UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO SOCIOECONÔMICO (CSE)
DEPARTAMENTO DE ECONOMIA E RELAÇÕES INTERNACIONAIS (CNM)
CURSO DE GRADUAÇÃO EM RELAÇÕES INTERNACIONAIS

Maria Carolina de Castro

As competências brasileiras na produção de recursos para o setor de defesa cibernética e suas implicações

Florianópolis
2020

Maria Carolina de Castro

As competências brasileiras na produção de recursos para o setor de defesa cibernética e suas implicações

Trabalho Conclusão do Curso de Graduação em Relações Internacionais do Centro Socioeconômico da Universidade Federal de Santa Catarina como requisito para a obtenção do título de Bacharel em Relações Internacionais
Orientador: Prof. Dra. Danielle Jacon Ayres Pinto

Florianópolis
2020

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

de Castro, Maria Carolina
As competências brasileiras na produção de recursos para o setor de defesa cibernética e suas implicações / Maria Carolina de Castro ; orientadora, Danielle Jacon Ayres Pinto , 2020.
108 p.

Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Santa Catarina, Centro Sócio Econômico, Graduação em Relações Internacionais, Florianópolis, 2020.

Inclui referências.

1. Relações Internacionais. 2. Segurança Cibernética. 3. Defesa Cibernética. 4. Brasil. I. , Danielle Jacon Ayres Pinto. II. Universidade Federal de Santa Catarina. Graduação em Relações Internacionais. III. Título.

Maria Carolina de Castro

As competências brasileiras na produção de recursos para o setor de defesa cibernética e suas implicações

Florianópolis, 04 de dezembro de 2020

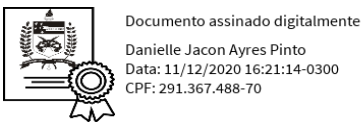
O presente Trabalho de Conclusão de Curso foi avaliado e aprovado pela banca examinadora composta pelos seguintes membros:

Prof. Dra. Danielle Jacon Ayres Pinto (Orientadora)
Universidade Federal de Santa Catarina (UFSC)

Prof. Dra. Graciela de Conti Pagliari
Universidade Federal de Santa Catarina (UFSC)

Ma. Jéssica Maria Grassi
Universidade Federal de Santa Catarina (UFSC)

Certifico que esta é a versão original e final do Trabalho de Conclusão de Curso que foi julgado adequado para obtenção do título de Bacharel em Relações Internacionais por mim e pelos demais membros da banca examinadora.



_____

Prof. Dra. Danielle Jacon Ayres Pinto (Orientadora)

Florianópolis, 2020

AGRADECIMENTOS

Primeiramente, gostaria de expressar quão estranho é chegar à tela de "agradecimentos" de seu Trabalho de Conclusão de Curso sem que se vivencie um turbilhão de sentimentos e memórias: os primeiros dias; as matérias desafiadoras, que às vezes se tornam as preferidas; a convivência com outros estudantes dentro da Universidade e a ocupação dos seus espaços múltiplos; e, por fim, a sensação de finalização, que vai se formando internamente conforme se aproxima o fim do curso.

Ter tido a oportunidade de cursar Relações Internacionais em uma Universidade pública, para mim, foi um dos maiores aprendizados que já vivenciei. A pluralidade e o choque de ideias, a abertura dos espaços de convivência, as realidades tão distintas de cada um que por ali passam. A Universidade pública, com certeza, permite e perpetua naqueles que nela estudam, lecionam e trabalham sentimentos ambíguos – aprendizado, cansaços, proximidades, embates, crescimentos –, que não são, por isso, menos impulsionadores.

É, ainda, em razão disso que, com base no pouco tempo que pude experimentá-la, perpetuo a frase do patrono da educação brasileira, Paulo Freire (2000): "Se a educação sozinha não transforma a sociedade, sem ela tampouco a sociedade muda". A Universidade pública é imperfeita, possui falhas, precisa ser aperfeiçoada, construída coletivamente, repensada em vários quesitos. Mas sem ela, é impossível transformar a sociedade brasileira de forma a possibilitar uma educação de qualidade a todos aqueles que a buscam.

Dito isto, quero agradecer, de forma geral, a todas as pessoas que passaram pela minha vida durante a graduação e que me marcaram de alguma forma. Aos meus amigos, Paula, Gustavo, Nilzo, Carolina, Henrique, João Paulo, Júlia, Bruna, Victória, e todos os outros, que apesar de não citados, estão permanentemente em minha memória. Às minhas amigas de infância, Isabella e Fernanda, pelo suporte incondicional e pela possibilidade de compartilhar nossos crescimentos sempre juntas. A meus professores, em especial à minha orientadora, Prof. Dra. Danielle Ayres, por ter persistido para que eu continuasse estudando essa temática, ainda tão incipiente no Brasil, e por ter concordado em me orientar e me dar suporte em meio à pandemia. E, finalmente, aos meus pais e à minha irmã, que, sempre me confortando com palavras de carinho e amor, estiveram ao meu lado durante esses 4 anos longe de casa, me impulsionando a crescer intelectualmente. Esse TCC é especialmente uma dedicatória do meu amor por vocês três.

“La Internet repitió la vieja paradoja de que la tecnología puede ser tan habilitante como amenazante. Lo que puede usarse para el provecho de la sociedad también puede usarse para su perjuicio.”
(KURBALIJA, 2016).

“Informação é conhecimento, e conhecimento é poder”

(HARDT; NEGRI, 2001).

RESUMO

O fenômeno da revolução tecnológica e, consequentemente, da última revolução da informação, que se deu de forma mais abrangente a partir dos anos 1970, proporcionou a introdução de novas tecnologias na sociedade, incluindo a criação da internet. A partir de sua comercialização e expansão, a internet conformou um novo espaço geográfico, de caráter artificial e humano, o espaço cibernético. Preocupados com a ascensão paulatina de ataques neste espaço, os Estados começaram a politizar a temática, tornando-a posteriormente uma preocupação securitária e, no presente século, problemática de cunho estratégico-militar, ou seja, problemática de defesa cibernética. Sob uma abordagem hipotético-dedutiva, a presente monografia tem como objetivo compreender como a criação de capacidades nacionais em defesa cibernética poderiam impactar as competências brasileiras na produção de recursos de defesa para este setor. Para tanto, põe-se o caso brasileiro à luz dos casos de China e Estados Unidos, expoentes em defesa cibernética, intencionando verificar se e como a trajetória desses países cabe ao caso do país latino-americano. Finalmente, para atingir este objetivo, utilizou-se de fontes primárias, a exemplo de documentos oficiais em matéria de segurança e defesa - incluindo segurança e defesa cibernética -, dos três países, além de fontes secundárias, como notícias de revistas e jornais, e interpretações de autores nacionais e estrangeiros concernentes à temática.

Palavras-chave: Segurança cibernética. Defesa cibernética. China. Estados Unidos. Brasil.

ABSTRACT

The phenomenon of the technological revolution and, consequently, of the last information revolution, which took place in a more comprehensive way since the 1970s, provided the introduction of new technologies in society, including the creation of the internet. From its commercialization and expansion, the internet has shaped the development of a new geographic space that has an artificial and human aspect, called cyberspace. Concerned with the gradual rise of attacks in this space, States began to politicize the theme, subsequently making it a security concern and, in the present century, a strategic-military issue, or, in other words, a problem of cyber defense. Under a hypothetical-deductive approach, this final paper aims to understand how the creation of national capabilities in cyber defense could impact Brazilian competencies in the production of defense resources for this sector. To this end, the Brazilian case is analyzed in the light of the cases of China and the United States, that are exponents in cyber defense, intending to verify if and how the trajectory of these countries suits the case of the Latin American country. Finally, to achieve this goal, primary sources were used, such as official security and defense documents - including cyber security and cyber defense - from the three countries, as well as secondary sources, such as news from magazines and newspapers, and interpretations of national and foreign authors concerning the theme.

Keywords: Cybersecurity. Cyber defense. China. United States. Brazil.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ABIN - Agência Brasileira de Inteligência

APF - Administração Pública Federal

ARPA - Advanced Research Projects Agency

BID - Base Industrial de Defesa

C3I - Sistemas de Comando, Controle, Comunicação e Inteligência

C&T - Ciência e Tecnologia

CDCiber - Centro de Defesa Cibernética

CEPESC - Centro de Pesquisas e Desenvolvimento para Segurança das Comunicações

CERT - Centro de Estudos para Resposta e Tratamento de Incidentes em Computadores

CERT.br - Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil

CGI.br - Comitê Gestor da Internet no Brasil

CGSI - Comitê Gestor em Segurança da Informação

CMID - Comissão Militar da Indústria de Defesa

ComDCiber - Comando de Defesa Cibernética

CONIN - Conselho Nacional de Informática e Automação

CS/ONU - Conselho de Segurança da Organização das Nações Unidas

C,T&I - Ciência, Tecnologia e Inovação

CTEx - Centro Tecnológico do Exército

CTIR.Gov - Centro de Tratamento e Respostas a Incidentes de Redes da APF

CW - Cyber Warfare

DCA - Defense Communication Agency

DEPIN - Departamento de Política de Informática e Automação

DES - Direitos Especiais de Saque

DHS - Department of Homeland Security

DoD - Department of Defense

DSIC - Departamento de Segurança da Informação e Comunicações

EED - Empresas Estratégicas de Defesa

ELP - Exército de Libertação Popular

EMBRATEL - Empresa Brasileira de Telecomunicações

EMCFA - Estado-Maior Conjunto das Forças Armadas

ENaDCiber - Escola Nacional de Defesa Cibernética

END - Estratégia Nacional de Defesa

EUA - Estados Unidos

FAPESP - Fundação de Amparo à Pesquisa do Estado de São Paulo

FMI - Fundo Monetário Internacional

GB - Gigabytes

GSI/PR - Gabinete de Segurança Institucional da Presidência da República

HTML - Linguagem de Marcação de Hipertexto

HTTP - Protocolo de Transferência de Hipertexto

IC - Intelligence Community

IDH - Índice de Desenvolvimento Humano

IPTO - Information Processing Techniques Office

LARC - Laboratório Nacional de Redes de Computadores

LBDN - Livro Branco de Defesa Nacional

LNCC - Laboratório Nacional de Computação Científica

MCT - Ministério da Ciência e Tecnologia

MERCOSUL - Mercado Comum do Sul

MINUSTAH - Missão das Nações Unidas para a Estabilização no Haiti

Nic.br - Núcleo de Informação e Coordenação do Ponto BR

NSA - National Security Agency

NSF - National Science Foundation

OEA - Organização dos Estados Americanos

OI - Operações de Informação

OMC - Organização Mundial do Comércio

ONU - Organização das Nações Unidas

OTAN - Organização do Tratado do Atlântico Norte

P&D - Pesquisa e Desenvolvimento

PCC - Partido Comunista Chinês

P,D&I - Pesquisa, Desenvolvimento e Inovação

PDN - Política de Defesa Nacional

PDP - Política de Desenvolvimento Produtivo

PED - Produtos Estratégicos de Defesa

PIB - Produto Interno Bruto

PND - Política Nacional de Defesa

PNID - Política Nacional da Indústria de Defesa

PTT - Ponto de Tráfego

RDS - Rádio Definido por Software

RMB - Renminbi

RNP - Rede Nacional de Ensino e Pesquisa

RST - Rede Sul de Teleprocessamento

SAIL - South Atlantic Inter Link

SEI - Secretaria Especial de Informática

SIC - Segurança da Informação e Comunicações

SIPRI - Instituto Internacional de Pesquisa para a Paz de Estocolmo

TCP - Protocolo de Controle de Transmissão

TELEBRÁS - Telecomunicações Brasileiras S. A.

TI - Tecnologia de Informação

TICs - Tecnologias de Informação e Comunicação

UNASUL - União de Nações Sul-Americanas

UFRJ - Universidade Federal do Rio de Janeiro

US$ - Dólares Americanos

US CyberCom - U.S. Cyber Command

US StratCom - U.S. Strategic Command

WWW - World Wide Web

SUMÁRIO

1 INTRODUÇÃO

Até o começo dos anos 1970, ainda no contexto da Guerra Fria, os estudiosos de Segurança Internacional limitavam a conceituação da Segurança à redoma estatal e unicamente militar e nuclear. Foi neste mesmo contexto que ascendeu a revolução tecnológica da informação, a qual se diferenciava das revoluções informacionais anteriores pela redução do custo da transmissão da informação. Entre os principais fatores de transformação tecnológica na geração, processamento e transmissão da informação, estava a difusão da computação e a subsequente criação da internet em seus moldes iniciais.

Neste sentido, as origens da internet remetem ao projeto do Departamento de Defesa estadunidense intitulado ARPANET, o qual, num período de corrida armamentista, visava alcançar superioridade tecnológica militar com relação ao adversário, a União Soviética, principalmente no tangente ao mundo universitário. Com a sua progressão, em termos de avanços tecnológicos, a internet persistiu mesmo depois do fim da Guerra Fria, chegando às mãos da maior parte das pessoas, incluindo empresários e sociedade, no meio dos anos 1990.

Não por acaso, a expansão da internet nos moldes em que ela fora projetada, trouxe, ao menos, três consequências: permitiu a criação de um espaço geográfico artificial e humano denominado espaço cibernético; perpetuou suas inseguranças, combinando os riscos de utilização das redes, o que culminou em crimes cibernéticos; e elevou as preocupações desses riscos à redoma estatal e privada, além de exportá-la para outros países, conforme a internet se expandia para além dos Estados Unidos. Principalmente com relação a este último fator, de elevação e de exportação da internet, é que esta monografia se pauta, pois foi esta condição que permitiu que os Estados securitizassem suas redes, avançando, no século XXI, para a exploração deste espaço de forma estratégico-militar.

Entendendo a securitização e a abordagem estratégico-militar do espaço cibernético como correspondentes à segurança e defesa cibernéticas, respectivamente, o presente trabalho pretende abordar a criação de capacidades nacionais cibernéticas, principalmente com relação à defesa cibernética de um país. Assim, utilizando-se do caso de dois dos Estados mais proeminentes na temática, China e Estados Unidos, vislumbra-se compreender como a criação de capacidades nacionais para este setor poderia impactar as atuais competências brasileiras em termos de defesa cibernética. A partir disso, buscou-se traduzir tal objetivo na seguinte pergunta de pesquisa: *De que forma a criação de capacidades nacionais em Defesa*

Cibernética poderia impactar as competências brasileiras na produção de recursos de Defesa para este setor?.

Sob a utilização de uma abordagem hipotético-dedutiva, parte-se da hipótese de que a capacidade nacional de defesa de um país está intimamente ligada à sua eficiência quando na dissuasão e na preservação de suas estruturas e interesses nacionais e que, portanto, a criação de capacidades nacionais em defesa cibernética, projetada através das três dimensões que compõem o espaço cibernético, o software, hardware e peopleware, impactaria as atuais competências brasileiras, ainda consideradas deficitárias, se comparadas a outras nações expoentes no setor.

Para averiguar esta hipótese, este trabalho, dividido em 3 (três) capítulos, tem como intenção, inicialmente, compreender a ascensão da temática cibernética a partir da criação da internet, interpretando os desdobramentos mundiais desta última no que tange aos seus impactos sociais, econômicos e políticos. Como já introduzido, infere-se que um dos desdobramentos políticos da ascensão da internet foi a sua securitização, sendo, portanto, fundamental no primeiro capítulo conceituar elementos como o espaço cibernético, as ameaças presentes neste espaço, a segurança e a defesa cibernéticas e, com relação majoritariamente à defesa, como podem ser definidas as capacidades estatais nacionais e como estas se formam. Aqui, reitera-se que o espaço cibernético não é conceituado, neste trabalho, como sinônimo de internet, mas que abrange, segundo Ventre (2012a), dispositivos como os satélites, os drones, os computadores, conectados ou não, os sistemas industriais informatizados, entre outros.

O segundo capítulo, à luz da introdução realizada pelo primeiro, propõe-se a analisar as capacidades reunidas tanto pelos Estados Unidos, pioneiro nas redes, quanto pela China, já que ambos configuram, na atualidade, expoentes em defesa cibernética. A partir da análise de suas forças e fraquezas individuais, projetadas, entre outros, em fatores como medidas militares, de inteligência, de desenvolvimento científico, tecnológico e de inovação, será possível interpretar por qual razão estas figuram como modelos na área e de que forma - também entendendo se há esta possibilidade - seus casos poderiam ser utilizados para se analisar o Brasil.

O terceiro e último capítulo, crucial para responder o questionamento proposto acima, pretende analisar o caso brasileiro em matéria de segurança e defesa cibernética. Focando-se em sua trajetória, desde empecilhos para inserção da internet no país e para a inserção de brasileiros na estrutura que abrange o espaço cibernético, até uma politização e

securitização tardia da temática, este capítulo não pretende esgotar comparações perante à China e os Estados Unidos, pois entende que a simples comparação esvazia a argumentação que se pretende realizar, mas sim entender suas particularidades e fragilidades.

Finalmente, com relação às fontes utilizadas para concretização desta monografia, procurou-se empregar tanto dados primários, quanto dados secundários. Em sua grande maioria, a bibliografia utilizada será composta por pesquisas de grandes organizações como o Banco Mundial e a Organização das Nações Unidas, para embasar os posicionamentos atuais dos países analisados no Contexto Internacional, e por documentos oficiais em matéria de segurança e defesa dos três países em análise. Além disso, são utilizados artigos e livros de autores nacionais e internacionais, os quais se dispuseram a interpretar tanto conceituações mais abrangentes, relativas à internet, ao espaço cibernético e à segurança e defesa na conjuntura das relações internacionais, quanto conceituações mais específicas, tangentes às capacidades detidas na contemporaneidade pela China, pelos Estados Unidos e, mais importante, pelo Brasil.

2 INSTITUCIONALIZAÇÃO E SECURITIZAÇÃO DA PAUTA CIBERNÉTICA NO MUNDO

No primeiro capítulo desta monografia, será analisada a ascensão da temática Cibernética[1] a partir de sua relação com a criação da internet, além das consequências mundiais do desenvolvimento da última no que tange aos seus impactos sociais, econômicos e desdobramentos políticos. Depreende-se aqui que a criação e a evolução da internet, produto da Revolução da Informação, desencadeou processos de institucionalização de caráter estatal e privado, além de esta sofrer com posterior securitização, como verificaremos ao fim do capítulo.

2.1 A 3ª REVOLUÇÃO INDUSTRIAL[2] E A CRIAÇÃO DA INTERNET

Segundo Castells (1999), a revolução tecnológica se caracteriza pela aplicação de conhecimentos e informação na geração de conhecimentos e dispositivos de processamento/comunicação em informação, os quais conformam um ciclo retroalimentativo entre a inovação e seu uso. Esta explicação pode ser ilustrada através dos estágios pelas quais passaram a utilização das novas tecnologias da informação: nos dois primeiros, compostos pela "automação de tarefas" e pela "experiência de uso", o progresso da inovação tecnológica baseou-se em aprender usando; no último, a "reconfiguração das aplicações", os usuários assimilaram a tecnologia fazendo, o que culminou numa reconfiguração de redes e numa descoberta de novas aplicações (CASTELLS, 1999). Para este autor, portanto, "as novas tecnologias de informação não são simplesmente ferramentas a serem aplicadas, mas processos a serem desenvolvidos. Usuários e criadores podem tornar-se a mesma coisa (...)" (CASTELLS, 1999, p. 69).

Em complemento, Nye Jr. (2012, p.152) discorre que a atual revolução da informação, também conhecida às vezes por "terceira revolução industrial"[3], é assim referenciada por se

---

[1] O termo cibernética, segundo Mandarino Jr. (2010, p. 66), deriva do grego *kybernetes*, que é aquele que "governa o timão ou leme", tendo a mesma raiz de governo. André-Marie Ampère (1834 apud MANDARINO JR., 2010, p. 66) utilizou o termo para descrever "a ciência da gestão de processos". Stafford Beer (1959 apud MANDARINO JR, 2010, p. 66), por sua vez, a descreveu como a "ciência da organização eficaz".

[2] Refere-se assim à atual Revolução da Informação em razão da nomenclatura utilizada por Nye Jr. (2012).

[3] A partir dos anos 2000, o mundo passou a encarar a sua "quarta revolução industrial", também chamada de "Indústria 4.0", que se caracteriza pelo "crescimento exponencial da capacidade de computação e combinação de tecnologias físicas, digitais e biológicas" (MAGALHÃES e VENDRAMINI, 2018, p. 42).

basear nos "rápidos avanços tecnológicos em computadores, comunicações e softwares", e se diferencia das revoluções informacionais anteriores não pela velocidade nas comunicações, mas pela redução do custo da transmissão da informação (NYE JR., 2012).

Os principais fatores de transformação tecnológica na geração, processamento e transmissão da informação que contribuíram para a formação desse novo paradigma sociotécnico incluem, por sua vez, para além de macromudanças da microengenharia de eletrônica e informação e da difusão da computação, a criação da internet (CASTELLS, 1999). Ao contrário do que se sucedeu perante outras revoluções tecnológicas, que ocorreram em apenas algumas sociedades com áreas geográficas relativamente limitadas, as novas tecnologias da informação difundiram-se pelo mundo, entre os anos 1970 e 1990, por meio de uma lógica descrita como a característica máxima dessa nova revolução: "a aplicação imediata no próprio desenvolvimento da tecnologia gerada, conectando o mundo através da tecnologia da informação" (CASTELLS, 1999, p. 70).

É de crucial importância para esta monografia, então, que neste capítulo introdutório se compreenda especificamente o papel que a criação de uma dessas tecnologias, a internet, desempenhou como objeto de mudanças sociais, as quais, segundo Toffler (1980 apud MANDARINO JR., 2010), transformaram o modo de vida de forma tão intensa apenas duas vezes anteriormente, isto é, quando a espécie humana passou de civilização nômade para civilização sedentária, há cerca de 10 mil anos, e quando a espécie humana deixou de ser predominantemente agrícola para se tornar industrial, há cerca de 330 anos.

As origens da internet, de acordo com Castells (2003), remontam ao projeto ARPANET, correspondente a uma rede de computadores montada pela agência estadunidense *Advanced Research Projects Agency* (ARPA) no ano de 1969. Formado pelo Departamento de Defesa norte-americano, esta tinha a missão de "mobilizar recursos de pesquisa, particularmente no mundo universitário, com o objetivo de alcançar superioridade tecnológica militar em relação à União Soviética" (CASTELLS, 2003, p. 13).

Para que fosse possível montar uma rede interativa de computadores, um dos departamentos da ARPA, *o Information Processing Techniques Office* (IPTO) utilizou-se de uma tecnologia de transmissão de telecomunicações, a comutação por pacote[4]. O próximo passo consistia na produção de protocolos de comunicação padronizados. Foi criado, portanto,

[4] Segundo Lopes Dias e Hadj Sadok (2001, p. 16), "A comutação por pacote consiste em "quebrar" os dados em pacotes ou datagramas que são rotulados para indicar a origem e o destino da informação e o encaminhamento destes pacotes de um computador a outro, até que a informação chegue ao seu computador final de destino".

em 1978, o Protocolo de Controle de Transmissão (TCP), o qual foi dividido em duas partes, o TCP/IP[5] - por meio do qual a internet continua operando no momento atual -, e o NCP, por meio do qual a ARPANET seguiu operando (CASTELLS, 2003).

Em 1975, tem-se a transferência da administração da ARPANET para a *Defense Communication Agency* (DCA). Intencionando disponibilizar a comunicação por computador entre os diferentes ramos das Forças Armadas estadunidenses, foi estabelecida a *Defense Data Network*, a qual possibilitava uma conexão entre várias redes sobre o controle da DCA e operava a partir de protocolos TCP/IP. Em 1983, contudo, preocupado com possíveis falhas de segurança, o Departamento de Defesa estadunidense criou a MILNET, rede independente para fins militares. A ARPANET tornou-se ARPA-INTERNET, dedicada à pesquisa (CASTELLS, 2003).

No começo dos anos 1990, por sua vez, a ARPANET, nos moldes em que havia sido criada, já era considerada tecnologicamente obsoleta, e foi retirada de operação. Como o governo dos Estados Unidos (EUA) havia descaracterizado a internet de seu ambiente militar, sua administração foi temporariamente confiada à *National Science Foundation* (NSF). No entanto, sua privatização foi logo providenciada, pois a tecnologia de redes de computadores já havia atingido o domínio público, e as telecomunicações passavam por plena desregulação (CASTELLS, 2003).

É importante frisar que o Departamento de Defesa deste país já estava decidido a comercializar a tecnologia da internet desde os anos 1980, tendo financiado então fabricantes de computadores para que estes incluíssem o TCP/IP em seus protocolos. Na década de 90, com tal privatização já encaminhada, a maioria destes computadores já possuía, portanto, capacidade de entrar em rede (CASTELLS, 2003).

Ainda nesta década, e como consequência da privatização da internet, "muitos provedores de serviços montaram suas próprias redes e estabeleceram suas próprias portas de comunicação em bases comerciais" (CASTELLS, 2003, p. 15). Somando-se à inserção do TCP/IP em protocolos de computadores comercializáveis, e finalmente, ainda mais importante, ao desenvolvimento do "www"[6] pelo pesquisador britânico Berners-Lee, este fato foi essencial para que a internet pudesse crescer rapidamente como uma "rede global de redes de computadores" (CASTELLS, 2003, p. 15).

---

[5] A sigla IP corresponde ao "protocolo intrarrede" (CASTELLS, 2003).

[6] A sigla "www" corresponde ao "*world wide web*", aplicativo que "organizava o teor dos sítios da Internet por informação, e não por localização, oferecendo aos usuários um sistema fácil de pesquisa para procurar as informações desejadas" (CASTELLS, 1999, p. 88).

Em conclusão, Castells frisa, no primeiro capítulo da obra: "A Galáxia Internet: reflexões sobre a internet, negócios e a sociedade", que,

> [...] embora a internet tivesse começado na mente dos cientistas da computação no início da década de 1960, uma rede de comunicações por computador tivesse sido formada em 1969, e comunidades dispersas de computação reunindo cientistas e *hackers* tivessem brotado desde o final da década de 1970, para a maioria das pessoas, para os empresários e para a sociedade em geral, foi em 1995 que ela nasceu (CASTELLS, 2003, p. 19).

Todavia, como argumentam Clarke e Knake (2010), os designers da internet não desejavam seu controle por governos, tendo arquitetado um sistema que se focou mais na descentralização do que na segurança. A consequência desta prioridade se refletiu em protocolos que permitiram, ao mesmo tempo, o crescimento maciço da rede e a criação da internet nos moldes que conhecemos atualmente, mas também perpetuou as problemáticas de segurança em seu modelo vigente (CLARKE; KNAKE, 2010), conforme veremos na próxima seção.

2.2 DA INSTITUCIONALIZAÇÃO À SECURITIZAÇÃO DO ESPAÇO CIBERNÉTICO

A ampliação significativa da internet, ao longo dos anos 1990 e 2000, foi possibilitada pela diminuição do preço dos computadores e do preço do acesso à internet, impulsionando sua popularização em escala mundial (SOUZA, 2013). A partir do século XXI, o número de internautas também aumentou, equiparando quantitativamente a evolução da rede mundial de computadores, e atingindo quase 300 milhões de usuários ainda no final do ano 2000 (LUPI, 2001, p. 199 apud SOUZA, 2013).

Estas expansões, especialmente no que tange ao presente século, segundo Moreira e Cordeiro (2014), instituíram o surgimento de um novo espaço, denominado espaço cibernético, o qual será apresentado mais minuciosamente nas duas próximas subseções.

2.2.1 Definindo o espaço cibernético

O termo espaço cibernético, também chamado de ciberespaço, apareceu pela primeira vez com o escritor de ficção científica William Gibson, em 1982, e se popularizou com o mesmo autor, em sua obra de 1984, *Neuromancer* (MANDARINO JR, 2010). Com fins de explicação do espaço cibernético mais direcionado à visão apresentada por autores de campos

de estudos próximos ao das relações internacionais, se utilizam aqui conceitos de Ferreira Neto (2014), de Ventre (2012a) e de Mandarino Jr. (2010), respectivamente. Antes de apresentá-los, no entanto, é importante frisar que este espaço ainda não apresenta um significado universalmente aceito, impossibilitando uma definição mais rigorosa (OLIVEIRA; PORTELA, 2017).

Para Ferreira Neto (2014), a cibernética pode ser vista de duas formas. Tanto como um recurso clássico à disposição da política, representado pela informação, quanto como um domínio espacial autônomo, conforme são conhecidos os domínios terrestre, marítimo, aéreo e extra-atmosférico. A definição considerada para esta monografia é preferencialmente a segunda, a qual atribui ao tema a dimensão de território, conhecida por espaço cibernético (FERREIRA NETO, 2014). Apesar de ser considerado artificial, em oposição aos espaços tradicionais (FERREIRA NETO, 2014), este é também marcado pelo fenômeno da territorialização, traduzido pela "tentativa de um indivíduo ou um grupo de atingir, influenciar ou controlar pessoas, fenômenos e relacionamentos, através de delimitação e afirmação do controle sobre uma área geográfica" (ROBERT SACK, 1986 apud FERREIRA NETO, 2014, p. 8). Isso implica tratar o ciberespaço como um local onde há a tentativa de exercer o poder, o qual, por ser objeto de uma relação, também é frequentemente confrontado (FERREIRA NETO, 2014).

Ventre (2012a), a seu modo, argumenta que o ciberespaço não se apresenta tal qual sinônimo de internet. Este pode ser definido como "os satélites, os drones, os sistemas de identificação por rádio frequência, os computadores - conectados ou não -, e os sistemas industriais informatizados" (VENTRE, 2012a, p. 34)[7]. Para além, o espaço cibernético, um subconjunto do espaço de informação, pode ser representado como um objeto detentor de três camadas: "uma camada inferior, de caráter físico, material, formado pela infraestrutura (hardware, redes); uma camada intermediária, representada pelos softwares e pelas aplicações; e uma camada superior, de caráter cognitivo" (VENTRE, 2012a, p. 34)[8].

Mandarino Jr. (2010), finalmente, considera este espaço como sendo o complexo virtual formado pela infraestrutura crítica da informação. Essa infraestrutura, vinculada à

[7] [tradução nossa]. No original, lê-se: "El ciberespacio es un concepto que no está bien definido. Algunos lo hacen sinónimo de Internet. Pero el ciberespacio es mucho más: los satélites, los drones, el RFID, los ordenadores conectados o no, los sistemas industriales informatizados, todos son componentes del ciberespacio".

[8] [tradução nossa]. No original, lê-se: "Y este, que es un subconjunto del espacio de información, se puede representar como un objeto formado por tres capas: Una capa inferior, física, material, que es la de la infraestructura (hardware, redes…); Una capa intermedia, la del software, de las aplicaciones; Y por último una capa superior, cognitiva.".

segurança da informação e às comunicações, por sua vez, compreende hardwares, softwares e equipamentos que se interconectam por meio de fibras ópticas ou pelo espectro eletromagnético; os locais de armazenagem, processamento e transmissão das informações; e as pessoas que interagem com essa infraestrutura (MANDARINO JR., 2010). Isso nos leva a compreender, em conclusão, que, assim como Ventre (2012a) este leva em consideração as três camadas: a de hardware, software, e cognitiva - esta última, também chamada de peopleware. Entretanto, como posto por Oliveira e Portela (2017), diferentemente de Ventre (2012a), Mandarino Jr. (2010), considera o usuário um participante do ciberespaço, enquanto o outro o aponta apenas como "operador e agente de territorialização" (OLIVEIRA; PORTELA, 2017, p. 81). Neste sentido, esses autores afirmam que a camada de hardware é estrutural, enquanto a de peopleware é operacional e a de software exerce as duas funções (OLIVEIRA; PORTELA, 2017).

O conceito final de espaço cibernético a ser utilizado neste trabalho, por sua parte, visa permitir a interação das considerações realizadas por esses três autores. Primeiramente, entende-se o espaço cibernético como um território artificial onde existe uma relação de poder entre os atores perpetuantes, que visam delimitá-lo e controlá-lo (FERREIRA NETO, 2014). Em segundo lugar, como posto por Ventre (2012a) e Mandarino Jr. (2010), propõe-se o estudo desse espaço por seu viés detentor de três camadas: uma de hardwares; outra de aplicações e softwares; e uma última, que envolve as pessoas atuantes neste espaço, ou seja, de peopleware. Para esta última, dá-se preferência à conceituação de Mandarino Jr. (2010), que considera as pessoas que se relacionam com esta infraestrutura usuários participantes deste espaço.

2.2.2 As vulnerabilidades do espaço cibernético e seus agentes perpetuantes

Segundo apresentado anteriormente, em razão de o novo sistema ter como foco majoritário a descentralização ao invés da segurança, este foi concebido de forma vulnerável (CLARKE; KNAKE, 2010), sem a preocupação com os elementos de confidencialidade[9],

[9] "Propriedade de assegurar que as informações não foram acessadas por indivíduos, sistemas e/ou equipamentos sem a devida autorização" (MANDARINO JR., 2010, p. 62)

integridade[10], disponibilidade[11] e autenticidade[12] que devem circundar a informação (MANDARINO JR., 2010).

Tal ideia é complementada por Cavelty (2012a), a qual argumenta que os sistemas atuais são vulneráveis pela convergência entre três fatores: a mesma tecnologia básica de rede; a mudança para sistemas menores e muito mais abertos; e o crescimento de redes extensivas ao mesmo tempo. Ainda em outra obra, esta mesma autora acrescenta que

> [...] o domínio informacional se tornou um multiplicador de forças ao combinar os riscos para o ciberespaço (o aumento de vulnerabilidades contidas na infraestrutura da informação) com a possibilidade de riscos através do ciberespaço (atores explorando essas vulnerabilidades) (CAVELTY, 2012b, p. 105)[13].

Essas vulnerabilidades, a seu modo, são exploradas no espaço cibernético por todo tipo de atores, os quais podem ser bem e mal intencionados, detentores de objetivos distintos. Mandarino Jr. (2010) reflete que, para propósitos negativos, pessoas e grupos, uma vez dissimuladas pela distância e pela possibilidade de anonimato, podem empenhar-se em burlar a segurança dos equipamentos e de sistemas de governos, empresas e indivíduos, tentando beneficiar-se da exploração de bens de informação[14].

Surgem assim, portanto, os chamados ataques cibernéticos, os quais, de acordo com este mesmo autor, contêm os mais variados métodos conhecidos, "indo desde ações simples (mas nem por isso menos criminosas) de "pichação" de páginas da web a roubos e adulterações de informações com graves consequências para vidas humanas" (MANDARINO JR., 2010, p. 18). Cavelty (2012b), diferindo deste autor em nomenclatura, divide o que chama de conflitos cibernéticos em seis classificações distintas: hacktivismo, crime cibernético, espionagem cibernética, sabotagem cibernética, terrorismo cibernético e guerra

---

[10] "Propriedade de assegurar que as informações não foram alteradas ou modificadas de forma ilícita em nenhuma das fases de sua existência, desde a origem de armazenamento ao destino" (MANDARINO JR., 2010, p. 62).

