UNIVERSIDADE FEDERAL DO PAMPA

RAFAELA DE SOUZA CORREA

A SECURITIZAÇÃO DO CIBERESPAÇO CHINÊS DURANTE O GOVERNO DE XI JINPING (2013-2020)

Santana do Livramento
2021

RAFAELA DE SOUZA CORREA

A SECURITIZAÇÃO DO CIBERESPAÇO CHINÊS DURANTE O GOVERNO DE XI JINPING (2013-2020)

Trabalho de Conclusão de Curso apresentado ao Curso de Relações Internacionais da Universidade Federal do Pampa, como requisito parcial para obtenção do Título de Bacharel em Relações Internacionais

Orientador: Profª Drª AnnaCarletti
De acordo

Santana do Livramento
2021

RAFAELA DE SOUZA CORREA

A SECURITIZAÇÃO DO CIBERESPAÇO CHINÊS DURANTE O GOVERNO DE XI JINPING (2013-2020)

Trabalho de Conclusão de Curso apresentado ao Curso de Relações Internacionais da Universidade Federal do Pampa, como requisito parcial para obtenção do Título de Bacharel em Relações Internacionais.

Trabalho de Conclusão de Curso defendido e aprovado em: 11 de maio de 2021.

Banca examinadora:

_____

Profª. Drª. Anna Carletti
Orientadora
(UNIPAMPA)

_____

Prof. Dr. Flávio Augusto Lira Nascimento
(UNIPAMPA)

_____

Prof. Me. Bruno Correa
(UNIPAMPA)

Ficha catalográfica elaborada automaticamente com os dados fornecidos pelo(a) autor(a) através do Módulo de Biblioteca do Sistema GURI (Gestão Unificada de Recursos Institucionais) .

C824s CORREA, RAFAELA
A SECURITIZAÇÃO DO CIBERESPAÇO CHINÊS DURANTE O GOVERNO DE XI JINPING (2013-2020) / RAFAELA CORREA. 88 p.

Trabalho de Conclusão de Curso(Graduação)-- Universidade Federal do Pampa, RELAÇÕES INTERNACIONAIS, 2021.
"Orientação: Anna Carletti".

1. Segurança Internacional. 2. Cibersegurança. 3. China. I. Título. C

AGRADECIMENTO

Agradeço a Professora Doutora Anna Carletti primeiramente pela paciência durante esta caminhada, nunca me esquecerei do que ela já fez por mim ao longo da graduação. Sim, isso inclui às vezes em que chorei no seu escritório no meio de uma tarde, pelos aconselhamentos e momentos em que a senhora esteve presente fazendo sendo a adulta responsável, orientando adolescentes perdidos em seu primeiro ano de graduação.

Aos professores Flávio Lira e Bruno Correa por estarem presentes neste momento tão importante que é a reta final desta graduação.

Aos meus amigos de Ipatinga Anne, Tallin, Erimar, Ítalo, Gabriel, Luiz, Hérick, Adriano, Kaio, Maju, Igor e Arthur de Ipatinga que em me apoiaram em uma das decisões mais sábias e mais estúpidas que já tomei em toda a minha vida.

Aos meus novos amigos Daniel, Letícia, Nicole, Leona, Erick, Rodolfo, Bruna Mandu, Érick Albani que tornaram a distância de casa mais suportável e que agora podem me fornecer abrigo em diversos estados do Brasil.

Aos meus webamigos que eu nunca conheci pessoalmente e que me dói no fundo nunca ter dado um abraço em nenhum de vocês. Obrigada Yaga, Dann, Sahs, Raffa, Mago, Fábio, Lara e Dani. Esta última merece uma menção honrosa pelo sumário.

Agradeço aos meus avós, meu padrasto e minha prima Mariana pelo apoio durante todos estes anos em que estive mais distante do que vocês gostariam.

Por fim e nunca menos importante, obrigada a minha mãe que sempre acreditou em mim mesmo quando eu não pude fazer isso.

“Subjugar o exército inimigo sem lutar é o verdadeiro pináculo da excelência.”

Sun Tzu

RESUMO

Este trabalho busca compreender os objetivos de securitização do ciberespaço chinês durante o governo do presidente Xi Jinping, considerando o conceito de securitização a partir de uma visão mais ampla que é adotada por Pequim ao longo do século XXI. Para isso, se analisou primeiramente o desenvolvimento do ciberespaço como um ambiente a ser securitizado e como este se tornou parte do jogo de poder entre as nações. Posteriormente foi observado o desenvolvimento da internet na China e como ocorreu o gerenciamento desta tecnologia por parte do Partido Comunista Chinês em âmbito doméstico para fins civis e econômicos. Finalmente, o emprego do ciberespaço como ferramenta a nível militar e diplomático durante o governo de Xi Jinping. Durante o trabalho se explora a ideia de que a atual política para o ciberespaço é resultado de fatores econômicos, sociais e políticos que remontam a períodos anteriores à chegada da internet ao país, mas que ao mesmo tempo rompe com projetos econômicos e diplomáticos seguidos desde o governo de Deng Xiaoping.

Palavras-Chave: Ciberespaço, Cibersegurança, República Popular da China, Indústria 4.0.

ABSTRACT

The main objective of this work is to understand the securitization of Chinese cyberspace during the government of President Xi Jinping, considering the concept of securitization from a broader view that is adopted by Beijing throughout the 21st century. For this, the development of cyberspace as an environment to be securitized was first analyzed and how it became part of the power game between nations. Subsequently it was observed the development of this in China and how it was managed by the Chinese Communist Party domestically for civil and economic purposes. Finally, the use of cyberspace as a tool at the military and diplomatic level during the government of Xi Jinping. During the work, the Idea is explored that the current cyberspace policy is the result of economic, social and political factors that go back to periods prior to the arrival of the internet in the country but that at the same time breaks with the economic and diplomatic projects followed since the government of Deng Xiaoping.

Keywords:Cyberspace, Cybersecurity, People'sRepublicof China, Industry 4.0.

LISTA DE SIGLAS

CNNIC – Centro de Informações da Rede de Internet da China
ELP – Exército de Libertação Popular
EUA– Estados Unidos da América
HTTP – HyperText Transfer Protocol
ICANN – Corporação da Internet para Atribuição de Nomes e Números
ISIS – Estado Islâmico do Iraque e da Síria
ITU – International Telecommunication Union
P&D – Pesquisa e Desenvolvimento
PCC– Partido Comunista Chinês
RPC– República Popular da China
TIC – Tecnologia da Informação e Comunicação
URSS – União das Repúblicas Socialistas Soviéticas

SUMÁRIO

1 INTRODUÇÃO

Desde que foi criada em 1969, a internet serviu em primeiro momento aos interesses do Estado. A invenção desta tecnologia para fins militares foi um resultado do boom tecnológico gerado pela Guerra Fria (GOLDONI e MEDEIROS, 2020). Sob o nome de Arpanet foi criada com a intenção de facilitar e estabilizar a comunicação entre laboratórios e bases militares dos Estados Unidos, mesmo em situações conflituosas. O uso comercial foi permitido, sendo esta tecnologia adotada de modo progressivo pelos países (LOPES, 2016).

Foi apenas no ano de 1994 que pela primeira vez um computador com acesso a internet foi utilizado na China, sendo que o objetivo primário era atender as necessidades das grandes universidades e instituições governamentais de Pequim. No ano seguinte foi permitido que o público progressivamente tivesse contato com a novidade, e em 1997 já havia cerca de 620.000 usuários de Internet segundo relatório divulgado pelo Centro Nacional de Informações de Rede da China (CNNIC) (NEGRO, 2019). A abertura de cyber cafés e o massivo apoio das empresas tradicionais de telecomunicação auxiliaram em sua difusão rápida na capital e outras grandes cidades do país.

Já em 2008 se tornou o país com o maior número de usuários, ou netizens como são chamados nos relatórios oficiais disponibilizados pela CNNIC, do mundo. E atualmente a China registra 939.8 milhões de netizens ao longo de todo seu território, tendo assim uma penetração do acesso a rede de 67% de sua população. A maior disparidade em relação a conexão está na zona rural que hoje possui apenas 52% de penetração, representando assim 30% de todos os usuários do país. Em maioria absoluta, 99.2%, as pessoas se conectam à internet por meio de aparelhos móveis e dedicam seu tempo em rede em aplicativos de mensagens instantâneas, vídeos online, redes sociais entre outros (CNNIC, 2020).

Porém a conectividade possui algumas desvantagens, como a exposição dos usuários a ataques cibernéticos, a facilidade em realizar certos crimes tradicionais como a pirataria, além da exposição de infraestruturas críticas aos riscos de atividades mal intencionadas de terceiros. E em casos especiais, como o da China, a internet

abre espaço para conteúdos estrangeiros não autorizados dentro do país. Isto inclui desde notícias, livros e artigos até a famosa deep web, que abre espaço para os atos criminosos, como a pedofilia, tráfico de drogas e de seres humanos.

Pensando nisso, de modo a expandir o uso da rede sem a influência de conteúdos externos ou talvez danosos, e exercer sua soberania pelo que reconhecem como uma extensão de seu território visível, o país iniciou uma forte política de controle de dados e acesso que hoje autores ocidentais citam como o Grande Firewall da China (NEGRO, 2019). Este projeto, que vem sendo construído desde 1997, estimulou também a massiva participação de empresas nacionais neste novo setor, minimizando a participação de companhias estrangeiras (NEGRO, 2019). O segundo projeto de defesa neste setor, o “Golden Shield”, atua como um grande sistema de vigilância interno e está ativo desde o ano de 2003.

Mesmo tendo estes dois grandes projetos de segurança e defesa de seu espaço virtual, apenas no governo do presidente Xi Jinping o ciberespaço se tornou uma pauta importante da política externa chinesa. Além de uma participação mais propositiva na ITU (United Nations specialized agency for information and communication technologies) e na ICANN (Corporação da Internet para Atribuição de Nomes e Números), o presidente também se colocou à frente do comitê de Segurança cibernética, liderando de perto a condução desta nova política para o ciberespaço (SEGAL, 2019).

Tendo em vista este momento de mudança no posicionamento chinês em relação ao seu ciberespaço, este trabalho acompanhará todo o período de governo de Xi Jinping até de 2013 até 2020, considerando que há substancial mudança na formulação da política chinesa doméstica e internacional durante este período. Sendo assim, este trabalho parte da seguinte problemática: levando em consideração a atuação estatal dentro do ciberespaço chinês,seus avanços em tecnologias de software e hardware, bem como os debates que vêm sendo levantados em torno disso, pergunta-se: quais são os objetivos da securitização do ciberespaço chinês adotada pelo atual presidente Xi Jinping?

Para responder esta pergunta este trabalho parte da hipótese de que a defesa da segurança cibernética se tornou, durante o governo de Xi Jinping, uma das mais

importantes estratégias nacionais para defender sua soberania e integridade territorial. A hipótese apresentada é de que a securitização do espaço cibernético esteja estritamente ligada à tentativa chinesa de se tornar uma potência mundial capaz de mudar as regras do jogo internacional até então ditadas pelos Estados Unidos, líder até este momento. Então, como objetivo geral, este trabalho pretende analisar quais são os objetivos da política de securitização do ciberespaço chinês adotada pelo atual presidente Xi Jinping no período de 2013 até 2020. Para conseguir percorrer todo o processo de securitização chinês este trabalho será então dividido em três capítulos além das considerações finais onde os resultados da pesquisa serão qualificados.

No primeiro capítulo será proposta uma análise do poder cibernético como um dos novos poderes para manutenção dos interesses nacionais do século XXI. Inicialmente será narrado o desenvolvimento do ciberespaço como um ambiente criado pelo homem e uma tecnologia desenvolvida para fins militares no contexto da Guerra Fria. Seguindo, analisaremos conceitos tradicionais da constituição de poder dentro do Estado Westfaliano, como por exemplo, a noção de soberania e território dentro do ciberespaço. Posteriormente será discutido o conceito de securitização teorizado pela Escola de Copenhague e aquele adaptado por Pequim durante os primeiros anos de governo de Xi Jinping. Por fim, sob a ótica de Nye será visto o que se configura como poder cibernético e suas implicações para a lógica de segurança dentro dos Estados.

Ao longo do segundo capítulo veremos que o ciberespaço, e por consequência a internet, é desenvolvido de modo bastante singular dentro da China, tendo como objetivo analisar a evolução do sistema cibernético chinês. A centralização de seu desenvolvimento nas mãos do Estado e suas regulamentações para o uso e interações de seus cidadãos dentro de rede é diferenciada do que é feito em demais países da comunidade internacional. Isto chama a atenção para debates por parte da comunidade internacional a respeito da neutralidade da rede e os limites do papel do Estado dentro de um ambiente virtual e como isto supostamente causaria um impacto negativo na capacidade chinesa de inovar e criar novas tecnologias para o ciberespaço. Em último momento veremos como o país se apropria da tecnologia da informação e comunicação (TIC) para seu crescimento e bem estar econômico ao longo dos anos e como isso possibilita que Xi Jinping faça um planejamento mais ousado para o país durante seu governo.

Por último será estudado de forma breve o processo de integração do ciberespaço às forças armadas da China e como o país habilmente equilibra suas desvantagens materiais de forma a manejar suas vulnerabilidades nos quesitos de defesa e segurança cibernética. Será acompanhada também a mudança de postura do país não somente em relação ao ciberespaço, como toda a política externa de Pequim após a posse de Xi Jinping em 2013. E tendo esta nova posição um impacto direto na relação da China com os demais países do Sistema Internacional será um objetivo deste capítulo identificar os impactos para o cenário internacional da atual política do presidente Xi Jinping para o ciberespaço.

A escolha deste tema se justifica ao considerarmos que em uma sociedade cada vez mais conectada, se faz necessário o estudo do desenvolvimento desta rede e como ela afeta relações humanas tradicionais, tanto da perspectiva privada quanto a estatal. Compreender as políticas desenvolvidas nesta área por parte dos Estados é essencial para uma percepção ampliada das RI no século XXI. A urgência deste trabalho pode ser justificada também pela escassez de conteúdos como este na língua portuguesa.

Além disso, a China é o quinto país mais atacado por ataques cibernéticos no planeta (KARSPERSKY, 2020), sendo os seus serviços públicos e infraestruturas críticas as mais afetadas por estas tentativas de causar danos a seus sistemas (AKAMAI, 2020). Ao mesmo tempo também é um dos Estados com grande número de acusações por tentativas de lesar o espaço cibernético de outrem. Entre as diversas alegações por parte dos demais países podemos citar o ataque a empresas inglesas em 2007, invasão de e-mails do governo estadunidense em 2008, e alguns ataques a empresas estrangeiras como o Google, todavia não há provas concretas do envolvimento chinês (VENTRE, 2012).

Por fim, a Universidade Federal do Pampa conta com um acervo considerável e crescente de materiais acadêmicos de qualidade para a região asiática, abordando temáticas variadas como economia, política internacional, cultura, história, entre diversos outros. Todavia, há uma escassez de trabalhos relacionados a assuntos de segurança, em especial segurança cibernética. E este trabalho pode fornecer um material útil para outros estudantes interessados na área, além de aumentar a gama de tópicos tratados dentro do curso de Relações Internacionais da universidade.

Para este trabalho utilizaremos do método qualitativo, obtendo os dados necessários por meio de documentos oficiais fornecidos por órgãos como, o Comitê Oficial para Assuntos do Ciberespaço Chinês, relatórios divulgados pela União Internacional de Telecomunicações**,** Corporação da Internet para Atribuição de Nomes e Números. Além de contar é claro, com estudos bibliográficos de modo a fundamentar esta pesquisa. Por meio do método hipotético-dedutivo tentaremos falsear a hipótese apresentada. E sendo impossível confirmar uma hipótese (MARCONI e LAKATOS, 2000) foram buscados elementos concretos que possam negar a afirmação feita inicialmente.

Era esperado que o idioma viesse a se tornar um fator limitador ao longo da pesquisa, pois diversos dos documentos disponíveis estavam em mandarim. Este receio foi parcialmente confirmado, pois embora muitas das fontes primárias estivessem em mandarim, a China disponibiliza versões em inglês de seus documentos mais importantes, como é o caso de seu Livro Branco e dos Planos Quinquenais. Porém a maior barreira encontrada foi aquela que exigiu a busca por materiais originais fossem disponibilizados em sites oficiais da administração pública chinesa, já que as pesquisas nestes sistemas deveriam ser feitas em hanzi. Para contornar esta dificuldade se utilizou de material bibliográfico de fontes diversas que divergiam em suas ideias e debates.

2 SMART POWER E DIFUSÃO DE PODER DENTRO DO CIBERESPAÇO

Este capítulo será dividido em duas partes, sendo a primeira “A origem do ciberespaço e seus problemas securitários” tratando sobre as origens da internet, a revolução da informação, territorialidade e soberania no espaço cibernético, ameaças encontradas e a securitização deste. Já em um segundo momento será discutido como o ciberespaço é “Um grande jogo de xadrez", as perspectivas de poder para os Estados e como o espaço digital pode ser convertido em poder cibernético.

2.1 A origem do ciberespaço e seus problemas securitários

A sociedade do século 21 é, em escala global, uma sociedade conectada. Em janeiro de 2019 foi alcançada a marca de 4.388 bilhões de pessoas utilizando serviços de internet, e seus acessos em sua maioria se deram por meio de dispositivos que cabem na palma de suas mãos (KEMPT, 2019). O crescimento do número de usuários em relação ao ano anterior foi de 366 milhões (9%), o que é mais do que a população do Brasil, Argentina, Uruguai, Chile, Peru, Colômbia e Equador somadas. Outro número que acompanhou o crescimento dos usuários de internet foi o tempo gasto por pessoa nos meios digitais, com a média mundial se estabelecendo em 6 horas e meia diárias.

Em sua pesquisa Kempt (2019) afirma também que foram registrados 5,112 bilhões de usuários únicos de telefones ao longo de 2018, sendo que 63.79% destes acessaram ao menos uma das diversas redes sociais disponíveis. O Google de forma não surpreendente foi o site mais acessado neste ano, seguido pelo YouTube e o Facebook. As relações humanas para o século XXI foram drasticamente alteradas com a chegada da era digital, hoje as noções de fronteira, espaço, língua e território foram modificadas e as maneiras de se absorver a informação e a realidade.

Mas em sua origem a internet não foi moldada como uma tecnologia para o público civil, na realidade esta foi uma criação tecnológica voltada para o uso militar durante a guerra fria. Segundo Adabo (2014), após o lançamento dos satélites Sputnik 1 e 2 por parte da União das Repúblicas Democráticas Soviéticas (URSS) o presidente dos Estados Unidos. Dwight Eisenhower instituiu o programa ARPA (Advanced Research Projects Agency), que visava o desenvolvimento de tecnologias de informação e comunicação. Segundo a autora, o propósito inicial desta tecnologia

seria para manter a comunicação entre os principais postos militares e acadêmicos do país durante e após um ataque nuclear.

Em 1963 o psicólogo e engenheiro Joseph Lickider apresentou ao grupo de cientistas do projeto a sua ideia de criar uma “Rede Intergalática de Computadores”, e somente 6 anos depois uma rede de comunicação conectada entre diferentes computadores foi apresentada (LOPES, 2014). O curioso é que até o ano de lançamento a ideia era completamente desacreditada pela maior parte da comunidade científica e empresarial da época devido ao alto custo que seria apresentado e inviabilizando sua operacionalidade na maior parte dos casos, como conta o professor Leonard Kleinrock em entrevista (BAY, 2018).

Em uma tentativa de preencher outras lacunas a respeito do surgimento da internet, Campbell-Kelly e Garcia-Swartz (2013) apontam que embora a ARPANET tenha sido criada em 1969, não se foi o único projeto no mundo que pretendia criar uma rede mundial de computadores. O seu sucesso em relação aos demais protótipos vem com a integração desta invenção a demais tecnologias desenvolvidas na década seguinte. A rápida proliferação de desktops dentro dos Estados Unidos, e posteriormente a criação de protocolos de internet para estas máquinas (TCP/IP),e a falta de organização política e econômica de possíveis rivais durante a década de 70 auxiliou em muito para que a ARPANET se tornasse a tecnologia de referência.

De fato, em termos técnicos o Transmission Control Protocol agregado ao Internet Protocol, o TCP/IP é um sistema de linguagem operacional que permitiu e permite que o ciberespaço se desenvolva a nível global, pois assim todas as máquinas podem se conectar em um mesmo idioma de programação. A ideia de criar protocolos que possibilitassem a identificação da máquina surgiu do mesmo princípio dos telefones fixos, onde se tem um número sem variação que possibilita a comunicação entre usuários. Embora o projeto tenha se iniciado em 1977, apenas em 1983 se tornou um projeto robusto, e somente se tornou um padrão global no início da década de 90 (CAMPBELL-KELLY e GARCIA-SWARTZ, 2013). Estes protocolos são divididos em quatro camadas que cumprem funções distintas e permitem a manutenção da integridade dos dados ali trafegados, sendo eles aplicação, transporte, rede e interface (MARTINS, 2012).

