferente a essa questão, alguns países da APEC e todos da ASEAN+3 estão comprometidos com a segurança cibernética do continente, que está começando a ser compreendida e priorizada. Enquanto a urgência e o rigor de como cada uma das nações responde à questão varia significativamente, todos os países examinados neste estudo estão comprometidos com o componente cibernético como um elemento do poder do Estado (ASPI, 2014; THOMAS, 2009).

Para tanto, o plano australiano funciona da seguinte forma: como resultado de diversas discussões com membros do setor privado, dos governos e com pesquisadores independentes,

[10] O termo maturidade, neste contexto, é compreendido como "a presença, implementação efetiva e operação de estruturas, políticas, legislações e organizações relacionadas à área cibernética" (ASPI, 2014:5, tradução livre).

o ASPI elaborou um medidor de maturidade cibernética que se baseou em quatro áreas: governança; aplicação militar; economia digital e negócios; e engajamento social (ASPI, 2014: 8). Essas áreas servirão de base informativa para que seja possível traçar um perfil cibernético para cada país, de modo a compreender quais as áreas em que os países se destacam e quais as que estão sendo negligenciadas. Além de fornecer um panorama da atual situação cibernética da região, o plano tem por objetivo identificar os pontos fracos em cada país buscando elaborar métodos para saná-los.

Ainda sobre o funcionamento do trabalho, o ASPI elaborou questões e dividiu as quatro áreas iniciais em subáreas. Assim, a área de governança passou a envolver estruturas organizacionais, legislação/regulação existente, engajamento internacional e a existência de CERTs. A área militar se manteve indivisível. O ponto sobre economia digital e negócios foi dividido entre diálogo governo-empresas e economia digital. Por fim, o tópico referente ao engajamento social tratou da consciência pública e da quantidade de usuários da Internet. Essa divisão, seus códigos e o peso que cada área recebeu no trabalho de pesquisa podem ser observados no Quadro 3:

Quadro 3 - Estrutura da Pesquisa

Peso	Grupo	Código	Categoria
8.4	1 – Governança	1.a	Estruturas Organizacionais
8.3	1 – Governança	1.b	Legislação/Regulação Existentes
6.9	1 – Governança	1.c	Engajamento Internacional
6.3	1 – Governança	1.d	CERTs
7.0	2 – Militar	2.a	Aplicação Militar
7.3	3 – Economia Digital & Negócios	3.a	Diálogo Governo-Empresas
7.4	3 – Economia Digital & Negócios	3.b	Economia Digital
4.9	4 – Engajamento Social	4.a	Consciência Pública
6.1	4 – Engajamento Social	4.b	Usuários da Internet

Fonte: Adaptada de ASPI (2014)

A pesquisa deu-se em quatro fases. A primeira serviu para a elaboração de questões qualitativas e quantitativas, só possível depois de fortes discussões no Centro Internacional de Políticas Cibernéticas do ASPI. Na segunda fase, as questões iniciais foram compartilhadas com grupos do governo, do setor privado e pesquisadores independentes, que muito debateram sobre as possibilidades de análise das respostas e as aperfeiçoaram. Na terceira fase, ainda sob discussão, foi dado peso aos indicadores de acordo com sua relativa

importância para a maturidade cibernética dos Estados. As partes interessadas deram nota de 1 a 10 para classificar os nove fatores escolhidos e a média dessas notas deu o peso que cada categoria recebeu (ASPI, 2014:12).

Por consenso, os fatores considerados de maior importância foram as estruturas organizacionais e a existência de regulamentação e/ou legislação encontradas no topo da tabela. O fator considerado de menor importância foi a consciência pública. Na última fase, cada país recebeu colaboração de participantes do setor privado e do governo para responder às questões relativas às nove áreas elencadas. A pesquisa contou com quinze países da região Pacífico Asiática mais o Reino Unido, servindo como referência adicional. Essa metodologia tem por objetivo principal o acesso às várias facetas das capacidades cibernéticas de cada uma dessas nações e o resultado quanto ao nível de maturidade dos países pode ser visualizado na Tabela 2:

Tabela 2 - Ranking de maior maturidade cibernética da região

Posição	País	Pontuação Ponderada
1	Estados Unidos	86.3
2	Reino Unido	81.2
3	Austrália	75.8
4	Coréia do Sul	75.5
5	Japão	75.3
6	Singapura	74.7
7	China	58.4
8	Malásia	57.9
9	Índia	45.9
10	Filipinas	43.4
11	Indonésia	42.4
12	Tailândia	41.6
13	Mianmar	29.7
14	Papua Nova Guiné	23.0
15	Coréia do Norte	20.7
16	Camboja	20.1

Fonte: Adaptada de ASPI (2014)

Na Tabela 2 é possível perceber que os países a ocupar os primeiros lugares do ranking são os Estados Unidos e seus aliados. Contudo, é importante ressaltar que o nível de maturidade cibernética está relacionado ao conjunto de ações implementadas na busca por minimizar os riscos provenientes do espaço cibernético, ou seja, diz respeito ao modo como os países estão lidando com a insegurança do ambiente cibernético e suas ações para torná-lo mais seguro; mas não se refere às capacidades cibernéticas dos Estados.

Na Tabela 3 é possível observar mais detalhadamente em quais aspectos cada país se saiu melhor ou pior.

Tabela 3 - Pontuação dos países por categoria

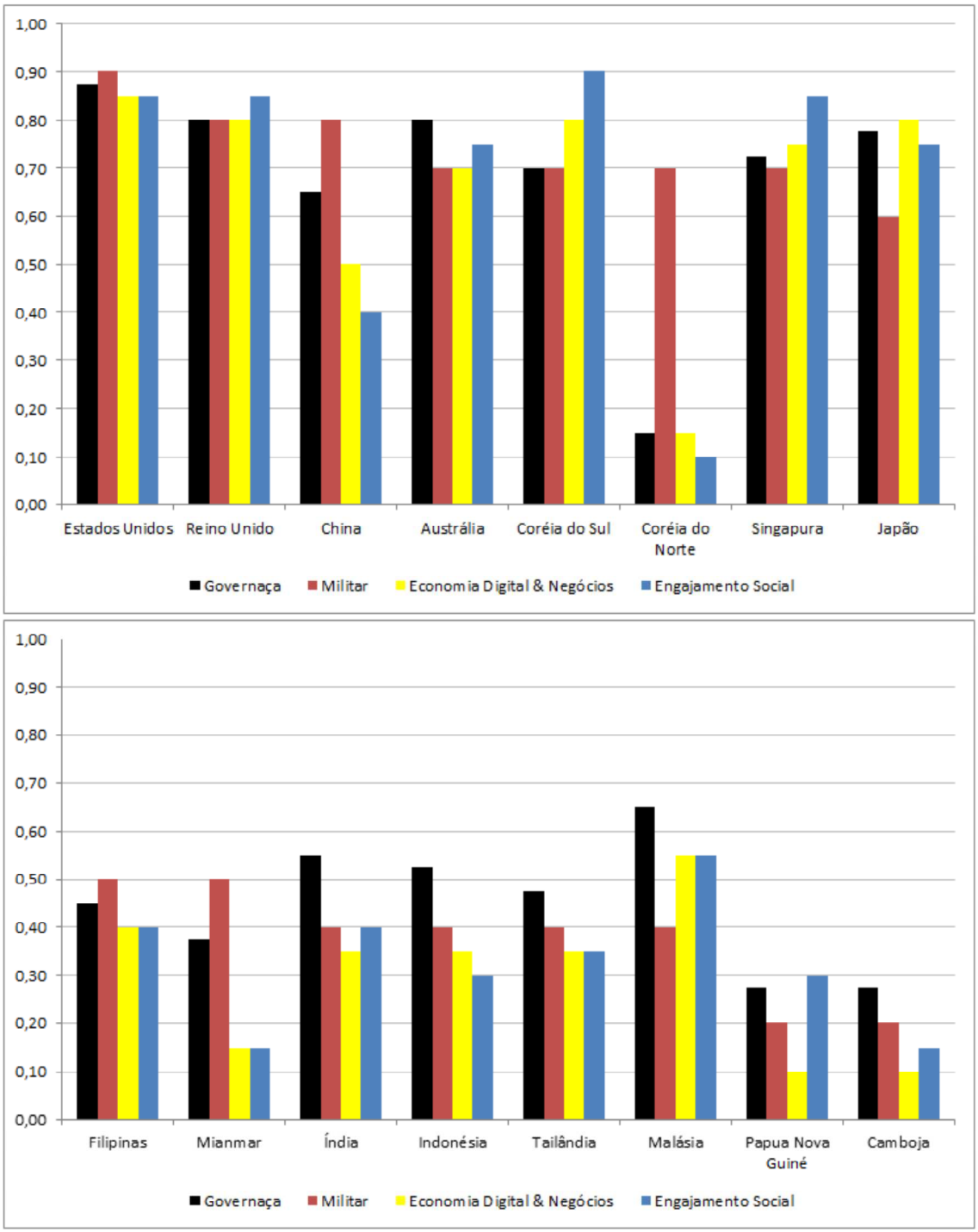
País	1.a	1.b	1.c	1.d	2.a	3.a	3.b	4.a	4.b	Total
Austrália	7	9	8	8	7	6	8	7	8	75.8
Camboja	2	3	3	3	2	1	1	2	1	20.1
China	6	5	9	6	8	3	7	4	4	58.4
Índia	7	5	5	5	4	3	4	6	2	45.9
Indonésia	5	4	6	6	4	3	4	4	2	42.4
Japão	7	7	8	9	6	8	8	7	8	75.3
Malásia	7	5	7	7	4	5	6	5	6	57.9
Mianmar	4	4	4	3	5	2	1	2	1	29.7
Coréia do Norte	3	1	2	0	7	1	2	1	1	20.7
Papua Nova Guiné	3	3	3	2	2	1	1	4	2	23.0
Filipinas	5	4	5	4	5	2	6	5	3	43.4
Singapura	8	6	7	8	7	8	7	9	8	47.7
Coréia do Sul	7	6	7	8	7	8	8	9	9	75.5
Tailândia	5	5	4	5	4	2	5	4	3	41.6
Reino Unido	9	8	9	6	8	8	8	9	8	81.2
Estados Unidos	9	7	10	9	9	8	9	9	8	86.3

Fonte: Adaptada de ASPI (2014)

A Tabela 3 apresenta a pontuação geral e parcial que cada país obteve por área. Assim, é possível constatar que a maioria desses países passa por dificuldades no que tange ao quesito 3a, que corresponde ao diálogo entre governo e empresas na busca conjunta por segurança cibernética. Outro item com relativo grau de carência é o 3b, que diz respeito à economia digital, ainda muito modesta em países como Mianmar, Papua Nova Guiné, Singapura e Camboja. No caso da China, por exemplo, o nível de interação entre empresas e governo no tocante a questões cibernéticas recebeu nota três, dado que reflete o desinteresse do país em trabalhar com empresas e a falta de coordenação entre o exército do PLA (*People's Liberation Army*) e o governo (ASPI, 2014:21).