[11] "Propriedade de assegurar que as informações estarão prontas para o acesso e utilização quando requisitadas por indivíduos, sistemas e/ou equipamentos devidamente autorizados para requerê-las" (MANDARINO JR., 2010, p. 62).

[12] "Propriedade de assegurar que as informações foram produzidas, expedidas, modificadas ou recebidas por determinado indivíduo, sistema ou equipamento" (MANDARINO JR., 2010, p. 63).

[13] [tradução nossa]. No original, lê-se: "In the 1990s, the information domain became a force-multiplier by combining the risks to cyberspace (widespread vulnerabilities in the information infrastructure) with the possibility of risks through cyberspace (actors exploiting these vulnerabilities)".

[14] A informação é um bem "incorpóreo, intangível e volátil" (MANDARINO JR., 2010, p. 37). Seus ativos, a seu modo, tornam-se os focos majoritários de atenção da segurança da informação, e podem ser representados por meios de armazenamento, transmissão e processamento da informação; por equipamentos como computadores; por sistemas utilizados; pelos locais onde se encontram esses meios e pelos seus recursos humanos (MANDARINO JR., 2010).

cibernética. Tais ameaças são classificadas consequentemente da que pode fazer menor estrago (hacktivismo) para a que pode fazer maior (guerra cibernética), e da que carrega maior probabilidade de ocorrer (hacktivismo) para a que carrega menor (guerra cibernética) (CAVELTY, 2012b). Suas definições específicas são aproveitadas nesta monografia e estão dispostas no Quadro 1.

Quadro 1 - Tipos de conflitos cibernéticos segundo Cavelty (2012b)

Tipos de conflitos cibernéticos	Descrição
Hacktivismo	"A combinação de hacking e ativismo, incluindo operações que usam técnicas de hacking contra um site de internet, que é alvo, com a intenção de interromper operações normais." (p. 116)
Crime cibernético	"Uma atividade criminal realizada com a utilização de computadores e da internet." (p. 116)
Espionagem cibernética	"A sondagem não autorizada para testar uma configuração de um computador de destino ou avaliar seus sistemas de defesa, ou a visualização e cópia não autorizadas de arquivos de dados." (p. 116)
Sabotagem cibernética	"A perturbação deliberada de um processo econômico ou militar para alcançar um objetivo específico (geralmente político) com meios cibernéticos." (p. 116)
Terror cibernético	"Ataques ilegais contra computadores, redes, e as informações nele armazenados, para intimidar ou coagir um governo ou seu povo em prol de objetivos políticos ou sociais. Este tipo de ataque deve resultar em violência contra pessoas ou propriedade, ou, pelo menos, causar danos suficientes para gerar o nível de medo necessário para ser considerado "ciberterrorismo". O termo também é usado livremente para caracterizar incidentes cibernéticos de natureza política." (p. 116)
Guerra cibernética	"O uso de computadores para interromper as atividades de um país inimigo, especialmente ataques deliberados aos sistemas de comunicação. O termo também é usado livremente para caracterizar incidentes cibernéticos de natureza política." (p. 116)

Fonte: Quadro elaborado pela autora a partir de definições encontradas em Cavelty (2012b), *tradução nossa*

Com relação aos atores que operam neste espaço e perpetuam os conflitos cibernéticos, é primordial diferenciá-los conforme o poder que detêm quando na possibilidade de territorialização - e de prejudicar, assim, outros atores. Nye Jr. (2012) observa que atualmente, desde *hackers* até grandes corporações desenvolvem códigos e normas da

internet, de certa forma longe do controle das Instituições políticas formais. Este tipo de sistemas privados, por sua vez, não desafiam os governos de Estados soberanos, mas apenas funcionam como um *locus* adicional onde estes Estados não detêm controle absoluto (NYE JR., 2012).

Propõe-se então, de modo a ilustrar a visão do autor, uma classificação que divide estes atores em três categorias: principais governos, organizações com redes altamente estruturadas, e indivíduos e redes fracamente estruturadas (NYE JR., 2012). Esta pluralidade aponta para "a redução relativa dos diferenciais de poder" (NYE JR., 2012, p. 173), ou seja, para a compreensão de que a distância entre atores estatais e não estatais, em nível de ação no *locus* cibernético, está se estreitando (NYE JR., 2012).

Isso não significa afirmar, no entanto, que a redução relativa é sinônimo de equalização (NYE JR., 2012). É por meio da possibilidade de exercer poder cibernético, entendido por Nye Jr. (2012, p. 163) como a "capacidade para obter resultados preferidos mediante o uso dos recursos de informação eletronicamente conectados do domínio cibernético", isto é, de obter resultados dentro do espaço cibernético, ou ainda, em outros domínios fora deste espaço, que pode-se, portanto, classificar hierarquicamente a seguir seus atores atuantes.

Os principais governos utilizam-se, como recurso de poder cibernético, da localização geográfica. Em outras palavras, isso acontece por causa da relação entre a infraestrutura da internet, que permanece vinculada à geografia, e da soberania destes governos sobre o seu próprio território. Ademais, afirma-se que estes atores realizam tanto atividades do tipo exploração cibernética para propósitos de espionagem, quanto ataques cibernéticos com propósitos destrutivos ou danosos (NYE JR., 2012), apesar de poucas destas poderem ser publicamente confirmadas, dada as dificuldades de atribuição a qualquer ataque[15].

Os atores não governamentais com redes altamente estruturadas, no que lhes dizem respeito, são compreendidos majoritariamente pelas grandes corporações transnacionais. Apesar de não possuírem a mesma competência que os grandes governos, algumas destas têm orçamentos enormes, além de recursos humanos especializados e controle de código confidencial, o que lhes atribuí recursos de poder maiores que os de muitos governos (NYE

[15] Kurbalija (2016, p. 108, *tradução nossa*) argumenta que uma das principais características dos ataques ou conflitos cibernéticos é a sua quase impossibilidade de atribuição, em razão do emprego de "armas complexas e sofisticadas que abrem caminho através de várias camadas *proxy*". Os servidores proxy, a seu turno, são geralmente utilizados como uma ponte entre a origem e o destino de uma requisição, e podem servir para controlar o acesso à internet, para filtrar o conteúdo, etc (BARBOSA, 2019).

JR., 2012). Contudo, visando preservar seus status legais e também os valores de suas marcas, estes atores possuem "fortes incentivos para permanecerem submissos às estruturas legais locais" (NYE JR., 2012, p. 178-179).

Os indivíduos com redes fracamente estruturadas, por último, podem facilmente manipular o domínio cibernético, devido ao baixo custo de investimento para sua entrada - para os quais são necessários apenas alguns instrumentos, a exemplo de um computador e de uma rede de internet -, pela anonimidade virtual e pela facilidade também da saída. Estes agem, por vezes, com a aprovação do governo, ou contra ele. Sua principal vulnerabilidade é a coerção legal e ilegal sofrida por parte dos governos e das organizações transnacionais, caso sejam descobertos. Esta porcentagem de captura, no entanto, como abordada, é relativamente baixa (NYE JR., 2012).

Em conclusão, a interação entre atores no espaço cibernético, seja para fins benéficos - a exemplo de novas formas de comunicação e trocas de informações, com mensagens instantâneas e trabalhos coletivos à distância, como ressalta Mandarino Jr. (2010), além do acompanhamento de e-mails e até da realização de transações bancárias (CANONGIA e MANDARINO JR., 2009) -, seja para fins mal intencionados - de exploração de vulnerabilidades, a título dos já explicados conflitos cibernéticos -, é um dos resultados da expansão e privatização da internet.

Foi em consonância com esta expansão paulatina da internet para o meio civil, portanto, que cresceu nos Estados Unidos a importância dada pelo meio político à temática da segurança cibernética, conforme será explorado na próxima seção. Essa atenção política apresentou-se, como previsto, pela combinação de contínuos incidentes cibernéticos, tais quais vírus de computadores, roubos de dados e outras penetrações em redes de computadores, e do aumento da atenção midiática, os quais criaram uma crescente sensação de ciber insegurança. Como resultado, o debate dividiu-se em duas direções: elevou a temática, ainda restrita ao nível dos especialistas técnicos, para os políticos e tomadores de decisão; e exportou a problemática, a qual era relevante apenas nos Estados Unidos, para outros países, que passaram a encabeçá-la em suas discussões institucionais e securitárias (CAVELTY, 2012b).

2.3 DA SECURITIZAÇÃO À MILITARIZAÇÃO DO ESPAÇO CIBERNÉTICO

O debate de segurança cibernética originou-se nos Estados Unidos nos anos 1970, ganhou impulso no final dos anos 1980 e expandiu-se para os demais países no final dos anos 1990 (CAVELTY, 2012b). Seu discurso nunca foi estático, pois aspectos técnicos da infraestrutura da informação estavam constantemente evoluindo, ou seja, mudanças na subestrutura técnica influenciaram a mudança do objeto referente (CAVELTY, 2012a).

De acordo com Cavelty (2012b), inicialmente os formuladores de política norte-americanos politizaram o assunto, apresentando-o como algo que necessitava a atenção dos atores estatais, não podendo ser resolvido pelas forças mercadológicas. Com a preocupação ascendendo, eles então securitizaram a temática, tornando-a um desafio que requeria a atenção prioritária e urgente do aparato de segurança nacional. Após 2010, finalmente, tendo como pano de fundo o incidente do Stuxnet, o debate foi além, e o que era inicialmente segurança cibernética tornou-se também problemática de estratégia militar, com foco em contramedidas de defesa e dissuasão cibernética[16] (CAVELTY, 2012b).

Faz-se necessário aqui traçar uma linha temporal e conceitual, delimitando de que modo esta temática foi politizada, tornando-se posteriormente preocupação securitária e, finalmente, no presente século, problemática de cunho estratégico-militar. Para atingir tal objetivo, primeiramente, deve-se apresentar o conceito de securitização, relacionando-o com o conceito de segurança e, finalmente, de defesa, o qual está fortemente atrelado a esta. Em um segundo momento, a partir deste embasamento, torna-se possível definir as conceituações acadêmicas atribuídas à segurança e à defesa cibernéticas, relacionando-as com as estruturas responsáveis pela sua manutenção. Em um último momento, compreenderemos de que forma esta temática foi exportada dos EUA para outros países do globo, e como ela tem sido crescentemente militarizada por vários destes.

2.3.1 Definindo segurança e defesa

A segurança, segundo Buzan, Wæver e Wilde (1998), é uma prática autorreferencial, ou seja, um assunto se torna uma questão securitária não porque há necessariamente uma ameaça existencial real, mas porque ele é apresentado tal qual uma[17]. Assim, atores do jogo político que intencionam a securitização de dado tema justificam assim tratá-lo com a

[16] O debate conceitual e de aplicação da segurança e defesa cibernéticas será realizado mais adiante.

[17] Para o autor, contudo, não basta a existência de um discurso que apresente dado assunto como ameaça existencial para que a securitização seja criada. Este apenas se torna securitizado, por conseguinte, quando a chamada "audiência" o aceita desta forma (BUZAN; WAEVER; WILDE, 1998).

utilização de meios extraordinários, rompendo com as regras políticas do jogo consideradas normais (BUZAN; WAEVER; WILDE, 1998).

De acordo com teóricos da Escola de Copenhague, ainda, qualquer questão pública está contida num espectro, onde pode se firmar em três etapas consequentes: esta pode ser não politizada, politizada, ou securitizada (SOUZA, 2013). Nas palavras de Buzan, Wæver e Wilde (1998),

> [...] ela varia entre não politizada (significa que o Estado não lida com ela e que esta não está de qualquer outra forma nas esferas públicas de discussão e decisão), politizada (significa que a problemática é parte da política pública, requerendo decisão governamental, alocação de recursos e, mais raramente, outras formas de governança comum), e securitizada (significa que a problemática é apresentada como uma ameaça existencial, requerendo medidas emergenciais e justificando ações fora do escopo normal do processo político) (BUZAN; WAEVER; WILDE, 1998, p. 23-24)[18].

Em adição, cada vez mais os estudos de securitização - baseados na ideia de clarificar a natureza da segurança - intencionam obter um entendimento mais preciso quanto a quem securitiza, sobre quais questões ou ameaças, para quem, por quais motivos, com quais resultados e, finalmente, perante quais condições (BUZAN; WAEVER; WILDE, 1998). Conforme apresentado com o caso dos EUA, com relação à temática da internet e sua ligação com o espaço cibernético, por conseguinte, entende-se que esta passou pelos três tipos de política, até chegar à última, de securitização.

Ademais, para propósitos de melhor compreensão da "segurança" em si, faz-se necessário diferenciar a segurança do tipo internacional da segurança nacional. Enquanto que a segunda, já abordada, segundo Buzan, Wæver e Wilde (1998), não deve ser idealizada, funcionando de modo a dar aos detentores de poder oportunidades de explorar "ameaças" para propósitos domésticos, e de reivindicar direitos para lidar com algo ou alguém sem determinados controles ou restrições democráticas, a primeira está firmemente enraizada nas tradições da política de poder, se ocupando da ameaça de existência de um dado objeto, da sua sobrevivência – seja Estado, Governo, território, sociedade, entre outros (BUZAN; WAEVER; WILDE, 1998).

---

[18] [tradução nossa]. No original, lê-se: "In theory, any public issue can be located on the spectrum ranging from nonpoliticized (meaning the state does not deal with it and it is not in any other way made an issue of public debate and decision) through politicized (meaning the issue is part of public policy, requiring government decision and resource allocations or, more rarely, some other form of communal governance) to securitized (meaning the issue is pre-sented as an existential threat, requiring emergency measures and justifying actions outside the normal bounds of political procedure)."

O termo “defesa”, no que lhe concerne, também se aproxima semanticamente, à primeira vista, do termo “segurança” (TEIXEIRA JR., 2011, p. 143 apud SOUZA, 2013). Teixeira Jr. (2011, p. 143 apud SOUZA, 2013) afirma que isso acontece, pois, intencionando garantir a segurança, é necessário se ter a defesa. Em complemento, Villa e Reis (2006), argumentam que, conceitualmente, a segurança apresenta uma referência defensiva, pois seu significado aporta, entre outros, mecanismos de organização e função do Estado-nação que têm relação com a “defesa da integridade territorial e de sua autonomia externa” (VILLA; REIS, 2006, p. 20). Por consequência, define-se a seguir o que se entende por defesa.

Souza (2013) enuncia que, quando se fala de defesa, refere-se à atuação militar na vida estatal, ou seja, nas Forças Armadas. Sua função máxima, em termos constitucionais, seria a de resposta ao contexto estratégico externo para a defesa da pátria (PROENÇA JR., 2011). Contudo, como argumentam Buzan, Wæver, Wilde (1998), em muitos países democráticos, a defesa do Estado se tornou apenas uma das funções plurais das Forças Armadas, as quais ainda incluem em seu escopo outras atividades. Entre outros empregos, a política de defesa pode ser aplicada por um governo quando na participação em missões internacionais, para uma ampla gama de atividades subsidiárias (PROENÇA JR., 2011), e, finalmente, para que as Forças Armadas desempenhem papel participativo em “sistemas de vigilância nacionais, fronteiriços, internacionais, articulados ou responsáveis por serviços de resposta de diversos tipos” (PROENÇA JR., 2011, p. 346).

Apreende-se, desta forma, que, apesar de “segurança” e “defesa” serem termos semanticamente aproximados à primeira vista, suas definições específicas diferem-nas. É importante reiterar, inclusive, que o conceito de “defesa” está mais próximo à conceituação de segurança internacional, se afastando da ideia de segurança tradicional, atrelada à segurança interna. Daí é que se trata da “defesa” como garantidora de preceitos de formação Estatal, da soberania, do território e, finalmente, da nação, como já especificado previamente a partir das ideias de Buzan, Wæver, Wilde (1998).

Ademais, há ainda uma forte corrente que advoga em benefício da separação entre Estudos de Segurança e Estudos de Defesa, para que possam ser analisados com mais detalhes assuntos sobre o desempenho dos principais atores e instituições em dados assuntos e ameaças (SOUZA, 2013). Contudo, como veremos ao diferenciar os conceitos de segurança e defesa cibernética, esta separação, especialmente na área cibernética, “é feita por uma linha tênue que em muitos momentos se desvanece, sendo difícil determinar ações de proteção específicas

para cada tipo de ameaça e quem seriam os seus responsáveis diretos" (PAGLIARI; AYRES PINTO; BARROSO, 2020, p. 153).

2.3.2 Definindo segurança e defesa cibernética

Souza (2013, p. 27) define segurança cibernética como sendo o "combate e a prevenção dos chamados crimes cibernéticos na esfera da segurança pública". Este ainda acrescenta que a segurança cibernética está retida à questão investigativa policial ou de ministérios públicos (SOUZA, 2013). Defesa cibernética, por sua vez, é o "conjunto de ações defensivas, exploratórias e ofensivas, no contexto de um planejamento militar, realizadas no espaço cibernético[...]" (CARVALHO, 2011a, p. 8). Assume-se, portanto, quanto à defesa cibernética, que esta diz respeito ao setor militar, pois, nos campos operacional e tático, são estas Forças que aplicam a estratégia, tendo a finalidade de prevenir ou de contra-atacar em casos extremos, como quando no de uma possível guerra cibernética (SOUZA, 2013).

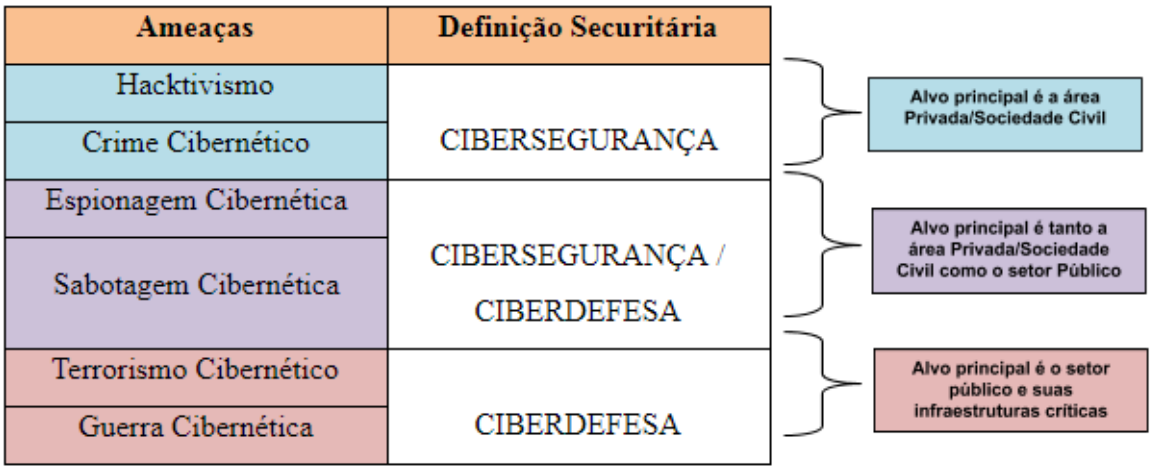
Na presente monografia, todavia, como intenciona-se, a propósito de sua problemática, explorar a produção de recursos específicos de defesa para o setor cibernético, é dada a preferência aos conceitos de segurança e, especificamente, de defesa cibernética, propostos em Pagliari, Ayres Pinto, Barroso (2020). Partindo das análises de Singer e Friedman (2014) e de Andress e Winterfeld (2011), as ameaças são divididas por essas autoras em duas dimensões: a defesa cibernética é voltada à proteção do Estado, preocupada com as infraestruturas críticas[19]; a segurança cibernética, a seu modo, corresponde mais à proteção de ameaças relativas ao setor privado, as quais possuem relação direta com a sociedade civil (PAGLIARI; AYRES PINTO; BARROSO, 2020).

Novamente, a separação conceitual entre "segurança" e "defesa" cibernética, apesar de existente, sofre na prática "com a interseccionalidade das ações ilegais cometidas na rede mundial de computadores" (PAGLIARI; AYRES PINTO; BARROSO, 2020, p. 156). Por isso, de modo a facilitar a compreensão, ilustramos o quadro de Ayres Pinto, Freitas e Pagliari

[19] Os subconjuntos dos ativos de informação, apresentados na nota de rodapé nº 14, formam uma base denominada infraestrutura de informação, a qual sustenta a sociedade da informação. As infraestruturas de informação são ditas "críticas" pois não podem sofrer com a possibilidade de descontinuidade, já que, sem elas, a sociedade da informação para, com consequências para a sociedade real (MANDARINO JR., 2010). Sua definição mais usual enuncia que infraestrutura crítica é "aquela que, uma vez prejudicada por fenômenos de causas naturais - terremotos ou inundações - ou por ações intencionais de sabotagem ou terrorismo, traz reflexos negativos para toda a nação" (MANDARINO JR., 2010, p. 38). São exemplos de infraestruturas críticas redes de telefonia, sistemas de captação e distribuição de água, fontes e redes de distribuição de energia (MANDARINO JR., 2010).

(2018, p. 48), a partir do qual se faz possível estabelecer uma relação entre a classificação de conflitos cibernéticos apresentados por Cavelty (2012b) - expostos aqui na seção 2.2.2., por meio do Quadro 1 -, as respectivas perspectivas de segurança e defesa cibernéticas e seus alvos principais.

Quadro 2 - Ameaças cibernéticas e suas definições securitárias



Fonte: Ayres Pinto, Freitas, Pagliari, 2018, p. 48.

Pagliari, Ayres Pinto, Barroso (2020), também se debruçando sobre as especificidades do Quadro 2 em sua obra, argumentam sobre a dificuldade de definir o alvo prioritário de cada ameaça, sabendo que muitas delas atingem tanto o setor público quanto o privado/sociedade civil. Contudo, é verdade que algumas dessas ações ilegais descritas podem ameaçar a soberania e a defesa de um Estado de maior forma do que outras. Por isso, quando se refere à alçada da defesa cibernética, mantém-se o foco em ameaças que possam causar grandes danos às infraestruturas críticas estatais, mesmo caso elas pertençam ao controle parcial ou total do setor privado. É, por consequência, o caso dos seguintes conflitos cibernéticos: espionagem cibernética, sabotagem cibernética, terrorismo cibernético e guerra cibernética (PAGLIARI; AYRES PINTO; BARROSO, 2020).

Ressalta-se, antes de passar para a próxima subseção, que existe um desafio que circunda a proteção das infraestruturas críticas, relacionado com a privatização e a desregulação de grande parte do setor público, nos anos 1980, e dos processos de globalização nos anos 1990, os quais colocaram grande parte dessas infraestruturas na mão de grandes corporações privadas. Tal movimentação criou uma situação onde nem as forças de mercado,

nem o Estado, sozinhos, possuem forças suficientes para prover o nível de segurança necessária para os setores relacionados às infraestruturas críticas, tendo ambos que atuar conjuntamente, atividade que se provou eficiente quando realizada por meio de cooperações de caráter público-privado (CAVELTY, 2012a).

2.3.3 A relação entre securitização e produção de capacidades nacionais cibernéticas pelos países

Como apresentado, o discurso securitário crescentemente elaborado em torno do espaço cibernético, de acordo com Cavelty (2012b), tornou esta temática um desafio urgente para o aparato da segurança nacional estadunidense, e a ampliação da internet no mundo durante os anos 1990 e 2000 (SOUZA, 2013) forneceu suporte para que a pauta fosse também paulatinamente institucionalizada e securitizada por outros países.

É importante reiterar, abordando de que forma ocorreu essa expansão, que o governo dos Estados Unidos foi o responsável por moldar tanto a percepção de ameaças, quanto as contramedidas que deveriam ser desenvolvidas por estes Estados (CAVELTY, 2012a). Como discorre Cavelty:

> [...] Por um lado, o debate foi decisivamente influenciado pelo contexto estratégico mais amplo do pós-Guerra Fria, no qual a noção de vulnerabilidades assimétricas, sintetizada pela multiplicação de atores mal-intencionados (tanto estatais quanto não-estatais) e suas capacidades crescentes de causar danos, começaram a desempenhar um papel fundamental. Por outro lado, as discussões sobre segurança cibernética sempre foram e ainda são influenciadas pela revolução da informação em andamento, que os EUA estão moldando tecnológica e intelectualmente, discutindo suas implicações nas relações para as relações internacionais e para a segurança e agindo de acordo com essas premissas (CAVELTY, 2012a, p. 364-365)[20].

Ademais, esta mesma autora entende que o discurso de segurança cibernética então criado pode ser abordado de três formas distintas, as quais estão inter relacionadas e se reforçam constantemente, mas que também possuem imaginários de ameaças, práticas de segurança, objetos referentes e atores-chave específicos. São estes: o discurso técnico

[20] [tradução nossa]. No original, lê-se: "On the one hand, the debate was decisively influenced by the larger post-Cold War strategic context in which the notion of asymmetric vulnerabilities, epitomized by the multiplication of malicious actors (both state and non-state) and their increasing capabilities to do harm, started to play a key role. On the other hand, discussions about cyber-security always were and still are influenced by the ongoing information revolution, which the USA is shaping both technologically and intellectually by discussing its implications for international relations and security and acting on these assumptions."

direcionado aos malwares[21] e às intrusões de sistemas; o discurso direcionado ao fenômeno do crime e da espionagem cibernéticos; e o discurso criado inicialmente pelas estruturas militares dos Estados Unidos, as quais se focaram, a princípio, na temática da guerra cibernética, e depois evoluíram para a proteção das infraestruturas críticas (CAVELTY, 2012a). Apesar de apresentar na presente monografia os três discursos, entendendo sua importância, pretende-se destacar a seguir o último deles.

Primeiramente, deve-se assimilar que o desenvolvimento da doutrina militar envolvendo o domínio da informação teve, nos EUA, forte fundamentação nos anos 1990, com destaque para o ano de 1991, quando a Guerra do Golfo foi o divisor de águas no tangente ao pensamento militar estadunidense sobre a temática da guerra cibernética. Limitada inicialmente às medidas militares em tempos de crise ou de guerra, esta passou a ser entendida, no meio da última década do século XX, por ações que tinham como alvo toda a infraestrutura de informação de um adversário - política, econômica e militar -, como foi o caso da operação da Organização do Tratado do Atlântico Norte (OTAN) na Iugoslávia em 1999, onde pela primeira vez se utilizaram os componentes da guerra de informação de forma total em combate (CAVELTY, 2012a).

O uso da internet durante este conflito, portanto, popularizou o termo guerra cibernética, referindo-se a este para denominar "basicamente qualquer fenômeno envolvendo o uso deliberado ou destrutivo de computadores" (CAVELTY, 2012a, p. 370)[22], e aplicando-o posteriormente para os confrontos entre os EUA e a China em 2001, para os ataques à Estônia em 2007 e para o confronto entre Rússia e Geórgia em 2008. Foi, contudo, com a descoberta do Stuxnet[23], em 2010, que a intensidade do debate mudou de forma brusca. Devido ao problema de atribuição, foi impossível confirmar quem esteve por trás deste ataque, apesar de suas suposições. Contrapuseram-se, no entanto, duas visões sobre ele: a de que este marca o início do uso não controlado de armas cibernéticas em agressões de caráter militar; e a de que

[21] É o termo usado para expressar a totalidade de ferramentas e modos de ataque utilizados por *hackers* (CAVELTY, 2012a). São exemplos os vírus e os *worms*, que são "programas de computador que replicam cópias funcionais deles mesmos com efeitos variados, que vão de meros aborrecimentos e inconveniências ao comprometimento da confidencialidade ou integridade das informações" (CAVELTY, 2012a, p. 364, *tradução nossa*).

[22] [tradução nossa]. No original, lê-se: "There-after, the term cyber-war came to be widely used to refer to basically any phenomenon involving a deliberate disruptive or destructive use of computers".

[23] Segundo Feitosa (2017, p. 15), o Stuxnet foi um vírus de tipo *worm,* "responsável pelo ataque mais repercutido na Comunidade Internacional, ocorrido em uma instalação nuclear de Natanz-Irã, em 2010, que danificou as capacidades daquele país no enriquecimento de urânio, causando danos em suas centrífugas, um exemplo claro de como um ataque utilizando software pode causar danos ao hardware de alguma infraestrutura crítica estatal".

é improvável que isto aconteça, em razão dos resultados incertos que uma guerra cibernética poderia trazer, da falta de motivação dos possíveis combatentes e da sua inabilidade em defender-se de contra-ataques[24] (CAVELTY, 2012a).

Finalmente, Cavelty (2012b) assinala que foi a descoberta do Stuxnet, somada às "ditas" numerosas espionagens chinesas, ao aumento da sofisticação de criminosos cibernéticos, e às atividades bem publicizadas de coletivos de *hackers,* que motivaram um número frequente de países a considerarem a segurança cibernética como um dos maiores problemas de segurança do futuro e, principalmente, a darem atenção ao assunto de forma estratégico-militar, preocupados com ataques que pudessem causar incidentes catastróficos envolvendo suas infraestruturas críticas. Deve-se considerar, é claro, que, apesar do marco do Stuxnet para ampliação da pauta no presente século, esse movimento de securitização e, como nomeia Cavelty (2012b), de militarização, já vinha acontecendo em alguns países desde os anos 1990 (VENTRE, 2012b).

Nesse sentido, compreende-se que a militarização do espaço cibernético está relacionada intrinsecamente com o papel atribuído para a defesa cibernética, o qual, como proposto de forma conceitual anteriormente, abrange ações por parte das forças militares que contenham caráter defensivo, exploratório e ofensivo no espaço cibernético (CARVALHO, 2011a), intencionando a proteção das infraestruturas críticas do Estado contra certas ameaças (PAGLIARI; AYRES PINTO; BARROSO, 2020). A busca dos atores pelo poder neste espaço, definido em termos de "um conjunto de recursos que estão relacionados com a criação, o controle e a comunicação de informações eletrônicas e baseadas em computador - infraestrutura, redes, software, habilidades humanas" (NYE JR., 2012, p. 163) é o que orienta, portanto, a criação de capacidades nacionais para esta área.

As capacidades nacionais, no que lhe concernem, são compreendidas em grande parte pela capacidade estatal, que é o aspecto de maior interesse no presente trabalho, já que a defesa cibernética tange às Forças Armadas e à proteção de infraestruturas críticas, como mencionado acima. Tilly (2007), em definição, apresenta o conceito de capacidade estatal, o qual mede

> [...] até que ponto as intervenções dos agentes estatais nos recursos, atividades e conexões interpessoais não estatais altera as distribuições existentes

[24] Corroborando com esta segunda visão, Ayres Pinto e Grassi (2020; s.p.) argumentam que, "apesar do uso do ciberespaço em conflitos, dos crescentes ciberataques e das preocupações futuras quanto ao seu desenvolvimento, uma verdadeira guerra cibernética ainda não existiu". A presente monografia, por sua vez, também se orienta de acordo com esta visão.

> desses recursos, atividades e conexões interpessoais, bem como as relações entre essas distribuições (TILLY, 2007, p. 16)[25].

Tais ações estatais afetam os recursos, as atividades e as conexões interpessoais de uma forma significativa, se predispostos em um regime de alta capacidade; ao contrário, em regime de baixa capacidade, os agentes estatais têm efeitos bem menos evidentes, não importando a intensidade com que eles tentem mudar as coisas. Este autor também elabora - corroborando para a discussão sobre capacidade estatal e democracia - que níveis diferentes de capacidade estatal interferem de maneira distinta nas condições fundamentais ao processo democrático[26]. Algumas dessas condições, a serem citadas, são, por exemplo, a integração de redes interpessoais de confiança nas políticas públicas, e a dissolução de centros de poder autônomos, que trazem consequências para o controle das políticas públicas e do Estado, como é o caso do narcotráfico e das organizações criminosas (TILLY, 2007).

É importante formular, ademais, que essa capacidade estatal propagada por Tilly (2007) pode ser vista por dois ângulos. Primeiramente, pelo seu aspecto interno – ou nacional –, o qual trata da capacidade estatal de penetração na sociedade, alterando as distribuições de recursos, como já tratado anteriormente (TILLY, 2007); e, por último, pelo seu aspecto externo – ou internacional –, influenciado pela relação Estado-sociedade, que se torna mais complexa dentro do sistema interestatal, em razão de os Estados serem definidos e diferenciados na atualidade pela sua capacidade de prover segurança e bem-estar aos seus cidadãos (CASTELLANO ET AL., 2012).

Nesse segundo sentido, o desempenho estatal e as condições para consolidação da democracia passam a ser avaliados também integrados às políticas sociais; à política externa, de defesa; e ao provimento da ordem pública: o Sistema Internacional pode, portanto, gerar incentivos para o fortalecimento da capacidade estatal, ou para enfraquecê-lo (CASTELLANO ET AL., 2012). Disso, em conclusão, interpreta-se que, no aspecto externo, alguns Estados possuirão a capacidade – e, portanto, o poder – de satisfazer suas próprias demandas com relação à determinadas agendas, sobrepondo-as às demandas dos demais atores.

---

[25] [tradução nossa]. No original, lê-se: "State capacity means the extent to which interventions of state agents in existing non-state resources, activities, and interpersonal connections alter existing distributions of those resources, activities, and interpersonal connections as well as relations among those distributions."

[26] Para o autor, níveis muito baixos e níveis muito altos de capacidade estatal desfavorecem os processos relacionados com a democratização (TILLY, 2007).

À nível cibernético, por sua vez, argumenta-se que estas capacidades, definidas por Lyu (2019) como o *cyber warfare*[27], abrangem muito mais áreas do que apenas a militar e a de inteligência. Um Estado, portanto, pode medir suas capacidades cibernéticas somando estes fatores a outros quesitos, tais quais o desenvolvimento científico e tecnológico (compreendido pela pesquisa e desenvolvimento) e as capacidades de inovação, as empresas do setor de tecnologia da informação, a escala de infraestrutura da internet, as influências dos sites de internet, a diplomacia de internet e as capacidades de política externa, a força militar cibernética, e a abrangência da estratégia realizada para o espaço cibernético (LYU, 2019).

O estímulo e consequente destaque na área cibernética, por sua vez, ecoando Tilly (2007) e Castellano et al. (2012), dependem diretamente do nível de promoção dessas capacidades internamente ao Estado, e de sua consequente projeção externa. Quando comparam-se países desenvolvidos aos países emergentes, por exemplo, identificam-se em vários casos da segunda fraquezas institucionais derivadas da fraca interação entre firmas privadas e centros de pesquisa públicos, da dependência de tecnologia estrangeira, e dos esforços domésticos de pesquisa e desenvolvimento (P&D) limitados por evasão de capital humano (MARTINS; GONZALO; SZAPIRO, 2018).

Além disso, com relação especificamente ao setor militar, entende-se que alguns Estados possuem maior e consequente organização do que outros, o que influencia em seu poder quando na criação - ou na ausência - de políticas estratégicas de segurança e defesa nacional que integrem a dimensão cibernética. Essa "nova era" de políticas, segundo Ventre (2012b), pode ser traduzida quando da publicação de Livros Brancos, de estratégias nacionais de segurança cibernética, de doutrinas militares, pela reorganização dos atores de segurança cibernética e pela criação de unidades de defesa cibernética, tanto civis quanto militares (a exemplo das agências de segurança cibernética, dos comandos cibernéticos, etc).