Duarte (2003) explica que a primeira camada, a de aplicação, permite que sua máquina envie e receba informações de outros programas, o exemplo mais popular está no HTTP, que é o protocolo responsável por sites da web em geral. O transporte

é um serviço intermediário que realiza o transporte dos dados armazenados em rede, atuando literalmente como um gigantesco sistema de transporte coletivo que opera em milésimos de segundo. Esta segunda camada é intimamente ligada à rede, pois esta camada é onde ocorre o gerenciamento logístico, empacotando os dados e etiquetando seu destino conforme os dados do destinatário, que neste caso é o IP. E após todo este processo é que finalmente os pacotes de dados são traduzidos de acordo com o tipo de protocolo de rede aplicado em cada máquina, a mais utilizada mundialmente é o serviço de Ethernet, que pode ser alterado caso, por exemplo, o usuário esteja recebendo seus dados em um Macbook que utiliza uma rede chamada FDDI.

O uso destas tecnologias garante o bom funcionamento do serviço de dados das máquinas conectadas à internet, pois cada sequência numérica é única e exclusiva, não encontrando uma cópia em qualquer outro lugar do mundo. De início foi utilizado o sistema IPv4, ou seja, uma sequência numérica composta por quatro blocos numéricos separados por pontos. Mas com o aumento do número de usuários, hoje a tecnologia foi ampliada para uma sequência de seis blocos numéricos separados por pontos, o IPv6 (TERHOCH, 2019). Todos estes protocolos são softwares que permitem o funcionamento do espaço cibernético, mas não somente eles são suficientes.

As infraestruturas físicas do sistema são chamadas de hardwares, e estes são diversos e se conectam a partes distintas destes protocolos. Placas de Rede (NICs) que são cartões conectados a placa mãe de máquinas que são basicamente caixas de correio, ainda usando a analogia da logística de transporte de pacotes, cabos que conectam desde máquinas locais até os gigantescos serviços ultramarinos de conexão entre servidores, hub que é um pequeno aparelho para controlar o tráfego, e que assim como os cabos pode tomar proporções locais ou mundiais, estes em específico atuam diretamente em conjunto com a terceira camada do TPC/IP. Outra função essencial para o funcionamento da rede está nos servidores que atua em um nível intermediário entre as máquinas comuns e o grande sistema de rede, estes são responsáveis por armazenar informações de diversos níveis por meio de processadores, bancos de memória, portas de comunicação. Entender a complexidade tecnológica para a execução do espaço cibernético é fundamental para que posteriormente seja possível visualizar as inseguranças proporcionadas por ele.

A transição desta tecnologia para além dos âmbitos acadêmicos e militares ocorreu durante a década de 80 até o ano de 1994, a partir da popularização da compra de computadores para uso pessoal e empresarial, juntamente com a completa privatização da rede. Também foi durante este período que a interface da web se tornou amigável ao consumidor por meio da criação do *World Wide Web*, também conhecido hoje como WWW (ADABO, 2014). Por fim, o último passo para a globalização da rede foi a sua desestatização, o projeto ARPANET foi vendido de forma progressiva para empresas privadas, visto que os órgãos de defesa e segurança dos Estados Unidos não permitiriam o uso comercial desta tecnologia (CAMPBELL-KELLY e GARCIA-SWARTZ, 2013).

A partir daí, diversos autores começaram a trabalhar com a temática da internet e as perspectivas de mudança que ela traria à humanidade. O termo “ciberespaço” foi cunhado por William Gibson em seu conto “Neuromancer” de 1982. Posteriormente esta expressão se popularizou entre os acadêmicos, militares, e também entre o setor de entretenimento, sendo o filme “Matrix” uma referência direta às obras de William Gibson. É curioso que o autor tenha não só criado anteriormente ao lançamento comercial da internet este termo, como também elaborado em suas tramas inseguranças que vivemos hoje, como o roubo de dados, contrabando de informações, exposição não autorizada de dados e a atuação de hackers no século XXI (OWENS, 2017).

Quase duas décadas depois Lévy (2000) também deixou contribuições significativas para os estudos do ciberespaço, afirmando que este é “ [..] espaço de comunicação aberto pela interconexão mundial dos computadores e das memórias dos computadores”. Esta definição se aproxima em muito com os primeiros objetivos da ARPA quando foi criada, todavia seu entendimento do conceito vai além, englobando especialmente às mudanças culturais proporcionadas pela tecnologia. Também afirma a artificialidade da rede com seu “caráter plástico, fluido, calculável com precisão e tratável em tempo real, hipertextual, interativo e, resumindo, virtual da informação que é, parece me, a marca distintiva do ciberespaço” que durante as décadas seria discutida dentro dos debates de segurança e territorialidade do espaço cibernético.

Em um acréscimo ao conceito apresentado por Lévy, Ventre (2012) afirma que não se deve desconsiderar os aspectos físicos do espaço digital, como os satélites em órbita, computadores em funcionamento, as próprias indústrias de produção e

criação de novas tecnologias que ampliam o espaço virtual. O autor também subdivide o ciberespaço em três: “a) Uma camada interior que é física e material (que é onde estão os hardwares, infraestrutura e etc, b) Uma camada intermediária, com os softwares e aplicativos, C) Uma camada cognitiva, ligada à capacidade humana de criação”. Esta divisão é interessante para os estudos de segurança e defesa cibernética, pois proporciona uma especificidade na hora de compreender estrategicamente os riscos e a tomada de decisão por parte dos Estados.

A assimilação gradual desta tecnologia afetou também o modo com que os Estados planejam sua própria segurança. Castells (2003) analisa que os grandes desafios à proteção dos países não viriam necessariamente de tentativas de hackear informações de departamentos de Defesa, mas que a sabotagem ao funcionamento de infraestruturas críticas que poderiam prejudicar a vida de seus cidadãos. Naquela época já havia ocorrido alguns episódios de invasão de hackers, como foi o caso da Indonésia no ano de 1998[1], porém sem grandes resultados ou danos infligidos (LOPES, 2014). Entretanto, os incidentes internacionais ocasionados por informações divulgadas por Edward Snowden e Wikileaks mantém os Estados alertas para a necessidade de defender seus dados.

E esta multiplicidade de fatores de risco é tomada em consideração pelos Estados quando estes vão formular suas estratégias de defesa. O Reino Unido, por exemplo, compreende que “o ciberespaço é um domínio interativo feito de redes digitais usadas para armazenar, modificar e comunicar informações. Isto inclui a internet, mas também os outros sistemas de informação que apoiam nossos negócios, infraestrutura e serviços[2]” (UK, tradução nossa, 2011). E esta visão é também adotada pelos Estados Unidos que salienta a necessidade de proteção de dados públicos e privados, das infraestruturas críticas e o desenvolvimento de novas tecnologias para o setor são fundamentais para a manutenção do poderio e status estadunidense perante o sistema internacional (EUA, 2017).

A República Popular da China segue este padrão, indicando conformidade com às ideias apresentadas anteriormente, e em seus documentos de modo geral

---

[1] Neste ano 3000 hackers comprometeram serviços de email dentro d Indonésia (LOPES, 2014)

[2]Cyberspace Is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the ther information systems that support our businesses, infrastructure and services.

acrescenta que o país “Defende a informação e cibersegurança, e também a manutenção da soberania cibernética, segurança da informação, e estabilidade social” (The State Council Information Office, tradução nossa, 2019)[3]. Em suma, os Estados apresentam em linhas gerais uma definição similar a respeito do que é o espaço cibernético e quais são suas responsabilidades, desafios e oportunidades. Em países onde o espaço cibernético é mais desenvolvido é possível encontrar referências mais claras a respeito da manipulação do espaço digital para os interesses governamentais.

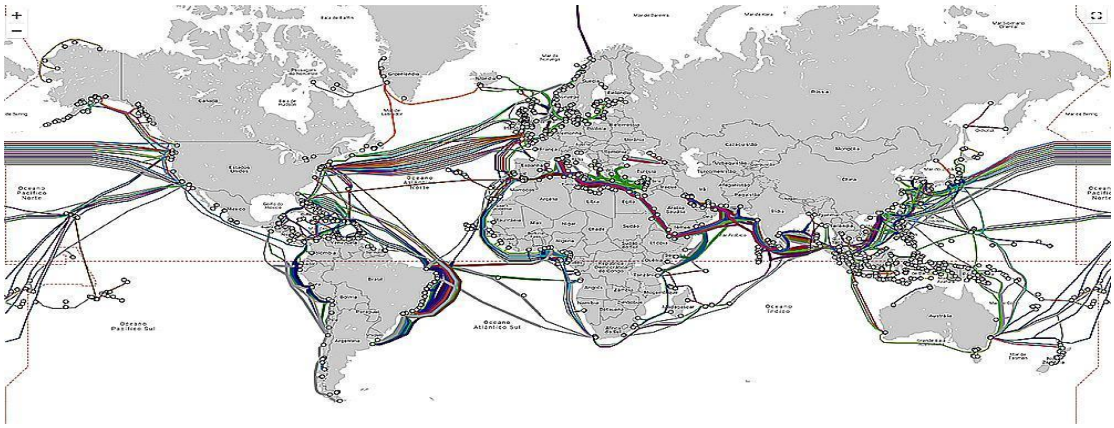
Ao considerar a divisão do ciberespaço em camadas como foi proposto por Ventre (2012) pode ser compreendido de modo mais amplo as políticas chinesas para o ciberespaço. A tomada de decisão da China em relação à Era da Informação é de arquitetura centralizadora, ou seja, todo o desenvolvimento de rede e das três camadas é ditado, limitado ou ampliado segundo o planejamento governamental (HU, 2015). O país mantém regras extremamente rígidas para o uso da internet por parte de sua população e este controle se expande para a forma com que as reformas econômicas são dirigidas, o que impacta diretamente na capacidade chinesa de investimento em pesquisa e desenvolvimento (P&D) de novas tecnologias da comunicação e informação (TIC) (AUSTIN, 2014).

Tendo então delimitado o conceito de espaço cibernético e discutido de forma breve as perspectivas dos Estados para com ele, é de interesse desta pesquisa compreender a relação entre as noções tradicionais de território e a artificialidade do espaço virtual. É uma característica da era da informação ser global, onde as barreiras geográficas neste meio não possuem mais a mesma importância, sendo a distância facilmente quebrada pela internet (KEOHANE e NYE, 2000). Entretanto, embora difuso dentro das discussões sobre o ciberespaço, o entendimento dos conceitos de soberania, e por consequência território, é uma discussão a ser realizada. Sendo o território um “conceito gerado por indivíduos organizando o espaço segundo seus próprios objetivos” (GOTTMAN, 2012), é possível discutir e adaptá-lo para o espaço virtual. O mais próximo a uma versão física de um mapa do ciberespaço poderia ser o sistema mundial de cabeamento submarino, sendo apenas um esqueleto para o que realmente configura todo este novo território.

---

[3] “They safeguard information and cyber security, and resolutely maintain national cyber sovereignty, information security and social stability”

Estrutura de cabeamento submarino



Orenstein, 2017

A partir deste mapa podemos compreender o interesse dos Estados em delimitar limites, mesmo que algumas vezes intangíveis. Estes cabos atravessam mares e continentes, mas o espaço em si como apontou Ventre (2012) possui diversas camadas que permanecem fora das vistas daquilo que é palpável. Neto (2018) discute justamente a territorialidade do espaço cibernético, pois compreende que se o domínio territorial em seu sentido tradicional é um aspecto do poder dos Estados, este não se perde em meio a artificialidade do meio digital.

Não é a primeira vez que limites territoriais são pensados por meio de uma perspectiva política mais abstrata. As definições de território marítimo e aéreo surgiram a partir de convenções e acordos políticos, sendo algo relativamente recente se compararmos com as fronteiras terrestres, tendo respectivamente seus direitos modernos estabelecidos através de acordos firmados após a segunda guerra mundial. Novamente ao firmar tais tratados os Estados buscavam regulamentar a sua soberania perante os demais países do sistema internacional. Uma exceção ao fenômeno da territorialização do ambiente está no espaço sideral propriamente dito. Por meio de diversas convenções e tratados firmados foi acordado que este não seria territorializado e que nenhum Estado deveria declarar soberania a respeito dos corpos espaciais. Este é o motivo pelo qual ninguém proclamou a Lua como sua, por exemplo, ou pelo menos por enquanto.

O ciberespaço possui uma condição única para a sua existência que é a vontade humana, pois sem os hardwares fabricados não é possível alcançar este espaço. Isto concede ao ciberespaço uma característica artificial e ao mesmo tempo

indica outra condição física do espaço cibernético: ele é replicável (SHELDON, 2016). Nos casos tradicionais já citados, possuímos a plena noção de que embora tenhamos dividido politicamente estes territórios, em um conceito puramente físico sejam unidades. Já dentro do espaço cibernético é possível replicar e expandi-lo a todo tempo, essencialmente os seres humanos estão projetando novas formas de criar e inovar nesta tecnologia a todo tempo.

O primeiro marco de uma tentativa de territorializar o espaço é bem simples de encontrar quando o endereço dos mais diversos sites no Brasil por exemplo é acompanhado de um ".br". Este é o sinal mais claro de domínio do espaço comum a ser encontrado à primeira vista (FERREIRA NETO, 2014). Elementos de defesa e segurança também são vistos como exemplos de territorialização, a criação por parte dos Estados de departamentos especializados no assunto como o National Cyber security Division dos Estados Unidos National Cyber Security Center são planejamentos para a demarcação, proteção e exercício de suas capacidades soberanas dentro do *Global Domain (HONG* e GOODNIGHT, 2019).

> "A segurança dos backbones, dos data centers; dos firewalls e demais elementos de filtragem, e da hospedagem de sítios são alguns dos exemplos de que há, "nitidamente", um exercício de poder no espaço cibernético, portanto havendo um território, e, por conseguinte, sua respectiva fronteira." (FERREIRA NETO, 2018, p. 9)

Este é um debate inicial que, assim como o próprio conceito de ciberespaço, não possui uma única interpretação. Os Estados se organizam através de seus próprios protocolos, não seguindo uma verdade universal, sendo então às interpretações territoriais sobre este espaço artificial completamente flexíveis perante o poder e às interpretações dos atores do Sistema Internacional. E esta indistinção clara é o que torna o universo virtual pluralista, onde as decisões são compartilhadas entre o sistema, a partir de interações constantes dentro do que pode ser chamado de "ciberesfera—definida como um conjunto histórico de camadas materiais, organizacionais, regulatórias e socioculturais de relações comunicativas entre

populações, máquinas e instituições desenvolvidas em escalas[4]"(HONG e GOODNIGHT, tradução nossa, 2019).

Assim como os debates a respeito de sua territorialização, às questões de soberania dentro do espaço cibernético também são imprecisas. HAO (2017) compreende que existem três perspectivas ao tratar da soberania no ciberespaço, a do indivíduo, a do Estado, e a da comunidade internacional, e que quando um destes grupos é desprezado em ações dos outros dois provoca pontos de atrito. Necessariamente haverá limitadores entre estes agentes, pois mesmo com o Estado limitando de diversos modos os dados disponíveis em rede, sempre haverá um marco impeditivo de limitações demasiadas que é a própria funcionalidade da tecnologia. E que ao tratarmos deste conceito haverá contradições pois a internet é livre, o direito à informação de forma irrestrita é visto como um direito humano (HAO, 2017), e que é a soberania é uma forma de concentrar poder nos Estados ignorando diversos grupos que atuam dentro nas redes (NYE, 2012).

Os países obtêm esta soberania por meio de legislações de modo a permitir ou limitar acessos dentro do país, proibir e coibir ações potencialmente prejudiciais ao Estado, e por fim, fortalecendo a todo tempo seu sistema de defesa contra ameaças externas (CHEUNG, LINDSAY e REVERON, 2015). A China é o principal país a defender a soberania estatal perante o espaço virtual. Em suma, deste modo pode manter o controle sobre as informações que circulam em seu ciber território, e também alia este discurso a suas aspirações de balancear o jogo de poder entre as nações, defendendo abertamente a necessidade de uma governança compartilhada e justa da internet (GJESVIK e SCHIA, 2017).

O país precursor da internet hoje é referência em relação a seus sistemas de defesa, prevenção de ameaças cibernéticas, e também para o uso ofensivo destas tecnologias. Em sua estratégia de defesa cibernética, divulgado em 2015 pelo Departamento de Defesa dos Estados Unidos, são traçadas metas em sua organização para controle e uso do ciberespaço: a) a proteção dos dados, rede e sistema do próprio departamento de defesa, b) Se preparar para defender o país e seus interesses contra ataques cibernéticos e suas consequências, c) estar preparado

---

[4]"cybersphere—defined as a historical ensemble of material, organizational, regulatory, and socio-cultural layers of communicative relations among populations, machines, and institutions developed across scales—

para combater apoiar operações militares e seus planos de contingência, d) fomentar e manter alianças internacionais visando a estabilidade e segurança do espaço cibernético. Por meio deste documento é possível observar a aplicação tática adotada para o ciberespaço, além do interesse em ampliar sua zona de segurança para além de seu próprio espaço cibernético.

Às preocupações com a integridade da rede e limitadores de acesso tomaram proporções mais alarmistas pelo globo a partir dos grandes eventos securitários do ciberespaço a partir de 2007. Antes desta data o perigo era real, porém ainda não havia tomado as devidas proporções dentro da comunidade internacional. Durante três semanas a Estônia foi alvo de ataques de Negação de Serviço Distribuído (DDoS)[5], comprometendo o uso de infraestruturas críticas durante este período (SPIRI, 2020). A Estônia foi o primeiro país a adotar o uso da internet de modo generalizado em suas estruturas de governo, sendo que praticamente todas as funções prioritárias para o funcionamento do país foram comprometidas (FOLHA, 2007). Além de ataques ao governo, os principais bancos do país ficaram comprometidos, e os sistemas de comunicação também foram hackeados (FOLHA 2007). Tudo isso se iniciou a partir de um desentendimento entre a Rússia e a Estônia quando o país atacado decidiu realocar monumentos oriundos da antiga União das Repúblicas Socialistas Soviéticas (CARR, 2011).

O ataque foi atribuído a hacktivistas russos independentes, e embora houvesse uma grande desconfiança internacional a respeito do envolvimento do governo da Rússia, nada pode ser comprovado. Esta na verdade é uma conclusão razoavelmente comum dentro de incidentes envolvendo o ciberespaço, devido a complexidade de fornecer nomes específicos para serem responsabilizados. E olhando para o complexo processo pelo qual a informação percorre entre o remetente e o destinatário não é algo assim tão surpreendente. Brito (2015) afirma que existem diversas portas ao longo do caminho de rede que são desconhecidas às vítimas, estas podem estar tanto nos softwares quanto nos hardwares e permanecer fora do conhecimento até que em algum momento seja útil utilizá-las.

E foi algo próximo a ideia destes malwares desconhecidos e silenciosos o que ocorreu no ano de 2010, com a sabotagem das centrífugas iranianas por meio de um

[5]Distributed Denial of Service

malware, um software malicioso que tem o objetivo de prejudicar funções gerais ou específicas da máquina em que for inserido. O enriquecimento de Urânio dentro do Irã era algo que causava desconfiança nos mais variados países do ocidente, sendo alvo de diversas acusações de um possível uso deste urânio para fins bélicos (COLLINS; MCCOMBIE, 2012). Este foi marcado como a primeira vez que um malware causou estragos físicos em uma infraestrutura física, entrando para a história como a primeira arma cibernética do mundo (LINDSAY, 2013).

Este vírus foi espalhado por mais países no mundo, como Índia, Rússia e Indonésia, mas em nenhum outro lugar causou tantos danos como no Irã, pois este foi desenhado para o tipo de estrutura específica presente neste país. Além de danificar a estrutura da centrífuga gradualmente, uma de suas configurações também envolvia a negação das funções de alerta dentro do maquinário, ou seja, caso não fosse identificado poderia levar a danos permanentes da estrutura e potencialmente causar até mesmo um desastre nuclear. Este vírus foi identificado por especialistas como algo extremamente sofisticado, reduzindo drasticamente a lista de suspeitos. Todavia, assim como o caso apresentado na Estônia, embora existam fortes suspeitas sobre a participação de Israel devido a suas disputas regionais com o país, nada foi comprovado.