Outro aspecto interessante é o destaque sínico para o engajamento internacional e a aplicação militar para a segurança cibernética, os respectivos pontos 1c e 2a, a receber as maiores notas. Isto significa que a China está comprometida com a cooperação para segurança cibernética da região inclusive por meios militares. Outro modo de visualizar a prioridade que os Estados dão por área é através do gráfico no Gráfico 2.

Gráfico 2 - Gráfico das áreas para a maturidade cibernética



Fonte: Baseada nas informações da ASPI Maturidade Cibernética na Região Ásia- Pacífico 2014

No Gráfico 2 é possível perceber que os Estados que obtém maior colocação no ranking além de possuírem maior nota com relação aos quesitos pesquisados, possuem também menor diferença entre as áreas. Estados Unidos, Reino Unido e Austrália mantém uma pequena diferença entre os quesitos considerados importantes para a construção de uma maturidade cibernética. Reiterando que Reino Unido consta apenas como referência adicional

e ressaltando que embora Estados Unidos e Austrália façam parte da região Pacífico Asiática, não são países asiáticos. A lista dos Estados asiáticos mostra maior distância entre os itens de maior e menor nota. Isso demonstra maior nível de preferência entre as áreas em vez da crença de que todas as áreas fazem-se igualmente essenciais à construção da maturidade cibernética.

Quanto às limitações desta pesquisa, posto que a grande quantidade de informação sobre áreas estratégicas está necessariamente vinculada ao sigilo governamental, o relatório baseou-se exclusivamente em informações de domínio público. Como os dados numéricos que cada Estado recebeu não se pretendem absolutos, mas servem de guia para uma rápida avaliação no nível de maturidade cibernética de cada país e, consequentemente, da região, estes dão espaço a interpretações. Ainda assim o relatório do ASPI pela maturidade cibernética da região Ásia Pacífico foi apenas o primeiro passo e sua metodologia será aprimorada a partir do *feedback* que receber (ASPI, 2014:12).

Desse modo foi possível perceber que os Estados da região Pacífico Asiática estão se mobilizando e que as ações necessárias para a construção da sua maturidade cibernética estão sendo tomadas por todos de todos os Estados envolvidos, embora de forma um pouco diferente em cada um. Também foi possível perceber que, a seguir pelos modelos com maior índice de maturidade cibernética, a resposta parece estar na igual importância que deve ser dada às quatro áreas destacadas. Resta, então, compreender qual a maturidade cibernética da China, seu desenvolvimento nesta seara e, consequentemente, sua condição como potência cibernética.

3. UTILIZAÇÃO SÍNICA DO ESPAÇO CIBERNÉTICO

1. A situação da China

Como apresentado no capítulo anterior, a China não se encontra em alto nível de maturidade cibernética, embora seja considerada potência cibernética de sua região. Com média 58.4 o país demonstra que, apesar de ter um grande número de agências do governo envolvidas em questões cibernéticas, há uma falha na coordenação das operações de tais agências além da falta de estratégia ou de metas mais abrangentes de política cibernética nacional (ASPI, 2014:21).

A China também se mostra comprometida com a elaboração e execução de leis que possam reger o espaço cibernético nacional e internacional e se revela participativa nos encontros internacionais para discutir tais aspectos. Zhang (2012:806-807, tradução livre) explica que embora a China não apresente uma estratégia cibernética oficial, sua visão é clara: ela pretende contribuir ativamente para o desenvolvimento de normas legais aplicáveis ao espaço cibernético e, para tanto, o governo chinês elaborou quatro princípios básicos:

- O princípio do respeito total pelas leis nacionais de cada país, que significa dizer que cada país possui direito de jurisdição sobre qualquer atividade doméstica ou externa que possa ameaçar sua segurança. Também implica dizer que as normas internacionais tradicionais de sobrevivência, integridade territorial e independência política devem se estender ao ciberespaço.
- O princípio do balanceamento, que considera que a tecnologia por si só é neutra, se servirá pra o bem ou para mau, depende de como será utilizada. Portanto, este princípio sugere que o uso e inovação da tecnologia não sejam prejudicados, mas que seja evitada a propagação de informações prejudiciais que possam ameaçar a segurança cibernética nacional ou internacional.
- O princípio do uso cibernético pacífico, que envolve a proteção das infraestruturas tecnológicas de informação global consideradas chaves e outros sistemas de informação de uso civil de serem alvos de ataques cibernéticos e também propõe que cada cidadão, Estado e atores não estatais se responsabilizem por seu uso do espaço cibernético, parando qualquer comportamento que ameace a paz e o desenvolvimento ordenado do ciberespaço. E que qualquer problema acima referido seja resolvido sem o uso ou ameaça da força.

- Por fim, temos o princípio do desenvolvimento equitativo, que significa salvaguardar os direitos e interesses dos países 'fracos' e se opor a exploração por aqueles que possuem vantagens tecnológicas no ciberespaço, ou seja, impedir a utilização de recursos internacionais de rede de informação ou infraestruturas fundamentais a fim de enfraquecer o controle de alguns países sobre tecnologia de informação e serviços.

O autor também explica que apesar da forte participação nas reuniões para discussão de questões cibernéticas, o país desaprova o papel exagerado que vem sendo dado à guerra cibernética (ZHANG, 2012:802). O uso irresponsável da mídia e a *misperception* pública servem para aumentar os julgamentos errôneos e as desconfianças entre os países, tornando a corrida armamentista online ainda mais feroz (ZHANG, 2012:804). Feakin (2013:1) afirma que a maior parte das informações publicadas pela mídia aponta para a 'onipresença' chinesa sem fornecer maiores informações.

Contudo, a China sabe que a origem dessa crescente atenção se dá por dois fatores importantes: 1) pela divulgação do relatório Mandiant, o qual descreve com precisão de detalhes a unidade 61398 de espionagem cibernética do PLA (*People's Liberation Army*), que "hackeou" sistemas de computador do *The New York Times* durante os anos de 2012 e 2013; 2) pela taxa crescente de anúncios públicos apontando o campo cibernético como área maior de priorização pelos Estados Unidos (FEAKIN, 2013:1; MANDIANT, 2013:7).

Como resultado desses dois acontecimentos, o sistema internacional se mobilizou para discussões e a segurança cibernética tornou-se assunto prioritário. As informações midiáticas e o envolvimento de agências militares e de inteligência chinesas com o setor corporativo promoveram desconfianças internacionais e quebra de contrato com empresas chinesas de telecomunicação, como fizeram a Austrália e os Estados Unidos. De acordo com uma reportagem de 2012 no jornal *Economist*, essas decisões foram tomadas com base na crença de que a empresa Huawei teria roubado propriedade intelectual australiana e teria sua expansão subsidiada pelo governo chinês, ansioso para utilizá-la (FEAKIN, 2013:3).

As desconfianças do sistema internacional se mantiveram, principalmente com relação às ações da República Popular da China. O grande número de ataques provenientes deste Estado, unido ao episódio do relatório Mandiant e à suscetibilidade internacional depois da descoberta de envolvimento entre agências militares e de inteligência chinesas com o setor corporativo, tudo isso manteve o país sob o foco das atenções (FEAKIN, 2013:1). Ainda que o ambiente cibernético dificulte a determinação da origem do ataque, grande número de

incidentes recai sobre a responsabilidade chinesa, como é possível observar por meio do discurso do ex-representante dos Estados Unidos no oitavo distrito congressional de Michigan, em 2011:

> A espionagem econômica da China tem alcançado um nível intolerável e eu acredito que os Estados Unidos e nossos aliados na Europa e Ásia tem a obrigação de confrontar Pequim e exigir que eles ponham fim à pirataria. Pequim está travando uma guerra comercial massiva sobre todos nós, e nós deveríamos nos unir para pressioná-los a parar. Combinados, Estados Unidos e nossos aliados na Europa e na Ásia, temos significativa influência econômica e diplomática sobre a China, e nós devemos usá-la a nosso favor para por fim a esse flagelo" (MANDIANT, 2013:1, tradução livre).

Em resposta, o Ministro de Defesa da China reiterou o discurso sobre a dificuldade de se descobrir a origem das ameaças no espaço cibernético – uma vez que, como apresentado no primeiro capítulo, o ciberespaço permite a falsificação de dados e elaboração de provas forjadas de modo a incriminar atores inocentes – e definiu como "pouco profissional e infundado acusar os militares chineses de lançar ataques cibernéticos sem qualquer evidência conclusiva" (MANDIANT, 2013:1, tradução livre).

O fato é que com ou sem provas, forjadas ou não, os organismos responsáveis pela segurança cibernética de vários países possuem indícios de infiltração e danos originários da República Popular da China. Conquanto, é importante destacar que apesar da origem, é difícil diferenciar se as ações estão de fato conectadas a organizações do Governo chinês ou se são resultado de grupos independentes. Como resultado de inúmeras acusações e de desentendimento internacional, houve mudança na quantidade de discussão pública sobre violações e no comportamento das organizações vítimas, que estão mais dispostas a falar abertamente sobre as intrusões que sofrem (MANDIANT, 2014:22).

Os políticos também estão expressando suas preocupações no âmbito nacional e internacional, mas o aumento da discussão e conscientização de violações de segurança não têm mudado a realidade atual, posto que violações de segurança são inevitáveis (*ibidem*). Assim, tendo em vista a situação atual em que a China se encontra, no que tange aos assuntos cibernéticos, e diante da grande quantidade de acusações de ciberespionagem para fins militares e econômicos, faz-se mister compreender seu processo histórico de desenvolvimento e interesse pelo mundo cibernético.

2. Conhecendo a China: Um breve histórico militar

Embora considerada uma das maiores forças militares do mundo (FRITZ, 2008:28), com um exército composto por 850 mil pessoas e sob sete áreas de comando militar, com 235

mil oficiais da marinha, uma força aérea de 398 mil homens e sete áreas de comando militar aéreo (CHINA'S DEFENCE WHITE PAPER, 2013), já classificada como potência nuclear e com o maior número de homens e mulheres nas forças armadas, a China está cada vez mais empenhada em modernizar seus sistemas nucleares e convencionais (SCOBELL, 2000:1).

O primeiro estalo para a modernização se deu nos anos de 1980, quando o líder chinês Deng Xiaoping resolveu priorizar a qualidade em vez da quantidade e cuja primeira atitude foi reduzir seu corpo militar e dispensar cerca de um milhão de integrantes (FRITZ, 2008:28). Líder na China de 1978 a 1989 e mais uma vez em 1992, apaixonado por modernização e tecnologia, o dirigente percebeu a possibilidade de destruir o sistema econômico implantado no governo de Mao Zedong e resolveu mitigar as políticas econômicas e sociais, que haviam impedido o crescimento da China, e dar início às relações comerciais com o Ocidente, atos responsáveis por tirar milhões de chineses da pobreza (VOGEL, 2011)[11].