Em conclusão, compreende-se que todos os Estados conectados ao espaço cibernético direcionam-se, ao menos em parte, a questões, apostas, problemas, desafios e dificuldades similares. Contudo, nem todos eles podem perseguir as ambições de maneira equivalente a Estados que detêm maior poderio, como é o caso de EUA e China, os quais desenvolvem fortemente suas capacidades nacionais estatais defensivas e ofensivas (VENTRE, 2012b).

---

[27] Souza (2013, p. 29-30) explicita que a expressão *cyber warfare* inclui "a utilização de armas e ataques cibernéticos e a própria guerra cibernética (*cyber war*)". Desta forma, *o cyber warfare* abrange ambas ações governamentais e não governamentais no espaço cibernético, para as quais se utilizam técnicas do tipo *hacker* (SOUZA, 2013).

2.4 CONCLUSÕES PRELIMINARES

Desse modo, buscou-se, neste primeiro capítulo, apresentar como a criação da internet, fruto da 3ª Revolução Industrial, figurou como um objeto de mudanças sociais importantes, e como a sua expansão consequentemente possibilitou a formação de um novo espaço geográfico, denominado espaço cibernético.

Arquitetada com o pensamento mais focado na descentralização que em sua segurança, a internet perpetuou, para este espaço, vulnerabilidades que passaram a ser exploradas por seus utilizadores, incluindo governos, corporações e indivíduos. O proveito de tais vulnerabilidades para fins maléficos, por sua vez, originaram as chamadas ameaças ou conflitos cibernéticos, que, conforme ascendiam, foram consideradas com preocupação, bifurcando o recente debate: a temática foi elevada de especialistas técnicos para políticos e tomadores de decisão estadunidenses, que a securitizaram; e, finalmente, exportada para outros países.

Além do movimento cada vez maior de securitização ao entorno do espaço cibernético, prosperou, sobretudo no presente século, a tratativa do assunto de forma estratégico-militar, dada a preocupação com ameaças que pudessem causar incidentes envolvendo infraestruturas críticas estatais. Entendendo o relacionamento criado no espaço cibernético pelos atores como uma tentativa de exercer o poder uns sobre os outros, concluiu-se que estes, incluindo os Estados, buscam como recurso ativo a sua própria capacitação, para que possam fornecer respostas apropriadas caso confrontados.

Como este trabalho intenciona compreender, em conclusão, como a formação de capacidades nacionais impactariam as competências brasileiras na produção de recursos de defesa cibernética - ou seja, de recursos estratégico-militares -, serão analisados no próximo capítulo dois países que figuram como modelos internacionais neste sentido, que são os Estados Unidos e a China.

3 MODELOS INTERNACIONAIS EM MATÉRIA DE DEFESA CIBERNÉTICA: OS CASOS DE ESTADOS UNIDOS E CHINA

Os Estados Unidos e a China ocupam, respectivamente, a 3ª e a 4ª posições dos países com maior extensão territorial do globo[28] (STATISTA, 2019). A nível populacional, estes também não ficam atrás: a China é o país mais populoso do mundo, tendo contabilizado 1,39 bilhões de habitantes em 2019. Os Estados Unidos, por sua vez, possuía, no mesmo ano de análise, uma população de 328 milhões de habitantes (THE WORLD BANK, 2020), ocupando a terceira posição do ranking mundial.

Em termos econômicos, os dois também vêm se consagrando como atores de grande relevância nos últimos anos. De acordo com dados do Banco Mundial, seus índices de Produto Interno Bruto[29] (PIB) de 2018, calculados em dólares americanos (US$), os colocavam nas duas primeiras posições mundiais. Destaca-se aqui o papel do dólar americano no sistema monetário mundial, o qual perdura atualmente como moeda de referência internacional, em razão de seu uso em reservas internacionais e pelo volume do comércio dos EUA (KISTLER, 2009).

A moeda chinesa - conhecida como yuan ou renminbi (RMB ou ¥) -, a seu modo, ainda persegue a sua internacionalização. São argumentos a favor as reformas econômicas internas do país e a escala da economia chinesa (MARTINS, 2018). Um passo importante nessa direção se materializou em 2016, através de sua inclusão na cesta de moedas que determinam o valor final dos Direitos Especiais de Saque (DES), a "moeda" do Fundo Monetário Internacional (FMI) (MARTINS, 2018). Essa inclusão representa, de certo modo, a busca chinesa pela reforma dos sistemas financeiro e monetário internacionais, já que o avanço do RMB nos mercados globais vai ao encontro da ambição desse Estado de desafiar a própria hegemonia do dólar e a ordem econômica global, até então dominada pelos EUA (LUNKES, 2016).

Além disso, em termos de política externa, tanto China quanto Estados Unidos integram o seleto grupo dos membros permanentes do Conselho de Segurança da Organização das Nações Unidas (CS/ONU), e desempenham papéis fundamentais na Organização Mundial

[28] De acordo com o Statista (2019), o território chinês detém a extensão de 9.596.960 km², enquanto o território estadunidense possui, em extensão, 9.833.517 km².

[29] Segundo tais dados, os Estados Unidos apresentava, em 2018, um PIB de US$20,5 trilhões, enquanto a China apresentava um PIB de US$13,6 trilhões (THE WORLD BANK, 2018).

do Comércio (OMC)[30]. Depreende-se, deste modo, que suas características territoriais, econômicas e políticas, entre outros fatores de destaque, os tornam países centrais no Sistema Internacional. Para manter sua estabilidade e posição neste cenário, portanto, os dois atores atentam-se a medidas de caráter geopolítico e militar, investindo, assim consequentemente, em políticas de defesa da nação.

Desta forma, é igualmente importante abordar como se dão, na contemporaneidade, os investimentos em defesa. Segundo o Instituto Internacional de Pesquisa para a Paz de Estocolmo (SIPRI) (2019 apud GAZETA DO POVO, 2019), quando em comparação com o percentual do PIB global de 2018, este tipo de investimento diminuiu ao redor do mundo, estimando, no mesmo ano, 2,1% do PIB. Apesar disso, as despesas globais perante este mesmo setor aumentaram em 2018, chegando a US$1,82 trilhões (SIPRI, 2019 apud GAZETA DO POVO, 2019). Analisando, isto posto, o ranking de investimentos no campo militar, constatou-se que, neste mesmo ano, estes foram liderados pelos Estados Unidos, seguidos proximamente pela China[31].

Com relação ao setor cibernético - o qual nos atentaremos especificamente aqui -, diversos autores apontam para a mesma recíproca. Da Cruz Jr (2013, p. 13) afirma que, atualmente, "os Estados Unidos e a China são os principais atores mundiais no ambiente cibernético". De acordo com o autor, os dois atores são analisados pela imprensa especializada como sendo responsáveis por ataques a diversos países, e também entre si (DA CRUZ JR., 2013).

No que concerne esta última afirmação, Cavelty (2012b) explora que um dos desenvolvimentos que acelerou a militarização do espaço cibernético foi o aumento de acusações sobre a China, colocando-a como responsável pela espionagem cibernética em sistemas de computadores de empresas e governos na Europa, na América do Norte, e na própria Ásia. A partir do entendimento de que as autoridades chinesas consideram o espaço cibernético um domínio estratégico, e que estes esperam aproximar-se dos EUA na questão militar, muitos oficiais estadunidenses se prontificam em acusar o governo chinês de

[30] Um estudo da Fundação alemã Bertelsmann (2019 apud CORREIO BRAZILIENSE, 2019) calculou que a participação na OMC aumentou o PIB de cada país, especialmente com relação à redução das tarifas que favorecem o comércio. Os Estados Unidos acumularam um diferencial positivo de US$87 bilhões, nos 25 anos de participação na organização. A China acumulou US$86 bilhões, desde que aderiu à OMC, em 2001 (FUNDAÇÃO BERTELSMANN, 2019 apud CORREIO BRAZILIENSE, 2019).

[31] Segundo dados do SIPRI (2019 apud GAZETA DO POVO, 2019), os Estados Unidos desembolsaram US$649 bilhões de gastos com defesa em 2018, enquanto a China gastou US$250 bilhões. Isso representou, respectivamente, 3,2% e 1,9% de gastos em parcela do PIB de 2018 (SIPRI, 2019 apud GAZETA DO POVO, 2019).

perpetuar ataques ou de coletar informações (CAVELTY, 2012b). Estas alegações, contudo, são difíceis de se comprovar, em virtude do problema de atribuição (CAVELTY, 2012b).

Em conclusão, como já citado em momento anterior, Ventre (2012b) argumenta que nem todos os países conectados ao espaço cibernético podem perseguir as mesmas ambições apresentadas por estes dois Estados, os quais podem acessar ao desenvolvimento tanto de capacidades defensivas quanto ofensivas relevantes. Em razão desse destaque dado, como intenção final deste capítulo, serão analisadas nas próximas três seções as capacidades de defesa cibernética apresentadas pelos dois países, entendendo suas forças e fraquezas, e comparando-os entre si. Começar-se-á pelos Estados Unidos, por este ter sido pioneiro nas questões relativas à internet e à segurança do ciberespaço.

3.1 ESTADOS UNIDOS

3.1.1 Inserção da Internet e securitização da pauta cibernética

Gagnon (2008) apresenta uma linha temporal, visando traçar a influência da internet – e, portanto, do espaço cibernético – na política da segurança estadunidense. Este autor a divide em três etapas: a infância, com o desenvolvimento militar-acadêmico da ARPANET; a adolescência, com a chegada dos provedores de serviços comerciais da internet; e a idade adulta, quando o espaço cibernético se torna um ambiente estratégico (GAGNON, 2008).

Como trabalhado no capítulo anterior, os Estados Unidos foram o país responsável pelo projeto do que futuramente se tornaria a internet, a ARPANET. Inicialmente um projeto que tinha como missão a mobilização de recursos de pesquisa para atingir a superioridade tecnológica no contexto da Guerra Fria, a ARPANET se descaracterizou ao longo dos anos, até que teve sua privatização encaminhada, em razão das tecnologias de computadores terem chegado ao domínio público e as telecomunicações passarem por uma desregulamentação (CASTELLS, 2003).

Elementos como a inserção de protocolos TCP/IP em computadores fabricados para fins comerciais, além da criação do Protocolo de Transferência de Hipertexto (HTTP), da Linguagem de Marcação de Hipertexto (HTML) - estes dois últimos responsáveis por dar "vida à rede mundial de computadores ou simplesmente WWW" (SOUZA, 2013, p. 36) -, e dos provedores de serviços da internet foram cruciais para que sua comercialização em larga escala e expansão fossem possíveis (SOUZA, 2013). A ampliação significativa da internet

entre os anos 1990 e 2000 também foi consequência da diminuição do preço dos computadores e do preço do acesso à internet (SOUZA, 2013).

Tal expansão, por sua vez, perpetuou as vulnerabilidades no novo espaço geográfico, o espaço cibernético, em razão de sua projeção mais descentralizada que segura (CLARKE; KNAKE, 2010), originando as ameaças cibernéticas. Esta, combinada com o aumento da atenção midiática, criou uma sensação crescente de ciber insegurança no país. Deste modo, a temática foi elevada do nível dos especialistas técnicos para o meio político, sendo politizada, e, posteriormente, securitizada (CAVELTY, 2012b). Como a segurança nacional sempre presume a existência da defesa, a discussão passou a englobar a problemática estratégico-militar referente ao espaço cibernético (CAVELTY, 2012b), ganhando proeminência maior especialmente neste século. Este debate em específico, com foco nas ações estadunidenses promovidas, será discutido na próxima subseção.

Antes disso, contudo, é importante compreender que o domínio dos Estados Unidos sobre a gestão da internet e sobre este espaço predomina até a contemporaneidade. Este argumento é reforçado por Souza (2013), que relata que o caso norte-americano é particular, pois aparece em quase todas as análises envolvendo a defesa cibernética, e por Gagnon (2008), que afirma que este país exerce, atualmente, "ciber-hegemonia sobre a internet" (GAGNON, 2008, p. 63)[3233]. Entre outros elementos, pode-se exemplificar este domínio através da apresentação de dados referentes aos cabos submarinos mundiais[34] e à difusão da internet entre sua população interna.

Do primeiro, visto na figura 1, interpreta-se que os Estados Unidos possui cabos submarinos que o ligam diretamente a todos os continentes do globo, incluindo ao próprio continente americano, à Europa, à Ásia, à África e à Oceania (TELEGEOGRAPHY, 2020d). Somado a isso, ainda, têm-se a informação de que a Subcom, empresa multinacional estadunidense, compõe a tríade de fornecedores de cabos submarinos que são responsáveis por quase 90% das novas construções desde 2015 (TELEGEOGRAPHY, 2019).

Com relação ao último, de acordo com o Internet World Stats, até o ano de 2019, a internet chegava à 89,8% da população estadunidense, totalizando 313.322.868 de usuários

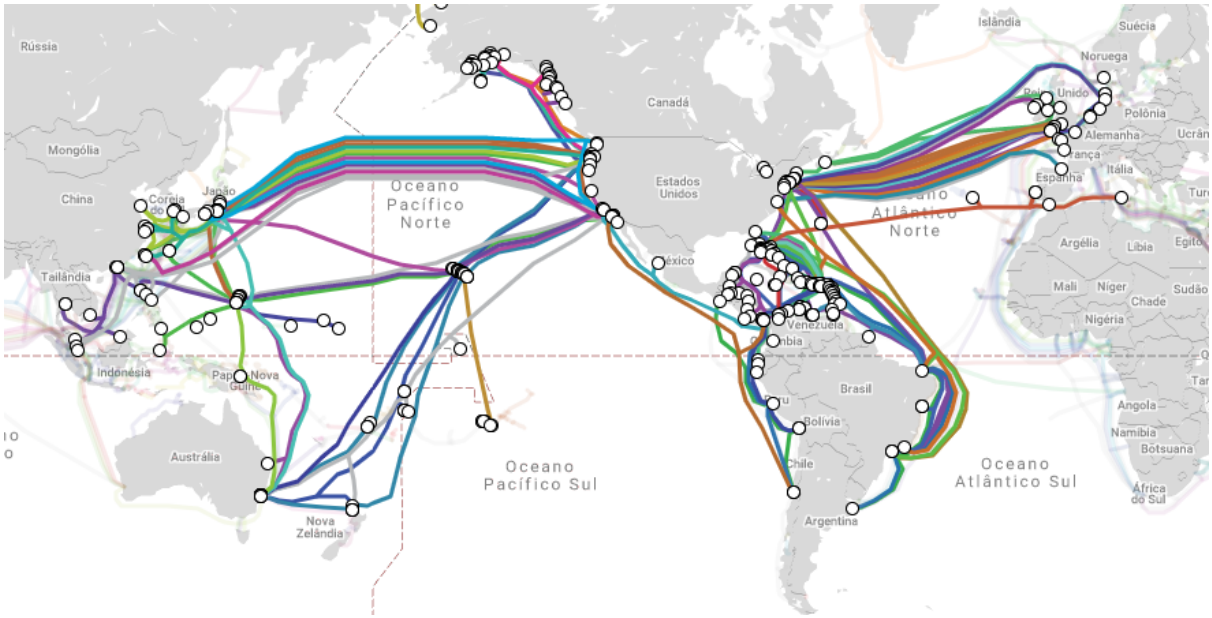
[32] [tradução nossa]. No original, lê-se: "The USA currently exercises "cyberhegemony" over the web [...]".

[33] Na conclusão de seu artigo, Gagnon (2008) também afirma que, apesar de os Estados Unidos exercerem, ainda neste momento, a ciber-hegemonia sobre a internet, a China está se aproximando cada vez mais deste.

[34] A malha de cabos submarinos possibilitou a existência da internet, e também a sua expansão, pois estes passaram a ser utilizados para a transmissão de dados (REINO, 2010). Ainda, como "mais de 90% do tráfego da internet passa por fibras óticas em cabos submarinos" (ZUCCARO, 2011, p. 58), este dado deve ser considerado.

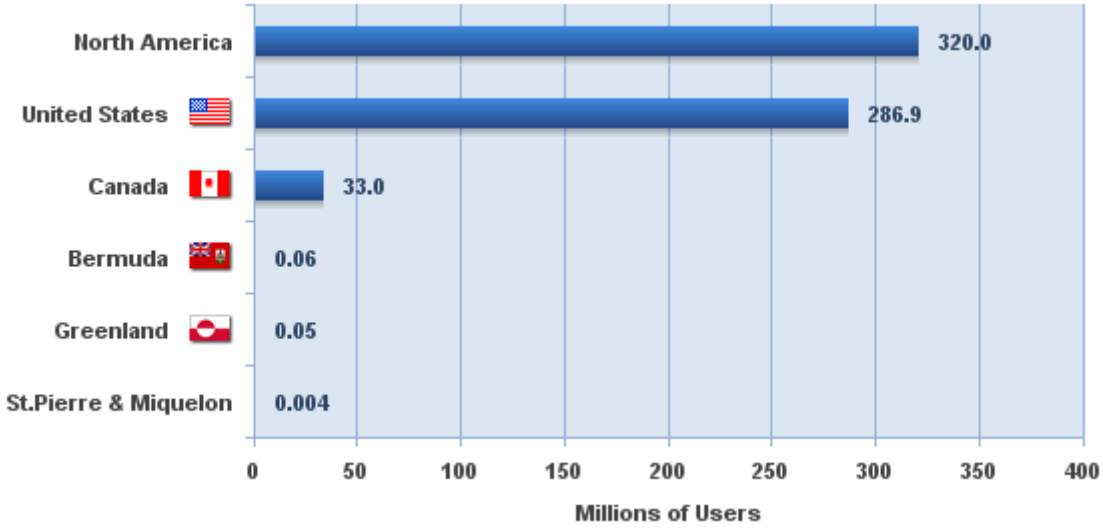
(INTERNET WORLD STATS, 2019b). Além do mais, os Estados Unidos ainda é o principal responsável pela disseminação da internet na América do Norte (INTERNET WORLD STATS, 2017), como demonstra a figura 2.

Figura 1 - Mapa dos cabos submarinos que conectam o território dos EUA a outros países do globo



Fonte: Telegeography (2020d)

Figura 2 - Usuários de Internet na América do Norte (em milhões)



Fonte: Internet World Stats (2017)

A figura 2 evidencia que, em 2017, do total de 320 milhões usuários norte-americanos da internet, aproximadamente 287 milhões eram estadunidenses, o equivalente a 89,6%. Na segunda posição, o Canadá detinha apenas 10,3%, quase o total completo de usuários restantes (INTERNET WORLD STATS, 2017). Somando esta informação às demais apresentadas anteriormente, confirma-se, por conseguinte, a ciber-hegemonia dos EUA sobre a internet e sobre o espaço cibernético, a qual fora proposta nas palavras de Souza (2013) e de Gagnon (2008). Além disso, como veremos a seguir, o espaço cibernético também configura, para os Estados Unidos e, especificamente, para o seu setor militar, mais um ambiente onde o poder pode ser projetado, um "novo espaço estratégico", considerado quase tão importante quanto suas contrapartes tradicionais, a dizer, a terra, o mar, o espaço aéreo e o espaço extra-atmosférico (GAGNON, 2008).

3.1.2 Esforços promovidos frente à defesa cibernética

Em matéria de defesa, é importante notar que a ligação entre infraestruturas de informação e segurança nacional já estava firmemente estabelecida nos escritos militares dos Estados Unidos depois da Segunda Guerra Mundial. Isso implica dizer que a conexão entre esses dois tópicos se tornou aceita nos pensamentos militares, e por isso, enfrentou pouca resistência quando foi institucionalizada, nos anos 1990, como uma das principais questões do pensamento estratégico estadunidense (CAVELTY, 2008).

Até 1980, as ameaças cibernéticas eram percebidas diferentemente do que aconteceria nos anos 1990: a tecnologia de informação (T.I.) era apenas vista como alvo, e não como arma (CAVELTY, 2008). Haizler (2017) chama essa primeira fase dos conflitos cibernéticos estadunidenses de "realização", pois nela, apenas os Estados Unidos e outros poucos países detinham capacidades cibernéticas. Foi também nesta fase que se deram ataques como o vírus Morris (1988), os quais serviram como sinais de aviso para as vulnerabilidades institucionais e para a falta de segurança (HAIZLER, 2017).

Neste sentido, as primeiras estruturas tangentes às ameaças cibernéticas e o começo desse debate estão ligados à presidência de Ronald Reagan (CAVELTY, 2008). O primeiro Centro de Estudos para Resposta e Tratamento de Incidentes em Computadores[35] (CERT), estabelecido pela DARPA após este incidente, por exemplo, "demonstrou a mudança de soluções *ad hoc* para equipes profissionais, os quais eram treinados e equipados para

[35] Em inglês, este conceito é conhecido como *Computer Emergency Response Team* (CERT).

coordenar eventos e prover avaliações e soluções para um dado ciberataque" (HAIZLER, 2017, p. 33)[36].

Todavia, foi apenas a partir dos anos 1990 que os militares se tornaram a força responsável pela percepção de ameaças. Como resultado, o tema central do debate tornou-se versado às vulnerabilidades assimétricas, em razão de os EUA, no pós-Guerra Fria, ter se tornado o único superpoder restante (CAVELTY, 2008), ou seja,

> [...] as vantagens oferecidas pelo uso e pela disseminação das tecnologias de informação e comunicação (TICs) envolveriam uma vulnerabilidade desproporcional, a qual levou especialistas a temer que os inimigos que levavam a probabilidade de falhar num conflito convencional com a máquina de guerra dos Estados Unidos, poderiam, ao invés disso, planejar deixar os EUA de joelhos, através do ataque a pontos vitais de seu território (BERKOWITZ, 1997 apud CAVELTY, 2008, p. 66)[37].

Tais pontos vitais seriam essenciais em matéria de segurança nacional e para o funcionamento preciso de sociedades industrializadas como um todo, não apenas para os militares. As contramedidas desenhadas sofreram, então, com esse impacto: para este Estado e para suas Forças Armadas, isso significava se preparar para se opor a uma "nova" ameaça (CAVELTY, 2008).

O primeiro teste combinando conceitos ligados à T.I. para propósitos ofensivos, por sua vez, veio na Guerra do Golfo, sob a gestão de George H. W. Bush (CAVELTY, 2008). Como consequência deste conflito, ascendeu o conceito de "Revolução nos Assuntos Militares", pois havia o desejo de integrar elementos como inteligência avançada, vigilância, e sistemas de reconhecimento, a sistemas armados de precisão que pudessem ser dominantes em futuros campos de batalha (O'HANLON, 2000 apud CAVELTY, 2008). Da mesma maneira, os pensadores dessa revolução intencionavam o desenvolvimento de um conceito conhecido como guerra de informação[38], no qual a habilidade de degradar ou paralisar os sistemas de comando, controle, comunicação e inteligência (C3I) de um oponente seria vantajosa (O'HANLON, 2000 apud CAVELTY, 2008).

---

[36] [tradução nossa]. No original, lê-se: "[...] the Computer Emergency Response Team (CERT) demonstrated the shift from *ad hoc* solutions to professional teams, which were trained and equipped to coordinate events and provide assessments and solutions to a given cyberattack".

[37] [tradução nossa]. No original, lê-se "[...] the advantages offered by the use and dissemination of information and communication technologies (ICT) were seen to entail a disproportional vulnerability, which led experts to fear that those enemies who were likely to fail in conventional conflict with the US war machine might instead plan to bring the United States to its knees by striking against vital points on its territory".

[38] Em inglês, este conceito é conhecido como *information warfare* (IW).

A contrapartida aos desenvolvimentos tecnológicos do pós-Guerra do Golfo manifestaram-se através da publicação de novos documentos de doutrina que incluíam o componente de informação (CAVELTY, 2008). O maior objetivo das Forças Armadas tornou-se, então, a superioridade de informação, ou,

> [...] a superioridade na geração, manipulação, e no uso de informação suficiente para assegurar a dominância militar do lado que a possui, o que requere sucesso em operações de guerra de informação tanto ofensivas quanto defensivas (LIBICKI, 1997 apud CAVELTY, 2008, p. 70)[39].

Apesar disso, não foi durante as gestões do antecessor Ronald Reagan e nem de George H. W. Bush que as ameaças cibernéticas foram respaldadas dentro da agenda de segurança nacional como uma ameaça de grande porte, mas sim a partir da administração Clinton. O Governo Clinton, demonstrando consideráveis mudanças com relação aos dois governos anteriores, deu menor ênfase à ameaça de inteligência estrangeira - apesar de ainda considerá-la -, e maior destaque aos Estados que utilizavam meios de guerra de informação e aos atores subestatais que utilizavam infraestruturas de informação para atacar. Expandiu-se, ainda, o vocabulário referente à utilização do espaço cibernético, incorporando termos como "guerra cibernética", "terrorismo cibernético" ou "Pearl Harbor eletrônico", os quais eram frequentemente utilizados em artigos de imprensa e entrevistas (CAVELTY, 2008).

A segunda fase estabelecida por Haizler (2017) começa a partir desta gestão, e é chamada de "decolagem". Aqui, já possuíam capacidades cibernéticas os EUA, a Rússia, e outros pequenos atores, e o destaque entre incidentes é dado para o Moonlight Maze (1998), considerado o primeiro ataque de espionagem cibernética em larga escala realizado por um ator bem organizado, ressaltando o papel do Estado em gerar e patrocinar incidentes de espionagem (HAIZLER, 2017). Neste mesmo ano, os militares americanos também desenvolveram uma Doutrina Conjunta para Operações de Informação, dando ênfase para os aspectos de planejamento estratégico, operacional e tático das operações de informação (OI)[40], demonstrando que o conceito utilizado nas doutrinas passou a ser o de OI (CAVELTY, 2008).

Os ataques terroristas de 11 de setembro de 2001, ocorridos na Gestão de George W. Bush, por sua vez, atestaram que estes atores podiam causar muito estrago ao atacar

---

[39] [tradução nossa]. No original, lê-se: "[...] superiority in the generation, manipulation, and use of information sufficient to assure military dominance for the side that possesses it, which requires success in both offensive and defensive IW operations".

[40] Em inglês, este conceito é conhecido como *Information operations* (IO).

infraestruturas críticas diretamente e fisicamente. Neste sentido, visando resolver os problemas de ameaças cibernéticas, foi criado o Departamento de Segurança Interna estadunidense[41] (CAVELTY, 2008). Em paralelo, também pode ser observado na mesma Gestão importante progresso no domínio militar, ligado especialmente ao desenvolvimento de capacidades de guerra de informação: Bush iniciou uma série de medidas com o objetivo de acelerar a transformação de capacidades, para torná-las mais adaptadas ao ambiente securitário (KREPINEVICH, 2001 apud CAVELTY, 2008). Isso implicou na apresentação da tecnologia como um possibilitador, ao invés de como fonte de vulnerabilidades (CAVELTY, 2008). A tecnologia militar e o sistema de armas se tornaram, então, o "hardware de qualquer operação" (CAVELTY, 2008, p. 109)[42].

Finalmente, a Estratégia Nacional para Proteger o Ciberespaço[43], publicada em 2003, apresenta a possibilidade do uso da força pelos Estados Unidos em resposta a ataques cibernéticos (THE WHITE HOUSE, 2003). Este documento tem ainda como propósito incentivar a coordenação entre atores estatais - governo federal, estaduais e locais -, o setor privado e o povo americano, para que estes atuem conjuntamente quando na proteção do espaço cibernético (THE WHITE HOUSE, 2003).

Isso significa que o Governo estadunidense atribui grande importância às parcerias de caráter público-privado com empresas, centro de pesquisas e universidades, entendendo que são através delas que são resolvidos problemas de coordenação, aumentadas a consciência e o treinamento, melhorada a tecnologia, etc (RODRIGUES PADILHA, 2016). A tentativa de securitização do espaço cibernético pelos EUA, por meio de uma visão estado-centrista da internet e de suas ameaças, também é relevantemente expressa no documento, pois este cita mais de 40 vezes o termo "espaço cibernético nacional"[44] (GAGNON, 2008).

Ademais, é a partir deste mesmo ano que Haizler (2017) estabelece sua última fase referente aos conflitos cibernéticos do país norte-americano, a qual intitula de "militarização". Para o autor, neste momento, já possuem capacidades cibernéticas Estados Unidos, Rússia, e outros atores importantes, tais quais a China. Entre os ataques cibernéticos destacados, estão o

[41] Em inglês, esta instituição é conhecida como *Department of Homeland Security* (DHS).
[42] [tradução nossa]. No original, lê-se: "Military technology and weapon systems, the hardware of any operation, became the new focal point."
[43] Em inglês, o nome do documento referente é *National Cyberspace Strategy*.
[44] Em inglês, este termo é expresso como "national cyberspace" (GAGNON, 2008, p. 51).

da Geórgia[45] e Estônia[46], mas principalmente, o Stuxnet - já tratado anteriormente -, no qual alega-se a participação do governo estadunidense. O conceito utilizado em doutrinas, a partir deste momento, a seu modo, é o de guerra cibernética[47] (HAIZLER, 2017).

Antes de passar aos feitos militares das últimas duas gestões, contudo, faz-se necessário entender sobre qual estrutura assenta-se a questão cibernética nos Estados Unidos, a qual se começou a dar maior atenção a partir da Gestão Reagan. O principal órgão responsável pela política nacional de segurança da informação é a Agência de Segurança Nacional[48], a qual se atribui as funções de todas as questões de segurança cibernética do governo norte-americano. Há sessenta anos, esta é a agência governamental responsável pela segurança das comunicações e tecnologias da informação dos órgãos federais do governo. Além disso, esta dá apoio ao Departamento de Defesa[49] - a quem se submete -, à Comunidade de Inteligência[50], a outras agências governamentais e aos parceiros industriais com produtos e serviços associados ao espaço cibernético (DA CRUZ JR., 2013).

A Comunidade de Inteligência, no que lhe concerne, é composta por dezessete agências e escritórios, os quais atuam conjunta e individualmente, conduzindo as principais atividades de inteligência para que a segurança nacional seja garantida (DA CRUZ JR., 2013). Haizler (2017) argumenta que a IC possui capacidades ofensivas e defensivas, e é a responsável última quando na resposta e no monitoramento da moderna guerra cibernética. Suas organizações-membro incluem agências de inteligência, inteligência militar, inteligência civil, e escritórios de análise que se inserem nos departamentos executivos federais. Juntas, estas totalizam 85% dos gastos totais dos fundos de inteligência estadunidenses (HAIZLER, 2017).

Em junho de 2009, já na Gestão Barack Obama, foi criado o Comando Cibernético dos Estados Unidos[51], responsável por coordenar ações de prevenção e de defesa cibernética

---

[45] Souza (2013) argumenta que o ataque cibernético ocorrido na Geórgia, em 2008, tem relação com o conflito internacional envolvendo este país e a Rússia, no que tange ao combate bélico pela independência da Ossétia do Sul. Caracterizado como um ataque de negação de serviço, os danos causados em termos de infraestruturas críticas foi crucial para que o governo e os militares daquele país não pudessem organizar-se adequadamente, ou seja, o conflito cibernético acabou por potencializar o tradicional (SOUZA, 2013).

[46] Soesanto (2019) argumenta que o ataque de negação de serviço contra a Estônia, em 2007, ocorreu em razão de um monumento da era soviética ter sido movido do centro de Talín, capital do país, para os arredores da cidade. Suspeitava-se que a origem dos ataques tivesse tido início na Rússia (SOESANTO, 2019).

[47] Em inglês, este conceito é conhecido como *Cyber Warfare* (CW).

[48] Em inglês, esta instituição é conhecida como *National Security Agency* (NSA).

[49] Em inglês, esta instituição é conhecida como *Department of Defense* (DoD).

[50] Em inglês, esta instituição é conhecida como *Intelligence Community* (IC).

[51] Em inglês, esta instituição é conhecida como *U.S. Cyber Command* (U.S. CyberCom).

norte-americanas. Como subunidade das Forças Armadas - e anteriormente subordinado ao Comando Estratégico Norte-Americano[52], do Departamento de Defesa -, este possui acesso e coopera tanto com as forças militares quanto com outros órgãos da IC (DA CRUZ JR., 2013). O ponto importante com relação à estrutura deste órgão é que seu comandante também exerce a função de diretor da NSA e chefe do Serviço Central de Segurança[53], do que Da Cruz Jr. (2013) interpreta que, apesar de o espaço cibernético deste país possuir várias frentes de cooperação, apenas uma pessoa figura atualmente como a responsável pela segurança e pela defesa estatais.

Já reconhecendo, no ano de 2010, o espaço cibernético formalmente como novo domínio da guerra (RODRIGUES PADILHA, 2016), o Governo Obama publicou, no ano seguinte, documentos tais quais a Estratégia para operar no espaço cibernético[54] e a Estratégia Internacional para o espaço cibernético[55]. Souza (2013) releva o primeiro em detrimento do segundo, pois este considera o segundo como sendo uma estratégia internacional - não nacional - e, portanto, como um documento de política externa. É relevante falar ainda que esta Estratégia Internacional, tendo sido lançada posteriormente ao Stuxnet, começou a otimizar a narrativa estadunidense (SOESANTO, 2019), o que Zetter (2014) aponta como uma ironia, pois, ao mesmo tempo que Obama autorizava tal ataque contra os sistemas de computador iranianos, este também estava anunciando novas medidas federais que pudessem assegurar o espaço cibernético e as infraestruturas críticas dos Estados Unidos.

A primeira referenciada, intitulada de Estratégia para operar no espaço cibernético, aponta, entre cinco iniciativas estratégicas, que o DoD deve tratar este espaço como um domínio operacional, de modo que este departamento tenha acesso total ao potencial cibernético, além de fazer parceria com outros departamentos governamentais, agências nacionais estadunidenses e com o setor privado, para que a estratégia envolva todo o governo. Finalmente, o Departamento de Defesa estadunidense também deve alavancar a engenhosidade da nação, através de uma força de trabalho excepcional no domínio cibernético e de rápida inovação tecnológica (DOD, 2011).

Por outro lado, a Estratégia Internacional para o espaço cibernético reforça a importância das parcerias, da abertura comercial, do respeito à propriedade e da promoção de

[52] Em inglês, esta instituição é conhecida como *U.S. Strategic Command* (U.S. StratCom).
[53] Em inglês, esta instituição é conhecida como *Central Security Service* (CSS).
[54] Em inglês, o nome do documento referente é *Strategy for Operating in Cyberspace* (EUA-SOC).
[55] Em inglês, o nome do documento referente é *International Strategy for Cyberspace* (EUA-ISC).

direitos universais, admitindo, todavia, o direito de defesa que não tome necessariamente as vias diplomáticas. Em suma, duas coisas são muito relevantes neste segundo documento: entende-se que, caso necessário, serão realizadas medidas coercitivas contra o setor privado, de modo a garantir a proteção das redes internas dos EUA, além de o texto deixar claro que tanto a segurança quanto a defesa cibernética estão mais relacionadas com a capacitação de pessoal, ou seja, à capacidade intelectual, do que com relação a produtos e equipamentos (DA CRUZ JR., 2013).