Estes dois casos colaboraram para que houvesse uma virada de chave dentro da compreensão global das necessidades de proteger o seu espaço cibernético, e embora houvesse sim movimentos pela segurança e defesa das redes foi a partir de eventos como estes que a sensação de insegurança se tornou palpável. A segurança é explicada por Buzan, Waever e Wide (1998) como a prática Estatal de tornar um problema em uma ameaça, não sendo exatamente necessário que aquela ameaça seja real. E este é o processo de securitização que é “essencialmente aberto, e subjetivo para influência de fatores exógenos.” (BUZAN e WÆVER, 2003). E este conceito quando confrontado com o cenário internacional engloba a compreensão sobre como “coletividades humanas se relacionam entre si em termos de ameaças e vulnerabilidades” (BUZAN, WÆVER e WILDE, 1998). Efetivamente o ciberespaço salta de um tópico politizado para securitizado com o próximo caso a ser analisado. A securitização envolve uma sensação de emergência, onde processos anteriormente custosos e burocráticos podem ser rapidamente aprovados, o que é efetivado em 2003.

É útil comentar que a China de Xi Jinping irá aplicar uma política para securitizar não somente o seu ciberespaço, como também diversos tópicos econômicos, militares e sociais durante a reestruturação da agenda securitária do país. Ji (2016) explica que em termos de segurança, a manutenção do regime mantido pelo Partido Comunista Chinês (PCC) estará sempre em primeiro plano na formulação de políticas domésticas e internacionais. Posteriormente durante o governo de Xi Jinping e sua postura distinta para as relações exteriores do país é a lista de riscos e necessidade de proteção ao espaço cibernético torna o ciberespaço um ponto vital para a proteção do ciberespaço.

O último caso a ser comentado aqui se diferencia dos demais, pois, não se trata de danos a infraestruturas críticas, e sim de um caso de espionagem por parte do governo estadunidense a diversos Estados e empresas. Edward Snowden era um agente da Agência de Segurança Nacional dos Estados Unidos (NSA), e divulgou o maior escândalo envolvendo ciberespionagem que o mundo presenciou até este momento.

Snowden começou a trabalhar para o governo estadunidense em 2006, e assistiu de perto a espionagem de inimigos ou então de “aliados que deveriam ser acompanhados”, e esta rede de espionagem contava também com empresas estadunidenses do setor, como o Google e o Facebook, pois a NSA possuía acesso a seus servidores (HARDING, 2014). Em suma, havia mais de um serviço com funções de espionagem, sendo eles o *PRISM, Boundless Informant, XKeyscore e o Stateroom.* Foram divulgados documentos provando esta ilegalidade, registrando inclusive o monitoramento de emails enviados por chefes de Estado como a presidente Dilma Rousseff e a primeira-ministra Angela Merkel (HARDING, 2014).

Embora neste caso se tenha não somente provas concretas de atos ilícitos por parte do Estado, ainda assim não houve grandes sanções por parte da comunidade internacional aos Estados Unidos. Mas isto obrigou aos demais atores estatais a providenciar, em maior ou menor medida, modos de melhorar a segurança de seus Estados, como foi o caso do Brasil com a aprovação do Marco Civil da Internet (BRASIL, 2014a), ou da China com a criação de seu próprio conselho especializado em defesa do ciberespaço (NEGRO, 2019).

Medidas efetivas de segurança só podem ser realizadas por países com plenas capacidades de desenvolvimento de seus próprios softwares e hardwares, pois em essência mesmo com aspectos regulatórios, a compra e uso de tecnologia estrangeira para fins de segurança do Estado apresentam riscos claros. É fácil abrir portas

invisíveis no sistema de defesa do outro quando quem criou o aparato tecnológico que ele utiliza é você (BRITO, 2015).

2.2 Um grande jogo de xadrez

O poder é um dos elementos de análise constantemente debatidos dentro das escolas teóricas de Relações Internacionais, divergindo algumas vezes entre escolas teóricas semelhantes (BARROS, 2015). Em termos generalistas, em seu dicionário de ciência política Bobbio define poder como

> Em seu significado mais geral, a palavra Poder designa a capacidade ou a possibilidade de agir, de produzir efeitos. Tanto pode ser referida a indivíduos e a grupos humanos como a objetos ou a fenômenos naturais (como na expressão Poder calorífico, Poder de absorção) (BOBBIO, 1998, p. 943)

Mas este considera também este como um conceito limitado, e que o poder em si pode ser visto como um poder relativo, pois a consideração do que é ou não poder ou que é ou não poderoso dentro de uma análise envolve especialmente onde está a métrica comparativa. Um pai pode ser mais poderoso em uma escala hierárquica do que seu filho, porém o indivíduo em comparação ao Estado se encontra em uma situação invertida, onde em condições normais, o Estado exercerá mais poder sobre ele (BOBBIO, 1998).

Já para Hobbes em O Leviatã (2003), o conceito de poder é específico para relações sociais, “o poder de um homem (universalmente considerado) consiste nos meios de que presentemente dispõe para obter qualquer visível bem futuro.” Mas como neste estudo iremos nos concentrar especialmente na visão estadocêntrica, podemos avançar um pouco neste mesmo texto e identificar que para o autor “O maior dos poderes humanos é aquele que é composto pelos poderes de vários homens [...]que tem o uso de todos os seus poderes na dependência de sua vontade: é o caso do poder de um Estado”. E junto a isso, a visão deste autor também é voltada para o recurso material possuído, que é refletida posteriormente na escola realista de relações internacionais.

No realismo o poder está centralizado na perspectiva estatal alterando as ações dos demais atores dentro do Sistema Internacional conforme a análise feita individualmente. Por exemplo, dentro da teoria do realismo ofensivo de Mearsheimer o foco em suas interpretações de poder entre os Estados está nos aspectos militares dos mesmos. Mesmo dividindo sua análise entre poder real e poder latente, onde o

primeiro é a capacidade militar atual do Estado e a segunda sendo sua capacidade de converter demais recursos em poder em caso de necessidade (RONCONI, 2015), o foco de seu estudo está completamente focado na interpretação bélica do poder.

Outro autor que também se debruça a compreender como o poder influencia na tomada de decisão por parte dos atores internacionais estatais é Waltz, que em sua teoria sobre o equilíbrio de poder admite que o sistema internacional em si é um ambiente competitivo onde o poder vale mais do que a justiça (PEREIRA, S/A), e que cabe aos Estados lutar individualmente por sua própria sobrevivência, pois não haverá nenhuma outra organização a fazer isto por eles. Existe um desequilíbrio de forças dentro do sistema não sendo do interesse de todos a disputa pelo ápice, mas aqueles com maiores capacidades de competição estarão mais interessados em competir por poder com os Estados mais potentes do sistema (WALTZ, 2001). A necessidade de obter mais poder perante os demais se dá pois segundo o autor “Como qualquer Estado pode a qualquer momento usar a força, todos os Estados têm de estar constantemente prontos para opor à força a força ou pagar o preço da fraqueza” (2001). Suas contribuições então para a renovação da teoria do equilíbrio de poder é que esta é um produto das forças anárquicas apresentadas dentro do sistema.

Keohane e Nye (2000) afirmam que “nós vivemos na era da interdependência”, com esta frase que os autores iniciam sua retórica a favor da teoria dos Regimes Internacionais. Interdependência na política internacional se refere a situações criadas por efeitos recíprocos entre países ou entre atores do sistema em diferentes países. Este também não é um sistema de benefícios mútuos, onde os Estados obterão os mesmos ganhos em uma negociação, o Estado que possui capacidade própria de produção de recurso ou monopólio de uma tecnologia cobiçada pelo mercado internacional estará em melhores condições dentro de um acordo do que aquele que não dispõe deste produto em seu território.

Nesta teoria, a visão do mundo em relação ao poder é mais abrangente do que aquela vista pela perspectiva realista, pois é compreendido que após a Segunda Guerra Mundial o globo se tornou mais conectado, e outros tipos de poderes também se mostram variáveis necessárias para a compreensão do sistema. "O poder pode ser pensado como a capacidade de um ator de levar os outros a fazer algo que de outra forma não fariam (e a um custo aceitável para o outro ator). O poder também pode ser

concebido em termos de controle sobre os resultados" (KEOHANE e NYE,tradução nossa, 2000, p.11)[6].

E para momentos em que a interdependência afeta de forma prejudicial os Estados, os autores dividem em dois casos, os atores podem ficar *sensíveis* ou *vulneráveis*. A sensibilidade é um momento de tribulação passageiro, não abalando a estrutura do Estado, sendo possível recuperar os danos causados pela mudança no status quo de seu acordo com os demais atores do sistema. Já a vulnerabilidade envolve condições mais complexas em que o Estado por uma série de razões não estava preparado para se reinventar diante da mudança. Dentro do contexto deste trabalho podemos considerar como exemplo o já citado caso de Edward Snowden, onde os Estados com maior capacidade de produção de tecnologia de defesa, e organização burocrática de sua soberania digital obtiveram um maior desenvolvimento de suas estratégias de defesa do que aqueles que são dependentes da tecnologia externa para a própria proteção de dados sigilosos.

E dentro do sistema globalizado da Era da Informação, onde há uma evolução das variáveis de análise, pois agora não apenas questões materiais estavam em jogo, mas também o mundo artificial do ciberespaço. Questões da política clássica permanecem válidas para este espaço, pois entender "Quem se beneficia?" ou "Quem governa? E quais são os termos desta governança" ainda são importantes e relevantes dentro deste novo contexto. Ainda nos anos 2000 os autores afirmam, e com razão, que os Estados irão tentar moldar o ciberespaço do mesmo modo que moldam o fluxo de comércio por suas fronteiras (CASTELLS, 2000). Em seus trabalhos futuros Nye trabalha o conceito do ciberespaço como um novo conceito para o século XXI, e para compreendermos isto é necessário que antes exista uma discussão a respeito de duas faces do poder, o *hard power* e o *soft power.*

O primeiro conceito abrange as perspectivas mais tradicionais das Relações Internacionais,o aspecto físico do poder abrangendo as sanções econômicas, diplomacia coercitiva, e forças militares (WAGNER, 2005). Este se distingue, pois o convencimento do outro ator vem por meio da coação, utilizando recursos tangíveis principalmente (GALLAROTTI, 2015). Exemplos do uso deste não são difíceis de

---

[6]Power can be thought of as the ability of an actor to get others to do something they otherwise wouldn't do (and at an acceptable cost to the other actor). Power canal sobe conceived in terms of control over outcomes. (KEOHANE & NYE, 1989, p.11)"

encontrar em portais de notícia, pois é o que mais chama a atenção dentro da mídia como, por exemplo, os conflitos entre o Paquistão e a Índia pelo território da Caxemira que tomou proporções bélicas três vezes ao longo do século XX. Outro caso que chamou a atenção, mas dessa vez da academia, foi desenvolvimento bélico chinês que por vezes foi interpretado de modo quase alarmista (MEARSHEIMER, 2006), onde sua projeção de futuro para o oriente envolveria uma guinada dos países vizinhos a uma aliança com os Estados Unidos de modo a enfraquecer o status chinês de potência regional.

O Soft power ou poder brando é o conceito mais desenvolvido ao longo dos anos, tendo diversos trabalhos discorrendo a respeito deste conceito, sendo este a capacidade de se obter ganhos de outros atores por meio da atração, sem envolver coerção física ou monetária (NYE, 2017). Em sua teoria, Nye argumenta que a globalização e a difusão de elementos culturais dos Estados seriam importantes para redesenhar as relações entre atores do sistema internacional. Este foi um conceito muito bem aplicado dentro da China, pois durante seu boom de crescimento e desenvolvimento aplicou um esforço considerável em se manter como uma potência de ascensão pacífica, de modo a tentar tranquilizar seus vizinhos a respeito de suas pretensões de desenvolvimento dentro do cenário global.

A preocupação chinesa com a visão passada aos demais países com a expansão de suas capacidades ao longo do século XX e XXI fez com que a discussão da alta cúpula do partido comunista chinês e a academia nacional ligasse com frequência o uso deste conceito aos anseios das políticas de Ascensão ou Desenvolvimento Pacífico (LI, 2008). O conceito é absorvido dentro do país a partir de uma visão voltada para a cultura é frequentemente aplicado ao âmbito doméstico, focando em uma revitalização da cultura chinesa em si e quando utilizado em sua política externa pode ser reconhecido em textos como Diplomacia Cultural. A crítica ocidental ao uso deste termo por parte do governo chinês vem por parte, especialmente, do próprio criador deste conceito. Nye (2017) aponta que não somente os aspectos culturais deveriam de ser observados para a formulação de estratégias bem sucedidas do uso do soft power, e que esta deveria ser uma estratégia de iniciativa muito mais orgânica da sociedade chinesa do que por vias institucionais

burocráticas, como é o caso dos diversos institutos confúcio espalhados pelo planeta[7]. A China possui ciência de suas capacidades díspares de influência e o Estado se organiza para contornar estes déficits de poder em relação ao ocidente de modo estratégico (LI, 2008).

Por fim, Nye(2011) em sua obra o futuro do poder define "poder é a capacidade de fazer coisas e em situações sociais afetar os outros e obter os resultados desejados[8]". O que por acaso vem a ser a definição mais simples dentre aquelas anteriormente debatidas, sendo segundo o próprio autor uma definição derivada do dicionário. Mas isto não significa que suas reflexões a respeito da natureza do conceito se encerre aí, em sua obra compreende o que o poder pode possuir dois caminhos iniciais, sendo que na primeira admite a perspectiva tradicional do poder baseado em recursos. Este aspecto normalmente é utilizado por policymakers pois lida principalmente com o que é físico, e além disso segue uma linha de raciocínio relativamente fácil de se compreender onde poder é igual aos recursos possuídos que são posteriormente convertidos em estratégia para alcançar os resultados mais desejados. Ter todos os recursos não fará com que necessariamente se obtenha ganhos em todas as situações, e por isso a capacidade de converter isto em um poder comportamental ou relacional extraindo o melhor resultado de acordo com a situação em que se encontra, e isto é a capacidade de um Estado de exercer o seu *smart power.*

Dentro desta perspectiva o autor ainda divide este conceito em três aspectos de estratégias aplicáveis dentro da política internacional para exemplificar este conceito:

> PRIMEIRA SITUAÇÃO: A usa de ameaças ou recompensas para mudar o comportamento de B, mesmo contrariando as preferências e estratégias iniciais de B. B sabe disso e sente o efeito do poder de A.
> SEGUNDA SITUAÇÃO: A controla a agenda de ações de forma que limita B em suas escolhas de estratégia. B pode ou não saber disso e estar ciente do poder de A.
> TERCEIRA SITUAÇÃO: A ajuda a criar e moldar as crenças e percepções básicas de B e suas preferências. É improvável que B esteja ciente disso ou perceba o efeito de Poder de A (NYE, 2011, P. 29)[9]

---

[7] É um pouco hipócrita criticar a intervenção do Estado para estes casos quando se possui internamente uma das maiores e mais importantes indústrias culturais em seu país, que é o caso de Hollywood, que a anos atua como um grande apoio a difusão da cultura estadunidense pelo globo.

[8] power the capacity to do things and in social situations affect others to get the outcomes we want

[9] FIRST FACE: A uses threats or rewards to change B's behavior against B' initial preferences and strategies. B knows this and feels the effect of A' power. SECOND FACE: A controls the agenda of actions in a way that limits B's Choice Of Strategy. B may or may not know this and be aware of A's

Estas são claramente uma combinação entre os dois poderes anteriormente citados, Gallarotti (2015) na Era da Informação o uso do soft power, e por consequência do smart power, possuem uma efetividade proveitosa, pois os custos para a aplicabilidade destes foram drasticamente reduzidos com o advento da quarta revolução industrial. O autor visualiza também que a união dos dois primeiros conceitos é algo complexo, pois a formação de uma estratégia de Estado para a condução de uma política externa visando o smart power depende de um bom entendimento da oportunidade apresentada no momento. Chong (2015) complementa esta visão, sintetizando que este poder é a união equilibrada e razoável entre os recursos tangíveis de um Estado e as ideias. O novo território a ser disputado pelos mais diversos atores é diretamente afetado pela forma com que estas políticas são implementadas, e, contudo, ainda assim ele mesmo é um novo recurso ao mesmo tempo material e imaterial a ser convertido em poder.

Embora estejamos focados na narrativa estatal, às perspectivas do século XXI e da atual fase de desenvolvimento tecnológico que vivemos permite ao Estado uma cadeira ao centro da mesa, permite às organizações internacionais que continuem se sentando ao lado e discutindo em uma grande mesa redonda desigual que é o Sistema Internacional, porém agora estes estão longe de serem os únicos presentes neste espaço. Hao (2017) afirmou que a discussão sobre o espaço cibernético deveria alcançar os desejos do indivíduo, e realmente hoje é possível se fazer ouvido, e não somente por representantes indiretos, mas por meio de sua própria conta em uma rede social, por exemplo. Este contato das redes oferece ferramentas que permitem a atuação para além das fronteiras previamente impostas, aproximando usuários que podem estar a oceanos de distância.

Estes são os usuários transnacionais, que já existiam por meio de ambientes tradicionais, reconhecemos, por exemplo, a atuação internacional da Igreja Católica através dos séculos, empresas multinacionais, Organizações Não Governamentais como a Cruz Vermelha, Médicos sem Fronteiras, Greenpeace (NYE, 2011). Porém nunca foi tão fácil ser uma organização globalizada quanto agora, basta segundos para que uma mensagem seja enviada para o outro lado do globo e está na maior

---

power. THIRD FACE: A helps to create and shape B’s basic beliefs, perceptions, and preferences. B isunlikelytobeawareofthisorto realize the effect of A’s power.

parte das vezes custa menos do que um centavo, como o caso de mensagens enviadas pelo WhatsApp ou Facebook. Mesmo entre indivíduos sem objetivo tão claro, redes sociais abertas como o Twitter e o Reddit aproximam usuários com interesses semelhantes através de seus algoritmos.

Mas nem somente de boas intenções são cotadas em ações transnacionais, organizações terroristas como o ISIS utilizam ativamente a internet para espalhar o terror, com os vídeos de decapitações e outras ações criminosas, ou para recrutar novos membros tendo inclusive um *modus operandi* para procurar seus novos convertidos e realizar atentados (BBC, 2015). O ciberterrorismo em si teria como objetivo realizar “um ataque cibernético com o fim de causar pânico, medo em uma sociedade e provocar graves prejuízos a um Estado” (LEHFELD, NUNES e SILVA, 2020), sendo uma das facetas maliciosas e prejudiciais desta transnacionalidade da rede.

Enfim, isto está relacionado com a capacidade destes agentes não estatais de canalizar o poder cibernético, sendo ele definido como:

> O poder cibernético pode ser definido em termos de um conjunto de recursos que se relacionam com a criação, controle e comunicação de meios eletrônicos e computadorizados de informações - infraestrutura, redes, software, habilidades humanas. Isso inclui não só a Internet de computadores em rede, mas também Intranets, celulares e comunicações baseadas no espaço. Definido comportamentalmente, poder cibernético e é a capacidade de obter os resultados preferidos por meio do uso do recursos de informação interconectados eletronicamente do ciberdomínio[10] (NYE, 2012, p. 11) .

Este novo poder é um complemento às capacidades militares, econômicas e políticas de um Estado ou ator do Sistema Internacional, não sendo um recurso finito e com um custo de manutenção relativamente baixo em comparação aos demais (SHELDON, 2011). Este também é uma ferramenta de poder que na maioria das vezes atua por trás da mesa de apostas,afinal "a inteligência funciona quando você não sabe dela” (BRITO, 2015).

Bebber (2017) irá também complementar que para que um ator, em especial o Estado, possa utilizar plenamente de suas capacidades para o poder cibernético,

---

[10]“Cyberpower can be defined in terms of a set of resources that relate to the creation, control, and communication of electronic and computer-basedInformation—infrastructure, networks, software, human skills. This includes not only the Internet of networked computers, but also Intranets, cellular technologies, and space-based communications. Defined behavior ally cyberpower is the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain”

precisará utilizar de seus recursos econômicos com sua capacidade de produção de novas tecnologias, militares e seu potencial de adaptação ao novo cenário, da cultura e sociedade com uma formação de cidadãos capazes de lidar de forma saudável com às novas tecnologias da informação, de uma estrutura de governo capaz de manter políticas institucionais úteis que façam uma conexão entre o público e o privado, e de um sistema internacional com normas que estabilizam o ciberespaço.

E dentro desta esfera de poder é possível encontrar ações que vão do soft ao hard power, tendo casos como o Stuxnet[11] como o exemplo máximo que podemos alcançar hoje puramente nos quesitos do espaço cibernético e a criação de novas normas de regulação de modo endêmico no sistema internacional como um efeito brando. Nye (2011) também analisa que existem três faces do poder cibernético, assim como havia feito anteriormente ao considerar situações tradicionais de poder. Segue os mesmos pressupostos apresentados anteriormente, porém considerando reações dentro do espaço cibernético.