Outro momento importante foi a atuação estadunidense na Guerra do Golfo, com a exposição de sua vasta superioridade militar, mas principalmente de sua capacidade de preparação para um distinto modelo de guerra, que prendeu a atenção dos chineses. A utilização dos computadores e outras tecnologias de ponta forneceu inteligência em tempo real e permitiu uma variedade de armamento inteligente. Não à toa, os militares da China se referem a esse acontecimento como "a grande transformação" e durante o restante da década de 1990 reuniu seus estrategistas para discutir de que modo a China poderia se adaptar ao novo campo de batalha (FEAKIN, 2013:2).

Depois de muita reflexão, grandes pensadores e estrategistas chineses – como o major general Wang Pufeng[12] e o major general Dai Qungmin[13] – avançaram no pensamento sobre como o país poderia utilizar o domínio cibernético e elaboraram o conceito de "guerra eletrônica de rede integrada" (FEAKIN, 2013:2). Em 1993, o presidente Jiang Zemin oficialmente anunciou a Revolução nos Casos Militares (*Revolution in Military Affairs* – RMA), uma parte da estratégia militar nacional para modernização. A partir do mesmo ano o orçamento da China vem crescendo drasticamente, com aumento médio de 9% ao ano (FRITZ, 2008:28-29).

---

[11] A versão online da obra não possui numeração nas páginas.
[12] Ex-diretor do Departamento de Estratégia, da Academia de Ciências Militares, em Pequim, especialista em guerra da informação/guerra cibernética (THOMAS, 2001:51).
[13] Diretor do Departamento de Comunicação do Estado Maior do PLA, responsável pela guerra da informação e pelas operações de informação (THOMAS, 2001:47).

Em um artigo de 1995, intitulado *The Challenge of Information Warfare*, o general Wang Pufeng retrata os desafios da guerra da informação e apresenta o que pode ser considerado a base do pensamento sínico no que tange à preparação para a guerra da informação (*Information War* - IW). O autor comenta que a capacidade cibernética do país é inferior à de muitos outros Estados e explica que a solução para tal desvantagem estaria no posicionamento ativo – em vez de reativo – durante o conflito; na utilização de seus pontos fortes a fim de atacar os pontos fracos dos inimigos; e, em última instância, ao defender que a IW é conduzida por pessoas, o general assegura que o grande plano é cultivar talentos adequados.

Ainda em 1995 é implementado o plano chinês para a Guerra da Informação (BALL, 2011:81). Em 1999, depois da exposição das dificuldades e possibilidades da China neste modelo de conflito, os coronéis do PLA, Qiao Liang e Wang Xiangsui, publicaram a obra intitulada *Unrestricted Warfare*, que propõe táticas para o desenvolvimento dos países, em particular da China, de modo a permitir que um Estado tire vantagens da fraqueza de um adversário com capacidades convencionais superiores. Ou seja, possibilita a utilização de meios para compensar a inferioridade militar e oferecer a vitória na IW, que os autores definem como "um modelo de guerra sem limites e sem regras, onde tudo é permitido e onde os países mais fortes elaboram regras, enquanto os países mais fracos as quebram e exploram suas brechas" (LIANG e XIANGSUI, 1999:2).

A obra parece corresponder à culminância entre os vários eventos anteriores somados à percepção chinesa da guerra tradicional, tornando-se manual sínico para a guerra da informação (FEAKIN, 2013:3). No entanto, na virada do século, a maior parte da força tradicional da China permaneceu ainda nos anos de 1950 a 1970, na era da tecnologia importada da Rússia e da engenharia reversa[14] (FRITZ, 2008:28). Em seu trabalho, Fritz (2008:28) explica que apesar do forte empenho em busca da modernização, a capacidade militar da China se encontra de uma a três gerações atrás de Estados Unidos e Rússia.

Isso ocorre porque a maior parte das armas da China é construída a partir de modelos soviéticos adquiridos antes da ruptura sino-soviética (no final dos anos 1950 e início de 1960) (FRITZ, 2008:28). O autor também explica que através do método de engenharia reversa o país se mantém em constante evolução. A falha, ainda segundo o autor, está na carência de

[14] A engenharia reversa "consiste em analisar um sistema ou ferramenta para criar uma representação dela" (CANHOTA Jr et al., 2005:6), ou seja, trata-se do estudo de um objeto com o objetivo de, através da reprodução, aprender a desenvolvê-lo.

transparência por parte da Rússia, que vende tecnologia gerações atrás da do momento da aquisição, uma vez que os Estados não pretendem desistir de suas vantagens (FRITZ, 2008:31-33). Entretanto, o grande erro nos parece estar mais na ingenuidade chinesa, ao demonstrar ignorar tal realidade.

Apesar de seus armamentos se encontrarem atrasados em comparação aos de potências militares ocidentais, a força total da China estabelece o país como potência dominante na região Pacífico Asiática, visto que seu poderio bélico ainda representa um impedimento significativo a ameaças externas. Assim, a China carece de projeção, de força para além de sua região, para acelerar seu desenvolvimento tanto na área beligerante quanto da informação e assegurar força além de seu continente, o país vem recrutando estudantes, pessoas de negócios, diplomatas, engenheiros e especialistas estadunidenses com experiência militar (FRITZ, 2008:39).

Segundo Pufeng (1995), o "cultivo de talentos adequados" se faz essencial à construção das habilidades necessárias para a obtenção da vitória no espaço cibernético. Para tanto, além do recrutamento de mão de obra especializada, a República Popular da China segue investindo em educação e treinamento específico para a IW (BALL, 2011). Outra forma de conseguir seus objetivos é mediante tráfico de influência dentro de empresas de alta tecnologia ou recorrendo a favores políticos de funcionários do governo, como o exemplo, temos um farto número de denúncias alegando que a decisão do presidente americano, Bill Clinton, com relação à venda de computadores sofisticados e de tecnologia de satélites para a China tenha sido resultado de uma contribuição de campanha (FRITZ, 2008:37).

Para Hachigian (2000:118-120), a China se apaixonou pela Internet. Mais do que isso, o Partido Comunista Chinês aparentemente se encantou com seu vasto potencial comercial e depois de testemunhar seu impacto na América, Europa e em outras economias asiáticas percebeu que nenhum outro modelo econômico oferecia futuro mais promissor. Ainda que a busca por desenvolvimento e a execução do plano de preparação para a guerra da informação datem do início dos anos de 1990, a autora comenta que a introdução da Internet na China aconteceu relativamente tarde. Apesar de tardia, sua incorporação levou o país ao posto de maior mercado da Internet, com consumidores cada vez mais sofisticados.

Na realidade, a China se apaixonou pela Internet e por tudo que a envolve (KHANISA), pois tão importante quanto a construção do desenvolvimento econômico é a preservação da segurança nacional. Na busca por tecnologia capaz de prover ambos os propósitos, a Internet vem sendo utilizada das mais diversas formas e alcançada através dos

mais distintos meios, como treinamento, tráfico de influência e favores políticos. A China também se esforça para obter tecnologia militar de dupla utilização[15] por meio de transações comerciais lícitas e ilícitas. Muitas tecnologias de dupla utilização – tais como *softwares*, circuitos integrados, computadores, eletrônicos, semicondutores, sistemas de telecomunicação e de segurança da informação – são vitais para a transformação do PLA em uma força capacitada para a rede, baseada na informação (FRITZ, 2008:37).

É por este histórico de sede de desenvolvimento que, de acordo com Mulvenon (1999:175-177), em 1999 a China foi considerada um dos três países a empurrar o desenvolvimento de estratégias de IW, atrás apenas de Estados Unidos e União Soviética. Seu programa já possuía características ofensivas e contou com recursos significativos. As revistas militares do país passaram a publicar cada vez mais artigos abordando o assunto e livros foram publicados nesse tema. Ainda segundo o autor, as aspirações chinesas já eram de utilização de armas assimétricas como meio de minimamente degradar ou atrasar a mobilização das forças e sistemas estadunidenses.

Logo, é possível concluir que a paixão da China pela Internet está rendendo frutos. Embora sua estrutura militar ainda não tenha se desenvolvido o suficiente, a curtos passos a China segue se desenvolvimento e na procura por criar suas próprias ferramentas, através da engenharia reversa. A troca de quantidade por qualidade vem sendo percebida com o destaque mundial dado às capacidades e estratégias cibernéticas do país. Mas qual o modo como o Governo chinês organiza sua estrutura para a utilização de armas assimétricas e quais as responsabilidades de cada departamento?

3. Organização da estrutura sínica de poder/segurança

É possível perceber que a China vem desenvolvendo sua estratégia para a Guerra da Informação e, para tanto, organizando e redistribuindo os cargos e funções necessárias entre os órgãos já existentes. Para melhor assimilação dessa sistematização, as agências chinesas e seus respectivos fins serão apresentados nesta seção. A Suprema Corte e a Suprema Procuradoria fogem do escopo deste trabalho, dado que estes organismos não tratam de questões de segurança, tampouco de desenvolvimento: seja ele econômico, político ou militar.

Sendo assim, a República Popular da China está organizada da seguinte forma: em primeiro lugar e com maiores responsabilidades encontra-se o presidente da República e representante do Estado, neste caso o Xi Jinping (desde 14/03/2013). Depois do presidente, o

[15] Diz respeito à tecnologia utilizada para fins civis e militares (EROPEAN COMMISSION, 2008).

Estado divide suas obrigações em duas instituições: o Conselho de Estado e a Comissão Militar Central. O Conselho de Estado da República Popular da China é descrito pela constituição do país como o mais elevado corpo administrativo do Estado e tem a função de supervisionar a burocracia estatal e gerenciar a administração do dia-a-dia do país, enquanto a Comissão Militar Central comanda suas forças armadas (LAWRENCE, 2013:2).

O Conselho de Estado, também conhecido como Governo Popular Central (*Central People's Government*), é, segundo a constituição chinesa, responsável pela implementação de políticas formuladas pelo Partido, de leis aprovadas pelo Congresso Nacional do Povo Comunista e é por meio deste que a China costuma conduzir suas relações externas. O Conselho é dirigido por um premier, nomeado pelo presidente, que conta com a assistência de outros quatro premiers. O Conselho de Estado possui um vasto leque de organizações e escritórios administrativos, incluindo a Supervisão de Ativos Estatais, a Comissão Administrativa do Conselho de Estado, a Administração Estatal de Impostos, a agência estatal de notícias (Xinhua) e comissões de regulamentação bancária, imobiliária, de seguro e de eletricidade (LAWRENCE, 2013:14).

Visando ao cumprimento de tantas atribuições, o Conselho de Estado ainda dispõe de duas agências civis: o Ministério da Segurança do Estado (*Ministry of State Security* – MSS) e o Ministério da Segurança Pública (*Ministry of Public Security* – MPS). O MSS é responsável pela contraespionagem, contra inteligência, inteligência estrangeira e inteligência doméstica. Suas capacidades são relativamente desconhecidas, uma vez que se tratam de informações sigilosas. Mas suas funções estão obviamente relacionadas à coleta de informação política, econômica e militar sobre governos estrangeiros, organizações não governamentais e sobre os que se opõem à República Popular da China (FEAKIN, 2013:3).