Após 2013, Haizler (2017) enfim aponta que a estratégia intitulada de guerra cibernética mudou sua abordagem de contra-ataque, partindo de uma abordagem operacional para uma estratégico-diplomática. Nesta nova abordagem, leva-se em conta para o ambiente cibernético violado fatores como política, leis internacionais, governança da internet e acordos, ou seja, fatores regulatórios. Dois exemplos que figuram no nível internacional e multinacional, os quais podem ser destacados, são o Acordo Cibernético China-Estados Unidos[56] (2015), e a Cúpula Mundial sobre a Sociedade da Informação (WSIS+10, 2015)[57] (HAIZLER, 2017). Vale ressaltar, finalmente, que os Estados Unidos, desde 2001, já era signatário da Convenção de Budapeste sobre crimes cibernéticos, tendo ratificado esta mesma convenção no ano de 2006 (COUNCIL OF EUROPE, 2020).

No momento em que Donald Trump (2016-2020) assumiu a administração do país, este enfrentou forte pressão pública para que confrontasse a Federação Russa, no tangente à alegação de que a Rússia teria interferido nas recentes eleições presidenciais dos Estados Unidos. Em contrapartida, iniciaram-se discussões políticas em meios como o Departamento de Defesa, o Congresso, e a Casa Branca, os quais buscavam a obtenção de uma postura de dissuasão cibernética que fosse mais agressiva. Em 2017, essa linha de pensamento levou à concretização da elevação do Comando Cibernético dos Estados Unidos a um Comando de Combate Unificado[58], compondo este o 10º dos EUA (SOESANTO, 2019).

---

[56] Acordo básico que intenciona "garantir que nenhum dos governos conduza ou apoie roubos cibernéticos de propriedade intelectual, incluindo segredos de comércio e outras informações de negócios confidenciais para obter vantagens comerciais" (HAIZLER, 2017, p. 36, *tradução nossa*).

[57] "Renovou o Fórum de Governança da Internet (IGF), local onde Estados-membro, sociedade civil e o setor privado debatem política da internet, segurança cibernética, vigilância, propriedade intelectual e direitos autorais" (HAIZLER, 2017, p. 37, *tradução nossa*).

[58] "Comandos de Combate Unificados são unificados através dos diferentes departamentos de serviço militar - Exército, Marinha e Força Aérea -, mas são divididos tanto por região geográfica quanto por função. Cada um "tem uma missão particular, e cada um pode estar envolvido em várias operações e exercícios". Um estatuto do Congresso de longa data autoriza o presidente a criar novos Comandos de Combate Unificados e revisar os já existentes. Um destes Comandos existentes - O Comando Estratégico Norte-Americano - abrigou o Comando Cibernético como uma unidade subordinada desde a sua criação, em 2010. Em 2016, alinhado com os objetivos

Ademais, no ano de 2018, a Administração Trump lançou uma nova Estratégia Cibernética Nacional, o que apontou para um interesse no aumento da capacidade militar quando na realização de operações cibernéticas defensivas (GALBRAITH, 2019). Um dos quatro pilares que sustenta a Estratégia inclusive expõe que, a partir deste momento, o espaço cibernético não será mais tratado como uma categoria separada de política ou atividade descolada de outros elementos que compõem o poder nacional, mas sim integrado a todo elemento de poder nacional (GALBRAITH, 2019).

Em conclusão, Soesanto (2019) explora que a evolução da Estratégia de Defesa para o espaço cibernético dos Estados Unidos seguiu uma trajetória clara, com direito a incidentes, experimentações e histórias de sucesso entre um ponto e outro. Para além, Rodrigues Padilha (2016) conclui em sua obra que, em razão de os EUA ser uma potência mundial, é comum que os outros países sigam sua trajetória. Como a crescente securitização leva à militarização, este Estado vem construindo seu discurso nesse sentido, "criando regimentos dedicados aos conflitos cibernéticos" e obtendo "crescente investimento por parte do Departamento de Defesa" (RODRIGUES PADILHA, 2016, p. 52).

3.2 CHINA

3.2.1 Inserção da internet e securitização da pauta cibernética

O documento Livro Branco sobre a Internet na China[59], de 2010, discorre, em seu primeiro capítulo, como se deu a inserção da internet no país. Nele, é observado que pesquisadores e acadêmicos chineses, já a partir do meio dos anos 1980, começaram a explorar a utilização da internet com o apoio de colegas que habitavam em outros lados do oceano. Nas conferências do INET decorridas nos anos de 1992 e 1993, por conseguinte, especialistas de computador chineses começaram a demandar por acesso à internet para toda a população chinesa, fato que se concretizou no ano seguinte (SCIO, 2010).

Em abril de 1994, durante a articulação do Comitê de Ciência e Tecnologia Sino-Estadunidense, os representantes presentes chegaram a um lugar comum com a Academia Nacional de Ciências Estadunidense sobre a possibilidade de acesso à internet pelos chineses. Neste mesmo mês, uma rede piloto com propósitos de pesquisa científica e educação foi

---

da Administração Obama, o Congresso instruiu que o Comando Cibernético deveria tornar-se um Comando de Combate Unificado." (GALBRAITH, 2019, p. 635, *tradução nossa*).

[59] Em inglês, o nome do documento referente é *White paper on the Internet in China*.

ligada à internet, por meio do distrito Zhongguancun, em Pequim. Esse fato configura, portanto, o marco formal para o ingresso das redes na China (SCIO, 2010).

No começo, apenas 2.000 computadores chineses possuíam acesso à internet, configurando um processo inicial "devagar". Dois anos depois, em 1996, os primeiros cybercafés abriram em Xangai e em outras cidades maiores, fazendo com que mais pessoas pudessem acessar a internet, mesmo antes de essas adquirirem seus próprios computadores. Esses mesmos autores descrevem que logo a primeira geração de usuários das redes emergiu, quando companhias locais como a Sina, a Sohu e a Netease abriram (FLORCRUZ; SEU, 2014).

A conectividade, que havia começado com as linhas de telefone sendo ligadas diretamente aos modems, evoluiu ao longo dos anos, passando das linhas de telefone para os cabos de fibra óptica, e depois, para o *wireless*[60] (FLORCRUZ; SEU, 2014). Somado a isso, tem-se ainda a internet móvel, meio pelo qual a China atingiu as eras do 3G e do 4G, alcançando atualmente o patamar do 5G[61]. Nessa perspectiva, esses resultados podem ser contabilizados como parte do investimento chinês para a construção de sua infraestrutura de internet: de 1997 a 2009, por exemplo, foram investidos ¥4,3 trilhões, com a edificação de uma rede de comunicação óptica com extensão total de 8,267 milhões de km (SCIO, 2010).

Ademais, no fim de 2009, as companhias de telecomunicações básicas do país detinham sete cabos submarinos e vinte cabos terrestres, os quais combinavam uma capacidade que excedia 1,600 Gigabytes (Gb) (SCIO, 2010). Em análise à figura 3, percebe-se que a quantidade de países que se ligam diretamente à China via cabos submarinos é ainda maior atualmente[62], e que esta conexão se confirma com relação a outros países asiáticos, à

---

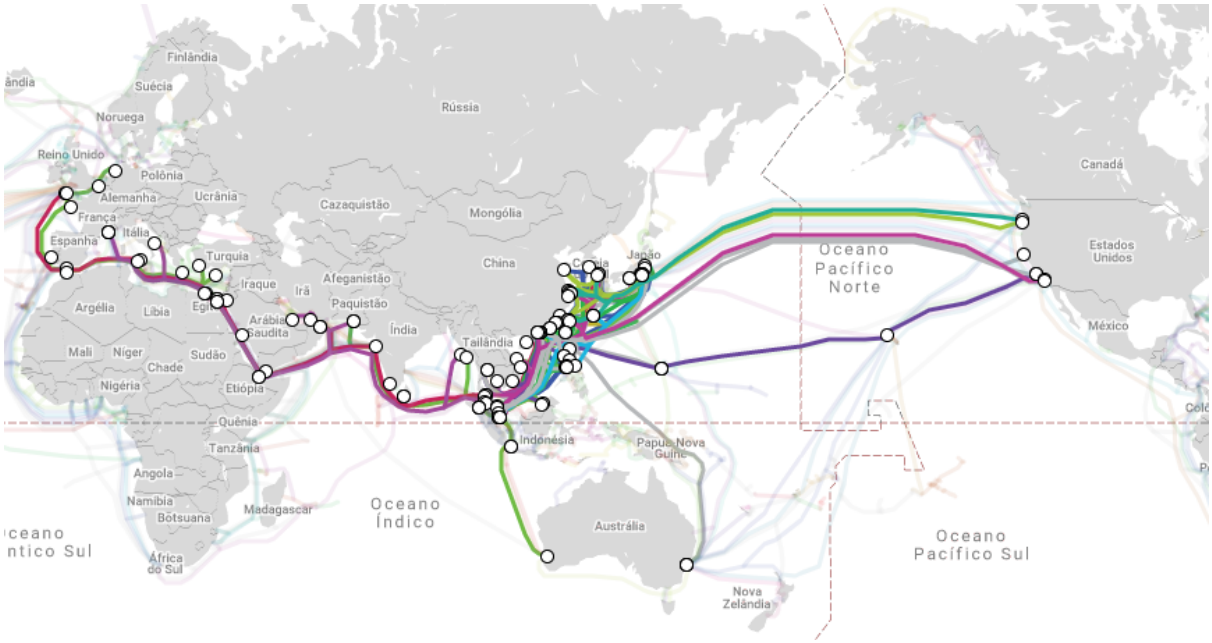
[60] A tecnologia *wireless*, em tradução livre, significa "sem fio". Esse tipo de tecnologia viabiliza que a conexão seja transmitida entre pontos distintos sem a necessidade da utilização de fios (FURTADO, 2011).

[61] O 5G compõe a quinta geração dos sistemas de telecomunicação sem fio (MAJEROWICZ, 2019). Segundo a autora, "O 5G promove a tendência de implementar semicondutores nos objetos, dos mais simples aos mais sofisticados, que passam a produzir sinais que serão comunicados, em larga medida, pela infraestrutura de telecomunicações sem fio. A chamada Internet das Coisas consiste na implementação de sensores e circuitos integrados (chips) nos objetos. Os sensores transformam os sinais analógicos em digitais, e os chips armazenam, processam e modulam/desmodulam sinais de radiofrequência que são comunicados por antenas e conectados pela infraestrutura de telecomunicações, permitindo sua utilização em rede e processamento/armazenagem na nuvem" (MAJEROWICZ, 2019, p. 17-18). A implementação do 5G é também campo de concorrência entre os Estados Unidos e a China, como será visto na próxima seção.

[62] Segundo Majerowicz (2019), a China tornou-se importante na construção de cabos de fibra ótica submarinos nos últimos anos, por meio da *joint-venture* Huawei Marine Networks, que foi criada entre a Huawei (51%) e a empresa britânica Global Marine (49%). A sua expansão inicial se deu principalmente através da consecução de projetos de ligações curtas, como é o caso de projetos no Sudeste Asiático e no Leste Russo. Em 2018, a empresa completou o primeiro grande projeto, ligando o Brasil à Camarões (MAJEROWICZ, 2019).

Oceania - via Austrália -, à Europa, e ao próprio Estados Unidos (TELEGEOGRAPHY, 2020c).

Figura 3 - Mapa dos cabos submarinos que conectam o território da China a outros países do globo



Fonte: Telegeography (2020c)

Da mesma forma, com a intenção de analisar como a China se impõe como um Estado dominante sobre a gestão da internet, busca-se interpretar dados referentes à difusão deste elemento entre a sua população. Até 2009, o número de usuários da internet no país era de 384 milhões, já 618 vezes maior que o número total de 1997. Neste mesmo ano, dizia-se que a internet havia alcançado 28,9% da população total (SCIO, 2010), apesar de esta ter se desenvolvido desigualmente entre as regiões[63]. Em comparação com estes números, em dezembro de 2019, este mesmo país detinha 904 milhões de usuários, o equivalente à 62,8% de penetração das redes (INTERNET WORLD STATS, 2019a).

É correto concluir, portanto, que a implementação da internet impactou na promoção do desenvolvimento econômico e social do país, transformando elementos como a indústria

[63] Até 2009, a internet havia atingido 40% da população do leste da China, mas apenas 21,5% da região oeste. Além disso, usuários das regiões urbanas compunham 72,2% do número total, enquanto apenas 27,8% era composto pelas regiões rurais (SCIO, 2010). Para mais, Dai (2003) também coloca que a localização dos sites da internet, neste país, sugerem que a maior parte está concentrada em áreas economicamente mais prósperas: Pequim, Xangai e Guangdong representam 48% do total de sites que estão registrados sob o domínio "cn".

até então tradicional chinesa, principalmente no que tange à T.I., mas também a indústria cultural - de *games*, animações, música, vídeos -, entre outras (SCIO, 2010). Além disso, o rápido crescimento entre sua vasta população ao longo dos anos é também apontado como o impulso para o começo das políticas domésticas com relação à internet (ZENG; STEVENS; CHEN, 2017). Alegando "regular o uso da internet pela lei"[64] (SCIO, 2010, p. 6)[65], o país vêm, desde 1994, estabelecendo uma série de regulações concernentes à administração da internet, incluindo regulações sobre as telecomunicações, sobre o direito de disseminação on-line de informações, e sobre a proteção dos sistemas de segurança da informação dos computadores, além de outras leis, as quais não são específicas à internet em si, mas que se aplicam a ela, como a Lei Criminal da República Popular da China[66] e a Lei da República Popular da China sobre punições de Ordem pública e da Administração de Segurança[67] (SCIO, 2010).

Somada a essa crescente regulação da internet no país, Zeng, Stevens e Chen (2017) argumentam que a China tem demonstrado o desejo de exportar suas normas de Governança da Internet, visando à própria modelagem da Ordem Internacional em seu favor. Em seu discurso de abertura na 2ª Conferência Mundial da Internet, em Pequim, no ano de 2015, o presidente Xi Jinping inclusive remarcou que, para que haja uma Governança Global das redes, um dos princípios deve ser o do respeito perante a "soberania da internet"[68] (JINPING, 2015). Ainda em respeito a este tópico, o presidente inclui que

> [...] o princípio da igualdade soberana consagrado na Carta das Nações Unidas é uma das normas básicas nas Relações Internacionais contemporâneas. Esse princípio cobre todos os aspectos referentes às relações Estado-Estado, a qual também inclui o espaço cibernético. Nós devemos respeitar o direito de países individuais de escolher independentemente seu próprio caminho de desenvolvimento cibernético, seu modelo de regulação cibernética e suas políticas públicas da internet, e participar da

[64] "O aumento do acesso à internet modificou as relações entre Estado e sociedade de várias formas" (ZENG; STEVENS; CHEN, 2017, p. 5, *tradução nossa*). Esse aumento de acesso, que levou ao próprio crescimento chinês, tem se conformado como uma preocupação para os líderes chineses (ZENG, 2015 apud ZENG; STEVENS; CHEN, 2017). Isto porque a transnacionalidade da internet permite uma "invasão" de ideias liberais ocidentais, como a democracia, as quais fragilizam a legitimidade de um Estado de um partido só, e a viabilidade do controle da informação centralizado por este Estado. Deste modo, o Governo chinês responde à altura, mobilizando esforços que previnam potenciais ideias desestabilizantes (ZENG; STEVENS; CHEN, 2017). Estas crescentes regulações, neste sentido, fazem parte desses esforços.

[65] [tradução nossa]. No original, lê-se: "China adheres to scientific and effective Internet administration by law […]".

[66] Em inglês, o nome da lei referente é *Criminal Law of the People's Republic of China*.

[67] Em inglês, o nome da lei referente é *Law of the People's Republic of China on Punishments in Public Order and Security Administration*.

[68] Em inglês, este conceito é conhecido como "internet sovereignty" ou "cyber sovereignty" (ZENG; STEVENS; CHEN, 2017).

> Governança Internacional do espaço cibernético em pé de igualdade (JINPING, 2015, s.p.)[69].

Apesar de não haver ainda um entendimento coletivo do que o país entende por "soberania da internet", em conclusão, pode-se visualizar que, a partir de suas ações no espaço cibernético, a China vem ativamente buscando a sua institucionalização e consequente securitização. Sob a Gestão Jinping, que demarcou o início de uma série de conceitos estratégicos e normativos, este país aumentou seu poder discursivo e sua influência (ZENG; STEVENS; CHEN, 2017): transformou-se de um "tomador de normas" em um "modelador de normas", além de figurar da mesma forma como um "contestador de normas" (ZENG; BRESLIN, 2016). Outrossim, depreende-se que na administração e na regulação da internet, o papel central é desempenhado pelo Governo, sendo este o responsável majoritário quando na administração da indústria da internet, incluindo na gestão de recursos básicos, tais quais os endereços de IP (SCIO, 2010).

A discussão acadêmica referente à parte de defesa, ou seja, de atribuição das Forças Armadas do país, por sua vez, similarmente começou a partir dos anos 1990. Influenciada pela atuação dos Estados Unidos na Guerra do Golfo e operações subsequentes[70] a China conformou o entendimento de que esta não conseguiria defender-se sem absorver as mudanças na forma de guerrear, dentro da qual agora as tecnologias desempenhavam majoritariamente papéis críticos (LYU, 2019). Os esforços chineses, como parte do que entendem por defesa cibernética, serão desenvolvidos na próxima subseção.

Antes de passar à próxima subseção, é importante reiterar que se desejou explorar inicialmente o fato de que a China, grande expoente no setor cibernético, vem, desde a implementação da internet no país, consagrando-se com relação à administração e regulamentação de suas redes. Visando centralizar essas tarefas exclusivamente ao Governo, o país propõe repetidamente, a nível internacional, o direito à autodeterminação, quando no modelo de regulação cibernética e quanto às políticas públicas da internet, além de uma Governança Internacional do Espaço Cibernético que seja coletiva entre os países. Ao mesmo

---

[69] [tradução nossa]. No original, lê-se: "The principle of sovereign equality enshrined in the Charter of the United Nations is one of the basic norms in contemporary international relations. It covers all aspects of state-to-state relations, which also includes cyberspace. We should respect the right of individual countries to independently choose their own path of cyber development, model of cyber regulation and Internet public policies, and participate in international cyberspace governance on an equal footing […]".

[70] Essa expectativa está de acordo com as ideias propostas por Cavelty (2012a), de que as percepções securitárias dos Estados Unidos ajudaram, de certa forma, a moldar as percepções de ameaças pelos países que a absorveram, e também as contramedidas desenvolvidas.

tempo, também se entende que, conforme cresce a sua influência e poderio internacional, o país intenciona, como fim último, modelar a então Ordem Internacional existente em seu favor.

3.2.2 Esforços promovidos frente à defesa cibernética

Lyu (2019) argumenta que as Forças Armadas chinesas começaram a ajustar suas estratégias militares em 1993, três anos após a Guerra do Golfo estadunidense. A partir disso, o objetivo básico de preparação para o combate militar tornou-se o de ganhar guerras locais com o apoio da moderna e alta tecnologia (LYU, 2019). Como ainda posto por Hughes (2003), dando voz ao testemunho de um oficial do Ministério da Defesa Nacional Taiwanês, os planos de guerra de informação começaram a se desenvolver em Pequim nos anos 1985, a serem implementados em 1995, e a serem conduzidos em 1997, a partir de exercícios com vírus de computadores que visavam interromper sistemas de comunicações militares.

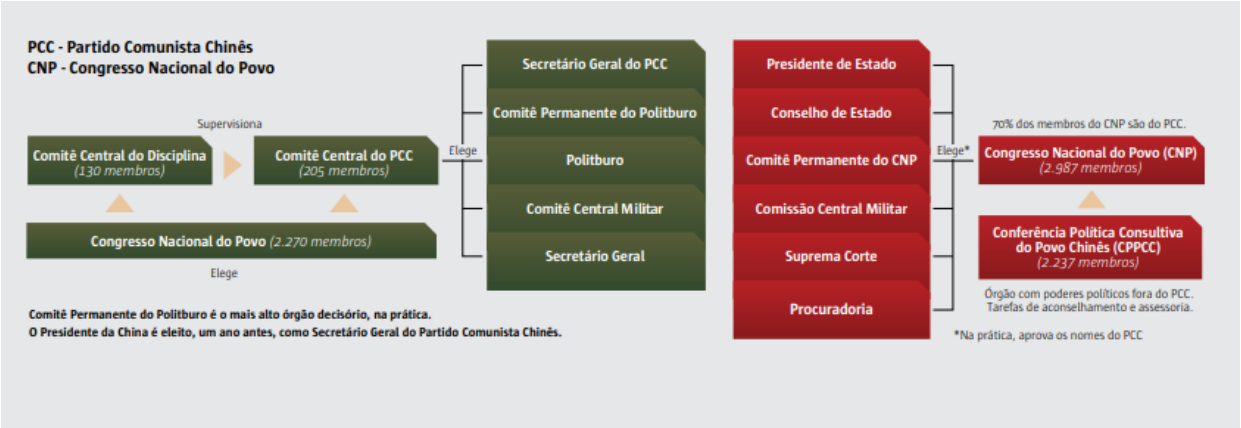
Em 2004, posteriormente à Guerra do Iraque, a preocupação modificou-se, atentando-se agora para a possibilidade de vencer guerras locais sob a condição de "informatização" (LYU, 2019). No documento Defesa Nacional Chinesa[71] de 2004, que confirma este entendimento, diz-se que a "informatização tornou-se o fator-chave no aprimoramento da capacidade de guerra das forças armadas" (LYU, 2019, s.p.)[72]. Isso pois entende-se que o papel das Forças Armadas ganha maior proeminência, em razão da sua transformação através do desenvolvimento de armas e equipamentos militares de grande porte tecnológico, além da realização de novas doutrinas militares (SCIO, 2004).

Neste sentido, faz-se necessário também entender a composição das Forças Armadas Chinesas. Intituladas de Exército de Libertação Popular[73] (ELP), estas são atualmente compostas por cinco elementos, incluindo o Exército, a Marinha, a Força Aérea, a Força de Mísseis e Foguetes (conhecida como 2ª artilharia) e a Força Logística Estratégica (GOMES FILHO, 2017). Ademais, o ELP submete-se ao poder majoritário do Comitê Central Militar do Partido Comunista (PCC), partido veiculante no poder, o qual tem como papel guiar a implementação de estratégias de defesa que protejam a soberania, a segurança e o

[71] Em inglês, o nome do documento referente é *China's National Defense*.
[72] [tradução nossa]. No original, lê-se: "[...] informationization has become the key factor in enhancing the warfighting capability of the armed forces […]".
[73] Em inglês, esta instituição é conhecida como *People's Liberation Army* (PLA).

desenvolvimento do país (GOMES FILHO, 2017). Para compreender melhor como o PCC relaciona-se com a estrutura governamental da China[74], tem-se a figura 4, exposta abaixo.

Figura 4 - Participação do PCC na escolha dos líderes na China



Fonte: Moretz-Sohn Fernandes (2014)

A maior mudança, por sua vez, veio no ano de 2013, com o documento A ciência da estratégia militar[75], quando essas Forças começaram a se endereçar publicamente à guerra cibernética de um ponto de vista mais abrangente. Enfatizando o espaço cibernético, esta normativa o reconheceu como um novo domínio de disputa militar na atualidade (LYU, 2019). Não coincidentemente, foi neste mesmo ano que Xi Jinping assumiu o cargo de presidente do país e, consequentemente, de Secretário-Geral do PCC, tornando-se o mais importante membro do Comitê Permanente do Politburo, órgão de maior controle do país[76] (MORETZ-SOHN FERNANDES, 2014).

Em matéria de políticas cibernéticas, Jinping é considerado importante, pois, como entendem Zeng, Stevens e Chen (2017), a China não havia promovido políticas domésticas relacionadas à internet numa escala global, com intenção de se beneficiar dos discursos de Governança Cibernética, até que ele assumisse o poder. Em dezembro de 2013, por exemplo, como parte dessa expansão e busca por poder, foi estabelecida a Comissão Central de Assuntos do Ciberespaço[77], dirigida pelo presidente, a qual estava incumbida de desenhar

[74] Moretz-Sohn Fernandes (2014, p. 6), entende que, "apesar de o PCC não ser explicitamente mencionado na composição do Governo, é dele que saem os principais líderes da China", ou seja, "a estrutura espelhada entre partido e governo faz do PCC um órgão decisório implícito".
[75] Em inglês, o nome do documento referente é *The Science of Military Strategy*.
[76] Xi Jinping é também o atual responsável pela Comissão Central Militar.
[77] Em inglês, esta instituição é conhecida como *Central Leading Group for Cyberspace Affairs*.

estratégias nacionais e políticas majoritárias para este espaço (YUEN, 2015). O seu escritório subordinado, a Administração do Ciberespaço da China[78], tornou-se uma autoridade independente e consolidada do espaço cibernético, possuindo significativos poderes[79] (YUEN, 2015).

A Estratégia Militar da China[80], lançada em 2015, no que lhe concerne, adota o mesmo tom do documento de 2013. Contudo, este último se diferencia por figurar como o primeiro documento militar oficial a endereçar-se à segurança cibernética[81]. Aqui, o espaço cibernético, além de pilar para os desenvolvimentos econômico e social, aparece como novo domínio para a segurança nacional, e há, finalmente, a declaração de que, em razão da competição estratégica internacional ter aumentado consideravelmente, a China se sente confrontada, com graves ameaças de segurança às suas infraestruturas cibernéticas (LYU, 2019).

Aproveitando ainda esta deixa para refletir o seu posicionamento em termos internacionais, propaga-se novamente a fala de Jinping (2015), sobre o princípio da igualdade soberana, a qual deve cobrir todos os aspectos das relações Estado-Estado, incluindo os aspectos cibernéticos. Em adição, Hsu e Murray (2014) argumentam que, de acordo com a presunção do Estado soberano e do princípio da não interferência aplicados ao espaço cibernético, este país prefere que as entidades governantes neste espaço sejam os Estados, assim como no mundo físico. Esta é uma das razões, inclusive, para a sua recusa em assinar a Convenção de Budapeste sobre crimes cibernéticos (HSU; MURRAY, 2014).

Além disso, sugere-se, a partir do modo como a China se posiciona no espaço cibernético em nível internacional, que esta rejeitará quaisquer medidas que indiquem que ela não conseguirá modificar o que, no momento, veicula como infraestrutura dominada pelos Estados Unidos. Por isso, esta prefere promover seu interesse na democratização da Governança da Internet via Organização das Nações Unidas (HSU; MURRAY, 2014). Em seu Livro Branco sobre a Internet na China, de 2010, já era possível visualizar esta orientação, como exemplificado nos dizeres "a China apoia o estabelecimento de uma organização

[78] Em inglês, esta instituição é conhecida como *Cyberspace Administration of China* (CAC).

[79] Este escritório tornou-se uma nova autoridade do espaço cibernético, e substituiu o Escritório de Estado da Informação na Internet (em inglês, conhecido como *State Internet Information Office* ou SIIO). A sua substituição, por sua vez, deu-lhe mais poder, já que separou o corpo regulatório da Internet, pertencente ao Conselho de Estado (em inglês, conhecido como *State Council*), e levou à fusão de entidades com diferentes níveis organizacionais (YUEN, 2015).

[80] Em inglês, o nome do documento referente é *China's Military Strategy*.

[81] Thomas (2009) argumenta que a palavra "cyber" não possui uso extremamente difundido na China, que prefere a utilização da palavra "informatização".

administrativa da internet internacional e oficial apenas sob o sistema da Organização das Nações Unidas (ONU), através de procedimentos democráticos numa escala mundial" (SCIO, 2010 apud HSU; MURRAY, 2014, p. 2)[82].

Nos dois anos seguintes - 2016 e 2017 -, a seu modo, foram lançados três documentos importantes em matéria de segurança cibernética, os quais devem ser citados aqui. O primeiro, a Estratégia Nacional de Segurança Cibernética[83], foi implementado em 2016 e redigido pela Administração do Ciberespaço da China. Nesta estratégia, releva-se tanto a importância da segurança cibernética para promoção dos interesses comuns da humanidade, do desenvolvimento e da paz mundial, quanto o mantimento desse tipo de segurança na China como importante medida para coordenar e promover a construção de uma sociedade de bem-estar e para que o governo possa governar de acordo com a lei. Para mais, o próprio Estado chinês se coloca, ali, numa posição de protagonista e defensor da sua soberania cibernética e de suas infraestruturas informativas críticas (CAC, 2016).

O segundo, intitulado de Lei de Segurança da População da República da China[84], foi lançado em 2017, e possui caráter implementativo mais interno ao Estado chinês. Seu propósito, como lei, inclui a salvaguarda da segurança cibernética, da soberania neste espaço, dos interesses e direitos legais dos cidadãos, de pessoas jurídicas e de outras organizações, entre outros. Outrossim, é relevante pontuar que, ao mesmo tempo em que o Estado se compromete com o desenvolvimento da segurança cibernética e da informatização, além de incentivar a inovação e a aplicação de tecnologias, este ator espera que a conduta online dos cidadãos seja honesta e civilizada, e que dissemine os valores socialistas centrais (NPC, 2017).

O terceiro e último, a Estratégia Internacional para Cooperação no Ciberespaço[85], de 2017, foi publicado pelo Ministério das Relações Internacionais da China. A partir deste documento de caráter internacional, a China reitera sua perspectiva e interesses quando na participação da Governança Global da Internet, a qual assimila como um instrumento de governança compartilhada, "multipartidária": não deve-se, portanto, buscar a hegemonia neste espaço, mas cooperar. Além disso, esta entende a nova realidade - referente às tecnologias de

---

[82] [tradução nossa]. No original, lê-se: "China supports the establishment of an authoritative and just international Internet administration organization under the UN system through democratic procedures on a worldwide scale".

[83] Em inglês, o nome do documento referente é *National Cyberspace Security Strategy*.

[84] Em inglês, o nome do documento referente é *Cybersecurity Law of the People's Republic of China*.

[85] Em inglês, o nome do documento referente é *Cyberspace International Cooperation Strategy.*

informação e comunicação -, como uma oportunidade, e, ao mesmo tempo, como um desafio para o Sistema Internacional, este segundo expresso em ações como o terrorismo cibernético, a vulnerabilidade das infraestruturas críticas de informação, os crimes cibernéticos e a espionagem cibernética (FMPRC, 2017).

O último documento lançado em matéria militar, a seu turno, denominado Defesa Nacional Chinesa na Nova Era[86], de 2019, visa

> [...] expor a política defensiva de defesa nacional e expor as práticas, propósitos e significados dos esforços chineses para construir uma defesa nacional fortificada e Forças Armadas fortes, visando auxiliar a Comunidade Internacional a compreender melhor a defesa nacional da China (SCIO, 2019, s.p.)[87].

A este respeito, as Forças Armadas, em nível cibernético, são descritas como aceleradoras da construção das capacidades nacionais, sendo também as responsáveis maiores no desenvolvimento da segurança e defesa cibernéticas e na construção de capacidades de defesa que estejam de acordo com o posicionamento internacional da China. Por último, estas devem se portar de modo a manter seu status como um dos atores mais relevantes do Sistema Internacional em termos de cibernética (SCIO, 2019).

De acordo com Lyu (2019), algumas conclusões podem ser tiradas a partir da forma com que a China vem lidando com sua própria segurança nacional, e com o espaço cibernético: as capacidades nacionais chinesas não se desenvolveram em um vácuo, mas sim como uma resposta às mudanças de abordagem e práticas de outros países, haja vista os Estados Unidos e a Rússia. Além disso, as visões do governo chinês com relação à própria guerra cibernética são consistentes com suas estratégias militares, e se modificam a partir do ambiente de segurança nacional, da situação doméstica e das atividades das Forças Armadas estrangeiras (LYU, 2019). Finalmente, a essa argumentação, adiciona-se a discussão anteriormente proposta por Hughes (2003), a qual entende que as respostas chinesas para a revolução da informação e para a expansão da internet têm sido fornecidas em todos os níveis, incluindo a partir da doutrina e do treinamento militares, da regulação doméstica, das políticas industriais, e da cooperação internacional.

---

[86] Em inglês, o nome do documento referente é *China's National Defense in the New Era*.

[87] [tradução nossa]. No original, lê-se: "The Chinese government is issuing China's National Defense in the New Era to expound on China's defensive national defense policy and explain the practice, purposes and significance of China's efforts to build a fortified national defense and a strong military, with a view to helping the international community better understand China's national defense."

3.3 CHINA X EUA: SEMELHANÇAS E DIFERENÇAS PRELIMINARES

Segundo Qian (2019), os fatores que concernem a segurança do espaço cibernético se tornaram uma variável importante nas relações China-Estados Unidos. Esta relação, por sua vez, passou por três estados de desenvolvimento: a de benefícios e ganhos mútuos (1994-1999); a de balanceamento difícil (1999-2010); e, por último, a de frequentes ocorrências de problemas de segurança das redes, que começou em 2010, e vigora até o momento presente (QIAN, 2019).

A primeira fase começa quando do primeiro acesso à internet pelo Estado chinês, e é marcada pela aceitação deste ator perante os arranjos de infraestrutura da internet perpetuados pelos Estados Unidos. A segunda fase decorre a partir de um ponto onde a tecnologia da China já está melhor desenvolvida, quando as contradições e diferenças existentes entre os dois atores diminuíram. A última, a qual nos ateremos aqui, começou após a retirada do Google da China[88], e tem como pano de fundo o aumento da tensão entre os dois atores, com acusações do lado estadunidense que pairam sobre a participação do governo chinês em golpes cibernéticos, no bloqueio de sites estrangeiros e na restrição da liberdade de expressão na internet, e, do outro lado, referente ao país asiático, com a alegação de resistência aos valores americanos, os quais suportam a pesquisa e o desenvolvimento para escapar dos *firewalls*[89] (QIAN, 2019).

Como dois dos atores mais relevantes junto ao espaço cibernético, faz-se importante delinear algumas de suas similaridades e diferenças em termos de capacidades nacionais cibernéticas, visando apreender algumas das motivações para o aumento dessas tensões. Primeiramente, a China coloca que o desenvolvimento de suas capacidades cibernéticas

---

[88] Inkster (2010) argumenta que o comportamento esperado dos provedores de serviços da internet estrangeiros, ao se instalarem na China, é o de que estes monitorem o conteúdo de suas páginas *web* e blogs. Foi, esta, portanto, uma das razões alegadas pelo Google quando este decidiu sair da China, em março de 2010 (INKSTER, 2010).