> Primeira face
> (A induz B a fazer o que B inicialmente não faria)
> Duro: ataques de negação de serviços, inserção de malwares, interrupções do sistema Scada, prisões de Bloggers.
> Brando: Campanha de informação para mudar o posicionamento de hackers, recrutamento de organizações terroristas
>
> Segunda face
> (A impede a escolha de B excluindo às estratégias de B)
> Duro: Firewalls, filtros de pressão sobre as companhias para excluir algumas ideias.
> Brando: Automonitoramento de ISPs e sites de busca, regras do ICANN sobre os domínios padrões de software amplamente aceitos.
>
> Terceira Face
> (A molda as preferências de B para que algumas estratégias nunca sejam consideradas)
> Duro: ameaças de punir os bloggers que disseminam material censurado.
> Brando: informações para criar preferência) como estimulação do nacionalismo, hackers patrióticos), desenvolvimento de normas de repulsa, como o caso da pornografia infantil. (NYE, tradução nossa, 2012. p. 171)

Dentro desta tabela Nye apresenta claramente a ideia de difusão do poder cibernético, pois frequentemente considera ações sobre indivíduos que normalmente não teriam poder em cenários tradicionais, como é o caso dos hackers. A revolução

---

[11] "um vírus para computadores cujas origens são desconhecidas, mas especula-se que tenha sido obra de um governo. A praga não tem o intuito de roubar dados bancários ou exibir anúncios. Na verdade, ela ataca sistemas usados no controle de equipamentos industriais, e teria chegado a infectar sistemas usados em instalações nucleares do Irã e da Índia" (ROHR, 2010)

informacional traz aos palcos da política internacional, novos atores que não mais necessitam de agentes intermediários e burocráticos tradicionais, para fazerem sua vontade ser reconhecida. Organizações Não Governamentais (ONG's), grupos terroristas, corporações privadas, e indivíduos possuem a capacidade de interagir e influenciar resultados como nunca antes foi possível. Nye (2012) ressalta que esta difusão da informação irá beneficiar aqueles que em um jogo de poder tradicional estariam frequentemente em desvantagem, como pequenos Estados e atores não estatais, todavia isso de modo algum significa que o "tamanho" não importa. A capacidade de criar, adaptar e utilizar a tecnologia da informação é essencial para a manutenção do poder, ou seja, embora exista uma difusão do poder entre antigos e novos atores, aqueles que possuem os recursos necessários para lidar com a tecnologia terão vantagem sobre os demais.

No próximo capítulo iremos analisar o desenvolvimento do ciberespaço chinês e como a formulação deste foi afetada pelo jogo de poder entre as necessidades do âmbito doméstico e as exigências do Sistema Internacional.

3 O PAÍS DO MEIO E SUA ARQUITETURA PARA O CIBERESPAÇO

A China possui distinta configuração para o seu ciberespaço e neste capítulo serão exploradas suas peculiaridades. Será tratado o seu sistema de filtragem de informações e às repercussões da interferência estatal dentro do espaço cibernético chinês e também o uso econômico desta nova tecnologia.

3.1 A muralha da internet chinesa

A China teve seu primeiro contato com a internet em 1987 ao receber seu primeiro e-mail, mas apenas em 1994 estabeleceu oficialmente sua conexão dentro da rede se tornando o septuagésimo país a realizar este feito (MULLER e YANG, 2014). A evolução da infraestrutura e configurações legais do ciberespaço dentro da China inicialmente seguem uma diretriz muito parecida com aquela delineada pela mídia tradicional. A academia e os investimentos governamentais foram fundamentais para estabelecer a rede, mas foram as companhias de rádio e televisão impulsionaram a propagação e popularização desta nova forma de comunicação dentro do território chinês após 1994 quando oficialmente a conexão de internet foi estabelecida no país (NEGRO, 2018). Diferentemente do que ocorreu nos Estados Unidos, a rede alcançou a sociedade civil como um produto a ser comercializado quase ao mesmo tempo em que foi incorporada aos setores burocráticos e militares do governo.

A chegada da internet a China, e sua consequente abertura para os dilemas do ciberespaço, representará uma faca de dois gumes. De um lado a informatização da economia, da sociedade e da política se torna um fator essencial para o desenvolvimento econômico chinês, modernizando o país, possibilitando a entrada do país em novos nichos de mercado que viria a se destacar com o passar das décadas, abertura para a comunicação rápida com outros Estados. Por outro lado, a internet também expõe a China a novas variáveis que não haviam sido plenamente calculadas por seu governo, como por exemplo, a enxurrada informacional depositada na web (BENSE, HENZE, FARSNWORTH, 2014).

Entre 1987 e 1993 ocorreu o que LU *et al. (*2001) caracterizam como a primeira fase da internet no país, onde a Academia Chinesa de Ciências pesquisava e desenvolvia o acesso à internet no território. No ano de 1987 uma delegação chinesa foi convidada para a sexta sessão do evento International Academic Networkshop,

ocorrido nos Estados Unidos. Como resultado desta visita a National Science Foundation (NSF) saudou os projetos incipientes de envio de emails e conexão de rede, a BITNET e a CSNET (CNNIC, 2012). Já em 1988 foram realizados primeiros testes de implementação de uma rede intermunicipal que abrangeria os membros do projeto China Research Network (CRN)em todo o território chinês. Um ano depois esta conexão foi efetuada entre universidades e alguns ministérios chineses, sendo possível o envio e recebimento de e-mails entre estas instituições[12] (CNNIC, 2012).

Em 1990 os professores Professor Wang Yunfeng e Werner Zorn conseguiram produzir um registro de nível superior[13], o ".cn" , junto à Corporação da Internet para Atribuição de Nomes e Números (ICANN). Como naquele momento a China ainda não possuía sua conexão plenamente instalada, este domínio ficou temporariamente hospedado pela universidade de Karlsruhe, na Alemanha. Neste período a burocracia estatal começava a dar seus primeiros passos para a conexão da RPC à World Wide Web e em 1992 o pesquisador Qian Hualin da Academia Chinesa de Ciências e na posição de representante oficial dos interesses de seu Estado se reuniu com membros do Departamento de Rede Internacional da Fundação Nacional de Ciência dos Estados Unidos. Os principais obstáculos observados nesta reunião eram compostos por entraves políticos. Em seu relatório oficial produzido pelo Centro de Informações da Rede de Internet da China (CNNIC), a China atribui ao governo americano a responsabilidade pela dificuldade burocrática encontrada (CNNIC, 2012).

No final do ano de 1992 a Universidade Tsinghua (TUNET) foi a primeira a programar o serviço de Bulletin Board System[14] e instalar sua conexão de rede acadêmica adotando a configuração de TCP/IP. Ao final deste ano também as instituições acadêmicas que faziam parte da rede de academias da Academia Chinesa

---

[12]Os membros do CRN incluíam: O Instituto do Ministério da Eletrônica e a Academia de Ciência Eletrônica do Ministério da Eletrônica em Pequim, Instituto do Ministério da Eletrônica em Chengdu, Instituto do Ministério da Eletrônica em Shijiazhuang, Fudan University e Shanghai Jiao tong University em Shanghai, e Southeast University em Nanjing (CNNIC, 2012).

[13]Um registro de nível superior, ou um top-level domain é a forma de identificar o propósito da página. Existem quatro tipos de domínio superior, o genérico, o patrocinado, o de infraestrutura e o código de país que é o apresentado neste trabalho (HOSTINGER, 2019).

[14]Um serviço que conecta via software o computador a um aparelho de telefonia que de forma isolada poderia enviar e-mails, abrir aplicativos e jogos. É considerado uma versão anterior a internet, pois embora pudesse responder a comandos de software ainda realizaria isto em um sistema fechado sem ligação com a World Wide Web.

de Ciências (CASNET) obtiveram seu acesso e mais de 30 institutos agora estavam conectados em uma rede fechada. Já no ano de 1993 ovice-premiê Zhu Rongji propôs a criação do primeiro portal público de informações econômicas, o “Golden Bridge Network Project".

O ano de 1993 foi marcado por encontros e reuniões que possibilitaram a chegada da internet ao país. No mês de abril os pesquisadores da CNNIC se reuniram para decidir, baseando-se naquilo que fora adotado em outros países, os nomes de domínio a serem adotados pelo Estado. Durante a conferência INET '93 o desejo chinês por sua conexão foi afirmado novamente, e pouco depois em uma reunião do CCIRN (Comitê de Coordenação para Redes de Pesquisa Intercontinental) a maioria dos participantes se mostrou favorável ao pedido chinês. Por fim, no início de abril de 1994, pouco antes da Conferência Sino-Americana do Comitê Conjunto de Cooperação em Ciência e Tecnologia, o vice diretor da Academia Chinesa de Ciências, Hu Qiheng, reafirmou o pedido junto à National Science Foundation (NSF) e foi reconhecido.

Em sua segunda fase, no ano de 1994, a “China Science and Technology Net (CSTNET)” foi conectada diretamente a world web e recebeu seu próprio domínio que é utilizado ainda hoje, o “.cn” sendo “frst.cn[15]” o seu primeiro web site propriamente dito. Durante este ano houve diversos testes de conexão, sendo um período de experimentação por parte da China e do mundo. Neste período de tempo também a RPC programou seu protocolo de TCP/IP e autorizou alguns provedores de rede incipientes, sendo eles a própria CSTNET, CHINANET, CERNET e CHINAGBN (LU et al, 2001).

Como pode ser visto, não há uma descentralização dos provedores de rede, tal qual ocorreu no ocidente, onde empresas diversas seriam autorizadas a abrir seu próprio negócio para ofertar aos usuários seus serviços de internet. Esta centralização das atividades de propagação e difusão da internet com a permissão de apenas algumas companhias específicas ocorreu através de uma legislação do ano de 1996 chamada “Regulamentações provisórias sobre interconexão internacional de redes de

[15]Hoje este site é apenas uma homepage anunciando este como o primeiro site da internet chinesa conectada ao mundo

informações de computadores a República Popular da China” que fazia com que o Estado tivesse que avaliar e autorizar as companhias interessadas em prestar este serviço (FOSTER; MUELLER e ZIXIANG, 1997).

Durante os primeiros quatro anos do consumo de internet dentro do país as regulamentações quanto ao uso eram um tanto nebulosas, não havendo especificamente uma legislação que cobrisse os interesses políticos e econômicos desta nova ferramenta, nem que amparasse os crimes e riscos cibernéticos que caminham em conjunto com o emprego da rede. O primeiro órgão burocrático a ser criado foi o Comitê Diretor da Infraestrutura Nacional de Informação, mas este possuía um caráter temporário e não reduziu as pressões entre os grupos de interesse que desejavam tomar a frente destas novas problemáticas. Outra questão que minou o potencial deste comitê é que este não possuía poder regulatório, sendo apenas responsável por julgar os crimes cometidos online. E por fim, ainda devia moderar suas ações e os interesses dos Ministérios da Correios e Telecomunicações, Ministério da Indústria Eletrônica, a Comissão Estadual de Educação, o Ministério da Radiodifusão, Filmes e Televisão, e o Ministério da Segurança Pública. Todos estes afirmavam ser de sua vontade ou responsabilidade, o manejo e regulação de aspectos diversos da vida dentro da internet (NEGRO, 2018).

Por fim, como resultado deste comitê se criou uma instituição específica para o controle de domínios em rede, o Centro de Informações de Rede de Internet da China (CIRIC), que ainda hoje é responsável pela divulgação de relatórios a respeito da propagação da internet dentro do país. E definiu-se por fim que apenas três ministérios e uma instituição acadêmica possuiriam alguma responsabilidade e influência sobre o “.cn”, sendo eles O Ministério dos Correios e Telecomunicações, o Ministério da Indústria Eletrônica, Comissão Estadual de Educação e a Academia da Ciência, responsável pelo (CIRIC). Posteriormente no ano de 1998 os dois primeiros departamentos citados foram unidos em um único ministério, Ministério da Indústria da Informação, sob o pretexto de unir as informações dispersas entre estes dois setores e apaziguar a pressão econômica sobre a necessidade de inovação da fabricação de eletrônicos e softwares.

O fator econômico e o interesse de tantos grupos burocráticos distintos podem ser facilmente explicados ao considerar que ao longo da década de 90 o crescimento

do setor de telecomunicações variou entre 30 e 50% em relação ao ano anterior, sendo a figura de proa da economia chinesa na década (FOSTER; MUELLER e ZIXIANG, 1997). E mesmo durante este período sem grandes definições da proposta chinesa para a internet já havia medidas iniciais para o controle e lembretes não tão sutis sobre a legalidade do comportamento dos usuários online. Em 1994 foi estabelecida uma lei que exigia o registro dos civis nominalmente para o uso da rede, esta só veio a ser implementada propriamente em 1996 (CHINA, 1994) (FOSTER; MUELLER e ZIXIANG, 1997).

Esta seria apenas a primeira regulamentação chinesa a gerar críticas pelo mundo, durante a década de 90 os ideais de que a rede seria um ambiente neutro, livre e inovador estavam funcionando a todo o vapor (TAUBMAN, 1998). Era esperado que o ambiente virtual viesse a enfraquecer regimes de governo não-democráticos e o ideal de uma tecnologia que pudesse conectar aquilo que antes era controlado pela esfera estatal agradou em muito aqueles que foram alcançados pela atmosfera liberalizante da época. Em argumentos técnicos as restrições chinesas de uso lesam diretamente o conceito da neutralidade da rede (STOVER, 2010).

Tim Wu (2003) cunha este termo ao analisar a evolução do processo legal de concorrência e inovação entre os provedores de internet nos Estados Unidos. No momento de sua análise os serviços de rede estavam atuando de modo a intervir nas escolhas de seus clientes no que diz respeito aos serviços de internet, seja aumentando os preços para o uso de determinadas tecnologias como o inovador wifi ou até mesmo limitando o acesso de clientes a determinados serviços e sites. Ele debate então o limite entre a auto-regulamentação do mercado e a interferência por meio de contratos ou leis, tentando compreender como manejar estes fatores para que a rede permaneça em evolução e inovação constante explorando a totalidade de seu potencial, ou seja, neutra.

Cerf (2009) argumenta que três pilares da rede a tornam naturalmente neutra, sendo eles a arquitetura de camadas, a centralização da informação nas mãos do usuário final e em terceiro lugar a natureza do IP. As camadas modulares dos blocos de construção da rede permitem as interações na superfície, como a criação ou exclusão de um novo aplicativo, sem danificar a estrutura. Isso nos leva ao segundo ponto de que o usuário final não somente pode consumir dados da web como também

postar informações e novos aplicativos, hoje mesmo o famoso aplicativo WhatsApp poderia ser deletado e mesmo assim a estrutura de rede continuaria funcionando sem alterações. E por fim, os protocolos de serviço (IP) ao transportar seus dados de uma ponta a outra não dependem do conteúdo de sua informação para funcionar, apenas fará aquilo que é proposto em sua programação que é carregar estes dados.

Mesmo que em 2003 este conceito estivesse sido cunhado em termos mais tecnicistas[16], ele exemplifica o pensamento de parte dos teóricos do ocidente naquela época, onde a internet era vista como um terreno fértil para a concorrência e livre iniciativa e que a intervenção do Estado para regular sua evolução seria contraproducente e limitante. Mas no fim, embora a tecnologia possa tender a neutralidade, a decisão a favor da neutralidade efetiva da rede é política.

Indo na contramão deste pensamento a RPC possui uma visão e estratégia de uso da rede que seja benéfica aos interesses de seu regime e ao mesmo tempo tentando se aproveitar ao máximo das benesses do ciberespaço. Até 2014 se somavam mais de sessenta conjuntos de regulamentações para a internet na China (BENSE, HENZE, FARSNWORTH, 2014). Ao contar o número de indivíduos trabalhando em todos os oito departamentos[17] que de alguma forma lidam com a supervisão, regulação ou controle da internet poderemos facilmente encontrar cerca de 30.000 pessoas.

Hoje ao ingressar em território chinês, após passar por todo o processo de desembarque, a primeira coisa a ser percebida quando acessar o seu celular é que você não é capaz de receber nem enviar mais nenhuma mensagem pelo WhatsApp e que o Google deixou de funcionar. Posteriormente também notará que o Facebook e o Youtube também se tornaram inacessíveis e que este não é um problema com o seu aparelho eletrônico, seja ele qual for, mas uma configuração de rede por parte da

[16]Tom Wu neste trabalho em específico “Network Neutrality, Broadband Discrimination" se debruça a compreender questões de estrutura que possam comprometer a neutralidade da rede, avaliando a inserção de novas tecnologias como a banda larga, o cabeamento e o wifi.

[17]Neste período o número de ministérios e departamentos envolvidos cresceu, sendo o Ministério da Indústria da Informação, o Comitê Permanente do Nacional, O Congresso do Povo, o Conselho de Estado, o Supremo Tribunal Popular e o Departamento Estadual de Proteção de Segredos, Administração Estatal de Imprensa e Publicações, e os Direitos Autorais do Estado.

própria RPC que não permite que informações de sites considerados sensíveis estejam disponíveis em seu território

A censura na internet chinesa ocorre em dois modelos, sendo o primeiro em nível doméstico, censurando conteúdos dos sites locais e o segundo em escala global ao bloquear o acesso a determinados links (TANEJA e WU, 2014). Desde 2002 quando foram instalados os primeiros sistemas de filtragem para palavras-chave ou sites considerados sensíveis vem sendo bloqueados da barra de pesquisa do povo chinês. Ao pesquisar informações sobre direitos humanos, Taiwan, Tiananmen, Falum Gong[18] e Tibet o internauta pode se deparar com algo como “a página não pode ser exibida” (THOMPSON, 2006). Ou até 2009 quando o Google ainda possuía permissão para atuar em território chinês, foi verificado que havia uma mudança recorrente nos resultados de pesquisa de determinados assuntos quando comparados com resultados recebidos fora do território chinês (MONTEIRO, 2016).

Juntamente com a chegada da internet e a crescente descomunal no número de usuários, a China se viu inundada de informações e sites ocidentais que não condizem com os ideais ou interesses do Estado chinês e com isso se deu início ao projeto “The Golden Shield”, ou “The Great Firewall” como é chamado pelo ocidente. Começa a ser projetado em 1997, este projeto tem como objetivo, ao menos em seu plano teórico, proteger os interesses do Estado chinês contra aquilo que é considerado danoso aos valores do país. Para isso a RPC utiliza um aparato gigantesco que conta com um sistema de segurança para o gerenciamento de informações, de armazenamento de dados sobre violações legais, informações sobre a entrada e saída do país, sistema de gerenciamento e supervisão do tráfego da informação (CHANDEL et al, 2019).

Este grande projeto é parte de três outros projetos de gerenciamento de informação por parte do governo chinês (DENG, 2017). Golden Bridge se destinava ao planejamento e construção de uma infraestrutura nacional que tornasse possível a difusão do ciberespaço no país. Golden card redesenhou o sistema de crédito e débito no país, difundindo o uso de cartões por parte de seus cidadãos. E por fim, Golden

[18] Esta seita possui raízes no Taoísmo e também no budismo, possuindo um conjunto de expectativas morais a serem seguidas, além de estimular a prática de atividade física. O líder desta seita, Li Hongzhi, também afirma que através de seu “terceiro olho" os praticantes podem adquirir benefícios que variam entre a reversão do processo de envelhecimento, cura de enfermidades e capacidade de enxergar para além da matéria física (ICP,__)

Tax informatizou o sistema de pagamento de impostos e taxas de modo a reduzir fraudes econômicas de qualquer tipo. Como pode ser notado, a China centralizou no Estado a responsabilidade de modelar o ciberespaço e suas informações desde o começo. Pequim estava profundamente interessada que as vantagens da Era da Informação não entrassem em conflito com os objetivos do PCC (AUSTIN, 2014) e por isso a filtragem da informação se tornou prioritária.

Compreendendo então que a censura virtual é

> O controle ou supressão do que pode ser acessado, publicado ou visualizado na Internet. Pode ser realizado por governos ou por organizações privadas a mando de governos, reguladores ou por sua própria iniciativa. Indivíduos e organizações podem se envolver em autocensura por razões morais, religiosas ou comerciais, para se conformar às normas sociais, devido a intimidação ou por medo de consequências legais ou outras[19] (Chomhaill et al, tradução nossa, 2015, p. 5)

O controle da informação para dentro e fora da China não se iniciou com a chegada da internet, mas impulsionou a melhoria nos métodos utilizados para a filtragem da informação. As críticas a este modelo de gerenciamento de rede sempre permeiam as discussões sobre os direitos humanos no país, porém às Olimpíadas de Pequim trouxeram ao país um grande holofote para a escolha política chinesa de manejo de dados.