O MSP é responsável pelo policiamento nacional e, em menor grau, pela inteligência doméstica. Também apoia ativamente a pesquisa de segurança da informação, a certificação de produtos comerciais para uso pelo Governo chinês, o controle de empresas de segurança de informação comercial e o financiamento de bolsas acadêmicas. Esses são alguns dos exemplos a comprovar que as agências militares e de inteligência da China se envolvem com o setor corporativo, inclusive investindo no roubo de propriedade intelectual, do que o país vem sendo acusado pela Austrália depois da quebra de contrato com a empresa Huawei (FEAKIN, 2013:3).

A Comissão Militar Central é responsável pelo comando das forças armadas e pela inteligência militar, atribuída ao PLA. Sua organização se dá pelo Departamento Geral do

Estado Maior, também chamado de quadro geral ou equipe geral do PLA, e pela subdivisão de mais três departamentos sob vigilância do Departamento Geral (FEAKIN, 2013:3). O Departamento Geral do Estado Maior cuida de funções operacionais e da realização de planos de modernização militar, além de funcionar como sede do exército do PLA (*PLA Ground Force* - PLAGF) e de dispor de diretórios para a marinha (*PLA Navy* – PLAN), a força aérea (*PLA Air Force* – PLAAF), e o corpo de segunda artilharia (*Second Artillery Corps* – SAC), assim como de um departamento de guerra eletrônica (FRITZ, 2008:36).

O Segundo Departamento Geral do PLA (*Second Department of the General Staff Headquarters*) é responsável pela coleta de inteligência estrangeira, sistema Adido de Defesa[16] (AD), inteligência de imagens aéreas e de satélite, reconhecimento tático e utilização de agentes clandestinos na realização de espionagem e análise das informações que países estrangeiros disponibilizam para o público (FEAKIN, 2013:3-4; FRITZ, 2008:36). Este Departamento também tem a função de supervisionar outros organismos militares, como a Inteligência Militar Humana (HUMINT), a Inteligência de Fonte Aberta (*Open Source Intelligence* – OSINT) e a Inteligência por Imagens aéreas e de satélites (IMINT). E vem aumentando seu foco na coleta de inteligência militar, científica e tecnológica (FRITZ, 2008:36).

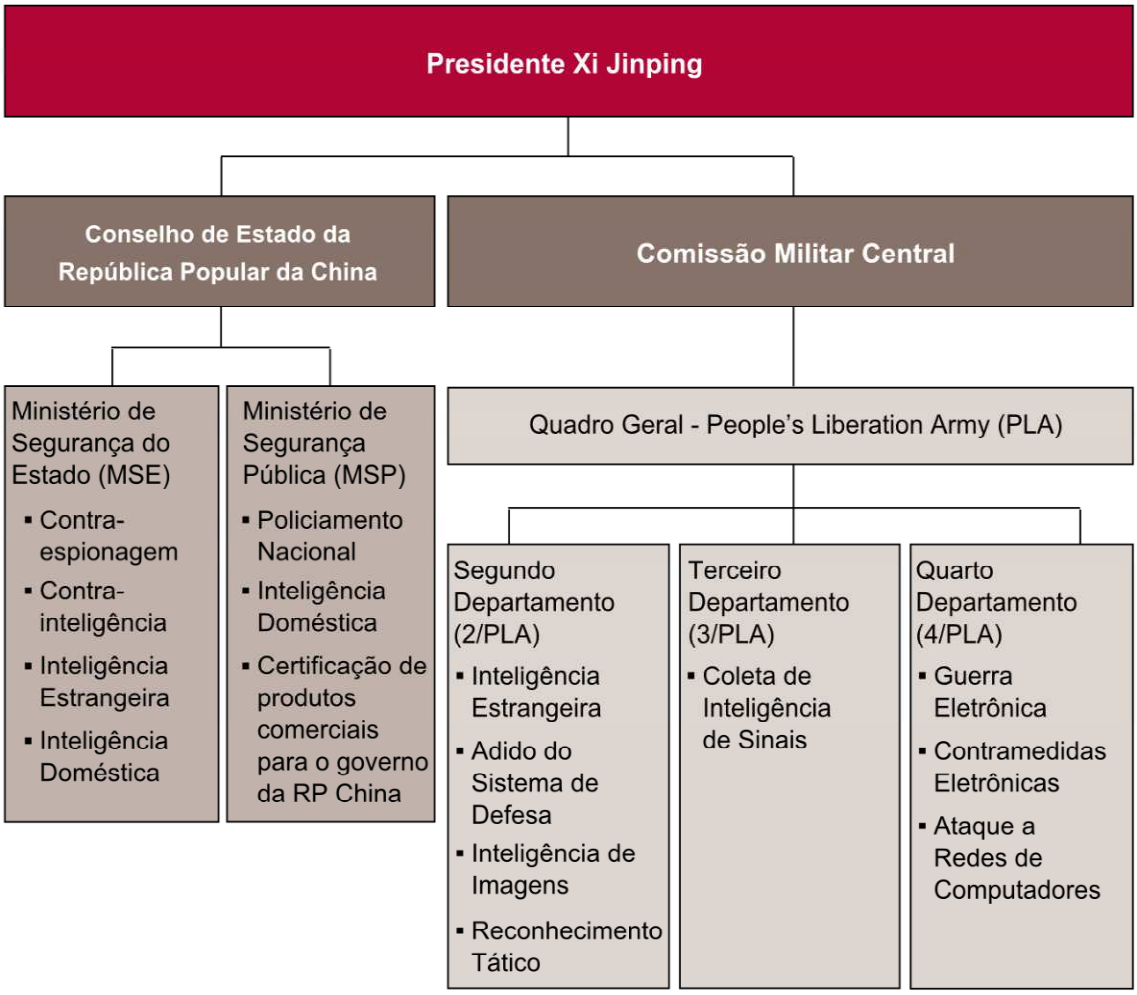
O Terceiro Departamento cuida do monitoramento das telecomunicações dos exércitos estrangeiros, mediante interceptação de comunicação e elaboração de relatórios com base nas informações militares recebidas. A captura de informação acontece não somente com os exércitos inimigos, mas também como modo de supervisionar e manter o controle sobre as várias áreas e comandantes de todas as regiões militares do país (FRITZ, 2008:36). Feakin (2013:3-4) complementa explicando que o Terceiro Departamento é a primeira agência de coleta e análise de sinais de inteligência (SIGINT) e o PLA é possuidor da maior e mais sofisticada rede de inteligência de sinais da região Ásia-Pacífico, gerenciando cerca de 12 agências operacionais e três institutos de pesquisa, e recuperando enormes volumes de coleta de dados.

O autor segue explicando que o Quarto Departamento é responsável pela guerra eletrônica, pelas contramedidas eletrônicas e pelos ataques a redes de computadores. Ou seja,

[16] Adido para a defesa (AD) "é um membro das forças armadas que serve em uma embaixada como representante do sistema de defesa de seu país no exterior e neste cargo goza de imunidade e de status diplomático. AD é um termo genérico que abrange todo o pessoal (staff) de todos os ramos dos serviços do exército, embora alguns países maiores possam indicar um adido para representar cada unidade das forças armadas (adido para representar a força aérea ou adido para a marinha, por exemplo)" (DCAF BACKGROUNDER, 2008:1).

é o principal departamento no que diz respeito às ações cibernéticas do Estado. Considerando que de uma forma ou de outra os outros departamentos também possuem determinadas atribuições relacionadas a capacidades cibernéticas. A principal diferença entre o quarto departamento e os demais está na característica ofensiva que ele possui (FEAKIN, 2013:4). A organização dessas estruturas e suas respectivas funções podem ser verificadas, de modo resumido, na Figura 1.

Figura 1 - Estrutura sínica de poder



Fonte: Adaptado de Feakin, 2013.

Ainda sobre os departamentos e suas respectivas ocupações, Fritz (2008:36) comenta a existência de outros departamentos que são subdivisões do Departamento Geral do Estado Maior e que detém ofícios que se sobrepõem. Alguns exemplos são o Departamento de Ligação Internacional, que realiza propaganda, operações psicológicas (PSYOPS), e contraespionagem contra a inteligência estrangeira; e o Departamento Político Geral (GPD),

responsável por supervisionar a educação política necessária para o avanço dentro do PLA e controlar o sistema prisional interno do PLA.

A questão que o autor colocou está relacionada à sobreposição de departamentos e à confusão que algumas vezes acontece entre eles, posto que alguns departamentos compartilham do mesmo propósito. Por este motivo, Feakin (2013:7-8) finaliza seu trabalho explicando que a coleta de informações militares, políticas, econômicas e tecnológicas pelos chineses nem sempre produz exploração bem sucedida. Primeiro, pelo fato de a China não possuir um mecanismo central, responsável pela exploração da informação e capaz de utilizá-la com maior qualidade.

Outro problema, ainda segundo o autor, diz respeito à autonomia com que as agências trabalham, posto que a liderança central não tem controle sobre quem pratica os ataques, onde ou como estes são feitos. Um fator a merecer destaque é a possibilidade de incidentes fora do controle antes que a liderança possa solucioná-lo, visto que a liderança não recebe informações suficientes. Em contraposição, o autor explica que essa falta de informação por parte dos líderes produz uma negação plausível quando respondendo a acusações das quais não tinha conhecimento. Sob as palavras do autor, essa é uma "feliz coincidência" (FEAKIN, 2013:7-8).

No mais, Feakin (2013:8) finaliza afirmando que a escala de ciberoperações chinesas não está em questão, mas que a sofisticação de alguns dos seus métodos está. E que talvez seja esse o motivo do grande número de ações sínicas descobertas, ou de acusações de infiltração cibernética que o país vem recebendo. Segundo Petter Mattis, é preciso entender como as agências de inteligência interagem entre si e como produzem seus resultados, pois não se sabe se a vasta quantidade de dados colhidos pelas agências chinesas é toda processada e se torna produto utilizável pela inteligência chinesa com valor para os *policemakers*, agências e organizações do país ou se são perdidas e/ou mal utilizadas (FEAKIN, 2013:8).

Evidenciada a estrutura como as instituições da China estão organizadas, foi possível constatar que todos os departamentos estão, de uma maneira ou de outra, conectados a aspectos da capacidade cibernética. O modo independente como cada departamento trabalha e a ausência de uma liderança central promovem certo grau de desorganização e produzem comunicação ineficaz entre as entidades. Contudo, a existência de tais departamentos e de suas respectivas atribuições demonstra interesse sínico no desenvolvimento da área e de suas capacidades.