[89] Segundo Costa (2020, s.p.), um *firewall* é "um recurso de software ou hardware que é responsável por filtrar toda a informação que chega a uma rede, garantindo a sua segurança. Se algum dado for considerado como malicioso pelo filtro, ele não poderá ser acessado e será automaticamente bloqueado". Este tipo de esforços vêm sendo desenvolvidos pelo próprio Governo chinês, o qual, alegando a prevenção contra ideias potencialmente desestabilizantes, lançou mão de planos como o "Grande Firewall da China" (conhecido originalmente, em inglês, como *Great Firewall of China*) (ZENG; STEVENS; CHEN, 2017). Tal projeto, em específico, "bloqueia o acesso a recursos de internet vetados e censura o tráfego de rede para frases e palavras-chave banidas." (ZENG; STEVENS; CHEN, 2017, p. 5, *tradução nossa*). Além disso, "este também encoraja mudança de comportamento em usuários da Internet, por medo de investigação e processo criminal, através de uma *matrix* de vigilância técnica, legal e de medidas regulatórias" (DEIBERT ET AL., 2011 apud ZENG; STEVENS; CHEN, 2017, p. 5, *tradução nossa*).

militares são um resultado - uma resposta defensiva - aos esforços estadunidenses hegemônicos de militarização deste espaço, do proveito de seu posicionamento de liderança tecnológica para o estabelecimento de normas em seu favor (HSU; MURRAY, 2014). Os Estados Unidos, por sua vez, justifica o interesse na construção de capacidades militares em outro domínio, o espaço, em razão das ações tanto da Rússia quanto da China, já que esta última, notadamente, criou um braço militar para priorizar capacidades de guerra no espaço (GALBRAITH, 2019). Disto, interpreta-se que, em alguma medida, as capacidades militares atualmente buscadas pelos dois atores nos mais diversos domínios figuram como respostas aos avanços do outro.

Além disso, como já dito, a China preza pelos Estados como as entidades governantes mais importantes no espaço cibernético (HSU; MURRAY, 2014). Já os Estados Unidos, como demonstrado na Estratégia de 2003, apesar de entender que o setor privado é mais bem equipado para lidar com ameaças cibernéticas, infere que existem situações onde a resposta governamental é mais apropriada (RODRIGUES PADILHA, 2016). Ainda mais adiante, na Estratégia Internacional de 2011, há uma adição a este entendimento, proferindo que, se necessário, medidas coercitivas poderão ser tomadas contra o setor privado, visando garantir a estabilidade e a segurança das redes internas (DA CRUZ JR., 2013).

Ainda sobre este ponto, para a China, os Estados, agindo sobre os seus próprios cidadãos, sobre os cidadãos estrangeiros, e também sobre Organizações dentro de suas fronteiras, deveriam reivindicar a soberania no espaço cibernético. Os EUA, divergindo deste primeiro, alegam atuar em favor da proteção da liberdade de expressão individual, e de outras liberdades, entendendo o controle de conteúdo online pelos Estados como "inapropriado"[90] (HSU; MURRAY, 2014).

Ademais, deve-se acrescentar que o entendimento chinês do espaço cibernético caminha numa direção diversa do entendimento estadunidense quanto ao mesmo domínio. Como explorado, as contramedidas norte-americanas de proteção à sua segurança nacional e às suas infraestruturas críticas foram desenhadas em favor da oposição "a uma nova ameaça"

[90] Ao mesmo tempo, essa posição estadunidense de "atuação em favor da proteção da liberdade de expressão individual" pode ser contestada pela atual proibição de transações relativas aos aplicativos chineses WeChat e TikTok em seu território, por exemplo (ROSS, 2020). Essas transações, proibidas pelo Departamento de Comércio Norte-Americano, foram justificadas com base na necessidade de salvaguardar a segurança nacional dos Estados Unidos (ROSS, 2020). Ross (2020, s.p., *tradução nossa*), atual Secretário de Comércio do Governo Trump, ainda argumenta que o Partido Comunista Chinês "demonstrou os meios e as motivações para utilizar estes aplicativos para ameaçar a segurança nacional, a política externa, e a economia dos Estados Unidos".

(CAVELTY, 2008). Esta nova ameaça previa, como publicado em documentos institucionais posteriormente, a possibilidade do uso da força pelos Estados Unidos, caso necessário (THE WHITE HOUSE, 2003). Os regimentos criados em dedicatória aos conflitos cibernéticos, além de investimentos massivos em organismos como o Departamento de Defesa e seus subordinados, também reforçam esta linha de pensamento.

A visão chinesa, a seu turno, como apresentada mais recentemente por meio do documento Defesa Nacional Chinesa na Nova Era, de 2019, explicita que o direcionamento estratégico chinês para esta nova era adere ao princípio de defesa, autodefesa e da resposta pós-ataque, ou seja, que este país manterá a postura de não atacar, a menos que seja atacada. Caso esta seja atacada, contudo, é informada a certeza do contra-ataque por parte dos atores chineses (SCIO, 2019). Outrossim, ao mesmo tempo que a China diz abordar esse novo domínio majoritariamente com a perspectiva e interesse na existência de uma Governança Global da Internet, onde figure uma governança compartilhada (FMPRC, 2017), esta tem demonstrado o desejo de exportar suas normas de Governança da Internet, visando à modelagem da Ordem Internacional em seu favor (ZENG; STEVENS; CHEN, 2017).

Em termos tecnológicos, ou seja, relativos à pesquisa, ao desenvolvimento e à inovação (P,D&I) - abrangendo a área militar -, os dois países também demonstraram serem atores significativos. Os Estados Unidos, tal como posto por Moreira Jr. (2014, p. 26-27), investe em um sistema nacional de inovação tecnológica que é capaz de garantir sua liderança científica em diversas áreas, incluindo a de pesquisas militares, "essencial para consolidar a capacidade efetiva de suas forças armadas e de gerar saltos tecnológicos em setores civis". O mesmo autor justifica esses esforços estadunidenses como uma intenção de manter seu controle sobre a Ordem Internacional (MOREIRA JR., 2014).

Nesse sistema de inovação, as incubadoras impulsionadoras do desenvolvimento de inovações no país são os grandes estabelecimentos de pesquisas básicas nas universidades, no governo e em um número significativo de empresas privadas[91] (MOREIRA JR., 2014). Atualmente, ainda, esse Complexo Industrial Militar Acadêmico vem desenvolvendo tecnologias de caráter dual, onde dispositivos e inovações para fins de segurança e defesa são incorporados "a sistemas de uso cotidiano e passam a potencializar o desenvolvimento

[91] Em suma, o que se intitula de complexo-industrial-militar-acadêmico se traduz como um componente de grande parceria entre o "conhecimento tecnológico oriundo da academia, a base material oferecida pela iniciativa privada e o estímulo e a orientação política provindos do Estado" (MOREIRA JR., 2014, p. 35).

industrial e comercial norte-americano, em processo denominado *spin-off*[92]" (MOREIRA JR., 2014, p. 36).

No sistema chinês, a seu modo, sempre teve importância o papel do Estado, e, por conseguinte, do Partido Comunista. A particularidade da preocupação com a dominação estrangeira[93], no que lhe concerne, faz também parte da própria especificidade da construção nacional chinesa, e da definição e implementação de muitas políticas, incluindo a produtiva e a de Ciência e Tecnologia (C&T). Deste modo, até a contemporaneidade, a importância dada à questão militar quando na política industrial e tecnológica é grande. Finalmente, no período compreendido entre 1995 e 2005, o sistema nacional de inovação e aceleração da industrialização se fortaleceu, possibilitando que, ao cabo, as políticas pudessem ser direcionadas para a criação de um ambiente receptivo ao desenvolvimento tecnológico e aos esforços de inovação nas empresas, sobretudo as pequenas e médias (CASSIOLATO, 2013).

Finalmente, em termos de empresas atuantes na área de tecnologia da informação e comunicação, relevam-se atualmente as ferramentas de busca Google, estadunidense, e Baidu, chinesa; de computação em nuvem Microsoft e Amazon, estadunidenses, e Alibaba Cloud e Tencent Cloud, chinesas; e de mídias sociais Facebook, Twitter e Instagram, estadunidenses, Tiktok, Weibo e Wechat, chinesas (SCMP RESEARCH, 2020). Somado-se a isso, têm-se ainda empresas tecnológicas de peso como a Huawei[94] e a Lenovo, chinesas (CASSIOLATO, 2013), e as estadunidenses Cisco Systems e Apple (YUEN, 2015).

A Huawei é, inclusive, motivo atual das últimas disputas envolvendo estes dois atores. Majerowicz (2019) alega que os EUA vêm alertando suas forças militares e aliados quanto às

---

[92] A partir de Fonseca (2000 apud MOREIRA; CORDEIRO, 2014, p. 102-103), entende-se que o processo de *spin-off* "consiste em um processo de disseminação tecnológica que pode ocorrer da indústria militar para a civil, em decorrência da intensidade e da adaptação da Pesquisa e Desenvolvimento - P&D - militar". Além do processo de *spin-off*, há também o processo de *spin-in*, por meio do qual técnicas, processos e tecnologias são importados do meio civil para o meio militar (MOREIRA; CORDEIRO, 2014).

[93] Essa preocupação com a dominação estrangeira, já explorada anteriormente, também aparece quando no ambiente cibernético, e mais especificamente, na parte de defesa. De acordo com Inkster (2010), muitos sistemas governamentais chineses ainda dependem dos hardwares e softwares ocidentais, os quais podem estar mais propensos a vulnerabilidades. Esse risco tem sido constantemente mitigado, com tentativas estatais chinesas de promover "redes soberanas e tecnologia internamente", "mas a contínua demanda por produtos ocidentais sugere que este ainda é um trabalho em progresso" (INKSTER, 2010, p. 64, *tradução nossa*). Moreira e Cordeiro (2014) também descrevem esse país como um exemplo de busca pela autonomia no setor cibernético, dada sua intenção de desenvolver tecnologia de defesa própria. São exemplos de resultados seu próprio sistema operacional, intitulado Kylin, e o desenvolvimento de um microprocessador seguro para a utilização de servidores e roteadores da Huawei (MOREIRA; CORDEIRO, 2014).

[94] Cassiolato (2013, p. 77) argumenta que "as grandes empresas privadas são majoritariamente públicas e vinculadas direta ou indiretamente com o complexo produtivo militar chinês", como é o caso das gigantes Huawei e ZTE. Essas duas, somadas à Lenovo, são produtos de *spin-off* das universidades chinesas (CASSIOLATO, 2013).

potenciais ameaças à segurança nacional representadas pela ascensão da China no emprego das TICs, principalmente no tangente ao fornecimento de equipamentos de telecomunicações para a implementação do 5G, como é o caso da Huawei. Suas alegações de perigo[95] se apoiam na afirmação de que as empresas chinesas possuem laços estreitos, "obscuros ou informais" (MAJEROWICZ, 2019, p. 10) com o intitulado partido-Estado, o qual ocorreria, por exemplo, através do Exército de Libertação Popular (MAJEROWICZ, 2019).

Todavia, Lyu (2019) entende que, se analisados todos os elementos propostos em termos de capacidades nacionais, o poder cibernético chinês ainda se posiciona atrás do estadunidense. Corroboram, em argumentação, elementos como a impossibilidade de autossuficiência total chinesa em tecnologias críticas[96], apesar do avanço na promoção de esforços; a baixa influência no todo da internet global, em razão de sua língua principal não ser largamente utilizada na internet fora do país[97]; e também o grande ataque que suas redes ainda sofrem (LYU, 2019). Em conclusão, apesar das discrepâncias e de uma se sobrepor à outra em termos de capacidades cibernéticas, é inegável visualizar os avanços destes dois países, os quais figuram atualmente como modelos em termos de defesa cibernética.

3.4 CONCLUSÕES PRELIMINARES

Observa-se, portanto, de acordo com os resultados apresentados pelos Estados Unidos e pela China, que estes dois configuram modelos em termos de capacidades em defesa cibernética. Fazendo referência à Lyu (2019) novamente, entende-se que o poderio e a influência cibernéticas, o *cyberwarfare*, não são medidos apenas pelas áreas militar e de inteligência, mas por fatores como o desenvolvimento científico e tecnológico, as capacidades

---

[95] A Casa Branca, em 2019, cortando a Huawei e suas subsidiárias das tecnologias americanas (MAJEROWICZ, 2019), justificou-se através do argumento de que "(...) os adversários estrangeiros estão crescentemente criando e explorando vulnerabilidades em tecnologias e serviços de comunicações e informações, que armazenam e comunicam vastas quantidades de informações sensíveis, facilitam a economia digital e sustentam infraestrutura crítica e serviços vitais de emergência (...)" (THE WHITE HOUSE, 2019, s.p., *tradução nossa*).

[96] "Apesar de a China possuir uma indústria tecnológica de larga escala e o potencial para competir com os Estados Unidos em alguns setores, a maioria de suas tecnologias centrais de rede, e hardwares e softwares chave, são fornecidos pelas companhias estadunidenses" (LYU, 2019, s.p., *tradução nossa*).

[97] Inkster (2010), sobre esse tema, discute que o hardware e o software da internet foram feitos por companhias ocidentais, tendo em mente os usuários ocidentais. Deste modo, esses sistemas não preenchem totalmente as necessidades dos chineses, já que estes carecem, por exemplo, de sistemas para o processamento de palavras em mandarim, os quais envolvem a digitação em pinyin (método de transliteração mais utilizado para o mandarim padrão).

de inovação, as empresas do setor de tecnologia da informação, a escala de infraestrutura da internet, entre outros, os quais foram também presentemente explorados.

Os Estados Unidos, pioneiro na implementação da internet e na questão da securitização deste espaço, ainda se posiciona na vanguarda das ações concernentes a este, detendo certa hegemonia quando na disposição de sua estrutura e de uma possível regulação internacional. A China, contudo, apesar de ainda não tê-lo alcançado em termos tecnológicos, além de também ficar atrás em razão do mandarim não ser uma língua difundida em linguagem programática como o inglês[98], tem buscado constantemente a sua internacionalização em termos econômicos, políticos e, finalmente, tecnológicos. Isso demonstra, portanto, que, estes Estados possuem semelhanças na abordagem do espaço cibernético, mas também diferenças, e que são observados, em matéria de práticas, por toda a Comunidade Internacional.

Deste modo, buscar-se-á no próximo capítulo, usá-los de modelos, quando ao analisar o caso particular brasileiro. O Brasil, já introduzindo o motivo de sua escolha, é um país que começou a tratar com maior seriedade a sua segurança e, principalmente, a sua defesa cibernética, apenas no presente século. O objetivo da projeção das práticas desses dois atores sobre o caso do país latino-americano, em conclusão, não é o de simplesmente compará-los, colocando-os em uma hierarquia cibernética, mas entender como estes primeiros, aqui retratados, podem - e se podem - servir de exemplo ou molde para o desenvolvimento de capacidades deste último.

[98] Apesar disso, de acordo com French (2006), o Governo chinês vem promovendo, desde o começo do século XXI, esforços para promover o próprio mandarim para outros países. Um exemplo disso foi a criação da rede global de Centros Culturais Chineses, intitulados Institutos Confúcio, os quais intencionavam ensinar a estrangeiros o idioma "com uma reputação proibitiva pela sua dificuldade" (FRENCH, s.p., *tradução nossa*). Com a ascensão dos aplicativos TikTok e WeChat entre a população jovem estadunidense (DELISLE, 2020), e também com o crescimento de sua popularidade entre outros países do globo, por sua vez, o mandarim pode vir a tornar-se futuramente um idioma – e, portanto, uma linguagem – central na disputa do discurso cibernético, o qual viria a ser benéfico para a China.

4 DEFESA CIBERNÉTICA NO BRASIL: PARTICULARIDADES E FRAGILIDADES

Segundo Oliveira et al. (2017, p. 60), "o tamanho colossal do Brasil é refletido em diversas de suas características. Por exemplo, ele tem uma das maiores florestas do mundo e apresenta uma diversidade considerável de biomas". Esse tamanho colossal, a seu modo, pode ser representado pela sua extensão territorial, quando calculada de acordo com a sua área total: o país detém 8.515.770 km², ocupando a 5ª posição mundial (STATISTA, 2019). Ademais, em termos populacionais, o país atingiu, no ano de 2019, a marca de 210 milhões de habitantes (IBGE, 2019).

Se compararmos esses dois dados - o de extensão e o de termos populacionais -, por sua vez, entende-se que o Brasil configura um país populoso, mas não extremamente povoado. Isso pois, interpreta-se que, dentre todos os países do globo, o Brasil é o Estado com a 6ª maior população (VEJA, 2019). Ao mesmo tempo, sua densidade demográfica - correspondente ao número de habitantes por km² -, demonstra que sua população encontra-se irregularmente distribuída pelo espaço territorial do país. As áreas litorâneas, a região do eixo Rio de Janeiro-São Paulo, e as regiões metropolitanas, de acordo com o IBGE (2010), são mais populosas. As áreas pertencentes ao Sertão Nordestino, à Amazônia e ao Pantanal do Mato Grosso, ao contrário, são regiões de vazios demográficos (IBGE, 2010).

Somado-se a isso, deve-se compreender, ainda, como o país se projeta interna e externamente em termos econômicos, sociais e políticos. A frente de qualquer outro país da região sul-americana, e também de qualquer outro país da América Latina, seu índice de Produto Interno Bruto, em 2018, totalizava US$1,8 trilhões, o equivalente à 9ª posição global (THE WORLD BANK, 2018). Um complemento a este resultado, no que lhe concerne, está representado no Índice de Desenvolvimento Humano (IDH) - índice que intenciona opor-se ao cálculo do PIB per capita, medida que considera apenas a dimensão econômica do desenvolvimento (PNUD, [201-]). Aqui, entende-se que o IDH, o qual leva em conta três medidas básicas do desenvolvimento humano - renda, educação e saúde - (PNUD, [201-]), transparece de melhor forma a real situação econômica dos indivíduos de uma sociedade. Em 2014, portanto, o país obteve a 75ª posição do ranking, o que o qualificava como "alto desenvolvimento humano", ficando, por exemplo, atrás dos Estados Unidos e à frente da China (PNUD, 2015).

Ademais, em matéria de política externa, o país contribui constantemente para discussões importantes, figurando como participante ativo na ONU[99], como integrante do agrupamento de países Brasil, Rússia, Índia, China e África do Sul, mais conhecido pela nomenclatura BRICS, e também como integrante do Mercado Comum do Sul (MERCOSUL), juntamente com Argentina, Paraguai e Uruguai. Finalmente, o Brasil também foi membro da União de Nações Sul-Americanas (UNASUL)[100].

Em razão, portanto, de seu tamanho colossal, já predisposto nas palavras de Oliveira et al. (2017), da necessidade de salvaguardar todas as regiões do país, principalmente àquelas fronteiras pouco povoadas, e de continuar perpetuando seu crescimento econômico e social e seu poderio político, o Brasil atenta-se à sua própria defesa. Novamente utilizando-se de dados do SIPRI (2019 apud GAZETA DO POVO, 2019), portanto, conforma-se que o país despendeu aproximadamente US$28 bilhões em investimentos no campo militar, para o ano de 2018, o que lhe rendeu o 12º lugar do ranking mundial.

Para o mesmo ano de análise, compreende-se que a tendência de gastos militares entre os países sul-americanos foi de um aumento de 3,1% (o equivalente a US$55,6 bilhões) (SIPRI, 2019 apud GAZETA DO POVO, 2019). No Brasil, esse crescimento é ainda mais acentuado, dado que o atual Governo é composto, em sua chefia mais alta do executivo, por um capitão reformado do Exército: o orçamento de defesa proposto para 2020 foi de R$105,7 bilhões; o encaminhado para o Congresso, neste ano, para 2021, prevê alta de 4,7% com relação a este mesmo valor (SCHREIBER, 2020).

Neste sentido, como já introduzido no capítulo 1, e discutido posteriormente no capítulo 2, para os Estados Unidos e para a China, o ponto de partida da institucionalização e securitização do espaço cibernético é a inserção da internet, e, ainda mais além, a dependência que os sistemas de infraestrutura de um país passam a ter para com ela, quando interligados. Por isso, o último capítulo desta monografia intenciona compreender qual o contexto dentro do qual a internet inseriu-se no Brasil, de que modo o Estado institucionalizou-a, e, finalmente, se - e como - as Forças Armadas securitizaram-na, atendo-se à melhoria de suas

[99] Além de advogar intensamente desde os anos 90 junto a outros países, tais quais a Alemanha, o Japão, e a Índia, pela implementação de reforma na estrutura do Conselho de Segurança (NETO, 2020), o Brasil abre todas as Assembleias Gerais da Organização desde 1955 (PIMENTEL; PANKE, 2016). O país também despendeu contínuas forças militares para participação em Missões de Paz da Organização desde a sua adesão à esta, com destaque para a Missão das Nações Unidas para a Estabilização no Haiti (MINUSTAH), que contou com a liderança brasileira (DINIZ, 2009).

[100] O Brasil formalizou sua saída da Organização em 2019, mas esta temática não será esgotada na presente monografia.

capacitações para defender-se e dissuadir no espaço cibernético. Antes de iniciar, contudo, é importante delinear uma premissa: entende-se que, diferentemente dos outros dois países tratados anteriormente, o Brasil passou a explorar e investir, militarmente, nesta pauta, apenas no presente século. Portanto, ao invés de esgotar comparações entre os atores aqui explorados - entendendo o Estados Unidos e a China como os principais atores no espaço cibernético -, pretende-se utilizar estes dois exemplos de forma a entender as particularidades do sistema de defesa cibernética brasileiro, identificando suas possíveis forças e fraquezas.

4.1 AS TELECOMUNICAÇÕES NO BRASIL E O SURGIMENTO DA INTERNET

Até os anos 1950, o Brasil ainda vivia a fase embrionária de suas telecomunicações. Com a tomada de poder pelos militares, quatorze anos depois, o Estado passou a empenhar-se fortemente para que o país dispusesse de uma infraestrutura mais moderna de telecomunicações, a qual era vista como necessária à segurança e ao desenvolvimento da integração regional (CARVALHO, 2006).

O modelo de telecomunicações até então existente, a seu modo, era dominado internamente por empresas privadas, o que não era visto como interessante pelos governos militares, já que deixava algumas regiões remotas desatendidas e, sobretudo, implicava que as comunicações estratégicas fossem conduzidas por empresas estrangeiras, contrariando a doutrina de segurança nacional então vigente[101]. Para tanto, foi constituída, em 1965, entre outros, a Empresa Brasileira de Telecomunicações (EMBRATEL), visando implantar uma rede nacional para adquirir o controle de concessionárias privadas e para assumir os serviços nacionais (CARVALHO, 2006).

Com os investimentos realizados paulatinamente na EMBRATEL, o serviço de telefonia de longa distância passou a obter um bom nível de qualidade já no início da década de 1970, porém, este ainda ficava muito aquém do que se considerava necessário para a telefonia urbana. Deste modo, visando resolver tal situação, foi criada a Telecomunicações Brasileiras S. A. (Telebrás), a qual instituiu, em cada Estado do país, uma empresa-polo que

[101] Nos anos 1980, surgiram as primeiras críticas a esse modelo, de caráter monopolista estatal, com relação ao setor de telecomunicações no Brasil. Todavia, apesar das críticas, a situação foi reforçada com a Constituição de 1988, que considerava o setor de telecomunicações estratégico, e, por isso, manteve-o sobre o controle governamental. Mudanças neste setor só aconteceriam em 1997, com a perda de validade do Código de Telecomunicações, já em meio ao processo de privatização das telecomunicações brasileiras (CARVALHO, 2006).

promovia a incorporação das companhias telefônicas existentes através da aquisição de seus acervos ou controles acionários (CARVALHO, 2006).

Como previsto, este caráter nacionalista das políticas industrial e tecnológica brasileiras foi fortalecido durante o período ditatorial, principalmente por meio do II Plano Nacional de Desenvolvimento, do Governo Geisel. Uma de suas principais intenções era fomentar a indústria de componentes e insumos eletrônicos, buscar a autonomia tecnológica e construir uma indústria nacional de equipamentos (CARVALHO, 2006). Intencionalmente, foi também neste período - mais especificamente, em 1975 -, que o Ministro das Comunicações decidiu que a EMBRATEL seria a responsável pela implementação, pela expansão e pela operação da Rede Nacional de Telecomunicações e da Rede Nacional de Transmissão de Dados, incluindo no tangente às conexões internacionais (KNIGHT, 2014).

Em 1979, já sob o Governo Figueiredo, foi criada a Secretaria Especial de Informática (SEI), subordinada ao Conselho de Segurança Nacional da presidência (CARVALHO, 2006). Knight (2014) afirma que esse organismo, caracterizado por um estilo autoritário, não inspirava confiança na comunidade tecnológica civil. Para o mesmo autor, ainda, a adoção dos protocolos TCP/IP, naquela época, seria vista pelos militares brasileiros como "uma representação da reafirmação da hegemonia americana", e, portanto, não poderia ser adotada (KNIGHT, 2014, p. 21)[102].

No fim do período militar, em 1984, a seu turno, a política referente ao setor de informática deixou de ser competência exclusiva do poder executivo. O Congresso Nacional, ao aprovar a "Lei de Informática", referendou princípios básicos de capacitação tecnológica e reserva de mercado, também democratizando o processo decisório por meio da criação do Conselho Nacional de Informática e Automação (CONIN) (CARVALHO, 2006).

Já com a instauração da Nova República, no ano seguinte, em 1985, a SEI foi transferida do Conselho de Segurança Nacional para o Ministério da Ciência e Tecnologia (MCT), e, cinco anos depois, no Governo Collor, foi extinta, dando lugar ao Departamento de Política de Informática e Automação (DEPIN) (CARVALHO, 2006). O que é importante relevar aqui, com relação à mudança gradual na política das telecomunicações e informações, é que

> [...] as preocupações acerca da segurança nacional e dos fluxos de poder por detrás do fluxo das informações, entretanto, foram paulatinamente sendo esquecidas, no

[102] [tradução nossa]. No original, lê-se: "For the Brazilian military at that time, adoption of TCP/IP would "represent a reaffirmation of American hegemony".

> Brasil e no mundo, com o advento da globalização e a expansão da Internet (CARVALHO, 2006, p. 62).

Ao mesmo tempo que se entende o papel do Estado na aceleração das telecomunicações do país, deve-se delinear o importante desempenho da comunidade acadêmica neste mesmo contexto. Com interesse na formação de redes que interligassem os computadores de diferentes universidades, acadêmicos do Estado do Rio Grande do Sul desenvolveram uma primeira iniciativa, no meio dos anos 1970: um projeto intitulado de Rede Sul de Teleprocessamento (RST). Este projeto, apesar de nunca ter obtido o sucesso requerido, abriu espaço para o aumento do interesse por pesquisas concernentes às redes de comunicação de dados entre as universidades brasileiras. Por exemplo, no fim de 1979, foi estabelecido o Laboratório Nacional de Redes de Computadores (LARC), uma entidade para ligar instituições que estavam desenvolvendo esforços neste sentido, com grande atividade por parte de centros como a Universidade Federal do Rio de Janeiro (UFRJ) e a PUC-Rio (KNIGHT, 2014).

Apesar da disposição das universidades brasileiras só ter aumentado com o passar dos anos, até 1986, nenhuma rede acadêmica havia saído do papel no país. Em 1988 e 1989, uma nova tentativa ocorreu, com três instituições estabelecendo, separadamente, ligações de rede com três universidades estadunidenses, utilizando-se da rede BITNET, a qual permitia a troca de e-mails e de arquivos: o Laboratório Nacional de Computação Científica (LNCC), do Rio de Janeiro; a Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP); e a UFRJ. Mesmo obtendo êxito na iniciativa, essas ligações tiveram que ser aprovadas pela EMBRATEL e pela SEI, as quais ainda estavam no controle das telecomunicações brasileiras (KNIGHT, 2014).

Finalmente, a criação da Rede Nacional de Ensino e Pesquisa (RNP), um projeto mais ambicioso do que todos os anteriormente promovidos, demandava por uma estrutura extensa e cara que só poderia ser efetivada com recursos governamentais. Com a decisão do MCT, em 1992, de financiar a RNP, esta pode começar a operar no Brasil, por meio de linhas alugadas. A ligação com a internet global no país, no que lhe concerne, ocorreu no mesmo ano, por meio de duas ligações internacionais providas por instituições acadêmicas, durante a Eco-92, a qual decorreu na cidade do Rio de Janeiro (KNIGHT, 2014).

Estes dois acontecimentos anteriores permitiram - junto à descontinuidade da NSFNET e do teste piloto da EMBRATEL -, portanto, que três anos depois, em 1995, a internet comercial fosse implementada internamente. A EMBRATEL logo efetivou o seu

serviço comercial, o que levantou um temor na comunidade brasileira da internet de que este organismo pudesse monopolizar a internet comercial do país. Como já explicitado anteriormente, contudo, a partir da metade dos anos 90, principalmente através do Governo Cardoso, o monopólio estatal perante as comunicações foi finalizado (KNIGHT, 2014). Somando-se a isso, o Ministério das Comunicações desse mesmo Governo decidiu que a EMBRATEL teria de encerrar suas atividades, quando no provimento de acesso a pessoas físicas (CARVALHO, 2006).

A partir daí, então, começaram a ser desenvolvidas novas legislações sobre o uso da internet dentro do Brasil, para também monitorar o seu próprio desenvolvimento, como foi o caso da criação do Comitê Gestor da Internet no Brasil (CGI.br)[103] em 1995, o qual seria responsável por coordenar e integrar todas as iniciativas de serviço da internet internas, além de promover qualidade técnica, inovação, e disseminação de serviços disponíveis (KNIGHT, 2014). Sem a competição da EMBRATEL e com a ampliação das possibilidades de serviços comerciais da Internet no país, começaram a surgir, paulatinamente, os provedores de acesso (CARVALHO, 2006).

Com uma infraestrutura ainda insuficiente para atender à demanda desses provedores e, principalmente, de seus usuários, muitos utilizadores ficaram impossibilitados de conectar-se à internet, ou seja, mesmo que alguns provedores conseguissem acesso a um *backbone*[104] de Internet, e à respectiva rede de suporte para transmissão de dados, não haviam linhas telefônicas suficientes para atender às chamadas de seus clientes (CARVALHO, 2006). Baseado nessas informações, portanto, a próxima seção pretende analisar se - e de que forma - o Brasil progrediu, quando na difusão das redes entre a sua população, quanto ao acesso às infraestruturas necessárias para tal, e quanto à politização e securitização da pauta cibernética.

4.2 DIFUSÃO DA INTERNET E SECURITIZAÇÃO DA PAUTA CIBERNÉTICA

Segundo Oliveira et al. (2017), o Brasil possuía, até 2014, um total de usuários equiparável à somatória de todos os demais usuários sul-americanos. Não sendo este um fato

[103] O CGI foi também o organismo responsável por dar suporte à recente internet comercial brasileira no tangente às cooperações de caráter público-privado (KNIGHT, 2014).

[104] Martins (2009) discorre que a palavra *backbone*, em inglês, significa literalmente "espinha dorsal". Esta ferramenta é assim identificada pois designa a rede principal por meio da qual os dados de todos os usuários da Internet passam. Ademais, é também por meio do *backbone* que torna-se possível enviar e receber dados entre as cidades brasileiras ou entre outros países e o Brasil (MARTINS, 2009).

recente, de certa forma, este país já começava a superar o número de usuários dos demais Estados da América do Sul no início do século XXI: o ápice dessa diferença se deu em 2006, quando o Brasil detinha 53,7 milhões de usuários, enquanto o restante do subcontinente totalizava 28 milhões. Em 2014, o Brasil retomou seu crescimento e superou novamente, em quantidade, os demais usuários sul-americanos (OLIVEIRA ET AL., 2017). Atualmente, a seu modo, o país detém 149 milhões de usuários das redes, com uma penetração total de 70,9% (INTERNET WORLD STATS, 2019c).

Apesar dessas estatísticas, a sociedade brasileira ainda não dispõe em sua totalidade de imersão digital. É visível essa limitação, por exemplo, ao defrontar-se com o fato de que metade da população brasileira apenas conseguiu acesso ao espaço cibernético após 2013, em razão da dificuldade de adesão dos brasileiros às novas tecnologias[105]. Ainda assim, desde 2002, o país apresenta uma penetração da internet superior à média dos demais países da América do Sul, ocupando a quarta posição em termos de população mais digitalizada nesta região (OLIVEIRA ET AL., 2017).

Com predominância da difusão de redes móveis entre a sua população, o Brasil obteve, em 2011, 20,9% de penetração móvel e 8,6% de penetração fixa. Três anos depois, em 2014, essa comparação era ainda mais díspar, já que a penetração móvel chegava à porcentagem de 78,1%, enquanto a penetração fixa, apesar de ter crescido, atingia apenas 11,5% da sociedade. A predominância de redes móveis, no que lhe concerne, sofre a influência do número de satélites que orbitam no seu espaço geoestacionário (OLIVEIRA ET AL., 2017).

Em termos do número de satélites, até 2017, o Brasil totalizava em sua órbita 15, sendo sete deles parte da iniciativa pública. Daqueles com propósitos de telecomunicações ou comunicações, apenas os pertencentes à família Brasilsat surgiram de demanda pública (OLIVEIRA ET AL., 2017). Com a privatização da EMBRATEL, nos anos 2000, esses satélites então públicos passaram às mãos do setor privado, o que Oliveira et al. (2017) interpretam, finalmente, como uma dependência deste país junto às empresas privadas nacionais e internacionais, quando para a realização de conexão móvel com o espaço

[105] De acordo com Diniz, Muggah e Glenny (2014), a atividade brasileira no espaço cibernético ainda reflete as desigualdades estruturais do país. Diferenças em termos de renda, de educação, e da própria influência da região geográfica determinam como e se a população terá acesso à internet. Por exemplo, até 2014, ano de publicação do artigo, 50% das famílias nos Estados do Rio de Janeiro, de São Paulo, e de Minas Gerais detinham acesso à internet, enquanto essa porcentagem despencava para 22%, analisando-se a região Norte (DINIZ; MUGGAH; GLENNY, 2014).

cibernético. O Quadro 3, disposto abaixo, ilustra de forma gráfica todos os satélites que orbitam no espaço geoestacionário brasileiro.