Em agosto do ano de 2007 a DW publicou uma matéria onde se lia no título “Olimpíadas 2008: Direitos humanos na fileira de trás?” onde replicou o questionamento de organizações como Anistia Internacional (AI), Human Rights Watch (HRW) e Reporters sans Frontières (RSF) a respeito das violações aos direitos humanos cometidas pela RPC, entre as indagações proferidas a acusação de que o país estaria deliberadamente distribuindo prisões domiciliares como forma de calar seus críticos realmente se destacou.

HRW observava de perto o sistema de justiça chinês e apontava para os casos crescentes de maus tratos de prisioneiros e condenações em massa, mas, sobretudo o que mais chamava a atenção dos ativistas era o controle de imprensa e o cerceamento da liberdade de expressão no Estado. Sendo a não interferência do

---

[19]The control or suppression of what can be accessed, published, orviewedonthe Internet. It maybe carried out by governments or by private organizations at the behest of government, regulators, or their own initiative. Individuals And Organizations May Engage in self-censorship for moral, religious, or business reasons, to conform to societal norms, due to intimidation, or out of fear of legal or other consequence

governo na cobertura jornalística dos Jogos Olímpicos de Pequim uma das promessas realizadas durante a candidatura chinesa para sediar o evento, era esperado que este momento fosse o primeiro sinal de uma possível, mesmo que pequena abertura do país à livre imprensa. O parlamento cumpriu parcialmente sua promessa ao promulgar uma lei que permitia que jornalistas estrangeiros pudessem atuar livremente no país até outubro de 2008.

> Daremos à mídia total liberdade para relatar quando eles vierem para a China... Estamos confiantes de que a chegada dos Jogos para a China não só promove nossa economia, mas também melhora todas as condições sociais, incluindo educação, saúde e direitos humanos[20]. (Wang Wei, 2001 apud Amnesty International, tradução nossa, 2007, p.5)

Pouco antes da abertura das olimpíadas, jornalistas reclamaram que embora a China prometesse esta liberdade, estes estavam sendo boicotados e tendo seu acesso a diversos sites, a se incluir o portal da Anistia Internacional, bloqueado. E então no dia 29 de julho de 2008 o portal de notícias Reuters divulgou que o Comitê Olímpico Internacional (COI) admitiu ter feito um acordo com o governo para que certos sites fossem bloqueados ou censurados. De acordo com o comitê, apenas sites que não fossem relacionados com os jogos se tornaram inacessíveis, mas isto não impediu que jornalistas de todo o mundo criticassem a atitude do governo e também a postura do COI perante esta questão.

Após críticas da mídia internacional a censura de sites relacionados aos direitos humanos, como a plataforma da Human Rights Watch, o governo revisou sua política de censura na comunidade internacional. Todavia, assuntos como protestos da Praça Tiananmen e sobre a seita espiritual Falun Gong permaneceram bloqueados. Em resposta o presidente Hu Jintao "O governo chinês e o povo chinês têm trabalhado sinceramente para honrar os compromissos assumidos com a comunidade internacional" (THE GUARDIAN, 2008), mas que a politização do evento não seria tolerada.

Essa era uma expectativa e pressão internacional que não se mostrava nem mesmo próxima a um compromisso factível. Após a obtenção do direito de sediar o

---

[20]We Will Give The media total freedom report when they come to China ... We are confident that the arrival of the Games in China not only promotes our economy, but also improves all social conditions, including education, health and human rights.

evento houve sim declarações favoráveis aos direitos humanos e a uma mudança mais liberal da estrutura de imprensa chinesa, alguns dos tópicos desejados por jornalistas compõem um aspecto sensível da política e história chinesa. Ao observar o quadro geral poderia ser até mesmo esperado que houvesse alguma limitação de pesquisa para a imprensa internacional. Seria errôneo especular que um país que possua um histórico informacional como o chinês permitisse acesso irrestrito a jornalistas estrangeiros, mesmo que somente durante o período do evento.

Este foi um incidente que tornou a vigilância da comunidade internacional a respeito da censura por parte da China ainda mais crítica. Neste período, empresas de TIC como o Google e o Yahoo! corroboraram com os ditames chineses e ativamente colaboraram com a política de censura de dados sensíveis em seu sistema de busca. Críticas por parte da comunidade acadêmica ocidental foram realizadas (DANM e HADDOW, 2007) e a relação entre estas multinacionais e o PCC se tornou mais desgastada conforme a primeira década do milênio se aproximava do fim.

A partir de 2005 o Google chinês acatou e se adaptou à legislação de filtragem de informação imposta pelo governo. A barra de pesquisa foi atualizada e os algoritmos modificados (THOMPSON, 2006). Agora não seria mais possível pesquisar os tópicos julgados como sensíveis, tendo sido completamente suprimidos da plataforma. Ao pesquisar as palavras “Massacre da Praça Tianmen” ou então sobre a seita “Falun Gong” não haveria mais as mesmas informações disponíveis a nível mundial, sendo elas suprimidas ou deletadas. Essa decisão de ceder livremente aos desejos chineses não foi muito bem recebida nos Estados Unidos e os executivos do Google foram convidados inclusive ao congresso americano e escutaram palavras não tão elogiosas que os comparavam a colaboradores nazistas (THOMPSON, 2006).

O Google não foi a primeira empresa estadunidense a abrir uma filial dentro da internet chinesa. O Yahoo anos antes já estava se aventurando em rede e descobrindo não somente as barreiras burocráticas do Estado, mas também culturais (GUNTHER, 2006). Diferenças culturais foram sentidas ao perceber que o layout de sites estrangeiros não atraiam a atenção do grande público que dava preferência para serviços nacionais de web, preferindo sites programados por chineses, isso obrigou às multinacionais a alterar suas interfaces para se aproximar daquele público e penetrar naquele nicho de mercado. Apenas citando outro grande choque, ao perceber que jovens chineses possuíam o costume de piratear músicas, filmes e

séries, o Baidu, um programa de pesquisa de origem chinesa, não somente considerou sensato manter estes links em funcionamento, como criou canais para facilitar a pirataria (THOMPSON, 2006). Ao considerarmos que propriedade intelectual é um cibercrime nos Estados Unidos podemos perceber que existe uma divergência na visão dos dois países em relação a como deve ser regulamentado o ciberespaço.

Na realidade, por muito tempo o Yahoo foi um colaborador ativo de Pequim ao permitir o acesso do governo a e-mails privados de seus cidadãos (GUNTHER, 2006), não muito diferente do que vimos com o caso Snowden anos depois. Este vazamento de informações privadas levou a prisões de dissidentes ao longo dos anos. A submissão de empresas estrangeiras à legislação do país em que desejam realizar ou expandir suas atividades gerou algumas críticas em relação a suas escolhas privadas de negócios. Danm e Haddow (2007) argumentam que seria antiético por parte destas empresas multinacionais concordar e envolver seus negócios em países com leis que violam os direitos humanos. Isto nunca seria um único fator determinante para estas empresas, não sendo posteriormente o fator humano a variável decisiva para suas escolhas estratégicas.

A situação do Google em si foi um tanto similar à experiência do Yahoo!,onde a necessidade de se adequar às leis chinesas com o tempo se tornou um incômodo maior do que economicamente valeria a pena. Com a pressão internacional para que a empresa não aceitasse as decisões governamentais chinesas, envolvendo inclusive lances de acionistas dentro da bolsa de valores para que a sua posição se fizesse ouvir, se tornou insustentável manter o escritório de Pequim aberto (YEO, 2016).

Deve ser compreendido que com a chegada do "google.cn" como link de pesquisa foi apenas o primeiro serviço fornecido pela empresa no país. Logo, apenas dois anos depois, o Google já havia estabelecido seus serviços para aparelhos móveis além de desenvolver novas aplicações visando exclusivamente o mercado de Pequim, como por exemplo, Pinyin Input Method, Google Life China, and Google Maps China (TAN e TAN, 2012). A expansão da empresa para dentro das fronteiras chinesas é fundamental para multinacionais do ramo da tecnologia da informação considerando que este é o maior nicho de clientes do mundo. O aspecto econômico é o fator chave para a aceitação inicial das condições de filtragem de informação, todavia a pressão corporativa internacional e a demanda do governo por mecanismos mais minuciosos

de controle dos dados tornaram inviável a permanência do servidor por mais de sete anos.

Mas o que torna a saída do Google como provedor de pesquisa do território chinês um evento marcante está nos diversos ataques cibernéticos coordenados direcionados à empresa em dezembro de 2009 e por todo o ano seguinte. Neste ano a companhia discutiu com o governo severamente sobre às exigências chinesas para censura de resultados da web e neste mesmo ano foi alvo de massivos ataques cibernéticos (CHANDEL et al, 2019) a partir do método de ataque de negação de serviço (DDoS[21]).

O Google foi, na realidade, apenas uma parte de toda esta rede de ataques e devido a tamanha internacionalização de seus serviços chamou a atenção da comunidade internacional. Mais de 34 companhias e instituições estadunidenses com links para a administração governamental tiveram seus espaços cibernéticos comprometidos, entre elas o próprio Pentágono (EUNJUNG e NAKASHIMA, 2010). De acordo com a investigação por parte do Federal Bureau of Investigation (FBI), os ataques foram programados por um grupo freelancer, mas Pequim tinha conhecimento do código fonte utilizado nos ataques (HJORTDAL, 2011). A RPC negou qualquer envolvimento com os ataques alegando que não participou do planejamento destes ataques e que nem mesmo possuiria a informações que pudessem antecipar o ataque.

Embora não tenha havido outro incidente internacional de grandes proporções, a legislação chinesa sobre filtragem de dados seguiu seu processo de evolução. Durante o governo de Xi Jinping é relatada a existência de mais de 2 milhões de “policiais da internet” que catalogam por meio de palavras-chave a opinião pública dentro da internet (HUNT, 2013). Ao final de 2017 duas legislações foram aprovadas de modo a regulamentar ainda mais a opinião da população chinesa dentro das redes sociais, sendo elas “Regulamento de Gestão de Fóruns e Comunidades da Internet” e “Regulamento de Gestão de Postagens e Serviços de Comentários na Internet”

[21]é uma tentativa de fazer com que aconteça uma sobrecarga em um servidor ou computador comum para que recursos do sistema fiquem indisponíveis para seus utilizadores. Para isso, o atacante utiliza técnicas enviando diversos pedidos de pacotes para o alvo com a finalidade de que ele fique tão sobrecarregado que não consiga mais responder a nenhum pedido de pacote (CANALTECH,)

(CLT, 2017). A exigência principal destas novas regulamentações é que o usuário deve fornecer aos provedores de suas respectivas redes sociais seus nomes e identidades reais para que sua conta possa se tornar operacional. Isso obviamente limita o desejo do usuário de expressar toda a sua opinião em rede pois se torna ainda mais fácil para o governo identificar e encontrar o netzen que fez determinado comentário que possa ser julgado como prejudicial (CHAN, 2017).

3.2 Made in China

Mesmo com toda a dificuldade causada por este choque cultural e de expectativa, as empresas estrangeiras, sejam elas do ramo de TIC ou não, ainda parecem dispostas a ingressar neste mercado e usufruir de seus benefícios. Um país com um quinto da população mundial, sendo o terceiro com maior extensão territorial do planeta e também possuindo o maior número de pessoas conectadas à web do mundo, são algumas das características de um país que pode revolucionar a economi global e ao mesmo tempo se reiventar para garantir que seus interesses sejam mantidos (CASSIOLATO, 2013).

A reforma econômica chinesa realizada pelo primeiro ministro Deng Xiaoping em 1978 abriu um novo leque de possibilidades para o desenvolvimento chinês que foi muito bem aproveitado. Breda e Silva (2009) explicam que este processo foi iniciado durante a terceira sessão plenária do 11º Congresso do Partido Comunista Chinês (PCC) e chamada pelo primeiro-ministro de “As quatro modernizações”. Este projeto buscava a modernização da agricultura, o crescimento econômico e o desenvolvimento da indústria, da tecnologia e das capacidades de defesa do Estado (BARBIERI e ZAGO, 2020). Paulino (2010) insiste que o êxito nestas reformas está na insistência chinesa em não seguir uma cartilha pronta e sim se debruçar sobre suas próprias peculiaridades criando soluções inovadoras.

> O que o êxito das experiências chinesa e indiana demonstram é que, ao contrário da tabula rasa do Consenso de Washington, é preciso identificar prioridades [...], é preciso reconhecer que há fatores que servem de esteio para o crescimento econômico; que o crescimento econômico é comandado por um conjunto inicialmente restrito de políticas e iniciativas institucionais, as quais constituem a estratégia de desenvolvimento de cada país.[...] Não há desenvolvimento nacional sem uma ideologia do desenvolvimento nacional, no sentido de um conjunto de idéias que interpretem a realidade nacional a partir de seus próprios valores, e se constituam no motor de transformação dessa própria realidade. (PAULINO, 2010, P. 18)

Ao identificar suas necessidades utilizando como referencial o seu cenário doméstico, Deng Xiaoping embarca neste projeto de desenvolvimento que possuía amplas áreas que necessitavam de investimento contínuo para que funcionassem, formulando assim uma nova política de Estado para a China (OLIVEIRA e MOTA, 2016). Ao conduzir uma industrialização e crescimento econômico que fossem baseados na ideologia socialista, o primeiro ministro assumiu que deveria abrir suas possibilidades para aquilo que o cenário internacional pudesse oferecer, absorvendo a experiência e a tecnologia aplicada internacionalmente e integrando esta nova china a um mundo cada vez mais globalizado (BARBIERI e ZAGO, 2020). Este processo se deu por meio da experimentação, assumindo que de fato não haveria um único caminho correto a ser tomado e que estas transformações sociais deveriam ser graduais (TRIGO, 2007).

O primeiro passo para que as reformas pudessem ser efetivas foi revitalizar o setor agrícola do país, pois ali estava concentrada cerca de 80% da população e o partido estava receoso de que a grande massa agrícola pudesse se tornar uma barreira entre a China e a industrialização (BREDA e SILVA, 2009). Houve então por meio de políticas públicas que incentivaram a população a abrir novos empreendimentos, um crescimento no número de pequenas e médias empresas que poderiam agora vender o excedente de seus produtos para o mercado internacional (TRIGO, 2007). Neste ponto os empreendimentos eram em sua maioria planejados ou ao menos apoiados pelo Estado, criando assim uma nova classe empresarial dentro da China de pequenos e médios empresários[22] onde a linha entre o público e o privado se tornou extremamente tênue. O governo instituiu um novo sistema de gestão dos produtos a serem comercializados pelas empresas estatais ao instituir o “Sistema de Responsabilidade Contratual” em que cada companhia se compromete a pagar determinado valor ao final do ano enquanto o excedente, ou o lucro, poderia ser reinvestido ou distribuído internamente (FARIAS e MARTINS, 2020).

Com os massivos investimentos em logística e infraestrutura, descentralização das permissões para importação e exportação, logo o país se destacou com a

[22]Anteriormente, após a Revolução de 1949 o que havia seriam comunas que foram instituídas pelo primeiro plano quinquenal, onde cada comuna deveria ser autossuficiente produzindo desde itens agrícolas até industriais que fossem necessários para aquela determinada comunidade.

exportação de itens de baixo custo, como têxteis e de vestuário (BREDA e SILVA, 2009). A China foi beneficiada perante o cenário internacional por seu status de país em desenvolvimento e de Nação Mais Favorecida, conquistando assim acesso facilitado a empréstimos internacionais com condições diferenciadas (FARIAS e MARTINS, 2020). Com este dinheiro pôde realizar os investimentos iniciais em moedas para câmbio e importar maquinário para o desenvolvimento de seu setor manufatureiro. Por fim, foram criadas Zonas Econômicas Especiais (ZEE) ao longo do litoral que gozavam de vantagens tais como a liberdade cambial e a isenção fiscal que tornavam estes locais extremamente atrativos para novas empresas. Esta foi a porta de entrada para multinacionais que poderiam sim instalar suas filiais na RPC desde que cumprissem algumas exigências, como por exemplo, a preferência pela compra de insumos locais e a associação com grupos comerciais chineses (MILARÉ e DIEGUES, 2019).

Esta nova filosofia chinesa possui uma relação direta com a forma com que as diretrizes para o ciberespaço foram criadas. Se traçarmos como parâmetro as reformas ocorridas em 1979 é possível verificar que o crescimento do Produto Interno Bruto do país até 2005 ocorreu um aumento médio de 9.6% por ano, sendo que ao compararmos com o período após a Revolução de Mao Zedong de 1960-1988 teremos uma taxa de apenas 5,3% ao ano (BENSE, HENZE, FARSNWORTH, 2014).

Esta margem de crescimento permanece durante as duas primeiras décadas do novo século XXI, em que no final de 2019 a China se torna o maior exportador do mundo, alcançando a marca dos 2,57 trilhões de dólares em bens e serviços comercializados com o exterior (OEC, 2020). O carro chefe de seus resultados são produtos gerados para a sociedade da informação, sendo equipamentos de transmissão, computadores, circuitos integrados, peças de escritório e celulares os itens que ocupam o topo da lista de produtos que foram comercializados. Em contrapartida, suas importações, que chegaram à casa dos 1,58 trilhões, sendo que petróleo cru, circuitos integrados, minério de ferro e gás natural os maiores bens importados neste período.

Milaré e Diegues (2019) dizem que para além de um projeto desenvolvimentista pautado dentro de limites razoáveis que observavam as necessidades da China individualmente, conforme argumentado por Paulino (2010), a China investirá em

projetos de longa duração para suprir suas necessidades econômicas. Pois foi através de seu planejamento a longo prazo, onde o controle das ações macroeconômicas eram medidas de forma a manter a autonomia chinesa perante o âmbito internacional. Segundo Xi Jinping (2020) “a indústria de cibersegurança e informatização representa uma nova produtividade e uma nova direção de desenvolvimento, e deve e pode levar a liderar na prática do novo conceito de desenvolvimento”. A inclusão da “cibereconomia” como um capítulo específico do 13o Plano Quinquenal da RPC (2016-2020) adicionou oficialmente o mercado da sociedade da informação como um tópico a ser debatido de modo distinto do restante das políticas econômicas do país.

Mesmo que a arquitetura do ciberespaço apenas tomasse um escopo bem definido durante o governo do presidente Xi Jinping, durante os primeiros passos da internet dentro do país já havia este cuidado maior para que a indústria da informação pudesse se desenvolver. Já nos anos 2000 a indústria de tecnologia da informação (TI) compunha cerca de 33% da produção da China (AUSTIN, 2014) Ao final dos anos 90 o foco era criar uma sociedade chinesa que fosse referência não somente na reprodução de tecnologias da informação como também a criação destas já estava sendo trabalhado pelos líderes do PCC onde em um discurso para a União Internacional das Telecomunicações (ITU) o ex-presidente Jiang Zemin (1993-2003) declarou que

> Devemos reconhecer profundamente o tremendo poder da tecnologia da informação e promover vigorosamente seu desenvolvimento. A velocidade e o escopo de sua transmissão criaram um espaço de informação sem fronteiras ao redor do mundo... A fusão da economia tradicional e da tecnologia da informação fornecerá o motor para o desenvolvimento da economia e da sociedade no século 21[23] (Zaemin, 2000 apud Tai Zixue, tradução nossa, 2006, p.126)

Neste cenário a China já estava em processo de desestatização ou descentralização das fábricas e indústrias, unindo o capital privado ao interesse público. Era uma preocupação dos líderes do governo que o país encarasse uma estagnação na produção por apenas repassar a tecnologia externa, sem produzir e criar sua própria tecnologia. O investimento em Pesquisa e Desenvolvimento (P&D)

[23]We should deeply recognize the tremendous power of information technology and vigorously promote its development. The speed and scope of its transmission have created a borderless information space around the world … The melding of the traditional economy and information technology will provide the engine for the development of the economy and society in the 21st century

do país nesta época era irrisório, apenas 0,7% do PIB, seu registro de patentes também era insignificante (AUSTIN, 2014). Ao longo dos anos diversos projetos foram realizados na área para multiplicar o número de empresas do ramo de tecnologia e também qualificar a mão de obra para trabalhar neste setor crescente.

Ao longo dos três Planos Quinquenais realizados entre os anos de 2001 a 2015, o ciberespaço em todos os seus aspectos ocupou um lugar vago entre as prioridades estabelecidas pelo Estado. Durante o 10º Plano a preocupação do governo era muito vaga a respeito do que fazer se concentrado principalmente no crescimento econômico do país e de efetivar os últimos estágios da reforma iniciada por Deng Xiaoping (ZHU, 2010). No planejamento posterior a necessidade de que a infraestrutura necessária para o funcionamento em alta velocidade das tecnologias que haviam sido agregadas ao convívio social fosse revitalizada é um dos objetivos elencados ao longo do documento (CHINA, 2005). É interessante analisar que neste período não somente a necessidade econômica havia sido exposta, mas também se enxerga a necessidade de utilizar o ciberespaço para a defesa de infraestruturas críticas do Estado. Esta nova visão é incorporada ao mesmo tempo em que os primeiros ataques cibernéticos a Londres ocorreram em 2005.