Cabe destacar que enquanto a China segue no processo de informatização na busca pelas vulnerabilidades dos outros países, suas próprias redes tornam-se cada vez mais suscetíveis ao ataque, dado que a China é altamente dependente do ciberespaço para seus programas militares e civis de governo. Segundo Inkster (2013: 62), a resposta para o aparente pouco interesse em infiltração em redes chinesas está no fato de que "há muita [informação] que a China deseja roubar do Ocidente, mas relativamente pouca que o Ocidente precise roubar da China", como será evidenciado no tópico subsequente.

4. Vantagens da ciberguerra para o desenvolvimento da China

Embora o ambiente cibernético seja um espaço a permitir revanches e favorecer o ataque em detrimento da defesa, Hjortdal (2011:3-4) defende que a utilização da espionagem cibernética como meio para obtenção de vantagens econômicas e/ou militares se faz mais interessante aos Estados em desenvolvimento, que vislumbram capacidades similares às das grandes potências e que podem, por meio da espionagem cibernética, avançar mais rapidamente em suas capacidades. Nesse contexto, o autor aponta a China como o Estado que mais se beneficiaria com o ataque cibernético, e os Estados Unidos como o maior alvo de tais tipos de ataque.

Segundo Ball (2011:81), a República Popular da China possui a capacidade de guerra cibernética mais extensa e mais praticada da Ásia, embora sua expertise técnica não esteja no mesmo patamar. A consciência dessa deficiência é a responsável pela utilização sínica do espaço cibernético em busca de vantagens econômicas e militares como meio de equilibrar o nível de desenvolvimento e de deter, por meio cibernético, agressões e imposições políticas ou econômicas por parte de potências militarmente mais fortes. Em síntese, a China é dona de capacidade cibernética muito destrutiva e relativamente pouco sofisticada e a utiliza de modo a prover vantagens assimétricas e buscar o equilíbrio de poder.

Hjortdal (2011:3), ao defender que o espaço cibernético é elemento decisivo na estratégia chinesa de ascensão no sistema internacional, corrobora o pensamento de Inkster (2013: 62) e explica que o interesse da China na utilização de capacidade cibernética ofensiva é maior que o de qualquer outra nação. Embora todos os Estados tenham pelo menos três motivos reais para investir em capacidade cibernética: 1) deter infiltração em suas infraestruturas críticas; 2) obter conhecimento estratégico militar, através de (ciber) espionagem tecnológica militar; e 3) obter ganhos econômicos onde o processo tecnológico tem sido alcançado, através de (ciber) espionagem industrial. Hjortdal defende que a

possibilidade de ganhos é maior para os que ainda buscam desenvolvimento econômico e militar.

Diante da busca chinesa por capacidades cibernéticas, com o objetivo de impedir certas imposições por parte de governos militarmente superiores, há que se pensar que no caso da República Popular da China possuir o mesmo poder econômico e militar que os Estados Unidos, por exemplo, não seria necessária a utilização de meios cibernéticos, visto que o país poderia responder no mesmo nível. Reiterando as informações de Hjortdal, a China vê no espaço cibernético a oportunidade de obtenção de vantagens políticas, econômicas e militares, além da economia de tempo e recurso em projetos independentes, já que o uso das informações militares estrangeiras para a construção de seu plano militar, por exemplo, pode garantir a recuperação do atraso e permitir que o país comece a trabalhar em nível comparável ao das grandes potências (FRITZ, 2008:37).

A guerra cibernética permite um salto por meio de transferência tecnológica e exploração das fraquezas dos adversários (FRITZ, 2008:37). A espionagem e a transferência de tecnologia prosperam nesse modelo de guerra, onde a presença física é desnecessária e as atribuições são cada vez mais difíceis. Isto também está em consonância com a estratégia chinesa de salto, que busca aquisição do conhecimento militar, político e econômico de países estrangeiros por meio da ciberespionagem a fim de, através da transferência tecnológica, alcançar nível comparável ao das grandes potências.

Desse modo, ao considerar os três motivos que, segundo Hjortdal (2011:3), justificam o investimento de qualquer Estado em capacidades cibernéticas, constatamos que Estados já desenvolvidos econômica e militarmente não precisam do espaço cibernético para deter outros Estados, uma vez que conseguem fazê-lo militarmente. Por meio do exemplo dos Estados Unidos é possível perceber que desde que a tecnologia militar americana se tornou inigualável, a espionagem visando conhecimento da tecnologia militar de outros Estados tem sido desnecessária. Do mesmo modo, ao se encontrar entre os níveis industriais e tecnológicos mais avançados do mundo, a espionagem industrial visando vantagens econômicas tem menos importância para os EU que para países com economia ainda em desenvolvimento.

Esses exemplos servem de fundamento para o envolvimento sínico na área cibernética. A ênfase dada à guerra eletrônica e da informação e os investimentos em ataques de precisão de longo alcance, mísseis terrestres e aéreos, forças de operação especial, helicópteros de aviação do exército e comunicação por satélite mostram que o PLAGF (PLA *Ground Force*) continua a reduzir seu tamanho total e que a China segue buscando mais tecnologia e força

móvel (FRITZ, 2008:29) e investindo em capacidade cibernética agressiva, embora alguns autores, como Fritz (2008) e Krepnevich (2012), discordem sobre a divisão entre capacidades cibernéticas agressivas ou não, ao argumentar que, ao se preparar para defender suas estruturas de rede faz-se imprescindível entender como acontece o ataque.

Há, então, que se destacar que as possibilidades oferecidas pelo espaço cibernético à China estão sendo aproveitadas. O país, que vê no ciberespaço a maior oportunidade de ganhos políticos, econômicos e militares além da capacidade de limitar ações impositivas por parte de potências militarmente mais fortes, vem utilizando todos os meios disponíveis no comprometimento com o avanço tecnológico, inclusive através de treinamentos e simulações de ataques cibernéticos, apresentados no tópico a seguir.

5. Ações da China

Observou-se que a República Popular da China vem sendo considerada uma das maiores potências cibernéticas, fato que se dá tanto pela forte participação neste modelo de conflito, seja como alvo ou suposto agressor, quanto por seu envolvimento em fóruns de discussão sobre a área. Outro fator importante diz respeito aos investimentos do país e ao modo como o espaço cibernético vem sendo utilizado visando ao desenvolvimento de outras áreas. A estratégia militar da China menciona capacidades cibernéticas como uma área em que o Exército de Libertação do Povo deveria investir e utilizar em larga escala (HJORTDAL, 2011: 5).

Antes de apresentar a construção dessas capacidades, que parecem ter nascido com o novo Ministério de Segurança do Estado, o qual, em 1983, combinou a coleta de funções externas do governo com as funções da contra inteligência e da contra espionagem (INKSTER, 2013: 48), parece interessante evidenciar a atual capacidade cibernética da República Popular da China. Dona da capacidade cibernética mais extensa e mais praticada da Ásia, e inversamente proporcional ao seu nível de conhecimento técnico (BALL, 2012: 81), a China se mantém sob os holofotes da mídia e das discussões internacionais, uma vez que é acusada de desferir ataques aos Estados, como forma de treinamento de suas habilidades cibernéticas.

Isto posto, a seção vigente tratará da exposição da atual situação cibernética do país, como é possível visualizar mais facilmente através do Quadro 4. Em sequência contará com a descrição dos fatos a motivar o interesse sínico no que concerne às capacidades cibernéticas e dos exercícios de treinamento de tais capacidades.

Quadro 4 - Capacidade Cibernética dos Estados/Nações Asiáticos

	China	Índia	Iran	Coreia do Norte	Paquistão	Rússia
Doutrina oficial de Ciberguerra	X	X			Provável	X
Treinamento em Ciberguerra	X	X	X		X	
Exercícios e Simulações de Ciberguerra	X	X				
Colaboração com a indústria de TI e/ou com Universidades Tecnológicas	X	X	X		X	X
IT Roadmap[17]	Provável	X				
Unidades de Ciberguerra	X	X		X		
Histórico de Ciberataques a Outras nações	X					X

Fonte: Adaptada de BILLO e CHANG, 2004.

Embora de 2004, o Quadro 4 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 (2012) – de que a China é possuidora da capacidade cibernética mais extensa deste continente – e concordar com a defesa de que os investimentos cibernéticos chineses têm levado a China à posição de destaque no cenário internacional. Outro a ratificar este ponto de vista é o Major General Wang Pufeng[18], 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. Desse modo, será inteiramente possível para a China conquistar a vitória global sobre o inimigo, mesmo sob condições de inferioridade em relação à Tecnologia da Informação. (PUFENG, 1995).

[17] *Roadmap* é um termo de língua inglesa que está relacionado a "um plano de ação a contribuir para os elementos de um sistema de pesquisa bem sucedido" (SCIENCE EUROPE ROADMAP, 2013).
[18] O Major General Wang Pufeng é um antigo Diretor do Departamento de Estratégia da Academia de Ciência Militar de Beijing, China.

Pufeng (1995) também expressa a possibilidade de obtenção de ganhos através do espaço cibernético, mesmo diante de sua inferioridade tecnológica. Vale ressaltar, contudo, que o investimento na área cibernética tem sido parte importante da história chinesa especificamente desde 1985, quando Shen Weiguang, um soldado em uma unidade de campo, começou a escrever sobre a Guerra da Informação e publicou um livro de mesmo nome que mais tarde foi publicado como artigo no *Diário do Exército de Libertação*. A doutrina da Guerra da Informação, entretanto, só recebeu atenção depois da Guerra do Golfo (de 1990 a 1991) e da crença de que a IW teria executado um papel importante na vitória dos Estados Unidos, e de que a próxima guerra seria parecida com o que foi a Guerra do Golfo (MULVENON, 1999: 179).

Em 1986 as exigências da inteligência externa chinesa nas áreas de ciências e tecnologia determinaram, aos olhos externos, que esta seria a chave para o desenvolvimento econômico chinês. O que ocorria na verdade era o desenvolvimento de um programa proposto por um grupo de cientistas de armas nucleares que primeiro focou no lado militar, mas que rapidamente envolveu projetos mais gerais que visavam eliminar a dependência chinesa de tecnologia estrangeira em áreas consideradas estratégicas (INCKSTER, 2013: 50).

Nos anos 1990 o exército de Libertação do Povo deu início aos exercícios militares que envolviam alguns aspectos da Guerra da Informação. Em 1995 a China implementou o plano da Guerra da Informação. Em 1997 um corpo de elite com 100 membros foi criado pela Comissão Militar Central para elaborar meios de implantar vírus de computador incapacitantes em sistemas americanos e de outros países do Ocidente. Além disso, a China começou a conduzir numerosos exércitos com a função de utilizar vírus de computador para interromper comunicação militar e sistemas públicos de radiodifusão (BALL, 2011: 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 tecnologia de informação e comunicação como a maior vulnerabilidade que a China poderia explorar na busca por vantagens assimétricas (LIANG e XIANGSUI, 1999).