Quadro 3 - Satélites que orbitam o espaço geoestacionário brasileiro

Satélite	Operador	Lançador	Iniciativa	Propósito	Ano
Brasilsat B-2	Brasil	Europa	Pública	Comunicação militar	1995
Brasilsat B-3	Brasil	Europa	Pública	Comunicação	1998
Amazonas 3	Espanha	Rússia	Privada	Telecomunicações	2013
Brasilsat B-4	Brasil	Europa	Pública	Comunicação	2000
CBERS 4	China / Brasil	China	Pública	Observação da Terra	2014
Amazonas 1	Espanha	Rússia	Privada	Telecomunicações	2004
Amazonas 2	Espanha	Europa	Privada	Telecomunicações	2009
EOS-PM Aqua	Brasil / Japão / EUA	Brasil	Pública	Observação da Terra	2002
SCD-1	Brasil	EUA	Pública	Meteorológico	1993
SCD-2	Brasil	EUA	Pública	Meteorológico	1998
Star One C1	Brasil	Europa	Privada	Comunicação	2007
Star One C2	Brasil	Europa	Privada	Comunicação	2008
Star One C3	Brasil	Europa	Privada	Comunicação	2012
Star One C4	Brasil	Europa	Privada	Comunicação	2015
Estrela do Sul 2	Brasil / Canadá	Rússia	Privada	Comunicação	2011

Fonte: Oliveira et al. (2017)

Mesmo com a predominância desse tipo de conexão internamente, é importante ressaltar também o papel da comunicação promovida via cabos submarinos, a qual ainda é utilizada entre países e a qual já foi retratada previamente no capítulo anterior, para os casos de Estados Unidos e China. O Brasil dispõe, na contemporaneidade, de cinco Pontos de Tráfego (PTT)[106] de conexão via cabos submarinos: três no Sudeste (SE) e um no Nordeste (NE) (OLIVEIRA ET AL., 2017).

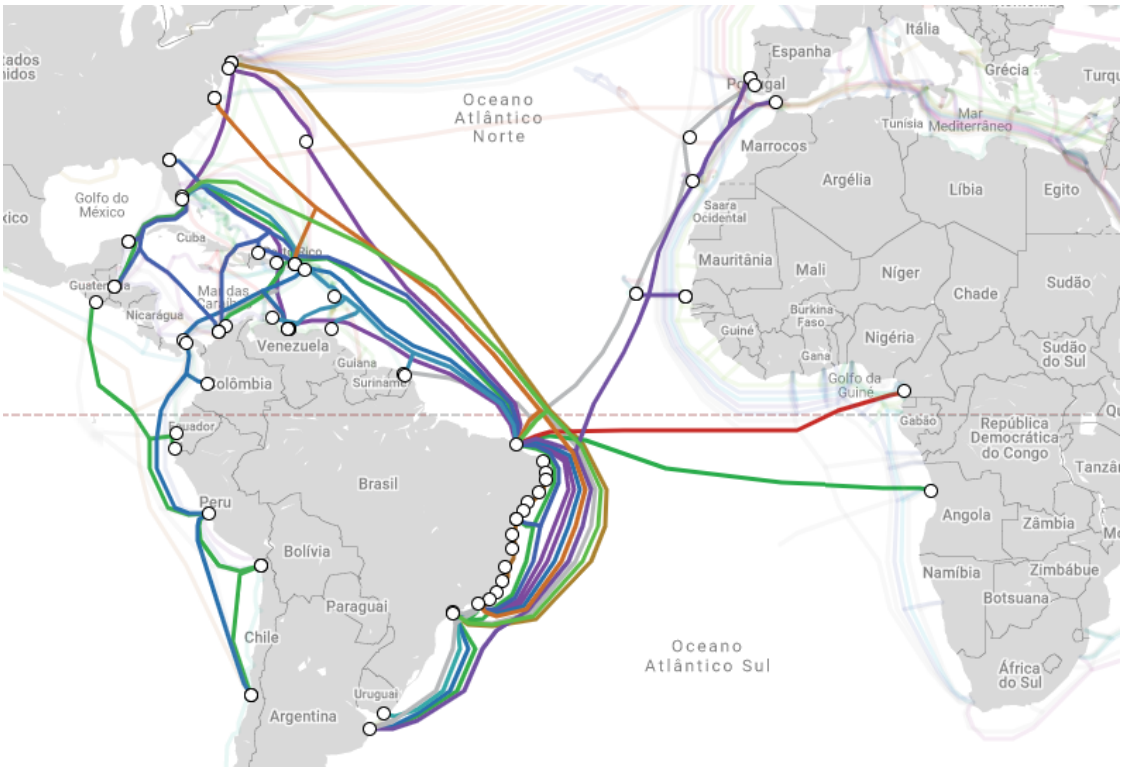
Os PTTs do Sudeste, especialmente os pertencentes à cidade de Santos (SP) e à de Praia Grande (SP), são os responsáveis pelas ligações com países vizinhos ao sul - e também pelas ligações desses países com os Estados Unidos. Enquanto isso, o PTT de Fortaleza, da região NE, faz a conexão com países e ilhas do norte da América do Sul e do Caribe, incluindo o Suriname e a Martinica, e países na Europa (Portugal) e na África (Angola) (OLIVEIRA ET AL, 2017). Ademais, uma das ligações mais atuais ao PTT de Fortaleza é o

[106] Os pontos de tráfego "consistem numa estrutura centralizada, onde várias redes podem se interligar. Dessa forma, não são necessários vários enlaces distintos para estabelecer relações de troca de tráfego com diferentes redes, mas apenas um enlace, para o PTT" (GETSCHKO; MOREIRAS, 2008, s.p.). Os PTTs não devem, contudo, serem confundidos com *backbones:* os primeiros são regionais, de caráter metropolitano, e não têm como função carregar o tráfego à grandes distâncias, mas sim melhorar os custos e a qualidade das conexões das redes de uma localidade comum (GETSCHKO; MOREIRAS, 2008).

cabo *South Atlantic Inter Link* (SAIL), o qual faz conexão direta com Camarões. Este projeto foi concluído em 2018, como fruto de investimento da empresa chinesa China Unicom e da empresa camaronesa Camtel. A construção por parte da engenharia, a seu modo, ficou à cargo da Huawei Marine Networks (TELEGEOGRAPHY, 2020a).

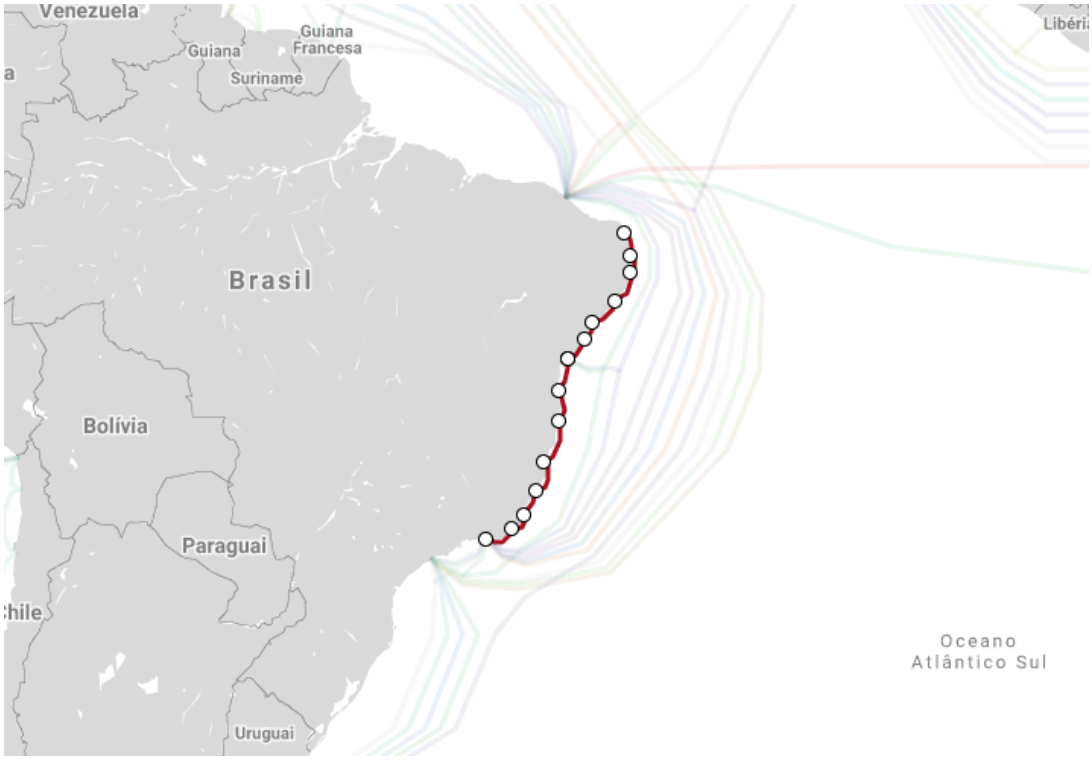
Em adição, o país detém um cabo estritamente brasileiro, o Brazilian Festoon, o qual interliga os principais Estados costeiros brasileiros, desde Rio de Janeiro à Natal. Neste contexto, tal cabo é muito importante em termos securitários, pois garante uma resiliência brasileira, caso os cabos de ligação anteriormente descritos sejam interrompidos (OLIVEIRA ET AL., 2017). Finalmente, dispõem-se abaixo duas figuras: a figura atualizada de todos os cabos submarinos com os quais o Brasil se liga atualmente; e a figura que apresenta exclusivamente as ligações permeadas pelo cabo Brazilian Festoon.

Figura 5 - Mapa dos cabos submarinos que conectam o território do Brasil a outros países do globo



Fonte: Telegeography (2020a)

Figura 6 - Cabo Submarino estritamente brasileiro: *Brazilian Festoon*



Fonte: Telegeography (2020b)

Como previsto, o aumento da dependência das informações de um país junto às infraestruturas cibernéticas, ou seja, do aumento da presença desse Estado no conjunto que conforma o espaço cibernético, aumenta sua susceptibilidade de sofrer ataques cibernéticos. O Brasil, o qual progrediu paulatinamente na inclusão de seus usuários na utilização das redes, portanto, não escapa dessas estatísticas, figurando como o país da América Latina que mais sofreu com ataques cibernéticos nos últimos anos[107] (OLIVEIRA ET AL., 2017). Neste sentido, faz-se importante destacar de que forma o país vêm reunindo esforços em matéria de segurança e defesa cibernética, intencionando a sua própria proteção, e também de seus usuários.

Como destaca Oliveira et al. (2017), as regulações e leis com relação ao tema cibernético são consideravelmente recentes no Brasil. Apesar de temas sobre privacidade serem abordados dentro da Constituição Federal - de 1988 - e do Código Civil, debates concernentes à proteção de dados, por exemplo, são mais recentes (OLIVEIRA ET AL., 2017). Em relação aos documentos de segurança e defesa cibernética, estes também vêm

[107] Além disso, o país ocupa a 3º posição do ranking mundial no tangente à realização de ataques cibernéticos (OLIVEIRA ET AL., 2017).

sendo pensados de forma mais institucionalizada a partir do século XXI (PAGLIARI; AYRES PINTO; BARROSO, 2020), período a partir da qual a estabilidade político-financeira do Brasil permitiu que este viesse a buscar maior representatividade do Estado junto à Comunidade Internacional, além de retomar investimentos em políticas de segurança e defesa, de acordo com seus objetivos estratégicos e geopolíticos (SOUZA; ALMEIDA, 2016). As definições e intenções propagadas por cada um desses documentos, por sua vez, serão debatidas na próxima seção.

É importante já ter em mente, antes de passar a esta, que a arquitetura cibernética brasileira ainda está em desenvolvimento. Entendendo as dificuldades estruturais do país (DINIZ; MUGGAH; GLENNY, 2014) - apesar do aumento da penetração da internet e da criação paulatina de estruturas capazes de suportá-la -, introduz-se o propagado nas palavras de Oliveira e Portela (2017), o qual será tratado de forma mais minuciosa a seguir: com relação às camadas existentes no espaço cibernético, o Brasil possui ainda hoje deficiência na camada de hardware, dado o baixo histórico de investimentos em Ciência e Tecnologia internamente; ademais, vem se posicionando como um dos maiores produtores de programas do mundo, no que tange ao software; e é conhecido pelos seus próprios *hackers*, que geralmente se colocam em boa posição, nas principais competições ciberespaciais do mundo, no correspondente ao seu ainda progressivo peopleware[108].

4.3 ESFORÇOS PROMOVIDOS FRENTE À SEGURANÇA E DEFESA CIBERNÉTICA

Conforme visto na primeira e na segunda seções deste capítulo, até o final dos anos 1990, documentos concernentes à segurança e defesa cibernética não haviam sido criados, e nem debates ou preocupações quanto aos riscos e às vulnerabilidades do espaço cibernético haviam sido observados ou estimulados, principalmente em razão da cibernética, no país, se encontrar em processo de formação e institucionalização, juntamente com as TICs. Ao perceber-se a importância de tal tecnologia para o país, há então uma institucionalização da questão, com designação gradual de capacidades e demarcação de conceitos (SOUZA; ALMEIDA, 2016).

[108] Como trabalhado no capítulo 1, o peopleware refere-se à camada superior do espaço cibernético, a qual compõe a dimensão cognitiva (VENTRE, 2012a). Em outras palavras, esta abrange as pessoas que interagem com a infraestrutura crítica de informação, ou seja, define-as como usuários participantes do ciberespaço (MANDARINO JR., 2010).

O marco doméstico para a politização da pauta é o ano 2000, quando é lançado o Livro Verde Sociedade da Informação no Brasil, pelo Ministério da Ciência e Tecnologia (SOUZA; ALMEIDA, 2016) do Governo Cardoso. Este documento, o qual apresenta "visão mais ampla para estabelecer contornos e diretrizes de um programa de ações rumo à Sociedade de Informação no Brasil" (SOUZA; ALMEIDA, 2016, p. 391), traça oportunidades e riscos de uma sociedade informatizada, além de, entre outros, entender a universalização dos serviços da internet como uma forma de cidadania, e explorar questões mais próximas ao P&D e à infraestrutura avançada (SOUZA; ALMEIDA, 2016).

Em matéria de segurança cibernética, foi publicado no mesmo ano o Decreto nº 3.505/2000, o qual instituiu a Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal (APF)[109] (SOUZA; ALMEIDA, 2016). Preocupado, sobretudo, com a proteção de dados e informações em termos de cibernética, o Governo também institucionalizou, por meio desse decreto, o Comitê Gestor em Segurança da Informação (CGSI) (PAGLIARI; AYRES PINTO; BARROSO, 2020).

Três anos depois, já na Gestão Lula, foi criado, por meio da Lei Federal nº 10.683/2003, o Gabinete de Segurança Institucional da Presidência da República (GSI/PR), o qual tinha como uma de suas atribuições a coordenação de atividades de inteligência federal e de segurança da informação (SOUZA; ALMEIDA, 2016). É, ainda hoje, este organismo o responsável pela segurança das infraestruturas críticas nacionais[110] (CARVALHO, 2011b) no âmbito da APF.

Para cumprimento da função de coordenação das atividades de Segurança da Informação, o GSI/PR possui dois órgãos subordinados, os quais o apoiam em nível organizacional. O primeiro deles, o Departamento de Segurança da Informação e Comunicações (DSIC), deve operacionalizar as atividades de Segurança da Informação e Comunicações (SIC) na APF, incluindo quando na representação do país junto à Organização dos Estados Americanos (OEA) em assuntos de terrorismo cibernético e quando na

[109] A seu turno, mais de uma década depois, entre os anos de 2015 e 2018, foi lançada a Estratégia de Segurança da Informação e Comunicação e de Segurança Cibernética da Administração Pública Federal, documento que intencionava dar suporte ao planejamento estratégico governamental durante esse período. Como parte da matriz de segurança cibernética, este documento respaldava o papel da segurança cibernética no Brasil, descrevendo a metodologia a ser utilizada na confecção da estratégia, e elaborando, por fim, um mapa estratégico que contemplasse objetivos e metas para a segurança cibernética no país (OLIVEIRA ET AL., 2017).

[110] Entre as áreas prioritárias, no tocante a estas infraestruturas críticas, estão o setor de energia, de telecomunicações, de transportes, de água, de finanças e de informação, sendo que este último permeia todos os anteriores, em razão de as infraestruturas críticas dependerem cada vez mais de redes de informação para sua gerência e controle (CARVALHO, 2011b).

administração do Centro de Tratamento e Respostas a Incidentes de Redes da APF (CTIR.Gov) (CARVALHO, 2011b).

O segundo, a Agência Brasileira de Inteligência (ABIN), tem como objetivo estratégico "desenvolver atividades de inteligência voltadas para a defesa do Estado democrático de direito, da sociedade, da eficácia do poder público e da soberania nacional" (CARVALHO, 2011b, p. 21). Uma de suas atribuições consiste na avaliação de ameaças internas e externas à ordem constitucional, incluindo em termos cibernéticos (CARVALHO, 2011b). Ademais, outros organismos também serviram para potencializar o surgimento da segurança cibernética no país, dentre eles, o brevemente introduzido Comitê Gestor da Internet, o Centro de Pesquisas e Desenvolvimento para Segurança das Comunicações (CEPESC), e o Núcleo de Informação e Coordenação do Ponto BR (Nic.br), o qual mantém o Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil (CERT.br) (SOUZA; ALMEIDA, 2016).

Apesar de os documentos oficiais e a criação dos órgãos citados anteriormente serem mais focados na área de segurança cibernética[111], é importante citá-los cronologicamente, pois, no entendimento Souza e Almeida (2016), até 2005, no Brasil, houve um processo de politização da temática - inicialmente tratada por segurança da informação. Não havia até então, portanto, uma preocupação com o tema em nível de ameaça existencial, e este configurava apenas um objeto de "preocupação inicial e de debate político" (SOUZA; ALMEIDA, 2016, p. 393).

A partir de 2005, com a Política de Defesa Nacional (PDN), estabelecida por meio do Decreto nº 5.484/2005, há as primeiras menções ao tema, com citações do termo "ataque cibernético". Essa PDN, por sua vez, também marca a ampliação da produção de documentos legais brasileiros, quando no fomento ao debate da Defesa Nacional, a qual inclui a segurança cibernética (SOUZA; ALMEIDA, 2016). Segundo o entendimento de Da Cruz Jr. (2013), portanto, se, por um lado, cabe ao GSI a gerência dos assuntos que afetam a segurança cibernética, por outro, o Ministério da Defesa, atribuindo a responsabilidade à esfera militar, deu principalmente ao Exército as funções de defesa cibernética. O primeiro documento que

[111] Ainda em matéria de segurança cibernética, é válido citar também o lançamento posterior do Livro Verde: Segurança Cibernética no Brasil, em 2010, o qual tinha como objetivo reunir propostas e diretrizes básicas quanto à temática (OLIVEIRA ET AL., 2017).

confirmou esta referência, assim posto, foi a Estratégia Nacional de Defesa (END), de 2008[112] (OLIVEIRA ET AL., 2016).

Esta END tem como principal objetivo a modernização da estrutura de defesa nacional, atuando a partir de três eixos: a reorganização das Forças Armadas; a reestruturação da indústria brasileira material de defesa; e a política de composição dos efetivos das Forças Armadas. Com relação especificamente ao primeiro eixo estratégico, este enumera no total, 23 diretrizes estratégicas, sendo que uma delas elenca três setores estratégicos de atuação, a saber, o nuclear, o espacial e o cibernético (SOUZA, 2013).

Em outras palavras, como posto por Souza (2013), tal Estratégia pauta esses três domínios como indispensáveis para a defesa nacional do Brasil, atribuindo a cada força o desenvolvimento de um destes setores. A Força Aérea, desta forma, deve ficar à frente das pesquisas na área espacial; a Marinha, se responsabilizar pelo desenvolvimento da tecnologia nuclear; e o Exército, pelo desenvolvimento do setor cibernético[113]. Sob esta última, pesa, portanto, o papel de defender o território cibernético nacional contra ameaças ciberexistenciais (SOUZA, 2013).

Ainda com relação a esta Estratégia, Oliveira et al. (2017) alegam que, nela, a defesa cibernética é tratada com finalidades indiretas e diretas. Indiretamente, esta geraria capacidade tecnológica autônoma ao país, a qual fomentaria, a seu turno, o desenvolvimento nacional. Importante para que as operações possam ocorrer em rede, a área cibernética também faz-se crucial para que este país latino-americano não dependa de tecnologias estrangeiras quando para a sua própria defesa. Diretamente, no que lhe concerne, este documento promulga que devem ser desenvolvidas capacidades industriais e militares na área cibernética, de modo a fomentar este tema na academia, na inteligência ou na defesa cibernética (OLIVEIRA ET AL., 2017).

Mais importante ainda para esta monografia, o documento traz um trecho que pauta como conseguir alcançar este desenvolvimento tecnológico e autonomia (OLIVEIRA;

---

[112] Para Oliveira e Portela (2017), a seu modo, a relevância deste documento está nele mesmo, já que consiste na primeira estratégia de defesa brasileira: a vocação pacifista do Brasil seria, em máxima instância, o maior impedimento, até então, para a promulgação de uma estratégia deste tipo, e as estratégias já publicadas somente direcionavam-se à guerra. Contudo, como a própria END reafirma, a defesa se faz necessária tanto para agressões quanto para prevenir ameaças (OLIVEIRA; PORTELA, 2017).

[113] Apesar disso, todas as demais forças também devem possuir as suas próprias estruturas de defesa cibernética, as quais atuarão em cooperação com o Comando de Defesa Cibernética (CDCiber) (OLIVEIRA ET AL., 2017), organismo este que será introduzido mais adiante.

PORTELA, 2017) - o que, como abordado no primeiro capítulo, envolveria as três camadas que circundam o espaço cibernético, a dizer, o hardware, o software e o peopleware:

> O futuro das capacitações tecnológicas nacionais de defesa depende mais da formação de recursos humanos do que do desenvolvimento de aparato industrial. Daí a primazia da política de formação de cientistas, em ciência aplicada e básica, já abordada no tratamento dos setores espacial, cibernético e nuclear (BRASIL, 2008, p. 13).

Depreende-se, portanto, que as capacitações humanas, ou seja, os recursos humanos, compreendidos pelo peopleware, seriam mais importantes para as capacitações tecnológicas nacionais de defesa do que o desenvolvimento de aparato industrial, este formado conjuntamente pelo hardware e pelo software[114] (OLIVEIRA; PORTELA, 2017). Esta Estratégia, revisada em 2012 (SOUZA; ALMEIDA, 2016), dando igualmente importância às capacitações tecnológicas para o país, acrescenta que, enquanto faltarem condições para o aprendizado, para o trabalho, e para a produção dos indivíduos, a independência tecnológica do país será impossível (OLIVEIRA; PORTELA, 2017).

A maior novidade da nova revisão de 2012 estaria conformada então no estabelecimento de prioridades para se alcançar as capacitações cibernéticas, seja para usos industriais, educativos ou militares, de forma a garantir a atuação em rede (OLIVEIRA; PORTELA, 2017). Dentre estas, pode-se citar como exemplo o "fortalecimento do Centro de Defesa Cibernética com capacidade de evoluir para o Comando de Defesa Cibernética das Forças Armadas" e o "desenvolvimento de sistemas computacionais de defesa baseados em computação de alto desempenho para emprego no setor cibernético e com possibilidade de uso dual"[115] (OLIVEIRA; PORTELA, 2017).

Dito isto, se faz crucial apresentar quais organismos se relacionam, na atualidade, com a área de defesa cibernética brasileira. Oliveira et al. (2017), com a mesma intenção, apresentam a estrutura do Sistema Militar de Defesa Cibernética, proposto na Doutrina Militar

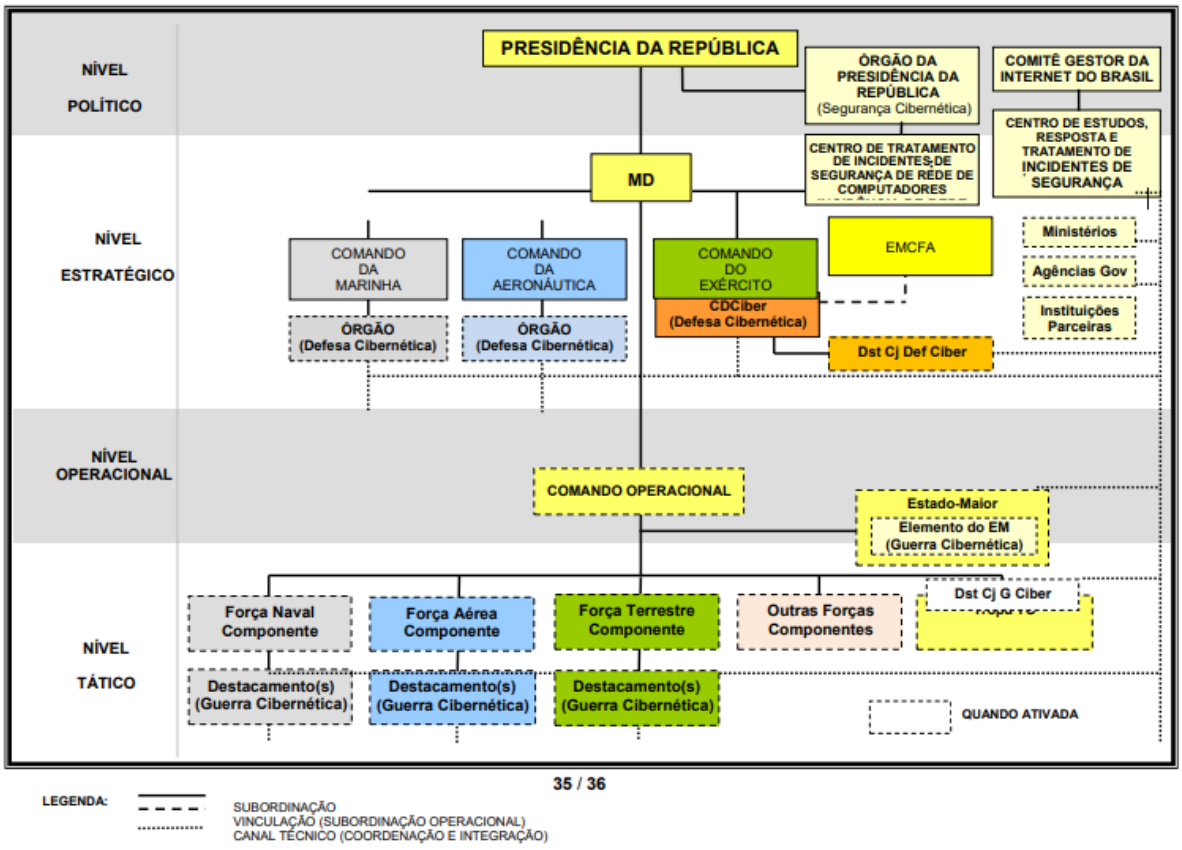
---

[114] Dando prosseguimento a esse entendimento, o atual Comandante de Defesa Cibernética, General de Divisão Guido Amin Naves, durante fala no XXI Ciclo de Estudos Estratégicos da Escola de Comando e Estado-maior do Exército (ECEME), em 2019, argue que "a cibernética não é intensiva em tecnologia, ela é dependente da tecnologia e o ambiente tecnológico é o nosso campo de batalha. A atuação nessa área requer conhecimento em conceitos bélicos e conceitos voltados à gestão administrativa" (AMIN NAVES, 2019, p. 31).

[115] Essa previsão de uso dual dos equipamentos de defesa cibernética instigava, a seu turno, maior rentabilidade para a indústria de defesa cibernética e uma possível independência tecnológica (OLIVEIRA; PORTELA, 2017). Contudo, ao contrário desta, a minuta do mesmo documento de 2016 não observava o uso dual e industrial no setor cibernético, dando ênfase majoritária à relação necessária entre ambientes militar e civil (OLIVEIRA; PORTELA, 2017). Finalmente, os avanços da indústria cibernética brasileira serão abordados de forma mais detalhada na próxima seção.

de Defesa Cibernética de 2014[116]. Visando aprofundar esta discussão, esta monografia também aproveita tal estrutura, que está representada abaixo.

Figura 7 - Estruturas e órgãos na concepção do Sistema Militar de Defesa Cibernética



Fonte: Ministério da Defesa do Brasil, 2014, p. 35

Obedecendo a uma relação permeada por níveis estratégicos, como visto na figura 7, a defesa cibernética no Brasil divide-se em quatro níveis: o nível político; o nível estratégico; o nível operacional; e o nível tático. Em nível político, os principais organismos são a Presidência da República, o GSI e o Comitê Gestor da Internet - estes dois últimos explicitados anteriormente, já que são dedicados à parte de segurança cibernética. As estruturas diretamente dedicadas à defesa cibernética, a seu turno, estão localizadas no nível estratégico. Aqui, encontramos o Ministério da Defesa, os organismos de defesa cibernética próprios de cada Força de combate, o Estado-Maior Conjunto das Forças Armadas (EMCFA) e o Destacamento Conjunto de Defesa Cibernética (OLIVEIRA ET AL., 2017). Com destaque

[116] Por ser uma doutrina militar, tal documento engloba, de forma geral, aspectos mais técnicos e operacionais sobre as ações militares em defesa cibernética (OLIVEIRA ET AL., 2017).

principal para a estrutura do Comando do Exército, objetiva-se explorar a seguir o papel do Centro de Defesa Cibernética (CDCiber), subordinado a este.

Apesar de não ter sido mencionado na END de 2008, o Centro de Defesa Cibernética foi ativado em agosto de 2010. Em 2012, com a atualização da END, previa-se que o Centro passaria a ser subordinado ao Comando de Defesa Cibernética (ComDCiber), fato este que apenas se materializou em 2016 (OLIVEIRA; PORTELA, 2017). De qualquer forma, é importante compreender que o ComDCiber[117] é um Comando Conjunto, e que o CDCiber é o seu braço operacional[118] (AMIN NAVES, 2019). Por último, no que corresponde ao nível tático, estão os destacamentos de guerra cibernética dos componentes operacionais de cada força. Com papel semelhante ao Destacamento Conjunto de Defesa Cibernética, estas são as unidades de linha de frente que devem lidar com a guerra cibernética (OLIVEIRA ET AL., 2017).

Após a compreensão do papel dos organismos brasileiros que se ocupam da defesa cibernética, consequentemente, deve-se voltar aos demais documentos de defesa já institucionalizados no Brasil, vislumbrando entender também de que forma estes exploram a questão cibernética. Além da END, constam no arcabouço brasileiro a Política Nacional de Defesa (PND) - a primeira PND, datada de 2005[119], já abordada acima - e o Livro Branco de Defesa Nacional[120][121].

---

[117] Sob a estrutura do ComDCiber, estão também o Departamento de Gestão Estratégica e a Escola Nacional de Defesa Cibernética (ENaDCiber), ativada em fevereiro de 2019 (AMIN NAVES, 2019). A ENaDCiber tem como missão "fomentar e disseminar as capacitações necessárias à Defesa Cibernética, no âmbito da Defesa Nacional, bem como contribuir com as áreas de pesquisa, desenvolvimento, operação e gestão de Defesa Cibernética e para a melhoria da qualificação da mão de obra nacional para o setor" (REDAÇÃO DEFESATV, 2019, s.p.).

[118] Apesar de pertencer ao Exército, o CDCiber atua sob orientação e supervisão direta do Ministério da Defesa. Este organismo, por sua vez, tem como uma de suas funções principais o fomento à integração técnica com outras instituições que contém atividades de cibernética (OLIVEIRA ET AL., 2017). Entre essas instituições, estão "o CERT.br, os órgãos das outras Forças que lidam com o tema, os Ministérios e as demais agências da Administração Pública" (OLIVEIRA ET AL., 2017, p. 74). Finalmente, o CDCiber foi o órgão responsável pela proteção das redes em eventos como a Rio+20, além de ter se envolvido na coordenação de segurança cibernética durante a Copa do Mundo de 2014 (DINIZ; MUGGAH; GLENNY, 2014).

[119] Em 2012, a Política de Defesa Nacional (PDN) foi renomeada para Política Nacional de Defesa (OLIVEIRA; PORTELA, 2017). Para estes autores, este fato demonstrou que a PND não se tratava "somente de um documento setorial do Ministério da Defesa para as forças singulares, mas de um documento que orientaria todos os setores envolvidos na segurança e defesa nacional" (OLIVEIRA; PORTELA, p. 83).

[120] Aqui, vale acrescentar que, dois anos depois da publicação da END de 2008, o Congresso Nacional brasileiro decretou a Lei Complementar nº 136/2010, a qual, entre outros fatores, impactou na publicação dos documentos de defesa do Brasil (OLIVEIRA; PORTELA, 2017). Em um de seus artigos, esta lei estabelece que, a cada quatro anos, a partir de 2012, o "Poder Executivo deve encaminhar para o Congresso Nacional atualizações de três documentos de defesa, a saber, a Política de Defesa Nacional, a Estratégia Nacional de Defesa e o Livro Branco de Defesa Nacional" (OLIVEIRA; PORTELA, 2017, p. 82).

A PND de 2012, no que lhe concerne, tem como objetivo "orientar, no âmbito do Ministério da Defesa, as atividades de Defesa Cibernética, no nível estratégico, e de Guerra Cibernética, nos níveis operacional e tático, visando a consecução dos seus objetivos" (OLIVEIRA ET AL., 2017, p. 70). Ademais, esta acrescenta uma abordagem do espaço cibernético com relação ao ambiente internacional, postulando o entendimento de que o desenvolvimento e a autonomia nacionais só podem ser alcançados a partir do domínio paulatino de tecnologias sensíveis internamente, sem que haja interferência estrangeira (OLIVEIRA; PORTELA, 2017).

Contudo, como na END de 2016, a minuta da PND, lançada no mesmo ano, discorda de tratativas anteriormente estabelecidas, entendendo o espaço cibernético dentro do ambiente nacional. Para Oliveira e Portela (2017), portanto, a partir dessas discordâncias, pode-se interpretar que as minutas lançadas em 2016 apresentam caráter mais crítico e real sobre a condição da defesa no Brasil, se comparados com as versões anteriores. Isso pode ser exemplificado com relação à temática da independência tecnológica, vista na PND de 2012 como almejada, e na minuta da mesma, de quatro anos depois, como uma impossibilidade, dados os recursos orçamentários escassos e a ausência de regularidade para aquisição de produtos de defesa (OLIVEIRA; PORTELA, 2017).

Finalmente, o Livro Branco de Defesa Nacional (LBDN) de 2012 visava - somado à END e à PND -, ser um documento que esclarecesse as atividades de defesa do Brasil. Entre alguns dos tópicos tratados no Livro, estão o fomento à Base Industrial de Defesa (BID)[122] e o fomento à inovação, além do entendimento de que o Brasil precisa passar a produzir componentes críticos, de modo a garantir sua própria independência tecnológica: a defesa cibernética é, isto posto, um projeto prioritário de equipamentos (OLIVEIRA; PORTELA, 2017).

Neste sentido, o Projeto de defesa cibernética para o Exército, disposto nesta versão, previa quatro ações específicas: a construção de sede para o CDCiber e a aquisição de

---

[121] Além disso, constam neste arcabouço documentos exclusivos em matéria de defesa cibernética, a exemplo da Doutrina Militar de Defesa Cibernética, de 2014, trabalhada anteriormente, e da Política Cibernética de Defesa, de 2012, que objetiva orientar, em todos os níveis estratégicos aqui explorados, a defesa cibernética no âmbito do Ministério (OLIVEIRA ET AL., 2017).