Poucos anos antes da elaboração do 12º Plano Quinquenal a Chinese Academy of Science (CAS) lançou uma série de livros que buscava analisar os setores estratégicos necessários para que as ambições chinesas fossem alcançadas. Um destes explora exclusivamente a rotina chinesa para as TIC e como as ações futuras deveriam ser pautadas em uma política que abrangesse a economia, a sociedade, a segurança e a cultura (LU, 2010). Este longo estudo gerou outros debates dentro da academia chinesa que agora se empenhava em entender estas novas perspectivas geradas pelos estudos da CAS.

A partir daqui a cibersegurança não mais se limita aos escopos engessados das noções de segurança da computação. Seria necessário ampliar esta segurança para uma visão ampla e irrestrita que englobaria todas as putas acima citadas (LU, 2010), pois a tecnologia dedicada à indústria de mais alta patente, como por exemplo os laboratórios física quântica e aquela de uso comum, como um celular, deveriam ser tratadas com seriedade se a China quiser se tornar referência para a Indústria 4.0. Em detalhes, 10 pontos foram elencados como assuntos primordiais de pesquisa a

serem alcançados pelo país até 2050, variando desde softwares de proteção de dados civis e militares até novos experimentos de rede física para melhorar a infraestrutura cibernética do país.

Este novo fôlego nas pesquisas de ciência e tecnologia da informação afetaram inclusive o andamento das reuniões para a publicação do 12º Plano Quinquenal que carrega uma nova visão do uso da informação. Embora não tenha sido enviado às instituições governamentais em um momento exatamente propício, pois os resultados deste estudo foram obscurecidos pela troca de governo e a ascensão de Xi Jinping ao mais alto cargo do governo, é possível verificar que houve um cuidado maior pelo espaço cibernético durante a elaboração deste.

Em primeiro lugar, o 12º Plano Quinquenal identifica que é necessário expandir o uso das tecnologias da informação para setores com potencial comprometido, como o setor de químicos e da saúde. E em segundo lugar a China se compromete a tentar criar mecanismos que pudessem equilibrar o desejo popular de expressar em rede suas opiniões políticas a respeito dos rumos que o país estaria tomando ao longo dos próximos anos. Ressalta-se que para este documento, que se refere aos anos de 2011 a 2015, a China já havia batido os Estados Unidos em número de netzens tornado-se assim o país com o maior número de internautas do mundo. Este fator implica em uma necessidade cada vez maior de gerenciamento de redes e de seus processos dentro do Estado.

É neste plano que o atual presidente Xi Jinping assumiu seu primeiro mandato no ano de 2012. Assumiu o protagonismo de liderar o setor cibernético governamental e geriu as estratégias de Estado de modo que os incentivos e objetivos do governo modificaram de *made* in china, o celeiro da pirataria, da cópia e da mão de obra barateada; para *design* in china, onde a China seria protagonista, inovadora e criativa (ARBIX et al, 2018).

A espionagem a nível industrial voltada para a cópia de modelos industrializados de outros países é um problema para países exportadores de tecnologia de ponta há algum tempo. Esta forma de espionagem permite que companhias espionem os projetos de outras organizações e façam suas próprias versões baseadas daquilo que foi encontrado. A China era acusada de usar a sua capacidade cibernética para estes fins em casos como o da “GhostNet” em 2009 onde

uma gigantesca rede de espionagem que envolvia indivíduos, empresas e governos de mais de 103 países. Esta operação não foi ligada ao governo chinês diretamente, mas especialistas afirmam que seria necessário um investimento consideravelmente alto para que funcionasse corretamente.

Ao tentar escapar dessa péssima publicidade, os esforços para a industrialização iniciados em 79 já haviam dado seus frutos e agora se tornou necessário para concretizar as ambições chinesas para uma ascensão pacífica dependeria de sua capacidade de se tornar pioneira no novo modelo industrial que estava surgindo, o da indústria 4.0.

> 1ª revolução no final do século 18 (“Indústria 1.0”): produção mecânica movido a vapor e água; a 2ª revolução no final do século 19 ("Indústria 2.0"): eletrificação de máquinas e produção em massa; a 3ª revolução na década de 1970 (“Indústria 3.0”): robôs industriais, programáveis controladores lógicos e gerenciamento de produção baseado em TI. (Wübbekeet al, tradução nossa, 2016, p. 13)

A indústria 4.0 vem então como o próximo passo óbvio para Pequim. Nesta Quarta Revolução Industrial o mundo digital, físico e biológico se tornam uma coisa só. A tecnologia 3D aplicada à produção, inteligência artificial, Internet das Coisas, biologia sintética e sistemas ciber-físicos são as novas áreas que prometem manter os países que melhor se adaptarem (INDÚSTRIA40).

Este investimento em tecnologias da quarta geração recentemente provocou uma certa tensão entre a China e os Estados Unidos. Desde o início de 2018 estes dois países têm se desentendido quanto a suas políticas comerciais. Isso começou quando o ex-presidente dos EUA Donald Trump (2017-2021), anunciou uma série de impostos sobre produtos chineses que foi retaliado pela China com imposição de impostos a produtos americanos. O objetivo desta política é reduzir o déficit comercial que o país possui com seu parceiro comercial asiático. Desde então diversas rodadas de negociação foram tomadas mas as tensões permanecem entre eles (TREVIZAN, 2019).

As relações entre os dois países não melhoraram nos últimos anos e a pandemia do COVID-19 serviu apenas para deteriorar ainda mais a aliança aparentemente positiva que existia anteriormente. Por fim, no ano de 2020 a Casa Branca anuncia o seu interesse em barrar alguns aplicativos chineses de atuar dentro

de seu país. A razão seria pelo roubo de dados de cidadãos estadunidenses por meio destes softwares, como é o exemplo do TikTok.

A preocupação pelo roubo de dados em redes sociais aumentou após 2016 com o caso da Cambridge Analytica que utilizou os dados fornecidos pelo Facebook para propósitos políticos sem o consentimento do usuário. Sendo assim, em agosto de 2020 Donald Trump emitiu uma ordem proibindo transações com as empresas Tencent e Byte Dance, proprietárias do WeChat e TikTok respectivamente (SEVEG, 2020). Esta decisão já estava sendo examinada desde julho pela Casa Branca e que especialistas já haviam chegado à conclusão que estas redes coletavam sim dados de usuários, o que é bastante comum entre redes sociais e de pesquisa de todo o mundo, a se incluir o Facebook e o próprio Google (CARBINATTO, 2020).

O país justifica esta decisão por receio de que os dados de seus cidadãos possam ser utilizados pelo governo chinês. Em 2017 uma nova Lei de Inteligência Nacional foi instaurada no país, e nela consta que toda companhia chinesa deve cooperar com o governo. Na visão estadunidense isso implicaria na entrega de dados por parte da Tencent e Byte Dance ao PCC representando então uma ameaça à segurança nacional.

A espionagem é um dos grandes medos dos Estados dentro do Sistema Internacional e a prioridade pela segurança da informação vem se mostrando a cada dia uma necessidade entre potências e potências emergentes. No próximo capítulo será visto como a China estruturou suas forças armadas para proteger seu ciberespaço e como XI Jinping vem exercendo a sua influência sobre ele.

4 A GUERRA SEM LIMITES

A expansão tecnológica chinesa não se limita ao uso da sociedade civil e para seu crescimento econômico e concomitantemente sua aplicação para o âmbito de defesa do Estado foi forçado a se adaptar a esta nova realidade. Neste capítulo iremos explorar as ações e reações chinesas a sua vulnerabilidade (NYE e KEOHANE, 2001) cibernética e com Xi Jinping realinhou esta política de defesa a sua ambição para a Ascensão chinesa como um ator protagonista dentro do sistema internacional.

4.1 Até Xi Jinping

A primeira vez que o termo Informational Warfare (IW) é aplicado à realidade e não mais como um conceito subjetivo é durante a operação estadunidense “Desert Storm” na Guerra do Golfo no ano de 1991, criando um novo tipo de guerra que envolveria o uso da tecnologia da informação e o desenvolvimento de novos tipos de armas inteligentes[1]. Atentos a este fato, o Exército de Libertação Popular (ELP) foi compelido a rever suas próprias capacidades e modernizar as suas forças armadas (WORTZElL, 2014).

Este esforço envolveu primeiramente a mobilização de diversos institutos de pesquisa do país, não concentrando somente nas mãos dos militares e sendo uma iniciativa conjunta entre os acadêmicos civis e do ELP. As pesquisas para a incorporação de TIC a guerra ocorreram no mesmo momento em que o país tentava estabelecer sua conexão de rede a nível global mesmo que estas não possuíssem um sistema de dependência para o seu sucesso embora estabelecer a internet a nível de país ainda fosse uma vantagem e uma preocupação extra a nível militar (WU, 2006). Para a elaboração de seus próprios recursos no campo prático e teórico Pequim uniu sua ampla experiência de guerra e sua própria filosofia e cultura ao que foi desenvolvido em outros países, em especial nos EUA e na antiga União Soviética (WORTZEIL, 2014).

Em uma perspectiva puramente teórica, o país ainda no ano de 1985 definiu como Guerra da Informação “o neurossistema (olhos e ouvidos) dos sistemas de operação militar das Forças. O IW da China abrange C4ISR (Comando e Controle, Comunicações, Computação, Inteligência, Vigilância e Reconhecimento), guerra

eletrônica, guerra de rede e outros assuntos relacionados[24]" (WU, tradução nossa, 2006). Este conceito foi apresentado, mas não aprofundado, por Shen Wei Kuan, um oficial de baixo escalão do exército chinês. Durante a Guerra do Golfo que realmente uma equipe se dedicou a entender o tópico e transformá-lo em uma política real das forças armadas chinesas.

Toda esta mudança no setor militar chinês só é possível graças ao boom econômico e tecnológico ocorrido com as Quatro Modernizações realizadas por Deng Xiaoping. Mas mesmo assim, o setor militar compete seus recursos e decisões com diversas áreas domésticas necessitadas da época, como por exemplo, a crise bancária da década, a crescente disparidade de desenvolvimento entre as áreas litorâneas e o interior, e do setor da saúde tendo que lidar ao mesmo tempo com os surtos de SARS e HIV (MULVENON, et al. 2006). Sendo assim, a década de 90 é marcada por uma arquitetura débil do ciberespaço chinês, em que as tentativas iniciais do alto comando militar não geraram resultados firmes ou muito proveitosos.

O custo foi um fator limitante para o desenvolvimento de grandes projetos, pois embora a cada ano se tornasse mais barata a utilização de ferramentas cibernéticas em detrimento das tradicionais, ainda há um custo relativamente alto em algumas atividades, tais como o investimento em um satélite próprio (WU, 2006). Mesmo assim, alguns projetos conseguiram ganhar uma estrutura definida com objetivos claros. Para o ELP a China deveria conquistar uma capacidade militar que pudesse suprir os objetivos de manter a superioridade da informação perante o inimigo, capacidade de interromper os serviços de informação e comunicação do alvo e ao mesmo tempo manter seu próprio sistema operacional (WORTZEIL, 2014). O ELP trabalhou então em um projeto que poderia unir a comunicação do próprio exército a setores prioritários, montando a primeira versão do que viria a ser o sistema chinês de defesa e segurança cibernética. Este novo modelo de operação seria capaz de proporcionar à China vantagem estratégica na formulação e execução de missões militares,

[24] "the neurosystem (eyes and ears) of the Forces' military operation systems. China's IW covers C4ISR (Command and Control, Communications, Computing, Intelligence, Surveillance and Reconnaissance), electronic warfare, network warfare and other related topics"

embora neste momento ainda estivesse em uma fase incipiente (COSTELLO e KANIA, 2018).

Wu (2006) irá observar que em suas primeiras formulações teóricas os acadêmicos chineses enxergavam dois cursos de ação baseados nas capacidades do país na época, uma estratégia defensiva e outra ofensiva. A primeira seria uma abordagem de desinformação do inimigo, sendo recomendada apenas para momentos em que a disparidade de recursos entre os atores em conflito fosse muito grande. O problema nesta opção estaria no fato de que ainda seria possível para os alvos inimigos hackear e rastrear os agrupamentos militares chineses em não muito tempo tornando esta estratégia inútil rapidamente. E por outro lado, em uma ofensiva envolveria a sabotagem das informações e equipamentos de seus inimigos, ainda mirando em uma situação onde a disparidade entre forças fosse notável. Considerando que sabotagem e espionagem são um dos ofícios mais comuns de serem utilizados em ataques cibernéticos, esta foi a opção adotada pela China por algum tempo.

Sun Tzu já prescrevia como a melhor solução para a guerra seria que em um primeiro momento não a iniciasse, mas caso não fosse possível a manutenção da paz, a estratégia deveria ser muito bem calculada, não deixando o espaço para o erro nem a enganação, bem, ao menos por sua parte. Espionagem, sabotagem e enganação serão narradas por ele como itens essenciais para a guerra e a sua ligação com o novo cenário cibernético não é complicada de ser feita (CHONG, 2014). Também é recomendado ao longo do livro que se busque a harmonia em seus caminhos, o que poderíamos traduzir como um princípio básico da espionagem, obtenha as informações necessárias, mas não seja pego no ato.

Na realidade, a aplicação de antigas teorias militares para o ciberespaço já causou inclusive alguns incidentes diplomáticos. Mao Zedong é um dos autores mais influentes diante da China pós-revolução, sendo sua teoria baseada na luta de classes defendida por Marx e Lênin. Este vai defender que em uma luta entre poderes desiguais será importante convencer a deserção e inflamar as massas em prol de seu objetivo, pois não seria papel de comandantes militares apenas lidar com assuntos de guerra, mas também seriam estes agentes políticos de mobilização e transformação social em favor de sua causa. A conquista de corações e mentes seria tão ou mais

importante que a estratégia militar organizada. Ao extrapolarmos para o cenário cibernético este princípio, a conversão ideológica favorável de grandes massas junto do anonimato oferecido pela rede criaria defensores ocultos espalhados e escondidos pela rede.

Em 1997 um general do alto escalão, PuFeng Wang, do Exército de Libertação Popular chegou a considerar que seria útil a China incorporar a seu ciberespaço o princípio de “Guerra do Povo” de Mao, onde a idéia que a internet seria um campo de batalha e os usuários especializados poderiam se tornar novos oficiais, sendo plenamente possível incorporá-los a ataques cibernéticos (WU, 2006). Esta ideia parece distante e não muito fácil de executar em um caso real de ataque cibernético por parte da China, mas a partir dos anos 2000 o país foi contemplado com o fenômeno dos “Hackers Patriotas”. Este grupo se mobilizou para atacar alvos que pudessem por algum motivo fossem contrários aos objetivos chineses.

Estes ciberativistas muitas vezes agem de modo a beneficiar o PCC, todavia isto ocorre somente até a página dois. É um mecanismo não oficial de retaliação por parte do governo, pois limpa o governo chinês de embaraços diplomáticos ao oferecer a saída simples de que efetivamente não seria um ataque estatal direcionado. Mas ao mesmo tempo este grupo não está sob o comando e desejos de Pequim, atuando em momentos que podem ser inconvenientes para sua política, gerando momentos de desconfiança entre as nações, como foi o caso do ataque ao Google em 2010.

Por fim, no período até o primeiro governo de Xi Jinping foi possível também traçar princípios basilares e duradouros da doutrina militar chinesa para a guerra tradicional e além dela, também chamada de teoria da Guerra Sem Limites ou Irrestrita (HAGESTAD, 2012). Neste sistema as barreiras da guerra tradicional não seriam um impedimento para as ações chinesas, como é apontado dentro do espectro da própria IW e que seriam as políticas e estratégias militares necessárias para o bom aproveitamento do potencial do ciberespaço dentro de condições racionais e possíveis. Neste contexto os coronéis Liang e Xiangsui (1999) vão então elencar como princípios: O “omnidirecionamento”, a sincronia, objetivos limitados, meios ilimitados, assimétrica, uso mínimo de recursos limitados.

Ao partir do prévio conhecimento de que a China poderia vir a enfrentar adversários com poderio bélico superior, a resposta militar integrada dentro do ciberespaço deveria considerar que a guerra seria omnidirecional, pois absolutamente todos os terrenos; solo, água, espaço sideral, ar e obviamente o ciberespaço; seriam os limites do combate podendo ele ser violento ou não violento, combatido por forças militares, para militares ou civis. A China deveria se preparar para se defender e atacar em qualquer cenário do século XXI (LIANG e XIANGSUI, 1999).

A Guerra será então traçada sem impedimentos de espaço ou tempo sendo o ataque a mais de um alvo perfeitamente possível e talvez até recomendado. A escolha de alvos dessa maneira se torna mais importante para essas operações síncronas. Ao limitar seus objetivos a escolhas que sejam possíveis e racionais torna a operação que, embora tenha perdido suas barreiras no tempo e no espaço, ainda levará em consideração a capacidade chinesa de executá-las com perfeição e sem o desperdício de recursos materiais e humanos. Ao selecionar os alvos deve-se manter em mente que para a obtenção de resultados positivos os meios devem ser ilimitados. As únicas regras seriam aquelas que feriram os objetivos a serem alcançados dentro do espaço cibernético.

Partindo disso, se entende que a maior parte dos conflitos chineses ocorreram e ocorrerão em um ambiente assimétrico, tendo os Estados Unidos como um ator de grande desconfiança. A China até e durante o governo de Xi Jinping entende que sua posição perante as forças estadunidenses são desiguais e que a superioridade da informação seria um fator chave para a vitória do país. Entendendo que a formulação dessa doutrina se deu no final do milênio não é surpreendente que junto de uma batalha de condições desiguais a China postule também a necessidade de se trabalhar com recursos mínimos. A palavra “racional” é utilizada diversas vezes por Liang e Xiangsuio (1999) e é continuamente aplicada ao lidar com o possível gasto de recursos dentro e fora de combate.

Por fim admite que em benefício do país as operações devam possuir uma coordenação multifacetada, aplicando não somente o esforço de militares, mas políticos, econômicos e civis. Ao compreender um conflito de dimensões ilimitadas é proposto que a esfera de ação e coordenação das atividades seja feita de forma ampla. E tudo isso sem que o controle da administração do evento se perca. Com a

presença de um sistema de comunicação bem desenvolvido é esperado que o país possa realizar operações militares sem o risco de que esta seja comprometida pela ausência da informação ou pela captação de informações falsas.

Mas tratando dos canais militares oficiais do governo, a partir dos anos 2000 vemos a evolução da Guerra Informacional para o sistema de operações Network Centric Warfare (NCW). Aqui vemos dois fatores motivadores que impulsionam a inovação dos sistemas de defesa cibernético chinês, o processo das Quatro Modernizações estava chegando ao fim e a crise econômica da década de 90 havia sido superada e para, além disso, o número de netizens na China e no mundo estava aumentando rapidamente, tornando Pequim cada dia mais sensível a não somente ataques de nações estrangeiras como também atores individuais.

Em 2004 a China publicou um White Paper focado em suas novas formulações de defesa e segurança. Nele consta que o país está preparado para adaptar suas forças para uma “Guerra Ilimitada com condições high tech” (RPC, 2004) e descreve ao longo do documento os planos e expectativas para os próximos 10 anos do ELP. As reformas em sua qualidade tecnológica são descritas como tendo o objetivo de “construir uma força informacional e vencer uma guerra informacional” e abrange as forças navais, aéreas e terrestres.

Como dito por Nye (2009) a difusão de poder dentro do ciberespaço torna indivíduos que antes não representavam grandes ameaças para países agora são atores potencialmente perigosos ao interesse do Estado. Outros atores também serão fonte de riscos para o país, em especial grandes potências como Estados Unidos ou a Federação Russa e também potências regionais que acompanharam a revoada dos gansos em sua primeira onda, como Japão e Coréia do Sul. Com a virada do milênio e uma quantia considerável de problemas financeiros menor e um fundo interno de investimento o país pode trabalhar em alternativas mais caras para a sua própria defesa, iniciando o longo caminho para reduzir as vulnerabilidades (NYE e KEOHANE, 2001) de Pequim no espaço cibernético.

Mas pensando neste momento apenas no contexto tradicional do conflito, o NCW é inicialmente pensado dentro do contexto estadunidense e gerava seu próprio

debate a respeito da possibilidade de que ao se implementar esta nova doutrina militar a essência da guerra seria alterada (DAHL, 2002).