A partir desse momento as unidades chinesas de guerra cibernética parecem trabalhar a todo vapor, embora seja difícil descobrir se as ações agressivas no espaço cibernético são oriundas de agências oficiais ou de internautas independentes. 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 ou que servidores sejam atacados por programas de negação de serviço.

Em 2000 a China estabeleceu a unidade estratégica da Guerra da Informação, que os observadores americanos chamaram de Força Net, projetada para combater a redistribuição de informação através de redes de computadores e para manipular sistemas de informação do inimigo. Neste mesmo ano, as unidades de Guerra da Informação do Exército de Libertação do Povo deram início ao desenvolvimento de procedimentos detalhados para a guerra na Internet, incluindo criação de *softwares* para exploração de redes, obtenção de senhas, quebra de códigos, roubo de informação, criação de *softwares* para efetivas contramedidas, entre outros. (BALL, 2011: 84).

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, dez missões de ataque cibernético foram praticadas, 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, estabelecimento de estações de redes espiãs, entre outros (*ibidem*).

Em outubro de 2000 um exercício organizado pelo chefe de equipe do Exército de Libertação do Povo simulou ataque cibernético e guerra eletrônica com países ao sul e ao oeste do deserto de Gobi. Em 2001, quarenta especialistas do PLA ficaram 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 do programa *Cavalo de Tróia* foi usada para invadir a rede do computador do Dalai Lama. E mais recentemente, disfarçado de documento do *Microsoft Word* e *PowerPoint*, este programa foi encontrado inserido em computadores de escritórios de vários governos ao redor do mundo (BALL, 2011: 82).

Há também uma versão do *Cavalo de Tróia* considerada dorminhoca, cuja utilização é estimada para períodos de paz. O programa, depois de instalado, pode levar anos até ser ativado e receber comandos. Depois de ativado, o programa pode danificar ou destruir sistemas, além de enviar informações confidenciais de volta a Pequim[19]. São exemplos o *Worm Downadup* e o *Worm Conficker* que infectam sistemas operacionais da *Microsoft* e podem permanecer imperceptíveis até que os comandos sejam enviados (PISCITELLO, 2010).

[19] Discos rígidos portáteis, de grande capacidade, muitas vezes utilizados por agências governamentais, foram encontrados transportando cavalos de Tróia que enviavam aos websites de Pequim tudo o que o usuário do computador salvava no disco rígido (BALL, 2011).

Em 2004, durante um exercício na região militar de Pequim, que possui uma Força Azul informatizada, esta Força Azul atacou a rede da Força Vermelha para tomar o controle de sua rede de comando poucos minutos após o início do exercício, cujo objetivo era a prática da invasão aos centros de comando e controle dos sistemas de informação do inimigo. No mesmo ano, *hackers* chineses atacaram *sites* do Ministério da Defesa Nacional na tentativa de interromper o *Han Kuang-20* (exercício anual de defesa) de Taiwan (BALL, 2011: 87).

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 da internet (*ibidem*).

Em maio de 2007 o secretário de Defesa dos Estados Unidos informou ao Congresso americano que o Exército de Libertação do Povo tinha as operações de redes de computadores como fundamentais para alcançar o domínio eletromagnético ainda no início de um conflito. O secretário resolveu seguir o exemplo chinês e incorporou as ofensivas operações de redes de computadores em seus exercícios principalmente como primeiro ataque às redes inimigas (BALL, 2011).

Em 2008 a culpa sobre o lançamento de um vírus anti-japonês caiu sobre a China. O vírus lê as chaves do registro, julga o tipo de sistema operacional usado e, ao perceber que a língua utilizada é a japonesa, ele destrói o disco rígido, preenche os dados com lixo, reinicia o sistema e paralisa o computador completamente. Depois de tal acontecimento o Departamento de Defesa Americano proibiu o uso de dispositivos de armazenamento USB, cartões de memória, pen drives e cartões de câmera fotográfica em todos os departamentos militares dos Estados Unidos.

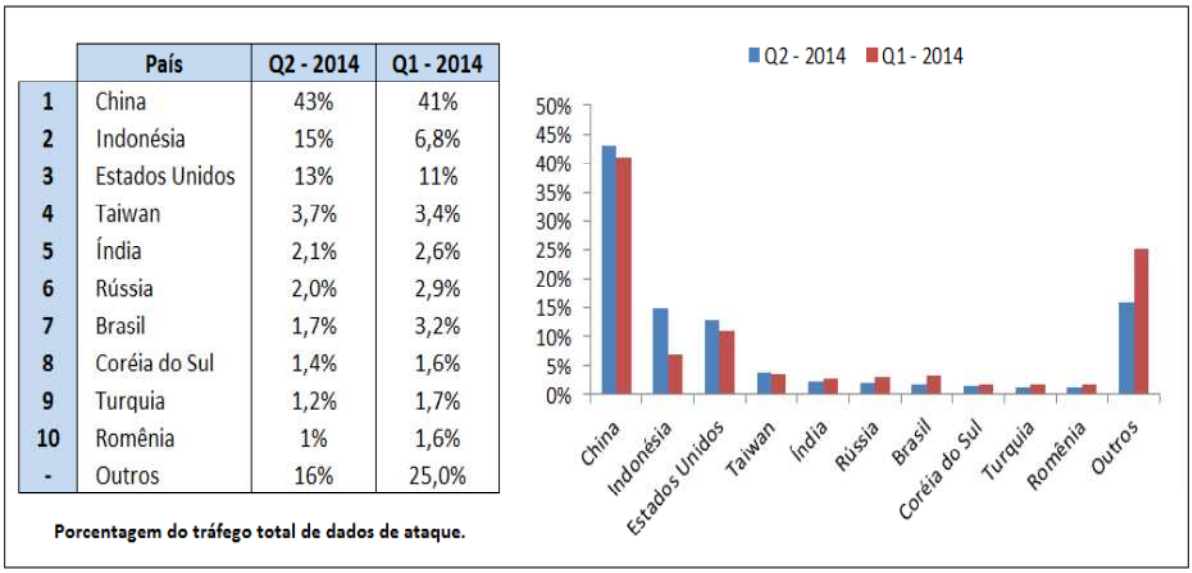
Em abril de 2009, *hackers*, que se acredita serem apoiados pelo regime comunista chinês, penetraram nos computadores críticos para o funcionamento de redes de energia elétrica dos Estados Unidos e instalaram um *software* que permitia interromper o serviço quando comandado. Em julho de 2009 *websites* do Gabinete da Presidência e do Ministério da Defesa de Seul 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 (ZHANG, 2013: 802).

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 de 2000 vezes por dia (BALL, 2011: 87). No mesmo ano a Coreia do Sul disse ter sido vítima de ataques no mesmo estilo dos ocorridos no ano anterior. As instruções envolveram ataques de negação de serviço e foram lançados a partir de 120 endereços de IP originários da China. Os *websites* teriam fornecido informações sobre serviços administrativos e políticas de governo. 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 (*ibidem*).

Em quatro de março de 2011 o Centro Nacional de Segurança Cibernética da Coreia afirmou que cerca de quarenta *websites* governamentais e privados haviam sido atacados no dia anterior, incluindo os do 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 (BALL, 2011: 86-87).

Ainda sobre as ações de participação chinesa, a empresa Akamai (2014) apresenta, no Relatório do Estado da Internet, os dados mais recentes referentes ao primeiro e ao segundo quarto do ano de 2014. O quadro apresentado na Figura 2 expõe as porcentagens do tráfego de dados de ataque cibernético mundial e aponta a China como provável responsável pelo maior número de ciberataques no mundo.

Figura 2 - Tráfego de dados relativos a ataques cibernéticos – Top 10



	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: Akamai (2014).

Os dados refletem uma tendência do comportamento chinês nos últimos anos. E conforme as informações, ainda nos permite inferir que a questão *ciber* é tratada como estratégica e prioritária no planejamento estatal chinês. Também é possível deduzir que, com os inúmeros exercícios de treinamento a desferir ataques, a porcentagem do tráfego de dados de ataque cibernético mundial a apontar para a China deve crescer nos próximos anos.

CONSIDERAÇÕES FINAIS

A informação sempre foi considerada elemento essencial na interação humana e gradualmente foi se transformando em diferencial estratégico até tornar-se insumo básico do processo decisório. Atualmente, a obtenção de informação confidencial produz inquestionáveis vantagens no ambiente competitivo e nos contenciosos internacionais, podendo ser classificada como artigo estratégico. Na busca por vantagens através do roubo de informação e da descoberta das vulnerabilidades do inimigo, o espaço cibernético tornou-se campo de batalhas e aumentou a insegurança.

A criação de termos com o prefixo *ciber* carrega a definição do ciberespaço como ambiente anárquico a produzir maiores vantagens aos que o utilizam de modo agressivo, uma vez que este espaço permite que identidades sejam facilmente fabricadas e que provas sejam plantadas com o objetivo de atribuir a outrem as agressões realizadas. Nesse contexto, a discussão sobre questões cibernéticas vem sendo destacada na sociedade internacional e a preocupação com a segurança cibernética tem sido tema das agendas internacionais. Visando à compreensão das estruturas e definições que circundam o termo cibernético, o primeiro capítulo discorreu sobre as atuais discussões, necessárias à compreensão do tema de modo geral e dos demais capítulos, em especial.

O segundo capítulo tratou da exposição de alguns conflitos cibernéticos com participação asiática, tendo como objetivo fornecer conhecimento quanto às capacidades cibernéticas dos Estados asiáticos e quanto ao modo como essas capacidades vêm sendo utilizadas pelos países da região. Daí podermos destacar que a utilização do espaço cibernético vem crescendo no continente e, com ela, as ações de ataque, roubo, entre outros danos às estruturas estratégicas dos Estados. Observou-se que o envolvimento asiático em guerras cibernéticas tem aumentado as tensões no continente e movido as atenções em sua direção.

Visto que o espaço cibernético, unido às tecnologias de informação e comunicação (TIC), tem servido de ferramenta responsável por crescimento econômico, transformação política e mudança social na região da Ásia-Pacífico, os países da região passaram a investir cada vez mais em tecnologias conectadas à rede que, embora tenham alavancado o comércio e facilitado a distribuição de recursos, expuseram estes países às ameaças cibernéticas. O investimento em tecnologia cibernética unido à utilização do espaço cibernético como

instrumento para o desenvolvimento militar e econômico dos países tem gerado conflito e intimado os países a participar das reuniões de discussão do tema.

Apesar da forte discrepância tecnológica, a exposição a ameaças cibernéticas tem incentivado a cooperação e produzido, por meio da troca de experiências, o desenvolvimento de ações necessárias para o êxito da segurança cibernética regional. Segundo Thomas (2009), essas ações precisam acontecer nos âmbitos doméstico, regional e internacional para ter impacto sob o ambiente anárquico e sem fronteiras. Com isso, os Estados pacífico asiáticos vêm seguindo planos de ação considerados necessários para a construção da maturidade cibernética da região e implementando política e legislação cibernética no âmbito doméstico.