[122] Amarante (2012, p. 11), define a Base Industrial de Defesa (BID) como "a infraestrutura de Ciência, Tecnologia e Inovação (C,T&I) dedicada à produção e ao "abastecimento" da tecnologia militar para as Forças Armadas". O site do Ministério da Defesa do Brasil (2020, s.p.), a seu turno, define a BID como "o conjunto das empresas estatais ou privadas que participam de uma ou mais etapas de pesquisa, desenvolvimento, produção, distribuição e manutenção de produtos estratégicos de defesa – bens e serviços que, por suas peculiaridades, possam contribuir para a consecução de objetivos relacionados à segurança ou à defesa do país."

infraestrutura de apoio; a aquisição de equipamentos e a capacitação de recursos humanos; aquisições de soluções de hardware e software de defesa cibernética; e a implantação dos projetos estruturantes do Setor Cibernético. Com previsão de curto prazo pelo Livro Branco, estes projetos intencionavam abranger as três camadas do espaço cibernético. Para tanto, seriam previstos gastos de R$839,9 milhões até 2031, com período final de execução até 2035 (OLIVEIRA; PORTELA, 2017).

Todavia, como demonstrado na fala do Gen. Amin Naves (2019), no Brasil, a série histórica de orçamentos para a área de defesa cibernética tem sido baixa. Enquanto o setor nuclear e o setor espacial possuem orçamentos anuais de R$1,2 bilhões e R$900 milhões, respectivamente, o setor cibernético opera atualmente com um orçamento de R$7 milhões anuais[123]. Atribuindo este orçamento baixo a uma demanda até então não estruturada, o General estima que, para operar com as capacidades necessárias, devam ser necessários recursos na ordem de R$150 milhões anuais (AMIN NAVES, 2019).

Por último, deve-se acrescentar, ainda, dois tópicos que compõem a gama contemporânea da área de cibernética brasileira: O Marco Civil da Internet; e alguns dos acordos de cooperação internacional que incluem a segurança e a defesa cibernéticas. O primeiro, uma legislação que se põe à disposição tanto da segurança, quanto da defesa cibernéticas, estabelece princípios, garantias, direitos e deveres para o uso da internet no país. Como parte do debate mais recente no que concerne à proteção de dados, e desenvolvido a partir de um processo participativo, o Marco Civil estabelece princípios fundamentais para a utilização da internet pelos usuários, incluindo no tangente à liberdade de expressão, à neutralidade das redes, e à proteção da privacidade[124] (DINIZ; MUGGAH; GLENNY, 2014).

O segundo, no que lhe diz respeito, divide-se em duas vertentes[125]. Os acordos de segurança cibernética, em geral, tratam da troca e proteção mútua de informações

[123] Em termos do dispêndio do PIB de 2018, contabilizado nessa monografia, os três setores estratégicos, nuclear, espacial e cibernético, totalizaram o percentual de investimentos na ordem de 0,06%, 0,05% e 0,00038%, respectivamente. Deste modo, interpreta-se que, apesar de os três setores serem considerados de alta importância para o desenvolvimento das próprias Forças Armadas, pouco investimento é destinado a estes.

[124] Diniz, Muggah e Glenny (2014, p. 21, *tradução nossa*) reiteram que "enquanto a intenção original do Marco Civil era a de estabelecer garantias e proteções constitucionais relativas à administração do espaço cibernético brasileiro, este também se tornou um ímpeto para a legislação preventiva quanto aos crime cibernéticos".

[125] O Brasil possui algumas aproximações em matéria de segurança e defesa cibernéticas com os Estados Unidos e também com a China. Aqui, para o primeiro caso, destaca-se o Convênio para Intercâmbio de Informações em Pesquisa e Desenvolvimento (MIEA), de 2017, fundamental para que os dois países levassem adiante a sua parceria em projetos de desenvolvimento tecnológico, e o Memorando de Entendimento (MdE), de 2016, que formalizava a cooperação em segurança cibernética entre os dois Estados (FAGUNDES ET AL., 2019). Para o caso chinês, no que lhe concerne, a temática da segurança cibernética é discutida no âmbito multilateral do BRICS.

classificadas, ou seja, de informações sigilosas que trafegam no espaço cibernético. Aqui, o Brasil coopera com países como Portugal (2005), Espanha (2007), Rússia (2008), Israel (2010) e Suécia (2014). Entre os acordos de defesa cibernética, por sua vez, destacam-se três: o acordo com a Suécia, de 2014, que inclui as três forças e procura identificar possibilidades de cooperação em defesa cibernética; o acordo com a Índia, de 2015, específico na temática de ciência e tecnologia, e o qual prevê o intercâmbio acadêmico de militares na área da defesa cibernética, no âmbito da Aeronáutica e do Exército; e a cooperação com a Argentina, que, apesar de não ser um acordo institucionalizado, permite que os dois países se encontrem para debater a defesa cibernética de ambos (OLIVEIRA ET AL., 2017). Além disso, o Brasil iniciou seu processo de adesão à Convenção de Budapeste em julho de 2019[126] (ITAMARATY, 2019).

Em conclusão, pode-se, portanto, interpretar a institucionalização paulatina de documentos de segurança e de defesa cibernética no Brasil como uma consequência da percepção pelo Estado da potencialidade e dos riscos de ataques cibernéticos às infraestruturas críticas e da segurança da informação no país. Ademais, entende-se que a tratativa da segurança pelo Estado Brasileiro apresentou uma evolução ao longo dos anos, caminhando para uma possível securitização no momento atual[127] (SOUZA; ALMEIDA, 2016).

Neste sentido, interpreta-se que a trajetória brasileira com relação à inserção da internet e à securitização do espaço cibernético torna-se ambígua. Ao mesmo tempo, esta contém avanços, a exemplo da inserção progressiva da população na estrutura que conforma o ciberespaço, da criação contínua de documentos e de organismos destinados à segurança e defesa cibernética e da presença de um cabo submarino exclusivamente brasileiro, o que lhe concede proteção e resiliência, caso hajam interrupções nos demais cabos de ligação ao qual este se conecta (OLIVEIRA ET AL., 2017).

---

[126] Vale reiterar que o Brasil foi convidado a aderir à Convenção de Budapeste neste mesmo ano, durante a Gestão Bolsonaro. Este convite surgiu após a iniciativa do Ministério da Justiça e da Segurança Pública, em conjunto com os esforços de um Grupo de Trabalho constituído para este fim (o qual envolvia organismos como o Ministério das Relações Exteriores, a Polícia Federal, o Gabinete de Segurança Institucional da Presidência da República, A Agência Brasileira de Inteligência, entre outros). Além disso, essa demanda também se soma a legislações internas já existentes, a exemplo do Marco Civil da Internet e da Lei nº 12.737/2012 (também conhecida como Lei Carolina Dieckmann, que dispõe sobre a tipificação criminal de delitos informáticos).

[127] Souza (2013) conclui em sua dissertação que o Brasil securitiza as ameaças ciberespaciais no século XXI. Para além, o mesmo autor entende que os Estados Unidos, se em comparação com outros países, inclusive o Brasil, está na dianteira do desenvolvimento dos arsenais cibernéticos (SOUZA, 2013). Entenderemos essas discrepâncias entre esses dois atores, a seu modo, na última seção do capítulo.

Por outro lado, o país possui recursos orçamentários escassos e não detém regularidade quando na aquisição de produtos da área de defesa (OLIVEIRA; PORTELA, 2017), destinando orçamento de defesa anual considerado baixo para a otimização da área cibernética (AMIN NAVES, 2019) e dependendo tecnologicamente de países estrangeiros. Para mais, Diniz, Muggah e Glenny (2014) argumentam que o foco das autoridades públicas, versado não apenas à criminalidade cibernética doméstica e ao ativismo cibernético, mas também à expansão da capacidade estatal de mitigar ameaças cibernéticas internacionais, pode ser errôneo. Isso pois, o investimento em respostas militarizadas, no caso brasileiro, é incomensurável com as reais ameaças que o país e sua sociedade realmente enfrentam: este, comparativamente, possui poucas ameaças externas - advindas de governos estrangeiros e de grupos terroristas -, enquanto sua criminalidade cibernética e protestos digitais estão em ascensão, mas não recebem tanta atenção e investimentos financeiros (DINIZ; MUGGAH; GLENNY, 2014).

Isto posto, a última seção deste capítulo, a decorrer a seguir, intenciona entender quais são as capacidades em defesa cibernética brasileiras perante o cenário internacional, aqui representado pelos seus expoentes Estados Unidos e China. A partir das particularidades do caso brasileiro abordadas até este momento, portanto, buscar-se-á verificar de que forma os dois casos anteriores lhe servem para o entendimento de suas próprias forças e fraquezas, além de verificar se lhe cabem de molde em termos de perspectivas futuras.

4.4 O BRASIL FRENTE AOS MODELOS CHINÊS E ESTADUNIDENSE: “QUEM SOMOS E PARA ONDE VAMOS?”

O primeiro entendimento que se deve ter, ao explorar os três casos conjuntamente, é de que os Estados Unidos foi o país pioneiro na realização do que se conhece atualmente como internet, entre os anos 1970 e 1990 (CASTELLS, 2003), enquanto a China introduziu esta mesma tecnologia em 1994, com propósitos de pesquisa e científica, a partir de uma rede piloto (SCIO, 2010), e o Brasil ligou-se às redes pela primeira vez de forma global durante a Eco-92, em 1992 (KNIGHT, 2014). Argumenta-se novamente que este deve ser o entendimento inicial pois, é a partir da inserção da internet em um Estado que torna-se possível politizar e securitizar a pauta da segurança e da defesa de suas redes.

A partir dessa assimilação, interpreta-se, em segundo lugar, que os primeiros esforços militares em matéria de defesa cibernética também aconteceram em momentos díspares nos

três Estados. Enquanto os Estados Unidos começou a incluir o componente de informação em seus documentos de doutrina no pós-Guerra do Golfo, a partir de 1991 (CAVELTY, 2008), a China, influenciada pela própria atuação estadunidense nesta Guerra e em outras operações subsequentes, conformou o entendimento de que deveria absorver as mudanças na forma de guerrear (LYU, 2019), implementando planos de guerra de informação a datar de 1995 (HUGHES, 2003). O Brasil, por último, começou a tratar da temática com visão securitizadora apenas no século XXI, em 2005, com a publicação da então Política de Defesa Nacional, que mencionou pela primeira vez o termo "ataque cibernético" em um documento militar (SOUZA; ALMEIDA, 2016).

A partir dessas duas primeiras informações, portanto, conclui-se que, apesar de a China e o Brasil terem seguido os Estados Unidos, e implementado as redes em seus países em épocas similares - e com objetivos semelhantes, inicialmente versados à pesquisa científica -, a China começou a politizar e securitizar a temática ainda no século passado, enquanto o Brasil, em razão da cibernética estar em processo lento de formação e institucionalização no país, junto com as TICs, não possuía discussões nesse sentido até o fim dos anos 90[128] (SOUZA; ALMEIDA, 2016). Soma-se tal processo prolongado às desigualdades estruturais presentes no país, determinantes para o nível de atividade brasileira no espaço cibernético - indicadores como educação, influência da região geográfica, e renda influenciam se e de qual modo a população terá acesso às redes (DINIZ; MUGGAH; GLENNY, 2014) -, as quais podem ser demonstradas no fato de que metade da população brasileira conseguiu seu primeiro acesso a este espaço depois de 2013[129] (OLIVEIRA ET AL., 2017).

Em termos do conteúdo dos documentos militares criados por estes três Estados no presente século, algumas conclusões também podem ser delineadas: é visível, já à primeira vista, que todos estes levam em conta a importância do uso da tecnologia neste novo domínio. Ao discorrer sobre os Estados Unidos, Cavelty (2008) reitera que, sob o Governo W. Bush, começa-se a apresentar a tecnologia como um possibilitador, ao invés de visualizá-la como uma fonte de vulnerabilidades. Além disso, na Estratégia para operar no Espaço Cibernético,

[128] Apesar de a internet comercial ter sido implementada no país em 1995, como tratado anteriormente por Knight (2014), a infraestrutura até então existente era insuficiente para atender a demanda dos provedores e dos usuários de internet.

[129] Não se pode esquecer, inclusive, que apesar de, na contemporaneidade, um total de 70,9% da população brasileira ter acesso à internet (INTERNET WORLD STATS, 2019c), a predominância da penetração das redes ainda é móvel (OLIVEIRA ET AL., 2017).

idealizada mais de meia década depois, há o reforço a este pensamento, já que atribui-se ao DoD a missão de alavancar a engenhosidade da nação através de força de trabalho de alto nível e de rápida inovação tecnológica (DoD, 2011).

A China, por sua vez, desde a implementação das redes em seu país, já conformava em seu pensamento acadêmico a necessidade de defender-se de forma efetiva e, portanto, de atentar-se ao fato de que as tecnologias passavam a desempenhar papéis críticos (LYU, 2019). Em vista disso, há cada vez mais a conformação do entendimento de que é através da "informatização" que se torna possível aprimorar as Forças Armadas, as quais passam a obter a possibilidade de operar armas e equipamentos militares de grande porte tecnológico (SCIO, 2004).

No caso brasileiro, desde a Estratégia Nacional de Defesa de 2008 - que tinha como objetivo máximo a modernização da estrutura de defesa nacional, incluindo quando na reestruturação da indústria brasileira material de defesa - (SOUZA, 2013), a defesa cibernética era vista como uma possibilitadora, dado que ela indiretamente traria capacidade tecnológica ao país, que, a seu turno, fomentaria o seu desenvolvimento nacional (OLIVEIRA ET AL., 2017). Por conseguinte, os documentos seguintes, incluindo a END, a PND e o Livro Branco de 2012, reforçam o desenvolvimento e a autonomia nacionais do Brasil como somente possíveis a partir do domínio paulatino de tecnologias sensíveis (OLIVEIRA; PORTELA, 2017).

Contudo, apesar de os três países atribuírem importância ao uso da tecnologia no espaço cibernético para defender-se, entende-se que estes estão em patamares diferentes quando no desenvolvimento destas. Como abordado no capítulo anterior, apesar da atual impossibilidade chinesa de autossuficiência no desenvolvimento de tecnologias críticas (LYU, 2019) - muitos sistemas governamentais do país ainda dependem de hardwares e softwares ocidentais (INKSTER, 2010) -, esta tem fortalecido seu sistema nacional de inovação e acelerado sua industrialização, abrindo espaço para o desenvolvimento tecnológico e para os esforços de inovação nas empresas de porte pequeno e médio[130] (CASSIOLATO, 2013). São exemplos de resultados concretos o seu próprio sistema operacional, intitulado de Kylin, e o desenvolvimento de microprocessador para servidores e roteadores da Huawei (MOREIRA; CORDEIRO, 2014). Ademais, em termos específicos de empresas atuantes em

[130] Aqui, reitera-se a já explorada ligação intrínseca entre a questão militar e as políticas industriais e tecnológicas (CASSIOLATO, 2013).

tecnologia da informação e comunicação, destacam-se a Huawei, a Lenovo (YUEN, 2015), o Alibaba Cloud, o Baidu, o TikTok e o Wechat (SCMP RESEARCH, 2020).

Os Estados Unidos, novamente como parte principal da dianteira deste tipo de esforços, possui forte colaboração entre a designada tríade indústria-militares-academia, parceria que utiliza-se do conhecimento tecnológico da academia, da base material proveniente da iniciativa privada, e do estímulo e da orientação política advindos do Estado (MOREIRA JR., 2014). Além disso, a utilização global de ferramentas como o Google, do sistema Microsoft, da cadeia da Amazon (SCMP RESEARCH, 2020), e das tecnologias criadas pela Cisco e pela Apple (YUEN, 2015), contribuem para o entendimento da sua influência no que se concebe como internet global e, sobretudo, com relação à predominância do inglês como idioma presente em grande parte das páginas da *web*[131].

O Brasil, a seu turno, voltou a dar maior suporte às políticas de P,D&I a partir do começo deste século, quando, em 2005, a indústria nacional de defesa tornou a ter maior espaço na pauta das políticas públicas do governo, culminando na criação da Comissão Militar da Indústria de Defesa (CMID)[132] pelo Ministério da Defesa, e na criação da Política Nacional da Indústria de Defesa (PNID)[133]. Em adição, os Governos, à época, lançaram mão de outras ações institucionais, a exemplo da Política de Desenvolvimento Produtivo (PDP), em 2008, a qual tornou o complexo industrial de defesa um dos Programas Mobilizadores em Áreas Estratégicas, e da Lei nº 12.598, de 2012, a qual estabelece normas especiais para as compras, as contratações e o desenvolvimento de produtos e de sistemas de defesa, além de dispor sobre regras de incentivo à área estratégica de defesa[134] (MOREIRA; CORDEIRO, 2014).

---

[131] Exprime-se tal predominância principalmente pelos Estados Unidos figurar como o país que concebeu a internet, como reitera Guesser (2007, p. 86) através da frase "a origem de nascimento da Internet, entretanto, conferiu a ela, juntamente com a nacionalidade, a sua língua materna". Para além disso, proferido através das palavras do mesmo autor, soma-se o fato de que "(...) a anglofonia no mundo não corresponde a um cenário que atenda a critérios de maioria; entretanto o inglês é hoje indiscutivelmente considerado, no universo dos países ocidentais, como a língua hegemônica, chegando-se a atribuir a ela, muitas vezes, o status de língua franca, como no caso da literatura acadêmica e no âmbito de operação de trocas científicas, o que faz alguns teóricos afirmarem que "o inglês é a língua da ciência" (GUESSER, 2007, p. 81). Contudo, entende-se que, apesar de o inglês ainda desempenhar atualmente papel hegemônico, esse status está declinando progressivamente no âmbito do espaço cibernético, em razão de haver, em muitos casos - como no caso africano -, uma crescente valorização de línguas locais quando na utilização e produção de conteúdo na internet (GUESSER, 2007).

[132] O CMID compõe um "Espaço permanente de diálogo entre o governo e a indústria bélica" (MOREIRA; CORDEIRO, 2014, p. 103).

[133] O PNID "Estabelece diretrizes destinadas a incentivar esta indústria" (MOREIRA; CORDEIRO, 2014, p. 103).

[134] Ademais, como posto por Moreira e Cordeiro (2014), essa regulamentação possibilitou o credenciamento de Empresas Estratégicas de Defesa (EED), a homologação de Produtos Estratégicos de Defesa (PED) e,

Em termos especificamente do investimento industrial cibernético, Moreira e Cordeiro (2014) reiteram que o setor cibernético brasileiro deve aproveitar-se do caráter dual dessa área. Assim, alguns projetos que estão em andamento atualmente - alguns dos quais já supracitados -, e os quais merecem ser citados, são: a criação da Escola Nacional de Defesa Cibernética (ENaDCiber), com missão de capacitar profissionais para exercerem funções no ramo cibernético; a criação do Rádio Definido por Software (RDS), uma parceria entre o Centro Tecnológico do Exército (CTEx) e a Odebrecht Defesa, que proporcionará ligações seguras para as três forças, caso envolvidas em ambientes de conflito cibernético; e a criação do antivírus Defesa.br, com colaboração entre a empresa Bluepex e o Exército, produto que visa a segurança digital para as empresas brasileiras (MOREIRA; CORDEIRO, 2014). Outrossim, em 2013, o Exército desenvolveu, em parceria com a TI Decatron, o primeiro Simulador Nacional de Operações Cibernéticas (Simoc), visando auxiliar as tropas brasileiras em treinamentos contra uma possível guerra cibernética (CANAL TECH, 2013).

Apesar desses avanços, contudo, entende-se que grande parte da tecnologia disponível nos setores críticos da sociedade brasileira, como é o caso do sistema financeiro, ainda são provenientes de atividade de importação, a exemplo de hardwares e softwares de gerenciamento de rede e de sistemas de segurança (MOREIRA; CORDEIRO, 2014). É neste sentido que tal independência tecnológica brasileira, vista como almejada em documentos já abordados - tais quais a END de 2008 e de 2012, a PND de 2012 e o Livro Branco de 2012 -, é entendida, na minuta da PND de 2016, como uma impossibilidade, em razão de os recursos orçamentários destinados para a defesa serem escassos, e pela própria ausência de regularidade quando na aquisição de produtos de defesa pelo país (OLIVEIRA; PORTELA, 2017).

Ademais, a END de 2008 nos acrescenta um ponto extremamente relevante com relação à produção de capacidades cibernéticas em termos de hardware, software e peopleware: estas dependeriam mais da formação de recursos humanos do que do desenvolvimento de aparato industrial (OLIVEIRA; PORTELA, 2017), ou seja, mais da última de que das duas primeiras[135]. Daí a necessidade da política de formação de cientistas, e

finalmente, o mapeamento das cadeias produtivas do setor. Esta também permitiu "estimular as compensações tecnológicas, industriais e comerciais e fomentar o conteúdo nacional da Base Industrial de Defesa (BID), bem como incrementar a pauta de exportações de produtos de defesa" (MOREIRA; CORDEIRO, 2014, p. 104).

[135] A Estratégia Internacional para o Espaço Cibernético, institucionalizada pelos EUA em 2011, segue a mesma linha de pensamento: a segurança e a defesa cibernéticas estão mais relacionadas, portanto, à capacitação de pessoal, também chamada de capacidade intelectual, do que à aquisição de produtos e equipamentos (DA CRUZ JR., 2013).

de ciência aplicada e básica[136], pois, enquanto faltassem condições para o trabalho e para a produção dos indivíduos, a independência tecnológica do Brasil seria impossível, como predispõe a END de 2012 (OLIVEIRA; PORTELA, 2017).

A partir deste ponto, pode-se deduzir algumas informações com relação à abordagem dos três países junto às entidades que governam o espaço cibernético. Como anteriormente tratado, a China preza pelos Estados como as entidades governantes máximas no ciberespaço, estes devendo então agir sobre seus cidadãos, sobre os cidadãos estrangeiros e sobre as Organizações, para reivindicar a sua soberania neste espaço (HSU; MURRAY, 2014). Os Estados Unidos, a seu turno, mesmo entendendo que medidas coercitivas poderão ser tomadas pelo Governo contra o setor privado, para garantir a estabilidade e a segurança de suas redes internas (DA CRUZ JR., 2013), preza continuamente em suas Estratégias pela proteção conjunta do espaço cibernético, reunindo, em coordenação, tanto atores estatais quanto privados, além do povo americano (THE WHITE HOUSE, 2003).

Neste cenário, de acordo com Zeng, Stevens e Chen (2017), o Brasil aproxima-se mais do modelo chinês, figurando como um país que suporta um regime orientado pela soberania, ou, em outros termos, pela linha tradicional do Estado ao centro. Tal argumento pode ser reforçado por uma série de demonstrações, como o fato de a temática estar centralizada, desde o princípio, à figura do Estado[137] - abrangendo, portanto, setor privado e academia apenas em arcabouços teóricos e práticos dos últimos anos, como visualizado por meio da Lei nº 12.598, de 2012, que visava fomentar a BID (MOREIRA; CORDEIRO, 2014), e pela ativação da ENaDCiber no ano passado (AMIN NAVES, 2019). Ademais, o modelo brasileiro também aproxima-se mais do chinês por este não entender o espaço cibernético necessariamente como um novo território onde predomina o conflito, e sim como um espaço de cooperação e governança multilateral, diferentemente do que propaga os EUA.

---

[136] Em termos de cooperação em tríplice hélice, quer dizer, onde são reunidos esforços conjuntos e contínuos das Forças Armadas-Academia-Setor privado, para fortalecer as capacidades de resposta a ataques e aprimorar concepções estratégicas conceituais, pode-se dizer que esta já existe na prática, no Brasil, em termos de segurança cibernética, mas não de defesa cibernética (PAGLIARI; AYRES PINTO; BARROSO, 2020).

[137] Com relação aos próprios organismos responsáveis pela segurança e defesa cibernéticas do Estado brasileiro, Da Cruz Jr. (2013) faz uma crítica essencial: enquanto nos Estados Unidos, só uma pessoa é responsável tanto pela segurança quanto pela defesa - o Comandante da USCyberCom também é diretor da NSA e chefe do Serviço Central de Segurança -, o que auxilia na tomada de decisões, já que muitas das ações se sobrepõem, no Brasil, segregou-se a direção das ações de segurança e defesa cibernética entre o GSI e o CDCiber. Como previsto, tal ação pode ser vista como prejudicial, já que "tende a fragilizar o programa de proteção cibernética nacional na medida em que passa a depender da afinidade, integração e colaboração dos dirigentes de tais instituições" (DA CRUZ JR., 2013, p. 27). Desta forma, a colaboração entre as duas repartições dependerá da conveniência do momento (DA CRUZ JR., 2013).

Por último, contrasta-se o próprio foco das autoridades públicas destes Estados - se estas estão mais voltadas para ameaças como o crime cibernético e o hacktivismo, ou para conflitos que, de fato, ameaçariam às infraestruturas críticas estatais, a exemplo da espionagem cibernética, da sabotagem cibernética, do terrorismo cibernético e da guerra cibernética, propagados por Pagliari, Ayres Pinto e Barroso (2020) no primeiro capítulo.

Enquanto os Estados Unidos e a China, expoentes em defesa cibernética no Cenário Internacional, figuram sempre entre os principais acusados e acusadores em termos de roubos de informações, invasões de redes e ataques de cunho político e/ou intelectual (DA CRUZ JR., 2013), a dizer, pelo que se conhece como ameaças externas, provenientes de governos estrangeiros e de grupos terroristas, o Brasil sofre, em maior quantidade, com a criminalidade cibernética e os protestos digitais (DINIZ; MUGGAH; GLENNY, 2014). Com maiores investimentos para respostas militarizadas, todavia, entende-se que o Brasil direciona-se de maneira a dar pouca atenção e investimentos financeiros às atividades que realmente o atingem (DINIZ; MUGGAH; GLENNY, 2014).

Conclui-se, portanto, que se analisadas as capacidades nacionais detidas por esses três Estados através do conceito que se propagou em Tilly (2007), de que a capacidade estatal mediria em que nível as intervenções dos agentes estatais nos recursos, atividades e conexões interpessoais não estatais alteraria as distribuições desses mesmos recursos, atividades e conexões interpessoais, os Estados Unidos, seguido proximamente pela China, possuem maiores capacidades cibernéticas que o Brasil. Como a intenção desta monografia não é compará-los, mas visualizar a progressão brasileira na temática, visualiza-se que o país latino-americano, por ter começado a tratar da pauta apenas no século XXI, vem reunindo paulatinamente capacidades nacionais - principalmente estatais -, de modo a favorecer sua atuação para a segurança e defesa cibernéticas.

Concebendo a institucionalização da defesa cibernética no país pela primeira vez a partir de 2005, com a publicação da então PDN, compreende-se que o país preocupou-se, à primeira vista, com a publicação de documentos e a criação de organismos mais focados na parte de segurança cibernética (ou segurança da informação), retendo a temática à redoma do debate político (SOUZA; ALMEIDA, 2016). A partir de 2008, então, com a publicação da primeira END - e com a posterior sequência de publicações desta, da PND e do Livro Branco de Defesa Nacional a cada quatro anos -, além da criação progressiva de órgãos voltados à defesa, a defesa passou a ser vista internamente como necessária tanto para agressões que

pudessem vier a ocorrer quanto para a prevenção de ameaças (OLIVEIRA; PORTELA, 2017), abrindo espaço para que a defesa cibernética se tornasse pauta estratégica no país.

Ao mesmo tempo, o Brasil ainda insere contemporaneamente seus indivíduos no que se entende pelo espaço cibernético. Refletindo as desigualdades estruturais do país (DINIZ; MUGGAH; GLENNY, 2014), e não dispondo ainda em sua totalidade de imersão digital (OLIVEIRA ET AL., 2017), o Brasil detém uma penetração de internet que totalizou 70,9% em 2019 (INTERNET WORLD STATS, 2019c). Somando tal fator à escassez de recursos orçamentários para a defesa (OLIVEIRA; PORTELA, 2017) - e, em específico, para a defesa cibernética (AMIN NAVES, 2019) -, torna-se impossível visualizar, na atualidade, a possibilidade da independência tecnológica, e para ainda além, da própria produção de tecnologias sensíveis (OLIVEIRA; PORTELA, 2017).

Para tanto, sugere-se que tal desenvolvimento, seguido de possível autonomia, só serão alcançados se as capacitações tecnológicas nacionais de defesa tiverem como foco principal a formação de recursos humanos (BRASIL, 2008) - construindo, portanto, o desenvolvimento de aparato industrial de forma concomitante e paralela a este. Aqui, ecoa-se o entendimento de que a ausência de condições para o aprendizado, para o trabalho, e para a produção individual, assim sendo, impossibilitam qualquer independência tecnológica intencionada (OLIVEIRA; PORTELA, 2017).

Ademais, e não se esquecendo da importância de investir-se em defesa cibernética, ou seja, de mitigar ameaças internacionais a partir de respostas militarizadas, se faz necessário alinhar o foco das autoridades públicas, para que as ameaças cibernéticas sejam corretamente endereçadas, de maneira a investir também nas devidas respostas à criminalidade cibernética e aos protestos digitais em ascensão no país (DINIZ; MUGGAH; GLENNY, 2014). De modo a progredir nesse sentido, o Brasil pode-se apoiar na cooperação internacional já firmada e em prospecção, tanto para a sua segurança, quanto para a sua defesa cibernética.

4.5 CONCLUSÕES PRELIMINARES

Buscou-se, neste último capítulo, analisar as capacidades nacionais brasileiras em defesa cibernética à luz daqueles Estados considerados expoentes na temática: Estados Unidos e China. Como apresentado anteriormente, as capacidades nacionais aqui embasadas foram propostas em simetria à conceituação de Tilly (2007), que entendia tais capacidades principalmente a partir do viés estatal, ou seja, que as capacidades poderiam ser utilizadas

como um recurso de poder caso este Estado conseguisse alterar as distribuições de recursos, atividades e conexões interpessoais não estatais - internas e externas.

Tendo, deste modo, se inserido formalmente na internet global a partir de 1992, e começado a comercializá-la em 1995, o Brasil posicionou-se, desde o princípio, na retaguarda da estrutura que conforma o espaço cibernético: no começo, não possuía infraestrutura suficiente para atender à demanda de provedores e usuários de internet, e, tampouco estimulava, até o começo do século XXI, debates quanto aos riscos e as vulnerabilidades presentes neste espaço.

Com maiores estímulos versados à área de defesa a partir de 2005, o país passou a impulsionar a criação de órgãos e documentos em matéria de cibernética - principalmente, com relação à defesa cibernética, já que documentos de segurança cibernética já haviam sido minimamente institucionalizados -, começando a debatê-la também em nível de ameaça existencial. A atualização da END, da PND e do Livro Branco a cada quatro anos, isto posto, demonstrou a intencionalidade de reorganização das Forças Armadas, incluindo com relação à reestruturação de sua indústria de defesa, a qual, do ponto de vista cibernético, seria estimulada de modo a garantir sua produção interna e, assim consequentemente, sua independência.

Todavia, em razão da produção ainda insuficiente no que tange o peopleware - já que metade da população brasileira só teve acesso ao espaço cibernético a partir de 2013, além da formação de recursos humanos junto à temática ainda estar em ascensão - e da dependência com relação aos softwares e hardwares externos - influenciados por investimentos insuficientes na área e pela ausência da regularidade quando na aquisição de produtos de defesa -, entende-se que o país latino-americano, apesar de securitizar a pauta na contemporaneidade, ainda está em progressão perante a sua criação de capacidades nacionais.

Deste modo, então, a China e os Estados Unidos podem servir-lhe de molde, mas não de parâmetro de comparação, já que, além de estarem na vanguarda da produção de capacidades nacionais, destacam-se com relação à fatores como sua grande influência perante o Sistema Internacional, sua própria indústria nacional constantemente fomentada, e também com relação à criação de estruturas militares que se endereçam consistentemente aos ataques cibernéticos sofridos por estes países, diferentemente do que ocorre no Brasil. Isso não quer dizer, contudo, que o Brasil não pode - ou que não deve - instigar a realização de acordos de cooperação em segurança e defesa cibernética com estes Estados, que podem auxiliá-lo quando no desenvolvimento de suas próprias capacidades nacionais.

5 CONCLUSÃO

A presente monografia teve como objetivo principal compreender de que forma a criação de capacidades nacionais - principalmente estatais - poderia influenciar as competências brasileiras para o setor de defesa cibernética, isto é, para a produção de recursos de defesa para as três camadas que compõem o espaço cibernético, o hardware, o software e o peopleware.

Para cumprir com este objetivo, intencionou-se, primeiramente, assimilar a ascensão mundial da temática cibernética, no que é possível relacioná-la com a criação da internet, entendendo não apenas desdobramentos sociais, econômicos e políticos, mas também inferindo quais foram os processos e atores principais envolvidos em sua disseminação.

Daqui, depreende-se que a expansão e disseminação da internet, já esvaziada de suas intenções iniciais do período da Guerra Fria, figurou como um objeto importante de mudanças sociais, e perpetuou a criação de um novo espaço, caracterizado pela presença essencialmente humana, o espaço cibernético. Arquitetada de modo descentralizado, e pouco pensada em termos de segurança do usuário e das próprias redes, a internet tornou-se um meio de exploração de vulnerabilidades, tanto por governos, quanto por corporações e por indivíduos, originando as ameaças ou conflitos cibernéticos.

Preocupados com essas reverberações maléficas, o Governo estadunidense - e, posteriormente, aqueles outros governos que absorveram a pauta, quando institucionalizaram a internet - elevaram-na do nível de especialistas técnicos para políticos e tomadores de decisão, securitizando-na e, posteriormente, tornando-a matéria estratégico-militar, ou seja, preocupação das próprias Forças Armadas, quando passaram a se deparar com a possibilidade de incidentes que envolvessem suas infraestruturas críticas estatais.

Entendendo o relacionamento criado em todos os domínios de disputa entre os Estados, incluindo o espaço cibernético, como uma tentativa de exercer o poder uns sobre os outros, buscou-se explorar, no segundo capítulo, como dois dos Estados mais relevantes atualmente em matéria de defesa cibernética, os Estados Unidos e a China, buscam como recurso ativo sua própria capacitação interna e externa, de modo a fornecer respostas apropriadas para possíveis confrontos.

A partir da utilização conceitual de capacidade estatal nacional de Tilly (2007), que interpreta a força do Estado como até que ponto a intervenção desses agentes nos recursos, atividades e conexões interpessoais não estatais altera as distribuições existentes, apreendeu-

se que, se analisados elementos tais quais capacidades militares, de inteligência, de ciência, tecnologia e inovação, de escala de infraestrutura da internet, e de empresas nacionais do setor de tecnologia da informação, o Estados Unidos ainda se posiciona na vanguarda das ações concernentes ao espaço cibernético, detendo certa hegemonia referente à sua estrutura e, assim consequentemente, sobre a própria Ordem Internacional.