> As operações centradas na rede podem ser amplamente descritas como derivadas do poder de uma rede rápida e robusta de pessoas bem informadas, e com combatentes geograficamente dispersos. Eles criam um ritmo opressivo e um estilo ágil de guerra. Usando operações de impacto, o objetivo é sustentar o acesso e impactar decisivamente eventos em terra. As operações centradas na rede se concentram na guerra operacional e tática, mas afetam todos os níveis da atividade militar do tático ao estratégico. É a teoria emergente da guerra para a era da informação[25] (ALBERTS, GARTSKA, STEIN, 2000, apud Dahl, tradução nossa, 2002, p. 4).

A grande vantagem do NCW estaria no link em que diversas tropas e entidades dentro e fora do conflito poderiam manter ao longo da batalha e tornar mais eficiente em termos de estratégia. A capacidade de um exército de invadir os sistemas inimigos, obter informações prioritárias e de sabotar o equipamento de seu alvo, ou seja, exercer a IW propriamente dita seria agregado à operação de modo geral. A formulação desta nova doutrina envolveria um constante desenvolvimento de não só tecnologias[26] na área da comunicação e sensores que fossem capazes de identificar alvos a distâncias cada vez maiores, mas também a elaboração de equipamentos defensivos cada vez mais sofisticados que fossem capazes de impedir a sabotagem ou a espionagem da informação por parte do inimigo (ALBERTS, GARTSKA, STEIN, 2000).

Em um primeiro momento o sistema NCW pode parecer um pouco descolado do termo guarda-chuva “cyberwarfare”, porém toda a operação está ligada a máquinas que fazem parte do ciberespaço como um todo, mesmo quando estão funcionando em um sistema fechado como é o caso de seu uso em operações militares (FRITZ, 2015). Ao utilizarmos a literatura proveniente da doutrina militar chinesa veremos que este termo foi ressignificado dentro do país e é frequentemente chamado de

---

[25]Network Centric Operations can be broadly described as deriving Power from the rapid and robust networking of well-informed, geographically dispersed war fighters. They create over powering tempo and a precise, agility maneuver warfare. Using effects based operations, the aim is sustain access and to decisively impact event ashore. Network Centric Operations focus on operational and tactical warfare, but they impact levels of military activity from the tactical to the strategic. It is the merging theory war for the information age

[26]Existe uma lista particularmente longa de itens de tecnologia que foram incorporados à doutrina militar chinesa por meio do INEW, estes itens são somados aqueles que são relacionados à guerra eletrônica, como é o exemplo de raios X, ultravioleta, infravermelho, microondas e rádio

“Integrated Network Electronic Warfare” (INEW), para a China este seria um modo de integrar operações militares sob condições informacionais (KREKEL, 2009).

A informatização do ELP durante a primeira década do século 21 é um processo híbrido em que retém grande parte da estrutura que já possuía e moderniza ou evolui aquilo que é possível utilizando o menor aporte de recursos; financeiros, humanos ou logísticos; que seja possível (KREKEL, 2009). A superioridade da informação se torna então o principal objetivo desta doutrina e por meio das informações obtidas os principais alvos deveriam ser a estrutura logística do inimigo e seu C4ISR[6]. Tudo isso seria focado em guerras locais ou contra adversários com capacidade militar ou tecnológica superior à chinesa.

No ano de 2010 a China declara completo o seu processo de integração entre as forças armadas e a tecnologia da informação ao publicar "China's National Defense in 2010” um documento contendo a evolução da capacidade de defesa e segurança chinesa ao longo da primeira década e as suas expectativas para a próxima. O investimento em P&D é um dos pontos chave no documento ao se falar sobre a informatização do ELP e a necessidade de melhoria constante e de desenvolvimento de tecnologias nacionais de defesa de alto nível que possam ser comparadas a aquelas utilizadas por grandes potências.

4.2 A Era de Xi Jinping

A dedicação do governo chinês em criar uma real arquitetura cibernética que possa servir aos propósitos de defesa do Estado é centrada na figura de Xi Jinping. Desde a sua gestão como vice-presidente durante o governo de Hu Jintao (2003-2013) demonstrou forte interesse pela área, assumindo cargos de importância relacionados ao logo dos anos, como a presidência da Comissão Militar Central, responsável por supervisionar as ações do Exército Popular de Libertação, desde 2012 (HAGESTAD, 2012). Seu ímpeto para modernizar as forças armadas chinesas se estendeu para além do ciberespaço, e ao assumir a presidência do país em 2013 iniciou reformas dentro da estrutura geral do ELP.

Embora as forças armadas tenham passado por revitalizações tecnológicas no período de desenvolvimento do INCW, a estrutura da organização em si era ultrapassada e limitante (SAUNDERS e WUTHNOW, 2017). Esta reforma visava

fortalecer os planos de P & D do exército, aumentar o próprio status das tropas ao remover peças reconhecidamente corruptas e criar cadeias de comando conjunto que fossem funcionais. Os serviços vinculados ao ciberespaço também foram reorganizados em diferentes departamentos, mas centralizava as principais decisões na figura do presidente. Como resultados desta operação, cerca de 300000 oficiais tiveram sua vida militar revista no ano de 2015 (CHAIN, 2018).

O primeiro órgão criado para este fim foi a Comissão Central de Segurança Nacional (CCSN) no mês de abril de 2014. Foi visto de forma positiva pela comunidade internacional pois sua estrutura se iguala em muito a aquelas adotadas por diversos outros Estados. É esperado que com esta nova agência às operações militares chinesas possuam um maior nível de coordenação dada a centralização de funções em apenas uma instituição. A exemplo da Escola de Copenhague a China adota um conceito de securitização ampla e em seu primeiro discurso para a Assembleia Geral desta comissão Xi Jinping elenca 11 tópicos a serem considerados como risco e prioridade para a segurança chinesa (JI, 2016).

Listando em seu aspecto mais amplo, Ji (2016) separa estes tópicos em seis categorias em ordem de prioridade. O tópico de segurança mais importante para o PCC seria a segurança política, assegurar a estabilidade do país e de seu regime é o cerne de sua securitização. Em segundo lugar está a necessidade de assegurar a integridade territorial chinesa, neste ponto elencamos o Mar do Sul da China como uma questão de soberania ainda não resolvida. Logo em seguida estão as forças armadas e a segurança cibernética que durante o governo de Xi Jinping se tornou um tópico de debate constante dentro do ELP. A segurança econômica e a segurança humana, que engloba os aspectos culturais da sociedade, são dois itens que se complementam dentro da agenda chinesa. Por fim, a segurança não tradicional vem como um grande guarda-chuva para abranger ciência e tecnologia, saúde, segurança alimentar e segurança da informação.

Qin (2014) explica que esta nova comissão permite que o presidente ignore barreiras burocráticas que existiam no sistema anterior e mobilize recursos de espectro amplo para formular estratégias de longo prazo. Este tipo de resolução centralizada em sua figura permite um maior poder de barganha dentro do cenário internacional e indica uma postura de política externa mais proativa por parte da

China. Isto combina perfeitamente com os planos ambiciosos de Xi para as Novas Rotas da Seda e seu Sonho Chinês. Esta política é uma ruptura com o sistema de freios e contrapesos estabelecidos por Deng Xiaoping há mais de 30 anos e estabelece um plano de ação que seja mais ativo e propositivo.

Ao assumir em 2012 Xi contava com uma forte base de apoio político e popular sendo um líder carismático e que carregava consigo propostas de mudanças que eram desejadas pelos mais diversos setores da China (HU, 2016).Possui a pretensão de realizar reformas estruturais propostas para sanar a dificuldade chinesa em administrar crises, coordenar operações de segurança (CHAIN, 2018) até uma reformulação na condução da política externa do país (QIN, 2014). O ELP admite que suas capacidades de resposta a ataques cibernéticos estão mais distantes do ideal do que gostariam e planeja superar estas deficiências durante o processo de reforma de Xi (CHINA, 2019). Embora a ideia da criação da CCSN não seja recente, pois é especulada pelo ex-presidente Jiang Zeming em 1997, apenas sai do papel anos depois. Para os próximos anos e décadas o ELP estipula três grandes objetivos a serem alcançados:

> alcançar a mecanização de modo geral até o ano 2020 com informação significativamente melhorada e capacidades estratégicas muito melhoradas;
>
> para avançar de forma abrangente a modernização da teoria militar, estrutura organizacional, pessoal militar e armamento e equipamento em sintonia com a modernização do país e basicamente concluir a modernização da defesa nacional e das forças armadas até 2035; e
>
> para transformar totalmente as forças armadas do povo em forças de classe mundial em meados do século 21. (CHINA, 2019, p. 10)

Hu (2016) lista como um fator motivador destas reformas o gigantesco crescimento econômico do país nos últimos anos que modificou as relações de poder entre a China e os demais países do Sistema Internacional. A China pela primeira vez se organiza em uma conferência com seus vizinhos para tratar de assuntos de diplomacia regional em 2013 e em 2014 realizou a primeira Central Conference on Work Relating to Foreign Affairs em mais de 10 anos. A partir destes encontros novas normativas para a diplomacia do país surgiram como forma de delinear melhor o que era a segurança que o país buscava internacionalmente. Sua diplomacia é formada com base em um sistema de países parceiros ao invés de alianças propriamente ditas. O país estabeleceu formas diferenciadas de tratar Estados diferenciados,

conquistando a parceria entre 67 países em diversos continentes. Estas relações são forjadas com base no interesse econômico daqueles com que a China estabelece suas relações.

Rahul (2018) explica que um de seus grandes projetos o “Sonho Chinês” é resultado da política de Ascensão Pacífica elaborada por Deng Xiaoping. Em 1989 a China lutava para sair de uma política externa isolacionista em um período de tempo em que seu regime doméstico poderia lhe causar transtornos diplomáticos e que, portanto deveria ser conduzida calmamente. Sua conduta envolvia não chamar a atenção internacional para si, entendendo que durante o seu crescimento o país não deveria tomar a liderança dentro do Sistema. Esta posição foi levemente alterada em 2004 com a mudança de sua estratégia para Desenvolvimento Pacífico, nela o país tentava assegurar a seus vizinhos que não representaria uma ameaça mesmo com seu crescimento econômico gigantesco ao longo da década.

Todavia, já em 2008 às declarações de Pequim indicavam mudança nos rumos da política externa do país com declarações favoráveis a um novo direcionamento condizente com aquele adotado por Xi Jinping anos mais tarde, em sua agenda oficial a diplomacia de Pequim falava sobre um novo posicionamento de uma China rica e próspera (RAHUL, 2018). Com o propósito de rejuvenescer a política chinesa, o Sonho Chinês possui dois grandes objetivos segundo Allison (2017), o primeiro é a duplicação do PIB até o final deste século e utilizar a riqueza gerada para elevar o índice de desenvolvimento humano, e o segundo é que até 2050 a China se torne uma nação desenvolvida aos olhos da comunidade internacional.

E no caminho para se tornar o ator destaque do Sistema Internacional (ALLISON, 2017) o ciberespaço e o poder cibernético terão seu próprio papel a ser cumprido. Como visto no capítulo anterior, Xi pretende explorar as opções econômicas disponíveis para a indústria 4.0 e utilizar deste recurso para que o seu projeto do Sonho Chinês seja viável. O *design china* parte do fato de que Pequim conseguirá gerar mais valor por meio de fomento à indústria de ponta e expansão de sua capacidade de criar TIC com patentes chinesas (ABRAX, 2018). Com os dois objetivos citados acima em mente, a China vai apoiar de forma agressiva projetos de inovação e que prometem maior competitividade dos produtos nacionais perante o mercado

estrangeiro. Segal explica que os maiores objetivos de Xi Jinping para o ciberespaço envolvem

> Operações de rede de computadores na China são realizados para fortalecer a competitividade da economia da China,acelerar a modernização do Exército de Libertação Popular (PLA), enfraquecer os oponentes do Partido Comunista Chinês (PCC), resistir pressão internacional e ideias estrangeiras, e compensar o domínio dos EUA em capacidades militares convencionais. Pequim também está apoiando agressivamente a inovação nativa de tecnologias emergentes que lhe darão novos recursos no ciberespaço, especialmente 5G, inteligência artificial e sistemas de informação quântica. (SEGAL, tradução nossa, 2020, p.2)

Esta nova maneira chinesa de lidar com sua política econômica internacional causa certo embaraço dentro da comunidade internacional com acusações frequentes de que há o emprego de suas capacidades cibernéticas para a espionagem industrial e roubo de dados de grandes empresas. Lewis (2014) insiste que o país utiliza desse mecanismo para suprir diferenças em relação a suas capacidades de P&D, mas que este potencial não é utilizado para fins bélicos de modo geral. O uso do ciberespaço estará para a China mais ligado a sua capacidade de gerar renda do que em seu aspecto militar ofensivo.

A espionagem industrial não se limita ao Estado Chinês, o poder de realizar a espionagem dentro do ciberespaço é difuso (NYE, 2009), por isso empresas e atores individuais dentro da própria China podem realizar esses ataques sem a ciência do PCC. Lewis (2014) vai estão categorizar em quatro tipos de abordagens para a espionagem de fins econômicos na China. a) Espionagem cibernética orientada e administrada pelo governo; b) Grupos contratados pelo ELP que podem examinar tanto tecnologia para propósitos civis quanto militares; c) empresas com grupos terceirizados ou não de hackers trabalhando a seu serviço; e d) hackers independentes que irão vender a informação obtida de acordo com seus próprios interesses.

Sendo o país asiático mais ativo dentro do ciberespaço (SEGEL, 2020), a China terá de lidar com alguns desafios para alcançar uma posição confortável de segurança de suas informações e infraestruturas. O país hoje é vulnerável em suas capacidades de defesa de suas infraestruturas críticas ao considerar que a maior parte da tecnologia empregada possui origem em países estrangeiros, o que é visto como um risco por parte dos analistas chineses de segurança cibernética (CHINA, 2019).

Em 2019 o governo de Pequim publicou outro Livro Branco intitulado “China’s National Defense in the New Era”, em que examina tópicos sensíveis para a segurança do País para os próximos anos. Nele elenca, de modo não surpreendente, os Estados Unidos como o principal ator de risco a sua segurança, afirmando que ações militares unilaterais por parte dos EUA ativam uma reação global em cadeia de desconfiança e busca por melhoria em suas capacidades de defesa e estimula a competição entre outros atores regionais pela inovação de seus aparatos de defesa, sejam eles relacionados a capacidade naval, aérea, terrestre, espacial e do ciberespaço. Também cita a Rússia como um dos atores relevantes para a segurança internacional, porém considera que o país utiliza de suas capacidades militares para fortalecer suas próprias defesas, sejam elas tradicionais ou não. Por fim, destaca a União Européia como um todo sem citar países específicos e destaca o esforço destes países em reduzir suas próprias sensibilidades em relação ao uso de tecnologia estrangeira para a defesa de seus interesses nacionais.

Para esta Nova Era o país reafirma que embora suas pretensões de Ascensão ou Desenvolvimento Pacífico sejam características de um tempo passado, não é intenção de Pequim a “busca por hegemonia, expansão ou esfera de influência”, sendo este um dos princípios não negociáveis para a defesa nacional. Mesmo com o “Sonho Chinês” elevando o país a uma posição mais propositiva dentro das relações internacionais, insiste em que seus interesses vão na direção contrária de confrontos bélicos de qualquer nível. Ainda assim resguarda seu direito de intervir a qualquer custo para que a integridade territorial do país não seja afetada por movimentos separatistas do Tibet e do Turquestão do Leste.

Este princípio de defesa do território e de sua soberania se estende também ao ciberespaço. A China em 2012 discursou a favor de um controle mais rígido por parte dos Estados a conteúdos de rede durante a Conferência Mundial sobre Telecomunicações Internacionais que ocorreu na sede da ONU (KOLTON, 2017). Os Estados Unidos foram contrários a este tipo de ação, defendendo que a governança de rede deveria envolver a participação livre de atores não estatais, como a sociedade civil e empresas privadas.

A China de Xi Jinping é ativa dentro das instituições internacionais e fóruns reguladores de rede. Seus marcos regulatórios e técnicos de controle do ciberespaço

representados pela ótica do “Golden Shield Project” geraram o que hoje é discutido como ciber soberania (SHEIN, 2016). Kolton (2017) afirma que a opinião chinesa contrasta com a proposta estadunidense de uma internet mais liberal, porém centrada em seus interesses que dominaram por muitos anos os debates e opiniões a respeito da condução da governança de rede. A China possui uma memória muito ruim do período que se submeteu aos caprichos de uma nação estrangeira e não pretende permitir que algo similar ocorra em seu espaço cibernético.

Negro (2019) contraria a visão de que a China estaria se trancafiando em uma gaiola criada por ela mesma com a adoção de métodos tão rígidos para a manutenção de sua ciber soberania. Em sua visão, cada vez mais o país assume posições de influência dentro de organismos internacionais como a Corporação da Internet para Atribuição de Nomes e Números (ICANN) e International Telecommunication Union (ITU). Em seu estudo constatou ampla presença de empresários do setor de registro de domínios de rede dentro da ICANN e presença ativa da academia chinesa nos fóruns de discussão da ITU. A participação puramente estatal dentro destes dois órgãos é limitada pela própria estrutura das organizações. A China, portanto adota uma abordagem de múltiplas partes interessadas, onde mesmo tendo a presença do Estado e de seus interesses, ainda expande o número de atores presentes na discussão.

No ano de 2016 há uma mudança de gestão por parte da ICANN, onde o Departamento de Comércio Administração Nacional de Telecomunicações e Informações encerra seu contrato de responsabilidade para com a ICANN e deixa esta vaga em aberto (KOLTON, 2017). Neste momento a organização não mais está vinculada aos Estados Unidos e era temido que países como a China tomassem uma grande influência dentro da instituição e alterassem o viés da ICANN para algo mais voltado a regulamentação de rede (NEGRO, 2019). Isto não ocorre e a China na realidade adota uma postura conciliadora, onde mantém os seus interesses de soberania em seu ciberespaço, porém não atua de modo incomodar em grande escala aqueles que são partidários de um ambiente mais livre.

A ciber diplomacia realizada pelos países de modo geral é vista como uma forma de gerir conflitos de interesse e tentar criar uma agenda comum de segurança e proteção contra ataques cibernéticos. Se difere do campo diplomático tradicional

pois é obrigada a lidar a todo o tempo com atores não estatais que fazem parte da arquitetura do ciberespaço, como por exemplo empresas como o Facebook e Tecent (BARRINHA E RENARD, 2017). Este é particularmente um desafio para a China em sua tentativa de conciliar uma governança global que seja definida pela agenda de soberania cibernética dos países, porém através de sua postura na ICANN (NEGRO, 2019) podemos notar que a calma e a prudência de Deng Xiaoping não foi esquecida pelas ambições de Xi Jinping.

5. CONSIDERAÇÕES FINAIS

Ao longo do primeiro capítulo acompanhamos o desenvolvimento da internet, explorando em detalhes como a ARPANET foi formada a partir da concorrência estadunidense para com a União Soviética após o momento em que esta lançou os satélites Sputinik 1 e 2 ao espaço. Inicialmente este projeto era um tiro no escuro que exigiu um trabalho conjunto de diversas equipes para que se tornasse algo real. Também vimos que embora a ARPANET tenha sido a primeira plataforma web a se tornar funcional, não era o único projeto no mundo a se encaminhar para criação de uma tecnologia da comunicação tão sutil e ao mesmo tempo tão poderosa.

A junção da tecnologia ARPA aos protocolos de rede TCP/IP permitiu que a comunicação entre máquinas atingisse potencial de comunicação global. A função destes protocolos é padronizar o envio e recebimento de dados entre as máquinas e identificá-las a partir de uma numeração. A união destas duas invenções funciona extraordinariamente bem e o protocolo IPV4 foi adotado por todas as empresas de tecnologia do mundo. E hoje com mais de 4,6 bilhões de usuários (ISTO É, 2021) já é inclusive necessário expandir o número de combinações possíveis para estes protocolos, sendo necessário o uso da segunda geração de IPs, o IPV6.

A transição da tecnologia de uso militar para o uso civil foi mais que bem aceita entre a sociedade e hoje possuímos acesso ao espaço cibernético diretamente da palma de nossas mãos por meio dos smartphones. Lévy (2000) diz que o mundo criaria uma cibercultura e hoje com nosso acesso às redes sociais como Facebook, WhatsApp, Instagram já fazem parte de uma nova cibercultura que domina o século XXI. Além de funções para a diversão, a internet aproximou pessoas, facilitou o comércio a nível mundial, redesenhou as noções de distância e tempo, pois afinal de contas estamos na Era da Informação onde tudo é acessível e tudo pode ser feito em um instante. Hoje as infraestruturas de energia elétrica, água, hospitais, governos, aeroportos possuem seu funcionamento ligado diretamente ao ciberespaço.