A China, considerada potência cibernética, vem participando ativamente das discussões e executando os planos definidos pelas organizações regionais. Apesar de possuir capacidade cibernética agressiva, com o processo de informatização, suas redes vêm se tornando cada vez mais suscetíveis a ataques de rede, uma vez que este país é altamente dependente do espaço cibernético para seus programas de governo, tanto de caráter militar quanto civil.

Essa vulnerabilidade nos remete a Inkster (2013), que defende que o aparente pouco interesse em infiltração em redes chinesas está no fato de que "há muita [informação] que a China deseja roubar do Ocidente, mas relativamente pouca que o Ocidente precise roubar da China". A República Popular da China também é considerada uma potência cibernética por 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.

A utilização do espaço cibernético tornou-se de extrema importância para os planos da China, uma vez que ele representa a extensão de sua estratégia nacional de governo, na busca pelo desenvolvimento de suas capacidades políticas, econômicas e militares. Para tanto, a China vem investindo massivamente, incluindo a distribuição de atividades de caráter cibernético em suas estruturas organizacionais. Destarte, é fato que 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 o ciberespaço como meio para espionagem, destruição de dados e de capacidades inimigas e como treinamentos para testar suas táticas de ciberguerra e implantar seus *softwares* maliciosos.

Além das simulações de ataques cibernéticos contra Taiwan, Índia, Japão e Coreia do Sul, há outros casos em que a responsabilidade dos ataques recai sobre o Estado chinês. 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 ser estabelecida alguma conexão com órgãos oficiais do governo chinês. Como proveniente da natureza cibernética, a dificuldade de comprovação quanto às origens dos ataques impossibilita a implementação de métodos punitivos e permite que os atores continuem a invadir sistemas e estruturas estratégicas de outros governos. Assim, o dragão asiático parece mostrar-se não só uma potência emergente no mundo real, mas também no virtual (ou cibernético).

Por fim, é possível perceber que os investimentos em tecnologia, além de trazer vantagens ao continente, expuseram os Estados asiáticos a novas vulnerabilidades. Tais vulnerabilidades serviram de estopim a incentivar a cooperação na região e a produzir modelos de comportamento e de planejamento necessário para promoção da segurança cibernética nacional, em primeira instância, e da segurança regional de modo geral. Assim, constatamos que a região Pacífico Asiática vem investindo em capacidades cibernéticas e que a China vem utilizando o ciberespaço como meio de obter vantagens para utilização da guerra assimétrica e para elaboração de seu plano estratégico de desenvolvimento

REFERÊNCIAS

AFCEA. **The Russo-Georgian War 2008: The Role of the cyber attacks in the conflict**. Disponível em: http://www.afcea.org/committees/cyber/documents/TheRusso-GeorgianWar2008.pdf. Acessado em dezembro de 2012.

AKAMAI. **State of the Internet Report**, Segundo quarto de 2014, 2014. Disponível em: http://www.akamai.com/dl/akamai/akamai-soti-q114.pdf. Acessado em agosto de 2014.

APEC. **APEC Cyber Security Strategy**. Moscow, 2012. Disponível em: https://ccdcoe.org/sites/default/files/documents/APEC-020823-CyberSecurityStrategy.pdf. Acessado em 6 de fevereiro de 2015.

ARQUILLA, John; RONFELDT, David. **Cyberwar is Coming! Comparative Strategy**, Vol 12, No. 2, Spring 1993, pp.23-60. Copyright 1993 Taylor & Francis, Inc.

ASEAN. **Asean E-Commerce Database Project**, 2010. Disponível em: http://www.asean.org/archive/documents/ASEAN%20eCommerce%20Database%20Project.pdf. Acessado em março de 2015.

BALL, Desmond. **China's Cyber Warfare Capabilities. In: Security Challenges**, vol. 7, No. 2 (winter 2011). pp. 81-103.

BARBOSA, Tânia Isabel Lopes. **A ajuda internacional e as guerras civis: uma relação perversa?**. Dissertação de Mestrado. Universidade Técnica de Lisboa. Instituto Superior de Economia e Gestão, 2005. Disponível em https://www.repository.utl.pt/bitstream/10400.5/646/2/Tese%20de%20Mestrado%20DCI.pdf. Acessado em outubro de 2014.

BILLO, Charles; CHANG, Welton. **Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States**. Institute for Security Technology Studies, Dartmouth College, 2004.

BONIFACE, Pascal. **Dicionário das Relações Internacionais**. Lisboa: Plátano Edições Técnicas, 1997.

BU, Zheng; BUENO, Pedro; KASHYAP, Rahul; WOSOTOWSKY, Adam. **The New Era of Botnets**, 2010. Disponível em: http://www.mcafee.com/in/resources/white-papers/wp-new-era-of-botnets.pdf. Acessado em novembro de 2014.

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

CANHOTA Jr, A. J. S. da; SOUZA, D. A. de; MOUTINHO, D. dos S.; LOHNEFINK, F. P. **Engenharia Reversa**, UFF: Niterói, 2005.

CAPLAN, Nathalie. **Cyber War: the Challenge to National Security**. In: Global Security Studies, Volume 4, Issue 1, 2013. pp. 93-115.

CARVALHO, Paulo S. M. de. **A defesa cibernética e as infraestruturas críticas nacionais**. CICLO DE ESTUDOS ESTRATÉGICOS, 1º, 2011, Rio de Janeiro. Apresentações. Rio de Janeiro: Escola de Comando e Estado-Maior do Exército, 2011. Disponível em: http://200.20.16.3/seer_ocs/index.php/CEE/XCEE/paper/viewFile/5/7. Acessado em dezembro de 2012.

CASTRO, Luiz Fernando Damaceno Moura e. **Estônia sofre ataque virtual**. IN: Conjuntura Internacional, PUC Minas, 2007. Disponível em: http://www.pucminas.br/imagedb/conjuntura/CNO_ARQ_NOTIC20070704113456.pdf?PHPSESSID=6639374fa11926e0d1f13e468e246346. Acessado em abril de 2013.

CHINA. **CHINA`S DEFENCE WHITE PAPER**, 2013. Disponível em: http://www.idsa.in/idsacomments/ChinasDefenseWhitePaper2012_rgupta_220413. Acessado em abril de 2015.

CLARKE, Richard A.; KNAKE, Robert K. **Cyber war: the next threat to national security and what to do about it**. 2. ed. New York: HarperCollins e-books, 2012.

CLAUSEWITZ, Carl Von. On War. Editado e traduzido por Michael Howard e Peter Paret. Princeton, New Jersey: Princeton University Press, 1989.

COLE, August. **Defense Industry Pursues Gold in "Smart Power Deals"**. IN: Wall Street Journal. 21 de março de 2010. Disponível em: http://www.mcleanllc.com/pdf/WSJ.pdf. Acessado em janeiro de 2014.

DCAF BACKGROUNDER. **Adidos para a Defesa**. 2008. Disponível em: file:///C:/Users/Ahmina/Downloads/port_defense_attachees%20.pdf. Acessado em abril de 2015.

DESLAURIERS, J.; KÉRISIT, M. **O delineamento de pesquisa qualitativa**. In: A pesquisa qualitativa: Enfoques epistemológicos e metodológicos. Petrópolis, RJ: Vozes, 2008. pp. 127-153.

DOBSON, W. A. C. H. **China, pasado y presente**. In: Revista Estudios de Asia y África. China: perspectivas sobre su cultura e historias. México: El Colegio de México. Centro de Estudios de Asia y África, 2006.

EUROPEAN COMMISSION. Annex I of the European Commission Export Control Regulation - **List Of Dual-Use Items and Technology**, 2008. Disponível em http://trade.ec.europa.eu/doclib/docs/2008/september/tradoc_140595 Acessado em maio de 2015.

E-ASEAN. **E-Asean Framework Agreement**. Disponível em: http:// www.asean.org news/item/e-asean-framework-agreement. Acessado em março de 2015.

E-ASEAN**, E-Asean Task Force**. Disponível em: http://www.e-aseantf.org/. Acessado em março de 2015.

FALLIERE, Nicolas; MURCHU, Liam O.; CHIEN, Eric. **W32.Stuxnet Dossier: versão 1.4**. 2011. Disponível em: http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-044.pdf. Acessado em abril de 2013.

FEAKIN, Tobias. **Enter de Cyber Dragon: chinese cyber capabilities**. 2013.

FERNANDES, José Pedro Teixeira. **A Ciberguerra como nova dimensão dos conflitos do século XXI.** In: Relações Internacionais, no.33, 2012, pp.53-69.

FRITZ, Jason. **How China will use cyber warfare to leapfrog in military competitiveness.** IN: Culture Mandala, Vol. 8, No. 1, 2008, pp.28-80. Disponível em: http://epublications.bond.edu.au/cgi/viewcontent.cgi?article=1110&context=cm. Acessado em março de 2015.

FARWEL, James P.; ROHOZINSKI, Rafal. **Stuxnet and the Future of Cyber War**. 2011. Disponível em: https://www.cs.duke.edu/courses/common/compsci092/papers/cyberwar/stuxnet2.pdf. Acessado em abril de 2013.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 5. ed. São Paulo: Atlas, 2008.

GILES, Keir. **"Information Troops": a Russian Cyber Command?** Conflict Studies Research Centre, Oxford, UK, 2011. Disponível em: https://ccdcoe.org/ICCC/materials/proceedings/giles.pdf. Acessado em 14 de setembro de 2014.

GLOBAL CYBER SECURITY CAPACITY CENTRE, **Computer Emergency Response Team**. 2014. Disponível em: http://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CERTs%20An%20Overview%20.pdf. Acessado em 26 de fevereiro de 2015.

HACHIGIAN, Nina. **China`s Cyber-Strategy.** IN: Foreign Affairs, Vol. 80, No. 2 (marc-abr 2001), pp. 118-133. Disponível em: http://www.jstor.org/discover/10.2307/20050069?uid=2134&uid=2493329973&uid=2&uid=70&uid=3&uid=60&uid=2493329963&purchase-type=none&accessType=none&sid=21106596575553&showMyJstorPss=false&seq =16&showAccess=false. Acessado em março de 2015.

HARRIS, Shane. **China's Cyber Militia: Chinese hackers pose a clear and present danger to U.S. Government and private-sector computer networks and may be responsible for two major U. S. power blackouts.** 2008.

HJORTDAL, Magnus. **China's Use of Ciber Warfare: Espionage Meets Strategic Deterrence**. CHINA_SEC, Centre of Military Studies, University of Copenhagen, 2011.

HERZOG, Stephen. **Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses**, 2011. Disponível em: http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1105&context=jss. Acessado em março de 2015.

INKSTER, Nagel. **Chinese Intelligence in the Cyber Age**. In: ***Survival Global, Politics and Strategy***. Volume 55, n 1, Fevereiro-Março,. Editora: Routledge, 2013.