A China, isto posto, apesar de enfrentar desafios como certa dependência tecnológica de softwares e hardwares ocidentais, e de não ter seu idioma oficial difundido em linguagem programática, tem avançado constantemente em termos de internacionalização cibernética. Não apenas sua indústria tecnológica têm se fortalecido ao longo dos últimos anos, mas esta também tem exportado para o ocidente softwares como o TikTok, além de hardwares como aqueles produzidos pela Huawei. Sua consolidação junto à organismos internacionais nas últimas duas décadas, e seu reforço interno em termos de documentação de defesa - e defesa cibernética -, também demonstram que este país deve ser observado em termos de práticas em defesa cibernética pela Sociedade Internacional nos próximos anos.

Em conclusão, esses dois países serviram de base para analisar-se o caso brasileiro no terceiro e último capítulo. Contudo, como dito recorrentemente ao longo desta monografia, longe de querer simplificar suas trajetórias pela comparação de capacidades, vislumbrou-se identificar, a partir destas, forças e fraquezas no caso brasileiro, para sugerir encaminhamentos futuros possíveis.

Identificando, desde o princípio, uma tratativa versada à segurança e defesa cibernéticas apenas no presente século, em razão da infraestrutura insuficiente para atender a todos os provedores e usuários de internet - as TICs estiveram em formação no país até o começo dos anos 2000 -, e da ausência de debates quanto aos riscos e vulnerabilidades presentes neste território - metade da população brasileira só teve acesso ao espaço cibernético em 2013 -, entendeu-se que o Brasil ainda está em desvantagem quando na produção de capacidades cibernéticas.

Isso não significa, contudo, que o país não tenha projetado avanços materiais significativos nessa direção: a partir de 2005, com a publicação do primeiro documento específico em defesa, e de 2010, quando o Congresso Nacional decretou a Lei nº136/2020, que estabelecia a obrigatoriedade do Poder Executivo em encaminhar para o Congresso, a cada quatro anos, atualizações nos três documentos de defesa, a PND, a END, e o LBDN, o Brasil institucionalizou a preocupação com a sua própria defesa e dissuasão, incluindo quando no tangente à área de *cyber*.

Ademais, estes mesmos documentos identificam, constantemente, a necessidade de reorganização das Forças Armadas, incluindo no que diz respeito à reestruturação da indústria de defesa, crucial para a construção de avanços em defesa cibernética. Observando, todavia, a camada de peopleware como a mais importante, uma das atualizações deste documento infere que, enquanto houver ausência de condições para o aprendizado, para o trabalho, e para a produção individual, a independência tecnológica, altamente almejada no concernente às tecnologias sensíveis, será impossível. Portanto, sugere-se aqui que o desenvolvimento brasileiro nesta área, com posterior autonomia, só será alcançado se houver maior destinação de recursos e foco à formação de recursos humanos, e, de forma paralela, o desenvolvimento de aparato industrial.

Como já apresentado, avanços materiais que podem ser apresentados neste sentido são a elevação do CDCiber em ComDCiber; a inauguração da EnaDCiber, em 2019, que estimulará a formação de recursos humanos para defesa cibernética; e as parcerias promovidas para a criação de hardwares e softwares, como é o caso do Rádio Definido por Software, colaboração entre o CTEx e a Odebrecht Defesa, do antivírus Defesa.br, colaboração entre o Exército e a Bluepex, e do Simoc, colaboração entre o Exército e a TI Decatron.

Duas últimas problemáticas levantadas pelo caso do Brasil, as quais relacionam-se entre si, foram relevantes para responder o questionamento inicialmente proposto. Em primeiro lugar, há forte argumentação de que as autoridades brasileiras focam-se mais em expandir sua capacidade estatal de modo a mitigar ameaças cibernéticas internacionais, ou seja, investindo em respostas militarizadas, do que em combater sua criminalidade cibernética e os protestos digitais em ascensão, que são analisados como sua real problemática atual. Em segunda instância, a série de orçamentos voltados para a resposta militarizada, de defesa cibernética, no Brasil, têm sido baixa, na ordem de R$7 milhões anuais, enquanto, para operar com as capacidades necessárias, estes recursos deveriam chegar a R$150 milhões anuais - e, assim consequentemente, os recursos orçamentários escassos e a ausência de regularidade na aquisição de produtos de defesa perpetuam a dependência tecnológica estrangeira.

Ecoando, finalmente, o questionamento proposto em introdução *De que forma a criação de capacidades nacionais em Defesa Cibernética poderia impactar as competências brasileiras na produção de recursos de Defesa para este setor?*, conclui-se que, à luz dos casos de China e Estados Unidos - que, lembrando, podem servir-lhe de molde, mas não de parâmetro comparativo, dadas as diferenças cruciais de desenvolvimento -, o Brasil ainda tem

um árduo caminho a percorrer, pois detém grandes capacidades nacionais em termos de legislação e normas voltada à defesa cibernética, mas poucas competências materiais práticas, a exemplo da formação de recursos humanos e de aparato industrial incipientes, da dificuldade quando de esforços voltados à pesquisa, ciência e inovação, entre outros. Ademais, aproximando-se mais da China, em termos de tratativa do espaço e do setor cibernético - os dois posicionam-se como países em desenvolvimento, abordando este espaço de forma não hegemônica -, este país pode e deve apoiar-se na cooperação internacional em matéria de segurança e defesa cibernéticas, visando facilitar o seu próprio fortalecimento interno e externo.

REFERÊNCIAS

AMARANTE, José Carlos Albano do. A base industrial de defesa brasileira. **Instituto de Pesquisa Econômica Aplicada (IPEA),** Rio de Janeiro, p. 1-44, ago./2012.

AMIN NAVES, Gen. de Divisão Guido. Setor Estratégico Cibernético. In: XXI Ciclo de Estudos Estratégicos: Ciberespaço: A Nova Dimensão do Campo de Batalha, Rio de Janeiro. **Anais [...].** Rio de Janeiro: ECEME, 2019, p. 30-44.

AYRES PINTO, Danielle Jacon; FREITAS, Riva Sobrado de; PAGLIARI, Graciela de Conti. FRONTEIRAS VIRTUAIS: UM DEBATE SOBRE SEGURANÇA E SOBERANIA DO ESTADO. In: Danielle Jacon Ayres Pinto; Maria Raquel Freire; Daniel Chaves. (Org.). **FRONTEIRAS CONTEMPORÂNEAS COMPARADAS**: **desenvolvimento, segurança e cidadania.** 1ed.Macapá: Editora da UNIFAP, 2018, v. 1, p. 39-52.

AYRES PINTO, Danielle Jacon; GRASSI, Jéssica. POLITIZE!. **Ciberguerra: o que é e quais suas possibilidades?**. Disponível em: https://www.politize.com.br/ciberguerra/. Acesso em: 20 mai. 2020.

BARBOSA, Daniel Cunha. O que é um proxy e para que serve?. **We live Security**, 20 Dez. 2019. Disponível em: https://www.welivesecurity.com/br/2019/12/20/o-que-e-um-proxy-e-para-que-serve/. Acesso em: 20 nov. 2020.

BRASIL. **Decreto no 6.703/2008: Estratégia Nacional de Defesa**. Brasília: Presidência da República, 2008.

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

CAC. **National Cyberspace Security Strategy**. Cyberspace Administration Of China. 2016. Disponível em: http://www.cac.gov.cn/gzzc/gzzc/A090401index_1.htm. Acesso em: 17 Jul. 2020.

CANAL TECH. Exército brasileiro começa a utilizar simulador de guerra cibernética, o Simoc. **Canal Tech**, 25 jan. 2013. Disponível em: https://canaltech.com.br/seguranca/Exercito-brasileiro-apresenta-simulador-de-guerra-cibernetica-o-Simoc/. Acesso em: 20 Nov. 2020.

CANONGIA, Claudia; MANDARINO, Raphael. Segurança cibernética: o desafio da nova Sociedade da Informação. **Parcerias Estratégicas**, Brasília, v. 14, n. 29, p. 21-46, jul./2009.

CARVALHO, Marcelo Sávio Revoredo Menezes de. **A trajetória da Internet no Brasil**: do surgimento das redes de computadores à instituição dos mecanismos de segurança. 2006. 261 f. Dissertação (Mestrado) - Curso de Engenharia de Sistemas e Computação, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2006.

CARVALHO, Paulo Sergio Melo de. A defesa cibernética e as infraestruturas críticas nacionais. In: CICLO DE ESTUDOS ESTRATÉGICOS, 10., 2011, Rio de Janeiro. **Apresentações.** Rio de Janeiro: Escola de Comando e Estado-Maior do Exército, 2011a.

CARVALHO, Paulo Sergio Melo de. O setor cibernético nas Forças Armadas Brasileiras. *In:* BARROS, Otávio Santana Rêgo (Org.). **Desafios estratégicos para segurança e defesa cibernética.** Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011b.

CASSIOLATO, José Eduardo. As Políticas de ciência, tecnologia e inovação na China. **Boletim de Economia e Política Internacional (BEPI)**, Brasília, v. 1, n. 13, p. 65-80, abr./2013.

CASTELLANO, Igor et al. Capacidade Estatal: Democracia e Poder na Era Digital. **ISAPE Debate**, Número 3, nov. 2012.

CASTELLS, Manuel. **A sociedade em rede: a era da informação: economia, sociedade e cultura.** 8. ed. São Paulo: Paz e Terra, 1999.

CASTELLS, Manuel. Lições da História da Internet. In: _____. (org.). **A Galáxia da Internet: Reflexões sobre a internet, os negócios e a sociedade**. Rio de Janeiro: Zahar, 2003, p. 13-33.

CAVELTY, Myriam Dunn. **Cyber-Security and Threat Politics**, London, New York: Routledge, 2008.

CAVELTY, Myriam Dunn. Cyber-security. In: COLLINS, Alan. **Contemporary Security Studies**. 3. ed. Oxford: Oxford University Press, 2012a. Cap. 25, p.362-378.

CAVELTY, Myriam Dunn. The Militarization of Cyber Security as a Source of Global Tension. In: Wenger, Andreas; Möckli, Daniel; Mahadevan, Prem. **Strategic Trends 2012: Key Developments in Global Affairs.** Zurique: Center for Security Studies (CSS), 2012b. p. 103-124.

CLARKE, Richard A.; KNAKE, Robert K. **Cyber War: the next threat to national security and what to do about it.** Harpercollins USA, 2010.

CORREIO BRAZILIENSE. EUA e China são maiores beneficiários da OMC, diz estudo. **Correio Braziliense,** Brasília, 31 Dez. 2019. Economia. Disponível em: https://www.correiobraziliense.com.br/app/noticia/economia/2019/12/31/internas_economia,817432/eua-e-china-sao-maiores-beneficiarios-da-omc-diz-estudo.shtml. Acesso em: 25 Jun. 2020.

COSTA, Matheus Bigogno. O que é Firewall. **Canal Tech,** 18 Fev. 2020. Disponível em: https://canaltech.com.br/internet/o-que-e-firewall/. Acesso em: 21 Jul. 2020.

COUNCIL OF EUROPE. **Chart of signatures and ratifications of Treaty 185: Convention on Cybercrime.** 2020. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures. Acesso em: 29 Jun. 2020.

DA CRUZ JÚNIOR, Samuel César. A segurança e defesa cibernética no Brasil e uma revisão das estratégias dos Estados Unidos, Rússia e Índia para o espaço virtual. **Instituto de Pesquisa Econômica Aplicada (IPEA)**, Brasília, p. 1-51, jul./2013.

DAI, Xiudian. ICTs in China's development strategy. *In*: HUGHES, Christopher R.; WACKER, Gudrun (orgs). **China and the Internet: Politics of the digital leap forward.** Londres: RoutledgeCurzon, 2003, p. 8-29.

DELISLE, Jacques. Foreign Policy through Other Means: Hard Power, Soft Power, and China's turn to Political Warfare to Influence the United States. **Foreign Policy Research Institute**, Pensilvânia, p. 1-33, fev./2020.

DINIZ, Eugenio. **O Brasil e a MINUSTAH**. Minas Gerais: Pontifícia Universidade Católica de Minas Gerais, 2009. p. 90-108. Disponível em: https://www.researchgate.net/profile/Eugenio_Diniz_Costa/publication/267797091_O_Brasil_e_a_MINUSTAH/links/5531360c0cf27acb0dea915c/O-Brasil-e-a-MINUSTAH.pdf. Acesso em: 06 out. 2020.

DINIZ, Gustavo; MUGGAH, Robert; GLENNY, Misha. Deconstructing Cyber Security in Brazil: threats and responses. **Igarapé Institute**, Rio de Janeiro, Strategic Paper 11, p. 1-35, Dez. 2014.

DOD. **Strategy for Operating in Cyberspace.** Department of Defense of the United States of America. Jul. 2011. Disponível em: https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf. Acesso em: 11 Set. 2020.

FAGUNDES, George Harrison Gonçalves et al. A Cooperação Internacional entre Brasil e Estados Unidos em matéria de segurança e defesa cibernética. In: XVI Congresso Acadêmico sobre Defesa Nacional (CADN), Rio de Janeiro. **Anais [...].** Rio de Janeiro: Escola Naval, 2019, 19 p. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/ensino_e_pesquisa/defesa_academia/cadn/artigos/xvi_cadn/aa_cooperaaoa_internacionala_entrea_brasila_ea_estadosa_unidosa_ema_materiaa_dea_segurana.pdf. Acesso em: 20 nov. 2020.

FEITOSA, Caio Vinícius Cesar. **Ataques cibernéticos: Estudo do caso Stuxnet**. 2017. 60f. Trabalho de conclusão de curso - Universidade Federal Fluminense, Niterói, 2017.

FERREIRA NETO, W. B. Territorializando o "Novo" e (Re)territorializando os Tradicionais: A Cibernética como Espaço e Recurso de Poder. **Coleção Meira Mattos**, Rio de Janeiro, v. 8, n. 31, p. 7-18, abr./2014.

FLORCRUZ, Jaime A.; SEU, Lucrezia. From snail mail to 4G, China celebrates 20 years of Internet connectivity. **CNN**, 24 Abr. 2014. Disponível em: https://edition.cnn.com/2014/04/23/world/asia/china-internet-20th-anniversary/index.html. Acesso em: 15 Jul. 2020.

FMPRC. **Cyberspace international cooperation strategy**. Ministry of Foreign Affairs of The People's Republic of China. 2017. Disponível em: www.cac.gov.cn/2017-03/01/c_1120552617.htm. Acesso em: 17 Jul. 2020.

FRENCH, Howard W. Another Chinese Export Is All the Rage: China's language. **The New York Times**, 11 Jan. 2006. Disponível em:

https://www.nytimes.com/2006/01/11/world/asia/another-chinese-export-is-all-the-rage-chinas-language.html. Acesso em: 12 Out. 2020.

FURTADO, Teresa. O que é wireless?. **Techtudo**, 28 Dez. 2011. Disponível em: https://www.techtudo.com.br/artigos/noticia/2011/12/o-que-e-wireless.html. Acesso em: 15 Jul. 2020.

GAGNON, Benoît. Cyberwars and cybercrimes. In: LEMAN-LANGLOIS, Stéphane (Ed.). **Technocrime:** technology, crime and social control. London, UK: Willan Publishing, 2008. cap. 4, p. 46-65.

GALBRAITH, Jean. U.S. Military Undergoes Restructuring to Emphasize Cyber and Space Capabilities. In: _____. **Contemporary Practice of the United States Relating to International Law (113:3 Am J Int'l L)**. Faculty Scholarship at Penn Law, 2019. p. 634-640.

GAZETA DO POVO. Os 15 países que mais investem em defesa no mundo. **Gazeta do Povo**, Curitiba, 29 Abr. 2019. Disponível em: https://www.gazetadopovo.com.br/mundo/os-15-paises-que-mais-investem-em-defesa-no-mundo/#ancora-1. Acesso em: 8 Jun. 2020.

GETSCHKO, Demi; MOREIRAS, Antonio M.. Os Pontos de Troca de Tráfego, o PTTMetro e a Internet brasileira. **Politics.** 2008. Disponível em: https://politics.org.br/edicoes/os-pontos-de-troca-de-tr%C3%A1fego-o-pttmetro-e-internet-brasileira. Acesso em: 07 out. 2020.

GOMES FILHO, Paulo Roberto da Silva. **Estratégia Militar da China para o Século XXI**. PADECEME, [S.l.], v. 10, n. 19, p. 13-24, ago. 2017. ISSN 1677-1885. Disponível em: http://ebrevistas.eb.mil.br/index.php/PADECEME/article/view/602. Acesso em: 17 Jul. 2020.

GUESSER, Adalto. A diversidade lingüística da Internet como reação contra-hegemônica das tendências de centralização do império. **Ciência da Informação**, Brasília, v. 36, n. 1, p. 79-91, abr./2007. Disponível em: https://www.scielo.br/pdf/ci/v36n1/a06v36n1.pdf. Acesso em: 24 out. 2020.

HAIZLER, Omry. The United States' Cyber Warfare History: Implications on Modern Cyber Operational Structures and Policymaking. **Cyber, Intelligence, and Security**, v. 1, n. 1, p. 31-45, jan./2017.

HARDT, Michael; NEGRI, Antonio. **Empire.** Cambridge, Mass: Harvard University Press, 2001.

HSU, Kimberly; MURRAY, Craig. **China and International Law in Cyberspace.** U.S. - China Economic and Security Review Commission Staff Report. 06 de maio de 2014. Disponível em: https://www.uscc.gov/sites/default/files/Research/China%20International%20Law%20in%20Cyberspace.pdf. Acesso em: 16 Jul. 2020.

HUGHES, Christopher R. Fighting the smokeless war: ICTs and international security. *In*: HUGHES, Christopher R.; WACKER, Gudrun (orgs). **China and the Internet: Politics of the digital leap forward.** Londres: RoutledgeCurzon, 2003, p. 139-161.

INKSTER, Nigel. China in Cyberspace. **Survival**, v. 52, n. 4, p. 55-66, set./2010.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). **Densidade demográfica**. 2010. Disponível em: https://brasilemsintese.ibge.gov.br/images/brasil_em_sintese/territorio/brasil_densidade_demografica.pdf. Acesso em: 03 Out. 2020.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). **Painel de Indicadores.** 2019. Disponível em: https://www.ibge.gov.br/indicadores. Acesso em: 03 Out. 2020.

INTERNET WORLD STATS. **ASIA: Asia Marketing Research, Internet Usage, Population Statistics and Facebook Subscribers.** 2019a. Disponível em: https://www.internetworldstats.com/asia.htm. Acesso em: 30 Jun. 2020.

INTERNET WORLD STATS. **Internet Users in North America**. 2017. Disponível em: https://www.internetworldstats.com/stats14.htm. Acesso em: 25 Jun. 2020.

INTERNET WORLD STATS. **NORTH AMERICA: Internet usage data and links to Bermuda, Canada, Greenland, Saint Pierre et Miquelon, and the United States of America.** 2019b. Disponível em: https://www.internetworldstats.com/america.htm#us. Acesso em: 25 Jun. 2020.

INTERNET WORLD STATS. **South America Internet and Facebook Users**. 2019c. Disponível em: https://www.internetworldstats.com/south.htm#br. Acesso em: 07 Out. 2020.

ITAMARATY. **Processo de adesão à Convenção de Budapeste - Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública**. 2019. Disponível em: http://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/21146-processo-de-adesao-a-convencao-de-budapeste-nota-conjunta-do-ministerio-das-relacoes-exteriores-e-do-ministerio-da-justica-e-seguranca-publica. Acesso em: 25 out. 2020.

JINPING, Xi. **Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference**. Wuzhen, 16 dec. 2015. Disponível em: https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml. Acesso em: 17 Jul. 2020.

KISTLER, Henri. O dólar como moeda internacional de referência: é possível sua substituição?. **Pontes**, São Paulo, v. 5, p. 11-12, set/out 2009. Disponível em: http://bibliotecadigital.fgv.br/ojs/index.php/pontes/article/view/77741/74376. Acesso em: 25 Jun. 2020.

KNIGHT, Peter T.. **The Internet in Brazil**: origins, strategy, development, and governance. Bloomington: Authorhouse, 2014. 176 p. Disponível em: https://books.google.com.br/books?id=SWE6AwAAQBAJ&pg=PA1&hl=pt-BR&source=gbs_toc_r&cad=4#v=onepage&q&f=false. Acesso em: 07 Out. 2020.

KURBALIJA, Jovan. **Introducción a la Gobernanza de Internet.** 7. ed. Malta: DiploFoundation, 2016. p. 1-288.

LOPES DIAS, Kelvin; HADJ SADOK, Djamel Fauzi. Internet móvel: tecnologias, aplicações e QoS. In: XIX SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES, Florianópolis. **Anais [...]**. Florianópolis: UFSC, 2001, p. 1-50.

LUNKES, Daniela Sallet. Direitos especiais de Saque: Significado da Incorporação do Renminbi. In: 3º Seminário de Relações Internacionais, Florianópolis. **Anais [...].** Florianópolis: UFSC, 2016, p. 1-16.

LYU, Jinghua. IPI GLOBAL OBSERVATORY. **What Are China's Cyber Capabilities and Intentions?**. Disponível em: https://theglobalobservatory.org/2019/03/what-are-chinas-cyber-capabilities-intentions/. Acesso em: 22 abr. 2020.

MAGALHÃES, Regina; VENDRAMINI, Annelise. Os impactos da quarta revolução industrial. **GV-Executivo**, São Paulo, v. 17, n. 1, p. 40-43, fev./2018.

MAJEROWICZ, Esther. A China e a Economia Política Internacional das Tecnologias da Informação e Comunicação. **DEPEC UFRN**, Natal, v. 1, p. 1-54, jul. 2019. Disponível em: https://ccsa.ufrn.br/portal/wp-content/uploads/2019/07/tddepec0012019majerowicz.pdf. Acesso em: 13 jul. 2020.

MANDARINO JR., Raphael. 2010. **Segurança e Defesa do Espaço Cibernético Brasileiro.** Recife: Cubzac.

MARTINS, Aline Regina Alves. A inclusão do renminbi na cesta de moedas dos Direitos Especiais de Saque: novo impulso à internacionalização da moeda chinesa?. *In*: LIMA, Marcos Costa (Org.). **Sobre a China.** Pernambuco: Editora UFPE, 2018. 429 p.

MARTINS, Elaine. O que é backbone?. **TecMundo**. 2009. Disponível em: https://www.tecmundo.com.br/conexao/1713-o-que-e-backbone-.htm. Acesso em: 07 Out. 2020.

MARTINS, Pedro; GONZALO, Manuel; SZAPIRO, Marina. Sistemas Setoriais de Inovação em Países Emergentes: o Software na Índia e no Brasil em Perspectiva Comparada. **BRICS Policy Center**, Rio de Janeiro, v. 8, n. 4, p. 1-33, ago./2018.

MINISTÉRIO DA DEFESA DO BRASIL. **Base Industrial de Defesa (BID)**. 2020. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/industria-de-defesa/base-industrial-de-defesa. Acesso em: 18 out. 2020.

MINISTÉRIO DA DEFESA DO BRASIL. **Doutrina Militar de Defesa Cibernética.** MD31-M-07. Brasília: EMCFA, 2014.

MOREIRA, Alexandre Santana; CORDEIRO, Sandro Silva. O Spin-in na Indústria de Defesa Brasileira voltada para o Setor Cibernético. **Revista da Escola Superior de Guerra**, Rio de Janeiro, v. 29, n. 58, p. 100-116, jun./2014.

MOREIRA JR., Hermes. Inovação, Militarismo e Hegemonia: o complexo industrial militar na estratégia dos estados unidos para a manutenção da liderança internacional. **Oikos**, Rio de Janeiro, v. 1, n. 13, p. 22-39, 2014. Disponível em: http://revistaoikos.org/seer/index.php/oikos/article/view/367/208. Acesso em: 21 jul. 2020.

MORETZ-SOHN FERNANDES, Thaís. Conhecendo o Sistema Político Chinês. **Apex-Brasil**, Brasília, p. 1-41, 2014. Disponível em: http://arq.apexbrasil.com.br/portal/ConhecendoOSistemaPoliticoChines.pdf. Acesso em: 17 jul. 2020.

NETO, Edmilson. Como funciona o Conselho de Segurança da ONU?. **POLITIZE!.** Disponível em: https://www.politize.com.br/conselho-de-seguranca-da-onu/. Acesso em: 06 out. 2020.

NPC. **Cybersecurity Law of the People's Republic of China**. National People's Congress Of The People's Republic Of China. 2017. Traduzido por Rogier Creemers, Paul Triolo, e Graham Webster. Disponível em: http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm. Acesso em: 17 Jul. 2020.

NYE JR., Joseph S. **O Futuro do Poder.** São Paulo: Benvirá, 2012.

OLIVEIRA, Marcos Aurélio Guedes de; PORTELA, Lucas Soares. As camadas do espaço cibernético sob a perspectiva dos documentos de defesa do Brasil. **Revista Brasileira de Estudos de Defesa**, Porto Alegre, v. 4, n. 2, p. 77-99, dez./2017.

OLIVEIRA, Marcos Aurélio Guedes de et al. **Guia de defesa cibernética na América do Sul.** Recife: Editora UFPE, 2017. Disponível em: https://pandia.defesa.gov.br/pt/acervo-digital/35-programa-%C3%A1lvaro-alberto-de-indu%C3%A7%C3%A3o-%C3%A0-pesquisa-em-defesa-nacional-e-seguran%C3%A7a-internacional/826-guia-de-defesa-cibern%C3%A9tica-na-am%C3%A9rica-do-sul,-por-marcos-aurelio-guedes-et-al. Acesso em: 09 jul. 2020.

PAGLIARI, Graciela de Conti; AYRES PINTO, Danielle Jacon; BARROSO, Juliana L. Viggiano. Mobilização nacional, ameaças cibernéticas e redes de interação num modelo de tríplice hélice estratégica: um estudo prospectivo. In: Marcos Guedes de Oliveira. (Org.). **Defesa Cibernética e Mobilização Nacional**. 1ed.Recife: UFPE, 2020, v. 1, p. 153-174.

PIMENTEL, Pedro Chapaval; PANKE, Luciana. Dilma Rousseff na Assembleia Geral das Nações Unidas: Análise dos Discursos de 2011 e 2015. In: XVII Congresso de Ciências da Comunicação na Região Sul, Curitiba. **Anais [...].** Curitiba: PUCPR, 2016, p. 1-14.

PNUD. **Desenvolvimento Humano e IDH**. [201-]. Disponível em: https://www.br.undp.org/content/brazil/pt/home/idh0.html. Acesso em: 06 out. 2020.

PNUD. **Relatório do Desenvolvimento Humano 2015**: o trabalho como motor do desenvolvimento humano. 2015. Disponível em: http://hdr.undp.org/sites/default/files/hdr15_overview_pt.pdf. Acesso em: 06 out. 2020.

PROENÇA JÚNIOR, D. Forças armadas para quê? Para isso. **Contexto Internacional**, v. 33, n. 2, p. 333–373, 2011.

QIAN, Xuming. Cyberspace Security and U.S.-China Relations. In: AICS, 2019, Wuhan. **Proceedings...** Wuhan: Association for Computing Machinery, 709-712.

REDAÇÃO DEFESATV. **Exército Brasileiro ativa sua Escola Nacional de Defesa Cibernética**. 2019. Disponível em: https://www.defesa.tv.br/exercito-brasileiro-ativa-sua-escola-nacional-de-defesa-cibernetica/. Acesso em: 15 out. 2020.

REINO, João Luis Ribeiro. **A Globalização Cultural e os Estados Unidos**: O poder da internet como agente propagador de cultura. Brasília, 2010. 67p. Trabalho de Conclusão de Curso (Relações Internacionais) - Universidade de Brasília, Brasília, 2010. Disponível em: https://www.bdm.unb.br/bitstream/10483/1128/1/2010_JoaoLuisRibeiroReino.pdf. Acesso em: 1 Jul. 2020.

RODRIGUES PADILHA, Marcus Vinicius. **Relações Internacionais e Espaço Cibernético: Sistemas de Defesa dos EUA e Brasil.** 2016. 59 f. Trabalho de Conclusão de Curso - Bacharelado em Relações Internacionais pela Faculdade de Ciências Jurídicas e Sociais do Centro Universitário de Brasília (UniCEUB), Brasília, 2016.

ROSS, Wilbur. Commerce Department Prohibits WeChat and TikTok Transactions to Protect the National Security of the United States. **U.S. Department of Commerce**, 18 Set. 2020. Disponível em: https://www.commerce.gov/news/press-releases/2020/09/commerce-department-prohibits-wechat-and-tiktok-transactions-protect. Acesso em: 12 Out. 2020.

SCHREIBER, Mariana. Os gastos bilionários que Bolsonaro propõe para a Defesa e que levarão a cortes em outras áreas em 2021. **BBC Brasil.** 2020. Disponível em: https://www.bbc.com/portuguese/brasil-53969636. Acesso em: 06 out. 2020.

SCIO. **China's National Defense in 2004**. State Council Information Office of the People's Republic of China. Beijing, Dez., 2004. Disponível em: http://en.people.cn/whitepaper/defense2004/defense2004.html. Acesso em: 15 Jul. 2020.

SCIO. **China's National Defense in the New Era**. State Council Information Office of the People's Republic of China. Beijing, jun., 2019. Disponível em: http://eng.mod.gov.cn/news/2019-07/24/content_4846443.htm. Acesso em: 18 Jul. 2020.

SCIO. **White paper on the Internet in China**. State Council Information Office of the People's Republic of China. Beijing, 2010. Disponível em: http://www.chinadaily.com.cn/china/2010-06/08/content_9950198.html. Acesso em: 15 Jul. 2020.

SCMP RESEARCH. **China Internet Report 2020**. 2020. Disponível em: https://research.scmp.com/products/china-internet-report-2020. Acesso em: 22 jul. 2020.

SOESANTO, Stefan. Trend Analysis: **The Evolution of US Defense Strategy in Cyberspace (1988 – 2019).** Zurique, Suíça: Center for Security Studies (CSS), 2019. p.1-38.

SOUZA, Eduardo André Araujo de; ALMEIDA, Nival Nunes de. A questão da segurança e defesa do espaço cibernético brasileiro, e o esforço político-administrativo do Estado. **Revista da Escola de Guerra Naval**, Rio de Janeiro, v. 22, n. 2, p. 381-410, ago. 2016.

SOUZA, G. L. Mâcedo. **Reflexos da digitalização da Guerra na Política Internacional do Século XXI: Uma análise exploratória da securitização do Ciberespaço nos Estados Unidos, Brasil e Canadá**. 2013. 129f. Dissertação (Mestrado em Ciência Política) - Centro de Filosofia e Ciências Humanas, Universidade Federal de Pernambuco, Recife, 2013.

STATISTA. **The 30 largest countries in the world by total area (in square kilometers).** 2019. Disponível em: https://www.statista.com/statistics/262955/largest-countries-in-the-world/. Acesso em: 6 jul. 2020.

TELEGEOGRAPHY. **Submarine Cable Map 2019**. 2019. Disponível em:https://submarine-cable-map-2019.telegeography.com/. Acesso em: 2 Jul. 2020.

TELEGEOGRAPHY. **Submarine Cable Map: Brazil.** 2020a. Disponível em: https://www.submarinecablemap.com/#/country/brazil. Acesso em: 8 Out. 2020.

TELEGEOGRAPHY. **Submarine Cable Map: Brazilian Festoon.** 2020b. Disponível em: https://www.submarinecablemap.com/#/submarine-cable/brazilian-festoon. Acesso em: 8 Out. 2020.

TELEGEOGRAPHY. **Submarine Cable Map: China.** 2020c. Disponível em: https://www.submarinecablemap.com/#/country/china. Acesso em: 2 Jul. 2020.

TELEGEOGRAPHY. **Submarine Cable Map: United States.** 2020d. Disponível em: https://www.submarinecablemap.com/#/country/united-states. Acesso em: 2 Jul. 2020.

THE WHITE HOUSE. **Executive Order on Securing the Information and Communications Technology and Services Supply Chain**. 15 Mai. 2019. Disponível em: https://www.whitehouse.gov/presidential-actions/executive-order-securing-informationcommunications-technology-services-supply-chain/. Acesso em: 11 Set. 2020.

THE WHITE HOUSE. **The National Strategy to Secure Cyberspace.** Washington, fev., 2003. Disponível em: https://us-cert.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf. Acesso em: 11 Set. 2020.

THE WORLD BANK. **GDP (current US$).** 2018. Disponível em: https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?most_recent_value_desc=true. Acesso em: 8 Jun. 2020.

THE WORLD BANK. **World Development Indicators**: population dynamics. 2020. Disponível em: http://wdi.worldbank.org/tables. Acesso em: 10 nov. 2020.

THOMAS, Timothy L. Nation-state Cyber Strategies: Examples from China and Russia. *In:* KRAMER, Franklin D.; STARR, Stuart H.; KENTZ, Larry K. (orgs). **Cyberpower and National Security.** Lincoln: Potomac Books, University of Nebraska Press, 2009, p. 465-488.

TILLY, Charles. **Democracy.** New York: Cambridge University Press, 2007.

VEJA. **Paquistão ultrapassa o Brasil em lista de países mais populosos do mundo**. 2019. Disponível em: https://veja.abril.com.br/mundo/paquistao-ultrapassa-o-brasil-em-lista-de-paises-mais-populosos-do-mundo/. Acesso em: 03 out. 2020.

VENTRE, Daniel. Ciberguerra. In: Academia General Militar. **Seguridad Global y Potencias Emergentes en un Mundo Multipolar**. XIX Curso Internacional de Defensa. Zaragoza: Universidad Zaragoza. 2012a.

VENTRE, Daniel. Introduction. In: _____. (org.). **Cyber Conflict: Competing National Perspectives.** Londres: ISTE Ltd. 2012b.

VILLA, Rafael D.; REIS, Rossana R. A segurança internacional no pós-Guerra Fria: um balanço da teoria tradicional e das novas agendas de pesquisa. **R. bras. de Informação Bibliográfica em Ciências Sociais (BIB)**, São Paulo, n. 62, 2o semest., 2006, p. 19-51.

YUEN, Samson. Becoming a Cyber Power: China's cybersecurity upgrade and its consequences. **China Perspectives**, Hong Kong, v. 2, p. 53-58, ago./2015.

ZENG, Jinghan; BRESLIN, Shaun. 2016. China's 'New Type of Great Power Relations': a 'G2' with Chinese Characteristics?. **International Affairs**, Oxford, jul. 2016.

ZENG, Jinghan; STEVENS, Tim; CHEN, Yaru. China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty". **Politics & Policy**, [s.l.], v. 45, n. 3, p. 432-464, jun. 2017. Wiley. http://dx.doi.org/10.1111/polp.12202. Disponível em: https://onlinelibrary.wiley.com/doi/abs/10.1111/polp.12202. Acesso em: 17 Jul. 2020.

ZETTER, Kim. 2014. **Countdown to Zero Day**. New York: Broadway Books.

ZUCCARO, Paulo Martino. Tendência Global em Segurança e Defesa Cibernética: reflexões sobre a proteção dos interesses brasileiros no ciberespaço. In: BARROS, Otávio Santana Rêgo (Org.). **Desafios estratégicos para segurança e defesa cibernética**. Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011.