HACHIGIAN, Nina. ***China's Cyber-Strategy***. IN: Foreign Affairs. Vol 80, n. 2, (março-abril de 2011), pp 118-133. Disponível em: https://www.foreignaffairs.com/articles/asia/2001-03-01/chinas-cyber-strategy. Acessado em Abril de 2015.

ITO, Yurie, **Introduction of APCERT**, 2005. Disponível em: http://www.oecd.org/sti/ieconomy/35492507.pdf. Acessado em 10 de março de 2015.

KARSPERSKY. **Karspersky Lab confirma relação entre Stuxnet e Flame**. 2012. Disponível em: http://brazil.kaspersky.com/sobre-a-kaspersky/centro-de-imprensa/comunicados-de-imprensa/kaspersky-lab-confirma-rela%C3%A7%C3%A3o-entre-st. Acessado em agosto de 2013.

KREPINEVICH, Andrew F. **Cyber warfare: a "nuclear option"?** Washington, D.C.: Center for Strategic and Budgetary Assessment, 2012.

KRISMAN, Khanisa. **A Secure Connection: Finding the Form of ASEAN Cyber Security Cooperation**, 2013. Disponível em: http://ir.binus.ac.id/files/2013/09/4.-Secure-Connection.pdf. Acessado em: 23 de fevereiro de 2015.

LEINER, Barry M. et al. **A Brief History of the Internet**. Acm Sigcomm Computer Communication Review, v. 5, n. 39, p.22-31, out. 2009.

LEWIS, James A. **The "Korean" Cyber Attacks and Their Implications for Cyber Conflict**. Center for Strategic and International Studies. 2009. Disponível em: http://dspace.africaportal.org/jspui/bitstream/123456789/26510/1/The%20Korean%20Cyber%20Attacks%20and%20Their%20Implications%20for%20Cyber%20Conflict.pdf?1. Acessado em agosto de 2013.

LIANG, Qiao; XIANGSUI, Liang. **Conjecturas sobre a Guerra e a tática na era da Globalização**. Beijing: Pla Literature and Arts Publishing House, 1999.

LIBICKI, Martim C. **Cyberdeterrence and Cyberwar**, Santa Mônica, Califórnia: Rand Corporation, 2009.

MARQUES, Oscar. Palestrante do tema: **Guerras cibernéticas e ameaças**. In: Palestra Técnica do CISL – Seminários Tecnológicos – Segurança da Informação. Disponível em: http://assiste.serpro.gov.br/cisl/semtec.html Acessado em dezembro de 2012.

MATROSOV, Aleksand. **Stuxnet Under the Microscope. Revision 1.31**., 2010. Disponível em: http://www.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf, 24 Sept. 2010. Acessado em 02 de fevereiro de 2015.

McNELLY, Mark. **Sun Tzu and the Art of Modern Warfare**. Oxford University Press, 2001.

MICHAEL, David C.; NETTESHEIM, Christoph e ZHOU, Yvonne. **China's Digital Generations 3.0: the online empire**., 2012. Disponível em: http://www.bcg.com.cn/en/files/publications/reports_pdf/BCG_China_Digital_Generations_3.0_ENG_Apr_2012.pdf. Acessado em Abril de 2015.

MORTON, K.F; GRACE, David. **A case study on Stuxnet and Flame Malware.** 2012. Disponível em: http://vixra.org/pdf/1209.0040v1.pdf. Acessado em abril de 2015.

MOURSUND, David G. **Introduction to problem solving in the Information Age**. Eugene, Oregon: Information Age Education. Retrieved, 2007. Disponível em: http://pages.uoregon.edu/moursund/Books/IAE-PS/PS-in-IA.pdf. Acessado em Junho de 2014.

MUELLER, Paul; YADEGARI, Babak. **The Stuxnet Worm**. 2012. Disponível em: http://www.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf. Acessado em abril de 2013.

MULVENON, James C. **The PLA and Information Warfare**. Editores: Mulvenon & Yang, IN: The People's Liberation Army in the Information Age, (Washington DC: RAND, 1999), pp.175-186.

NBC NEWS. **A look at Estonia`s cyber attack in 2007**. Disponível em http://www.nbcnews.com/id/31801246/ns/technology_and_science-security/t/look-estonias-cyber-attack/#.VP2qwfnF8s8. Acessado em maio de 2015.

NICHOL, Jim. **Russia-Georgia Conflict in August 2008: context and implications for US interests**. 2009. Disponível em: https://www.fas.org/sgp/crs/row/RL34618.pdf. Acessado em abril de 2013.

NYE, Joseph S. **Cyber Insecurity**. dez. 2008. Disponível em: http://belfercenter.ksg.harvard.edu/publication/18727/cyber_insecurity.html. Acessado em janeiro de 2013.

NYE, Joseph S. **O Futuro do Poder**. Tradução de Magda Lopes. 1ª ed. São Paulo: Benvirá, 2012.

OLIVEIRA, Maria Engel de. **Orkut: o impacto da realidade da infidelidade virtual.** 2007. Dissertação (Mestrado) - Curso de Psicologia, Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2007.

PATRASCU, Alecsandru; SIMION, Emil. **Meet Flame, the most outrageous malware yet**. In: PĂTRAȘCU, Alecsandru; SIMION, Emil. Cryptography and cyber security. Practical Scenarios. U.P.B. Sci. Bull (Série C), 2013. (Apêndice). Disponível em: http://www.cert-ro.eu/articol.php?idarticol=613. Acessado em agosto de 2014.

PENIN, Aquilino Rodríguez. **Sistemas SCADA**. 2. ed. Marcombo, S.A., 2007.

PISCITELLO, Dave. **ConfickerSummaryandReview: ICANN**, 2010. Disponível em: https://www.icann.org/en/system/files/files/conficker-summary-review-07may10-en.pdf. Acessado em agosto de 2014.

PUFENG, Wang. **The Challenge of Information Warfare**. China Military Science, Spring 1995, disponível em http://www.fas.org/irp/world/china/docs/iw_mg_wang.htm. Acessado em outubro de 2014.

SAMPIERI, Roberto Hèrnandez; COLLADO, Carlos Fèrnadez; LUCIO, Pillar Baptista. **Metodologia da Pesquisa**. São Paulo: Mc Graw-Hill, 2006.

SANTOS, Loureiro**. Reflexões sobre Estratégia**. Temas de Segurança e Defesa. Instituto de Altos Estudos Militares. Publicações Europa-América, 2000.

SCIENCE EUROPE ROADMAP. 2013. Disponível em http://www.scienceeurope.org/uploads/PublicDocumentsAndSpeeches/ScienceEurope_Roadmap.pdf. Acessado em janeiro de 2014.

SHAH, Aaushi; RAVI, Srinidhi. **A to Z of Cyber Crime**. Asian School of Cyber Laws. 2012. Disponível em: https://ensaiosjuridicos.files.wordpress.com/2013/06/122592201-cybercrime.pdf. Acessado em março de 2014.

SINGER, Peter W.; FRIEDMAN, Allan. **Cybersecurity and Cyberwar: what everybody needs to know**. New York: Oxford University Press, 2014.

SILVEIRA, Denise Tolfo; CÓRDOVA, Fernanda Peixoto. **A Pesquisa Científica**. In: Métodos de Pesquisa. Org. GERHARDT, Tatiana Engel e SILVEIRA, Denise Tolfo. Porto Alegre: Editora da Universidade Federal do Rio Grande do Sul - UFRGS, 2009.

SOUZA, Gills Lopes Macêdo. **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 em Relações Internacionais) Universidade Estadual da Paraíba, 2010.

SOUZA, Gills Lopes Macêdo. **A emergência do tema ciberguerra: contextualizando a criaçãodo Centro de Defesa Cibernética à luz da Estratégia Nacional de Defesa**. In: SEMINÁRIO DO LIVRO BRANCO DE DEFESA NACIONAL, 6., 2011, São Paulo. Anais... Brasília: Ministério da Defesa, 2011a. Disponível em: http://defesa.gov.br/projetosweb/livrobranco/arquivos/apresentacao-trabalhos/artigo-gills-lopes.pdf. Acessado em outubro de 2013.

SOUZA, Gills Lopes Macêdo. **Análise sobre o Impacto das Novas Tecnologias de Informação e Comunicação nas Estratégias Nacionais de Defesa e Segurança Cibernéticas do Século XXI**. In: III Simpósio de Pós-Graduação em Relações Internacionais do programa "San Thiago Dantas" (UNESP, UNICAMP e PUC/SP). ISSN 1984-9265, 2011b.

SYSTEMS RESEARCH CENTER. **In Memorian: J. C. R. Licklider 1915-1990**. 1990. Disponível em: http://web.stanford.edu/dept/SUL/library/extra4/sloan/mousesite/Secondary/Licklider.pdf. Acessado em julho de 2014.

TERADA, Takashi. **The Genesis of APEC: Australia-Japan Political Initiatives**. Pacific Economic Papers, No. 298, December 1999, pp. 51

TETI, A. **Ottobre Rosso, un esempio di Cyber-spionaggio**, GNOSIS, Rivista Italiana di Intelligence, n. 1-2013, ISSN 1824-5900, 2013, pag. 63-83.

THÉVENET, Cédric. **Cyberterrorisme, mythe ou réalité?** Université de Marne-La- Vallée. Institut Francilien d'Ingénierie et des Services. Centre d'Etudes Scientifiques de Défense – CESD. 2006.

THE ECONOMIST. **Estonia has faced down Russian rioters. But its websites are still under attack**. Disponível em: http://www.economist.com/node/9163598. Acessado em abril de 2010.

THE GUARDIAN. **Russia accused of unleashing cyberwar to disable Estonia**. Disponível em: http://www.theguardian.com/world/2007/may/17/topstories3.russia. Acessado em abril de 2010.

THE NEW YORK TIMES. **After Gunfire, Cyberattacks**. Disponível em: http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0. Acessado em abril de 2010.

THOMAS, Nicolas. **Cyber Security in East Asia: Governing Anarchy**. 2009 Disponível em: http://www.tandfonline.com/doi/pdf/10.1080/14799850802611446. Acessado em 13 de janeiro de 2015.

TRAYNOR, Ian. **Russia accused of unleashing cyberwar to disable Estonia**. In: The Guardian. maio de 2007. Disponível em: http://www.theguardian.com/ world/2007/may/17/topstories3.russia. Acessado em maio de 2014.

TZU, SUN. **A Arte da Guerra: os treze capítulos originais**. Tradução de Henrique Amat Rêgo Monteiro. 2ª ed. São Paulo: Clio Editora, 2012.

U. S. DEPARTMENT OF STATE, 2015. **Association of Southeast Asian Nations**. Disponível em: http://www.state.gov /p/eap/regional/asean/. Acessado em fevereiro de 2015.

ZHANG, Li. ***Chinese perspective on cyber war***. IN: International Review of the Red Cross, Volume 94, N 886, 2012. Disponível em: https://www.icrc.org/eng/assets/files/review/ 2012/irrc-886-zhang.pdf. Acessado em dezembro de 2014.