Os Estados incorporaram muito rapidamente a internet ao seu funcionamento, pois de fato às regulamentações, burocracias e taxas se tornam muito mais administráveis quando se tem a sua disposição uma ferramenta que possa tornar todas as funcionalidades que são necessárias em apenas um ambiente virtual. E a cada dia que passa a perspectiva é que o ciberespaço se vincule ainda mais à

realidade e ao cotidiano destes governos e cidadãos. Os casos de países ultra conectados apenas crescem, como é o exemplo da Estônia que é referência em cidades inteligentes.

Todavia esta ferramenta foi criada para fins militares e de guerra, embora tenha sido adaptada ao uso civil, seu potencial de causar danos a Estados, organizações, empresas e indivíduos não deve ser esquecido. O primeiro exemplo que exploramos foi o caso da própria Estônia que em 2007 sofreu um ataque de Negação de Serviço Distribuído (DDoS), onde seus sistemas governamentais se tornaram inoperacionais e até mesmo suas instituições financeiras foram severamente afetadas. Especula-se que este ataque foi realizado devido a decisão do país de realocar monumentos históricos que homenageavam a URSS.

O próximo caso a ser comentado foi o ataque às centrífugas de enriquecimento de urânio do Irã que foram sobrecarregadas devido a presença de um vírus, um malware, que causou um mau funcionamento da máquina. Isto aconteceu em 2010 e nesta época havia uma grande desconfiança por parte da comunidade internacional de que estas usinas estariam enriquecendo urânio para fins bélicos, o que foi negado com veemência por parte do governo iraniano. Especialistas alertaram para a complexidade do vírus, pois este era muitíssimo bem trabalhado e possui dupla função, além de negar o serviço operacional da máquina, também impedia que as funções de alerta do sistema funcionassem corretamente de modo a alertar os funcionários para a necessidade de encerramento das atividades da usina. As principais suspeitas recaíram sobre Israel e Estados Unidos, embora as investigações finais não tenham levado a nenhum culpado final.

Casos como este colaboraram para que os países intensificassem a segurança investida para o ambiente virtual. E sendo o processo de securitização baseado em decisões políticas que transformam problemas em questões de segurança, logo observamos que países desenvolvidos ou em desenvolvimento voltam seus olhos para a sua segurança cibernética doméstica. A China em específico possui um processo de securitização interessante, pois a sua prioridade está em assegurar a estabilidade do Estado e a manutenção do regime, e com a chegada da internet ao seu país diversos setores sofrem os efeitos desta securitização política, desde a sociedade civil e seu acesso a rede até em setores puramente militares.

A segurança de rede se torna então um grande jogo de xadrez (NYE, 2009), onde diversos atores que antes não possuíam voz e vez perante o sistema internacional agora possuem acesso a plataformas que tornam suas vozes potentes ferramentas de expressão da opinião pública. O poder dentro do ciberespaço é difuso e assimétrico e novos atores brigam por seus espaços dentro de rede, tanto de modo legalizado quanto fora dos regimes legais, como o WikiLeaks.

A China usará o ciberespaço inicialmente para fins econômicos, pois suas ambições de desenvolvimento exigiram uma rápida adaptação a estas novas ferramentas que antes estavam fora do alcance civil. Ao contrário do que ocorreu nos EUA, o Estado conquistou o acesso à internet quase que ao mesmo tempo que a população civil, no ano de 1994. Este feito ocorreu por meio da colaboração entre instituições de ensino superior, o exército chinês e o Partido Comunista Chinês. Não havia em um primeiro momento grandes regulamentações a respeito do acesso de rede por parte dos usuários, mas o controle de Pequim se deu por meio das autorizações aos provedores para que estes pudessem comercializar a internet dentro do país.

Com o avançar da década, as primeiras legislações sobre o ciberespaço foram lançadas e isso gerou um sinal de alerta para pesquisadores de todo o mundo que possuíam receio de que a China limitasse e censurasse o uso da internet por parte de seus cidadãos. Aqueles adeptos a teoria de que a rede deveria ser neutra temiam que a interferência chinesa pudesse suprimir a inovação do ciberespaço do país, pois estes conectam a liberdade e democracia da internet diretamente ao seu potencial como tecnologia a ser explorada economicamente.

Ao considerar que a prioridade da segurança estatal está na manutenção do regime e na estabilidade política do país, não é inesperado que iniciativas como o “Golden Shield” surjam no desenvolvimento de políticas e legislações para o ciberespaço. A China possui grande receio do que poderia acontecer caso conteúdos estrangeiros não controlados chegassem ao país. O medo de que a influência externa provocasse uma perturbação no modo que desestabilizasse o regime ou prejudicasse a paz.

O sistema de filtragem de conteúdo por parte da China, ou seja, censura em rede chamou a atenção da comunidade internacional durante muito tempo. Todavia,

às Olimpíadas de Pequim tornaram este tema ainda mais relevante para o cenário internacional, especialmente com a presença de organizações como a Anistia Internacional que cobravam ativamente uma maior liberdade de imprensa por parte da China. O país havia se comprometido ao ser escolhido para sediar o evento a não censurar os serviços das equipes de jornalistas presentes na cobertura do evento, entretanto houve algumas limitações a esta liberdade. Inicialmente, sites críticos ao PCC não possuíam acesso dentro da internet chinesa. Posteriormente, apenas tópicos considerados sensíveis foram barrados por parte do governo. Nada disso é surpreendente ao considerarmos o contexto de controle da informação em que Pequim armou para si.

Outro caso, mas tratando da iniciativa privada e da participação de empresas estrangeiras no país, a saída do Google como provedor de pesquisa da China foi um evento marcante. Embora tenha em 2005 estabelecido seus serviços concordando com os termos de censura que o país impunha na época, logo a pressão por parte de investidores estrangeiros e as contínuas exigências por parte do PCC por cada vez mais informações ou limites de pesquisa tornou insustentável a manutenção da companhia. O fim de tudo se deu quando o Google sofreu um ataque cibernético massivo nos anos de 2010 e 2011 e decidiu retirar o seu escritório para Hong Kong.

O processo de abertura econômico iniciado por Deng Xiaoping em 1979 com as Quatro Modernizações gerou um ambiente propício para o investimento chinês em tecnologia da informação. As primeiras décadas do século XXI elevaram a China ao status de potência econômica, o que possibilitou que mais tarde que Xi Jinping avançasse com suas políticas altivas e assertivas para a economia chinesa de modo geral. O “Sonho Chinês” depende de um bom desempenho por parte do país em desenvolver pesquisas inovadoras dentro dos campos da indústria 4.0.

A incorporação do ciberespaço pelas forças armadas chinesas só é possível graças a este mesmo boom tecnológico proporcionado pela economia. É um processo lento, feito por partes que convergiam com o momento econômico que o país estava passando. Durante a década de 90 a instabilidade e recuperação econômica aliado ao fato de que o ciberespaço ainda era algo extremamente novo dentro da China, não há muitos avanços a nível militar. Há algum planejamento inicial e formulação de uma nova doutrina para o próximo século, mas isto está apenas no campo teórico.

Já nos primeiros anos do novo milênio há a absorção do conceito de Guerra Ilimitada por parte do ELP, onde a China assume a sua posição assimétrica de poder perante o sistema e busca alternativas para trabalhar suas vulnerabilidades. Há a assimilação do conceito de Network Centric Warfare, adaptando ao contexto de Pequim e priorizando a obtenção da informação sobre o inimigo. Em suma, o uso do ciberespaço para o ELP está mais relacionado a melhora na sua capacidade de buscar e encontrar informações sensíveis a respeito de seu alvo do que para o ataque, entendendo que a disparidade tecnológica em relação a demais atores estatais não permitiria um avanço racional deste tipo.

A hipótese é parcialmente comprovada ao longo deste trabalho, pois se entende que sim, a China está utilizando das novas estratégias do ciberespaço para garantir sua soberania e integridade territorial. Porém, para, além disso, também vemos que em âmbito doméstico esta securitização tem como objetivo manter a estabilidade do regime e impedir que a influência estrangeira possa atrapalhar de qualquer modo os objetivos do partido. Para isso a China contará com um sistema gigantesco de filtragem de informação, o seu Grande Escudo Dourado, e está preparada para lidar com a pressão internacional ao adotar esta postura. O país também usará do ciberespaço para fins de crescimento econômico, embora não demonstre a ambição de se tornar uma potência conflituosa, pretende continuar o seu sonho ambicioso pacificamente ao mesmo tempo que se prepara para defender de forma firme seus interesses.

REFERÊNCIAS BIBLIOGRÁFICAS

ADABO, Gabrielle. Ciência e guerra: era uma vez a internet. **Comciência**, Campinas, v. 168, p. 1-4, maio 2014. Disponível em: http://comciencia.scielo.br/pdf/cci/n158/02.pdf. Acesso em: 17 nov. 2020.

ALBERTS, Avid S.; GARSTKA, John J.; STEIN, Frederick P.. **Network Centric Warfare:**: developing and leveraging information superiority. 2. ed. __: Ccrp, 2000. 334 p.

ALLISON, Graham. The Atlantic. The Atlantic. Disponível em: <https://www.theatlantic.com/international/archive/2017/05/what-china-wants/528561/>. Acesso em: 28 Apr. 2021.

ARBIX, Glauco; MIRANDA, Zil; TOLEDO, Demétrio; ZANCUL, Eduardo. Made in China 2025 e Industrie 4.0: a difícil transição chinesa do catching up à economia puxada pela inovação. **Tempo Social**: revista de sociologia da USP, [*s. l*], v. 3, n. 30, p. 144-170, 2018.

AUSTIN, Greg. **CYBER POLICY IN CHINA**. Londres: Uk Copyright, Designs And Patents Act, 2014. 200 p.

AUSTIN, Greg. **Cybersecurity in China**: the next wave. Londres: Springerbriefs, 2016. 130 p.

BARBIERI, Mariana Delgado; ZAGO, Lisandra. Modernização, incorporação e sobrevivência da população rural: o caso chinês pós 1978. **Revista Cadernos de Ciências Sociais da Ufrpe.** Campinas, p. 1-22. jan. 2020.

BARRINHA, André; RENARD, Thomas. Cyber-diplomacy: the making of an international society in the digital age. **Global Affairs**, [S.L.], v. 3, n. 4-5, p. 353-364, 20 out. 2017. Informa UK Limited. http://dx.doi.org/10.1080/23340460.2017.1414924

BARROS, Vinícius Tijolin. **Waltz, Keohane e Wendt:**: análise de construções conceituais sobre o poder. 2015. 61 f. TCC (Graduação) - Curso de Relações Internacionais, Faculdade de Direito e Relações Internacionais, Análise de Construções Conceituais Sobre O Poder, Grande Dourados, 2015. Disponível em: http://repositorio.ufgd.edu.br/jspui/bitstream/prefix/3875/1/ViniciusTijolinBarros.pdf. Acesso em: 27 nov. 2020.

BAY, Morten**. Conversationwith a pioneer: Leonard Kleinrockontheearlydaysof networking, the ARPANET…andwinning in Las Vegas**, Internet Histories, DOI: 10.1080/24701475.2018.1446239

BBC. **'A tática do Estado Islâmico para me recrutar - e como eu resisti'**. 2015. Disponível em:

https://www.bbc.com/portuguese/noticias/2015/08/150824_ei_tatica_radical_fd. Acesso em: 01 dez. 2020.

BOBBIO, Norberto (org.). **Dicionário de Política**. 11. ed. Brasília: Unb, 1998. 1200 p. Disponível em: http://professor.pucgoias.edu.br/SiteDocente/admin/arquivosUpload/17973/material/Norberto-Bobbio-Dicionario-de-Politica.pdf. Acesso em: 27 nov. 2020.

BRASIL. Doutrina Militar de Defesa Cibernética. Ministério da Defesa. Brasília, 2014. Disponível em: https://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_de fesa_cibernetica_1_2014.pdf. Acesso em 10 out. 2020

BRITO, Vladimir. Agente da PF revela - Como os EUA interferem em governos de outros países. 2015. Disponível em: https://youtu.be/3zf85w2g2-A

BUZAN, Barry; WÆVER, Ole; WILDE, Jaap de. Security Analysis: Conceptual Apparatus. In: BUZAN, Barry; WÆVER, Ole; WILDE, Jaap de. **SECURITY**: a new framework for analysis. Londres: LynneRiennerPublishers,, 1998. Cap. 2. p. 21-47.

BUZAN, Barry; WÆVER, Ole. Introduction:developing a regional approach to global security. In: BUZAN, Barry; WÆVER, Ole. **RegionsandPowers**: thestructureofinternationalsecurity. Londres: Board, 2003. Cap. 1. p. 3-83.

CAMPBELL-KELLY, Martin; GARCIA-SWARTZ, Daniel D.. The Historyofthe Internet::themissingnarratives. **Ssnr**, Warwick, v. 1, n. 1, p. 1-65, 2 dez. 2005. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=867087. Acesso em: 25 nov. 2020.

CARBINATTO, Bruno. Por que os EUA estudam banir o TikTok do país? **Super**. Disponível em: <https://super.abril.com.br/tecnologia/por-que-os-eua-estudam-banir-o-tiktok-do-pais/>. Acesso em: 26 Apr. 2021.

CASSIOLATO, José Eduardo. AS POLÍTICAS DE CIÊNCIA, TECNOLOGIA E INOVAÇÃO NA CHINA. **Boletim de Economia e Política Internacional**: As Políticas de Ciência, Tecnologia e Inovação na China, __, v. 1, n. 1, p. 66-90, jan. 2013.

CASTELLS, Manuel. **A Galaxia da Internet**: reflexões sobre a internet, os negócios e a sociedade. São Paulo: Zahar, 2003.

CERF, Vint. The open Internet:: what it is, and why it matters. **Telecommunications Journal Of Australia**, [*s. l*], v. 9, n. 52, p. 1-18, jan. 2009.

CERF, Vint. The open Internet:: what it is, and why it matters. **Telecommunications Journal Of Australia**, [*s. l*], v. 9, n. 52, p. 1-18, jan. 2009.

CHAN, Susanne. Cybersecurity under Xi Jinping. __**.** __, p. 1-12. jan. 2018.

CHANDEL, Sonali; JINGJI, Zang; YUNNAN, Yu; JINGYAO, Sun; ZHIPENG, Zhang. The Golden Shield Project of China: a decade later ∴ an in-depth study of the great firewall. **2019 International Conference On Cyber-Enabled Distributed Computing And Knowledge Discovery (Cyberc)**, [S.L.], v. 1, n. 1, p. 1-25, out. 2019. IEEE. http://dx.doi.org/10.1109/cyberc.2019.00027.

CHINA, People'SRepublic Of. **China'sNationalDefense in the New Era**. Beijing: ForeignLanguages Press, 2019. 51 p. Disponível em:

CHINA. Guerra comercial: entenda as tensões entre China e EUA e as incertezas para a economia mundial. **G1**. Disponível em: <https://g1.globo.com/economia/noticia/2019/08/16/guerra-comercial-entenda-a-piora-das-tensoes-entre-china-e-eua-e-as-incertezas-para-a-economia-mundial.ghtml>. Acesso em: 26 Apr. 2021.

China (CHN) Exports, Imports, and Trade Partners. Oec.world. Disponível em: <https://oec.world/en/profile/country/chn>. Acesso em: 18 Apr. 2021.

China's development of cyber warfare doctrine: a conceptual and historical investigation.

CHONG, Alan. Information Warfare? **Armed Forces & Society**, [S.L.], v. 40, n. 4, p. 599-624, 9 maio 2013. SAGE Publications. http://dx.doi.org/10.1177/0095327x13483444

*CHOW, Gregory. Important Lessons from Studying the Chinese Economy. **China As A Leader Of The World Economy**, [S.L.], p. 111-131, out. 2011. WORLD SCIENTIFIC. http://dx.doi.org/10.1142/9789814368810_0015.*

COLLINS, Sean; MCCOMBIE, Stephen. Stuxnet: theemergenceof a new cyber weaponand its implications. **JournalOfPolicing, IntelligenceAndCounterTerrorism**, [S.L.], v. 7, n. 1, p. 80-91, abr. 2012. Informa UK Limited. http://dx.doi.org/10.1080/18335330.2012.653198.

CYBERTHREAT REAL-TIME MAP. MAP | Kaspersky Cyberthreat real-time map. MAP | Kaspersky Cyberthreat real-time map. Disponível em:
DAHL, Erik J.. Network centric warfare and the death of operational art. **Faculty Of The Joint Military Operations Department.** Rhode Island, p. 1-26. jan. 2002.

DANN, G. Elijah; HADDOW, Neil. Just Doing Business or Doing Just Business:: google, microsoft, yahoo! and the business of censoring chinas internet. **Journal Of Business Ethics**, [*s. l*], n. 79, p. 219-234, jan. 2008.

DA REDAÇÃO. Número de usuários de Internet no mundo chega aos 4,66 bilhões. ISTOÉ DINHEIRO. Disponível em: <https://www.istoedinheiro.com.br/numero-de-usuarios-de-internet-no-mundo-chega-aos-466-bilhoes/>. Acesso em: 28 Apr. 2021.

DEFENSE, The Department Of. **The DoDCyberstrategy**. 2015. Disponível em: https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf. Acesso em: 17 abr. 2015

DEUTSCHE WELLE (WWW.DW.COM. **Olimpíadas 2008: direitos humanos nas fileiras de trás? | DW | 09.08.2007**. DW.COM. Disponível em: <https://www.dw.com/pt-br/olimp%C3%ADadas-2008-direitos-humanos-nas-fileiras-de-tr%C3%A1s/a-2730260>. Acesso em: 14 Apr. 2021.

DOMINGO, Francis C.. China's Engagement in Cyberspace. **Journal Of Asian Security And International Affairs**, [S.L.], v. 3, n. 2, p. 245-259, 29 jul. 2016. SAGE Publications. http://dx.doi.org/10.1177/2347797016645456.

DUARTE, Otto Carlos Muniz Bandeira. IP SECURITY. UFRJ, 2003. Disponível em: https://www.gta.ufrj.br/grad/03_1/ip-security/paginas/main.html. Acesso em: 03/12/2020

EUNJUNG, Ariana. NAKASHIMA, Ellen. **Google China cyberattack part of spy campaign**. NBC News. Disponível em: <https://www.nbcnews.com/id/wbna34855470>. Acesso em: 15 Apr. 2021.

Falun Gong - A seita que abalou o comunismo na China - Instituto Cristão de Pesquisas. Icp.com.br. Disponível em: <https://www.icp.com.br/df33materia1.asp>. Acesso em: 15 Apr. 2021.

FARIAS, Helio Caetano; MARTINS, Pedro Mendes. A geoeconomia do desenvolvimento chinês:: das quatro modernizações à belt and road initiative (bri). **Mural Internacional.** __, p. 1-22. maio 2020.

FERREIRA NETO, Walfredo Bento. TERRITÓRIO: da dimensão terrestre ao ciberespaço - espaço, poder, segurança e oportunidades econômicas. **Revista Agulhas Negras**, Resende, v. 1, n. 2, p. 88-99, dez. 2018. Disponível em: http://www.ebrevistas.eb.mil.br/index.php/aman/article/view/1877/1516. Acesso em: 01 nov. 2020.

Folha de S.Paulo - Governo na Estônia é alvo de hackers - 18/05/2007. Uol.com.br. Disponível em: <https://www1.folha.uol.com.br/fsp/mundo/ft1805200713.htm>. Acesso em: 9 Dec. 2020.

Fritz, J. (Author). 2015 Student thesis: Doctoral Thesis link: https://research.bond.edu.au/en/studentTheses/chinas-development-of-cyber-warfare-doctrine-a-conceptual-and-his

GALLAROTTI, Giulio M.. Smart Power: definitions, importance, andeffectiveness. **JournalOfStrategicStudies**, [S.L.], v. 38, n. 3, p. 245-281, 11 mar. 2015. Informa UK Limited. http://dx.doi.org/10.1080/01402390.2014.1002912.

GJESVIK, Lars; SCHIA, Niels Nagelhus. China’s cyber sovereignty. **NorwegianInstitute For InternationalAffairs**, Oslo, v. 1, n. 1, p. 1-5, dez. 2017. Disponível em: https://www.jstor.org/stable/pdf/resrep07952.pdf?ab_segments=0%2Fbasic_SYC-5187_SYC-5188%2Ftest&refreqid=fastly-default%3Aa682f414240131a4cbead2b466c1cc46. Acesso em: 01 dez. 2020.

GOTTMANN, Jean. A evolução do conceito de território. **Boletim Campineiro de Geografia**, Campinas, v. 3, n. 2, p. 523-545, nov. 2020.

GUNTHER, Mark. **Yahoo’s China problem - Feb. 22, 2006**. Cnn.com. Disponível em: <https://money.cnn.com/2006/02/21/news/international/pluggedin_fortune/>. Acesso em: 15 Apr. 2021.

HAGESTAD, Bill. **21st Century Chinese Cyberwarfare**. __: Itgovernance, 2012. 500 p

HAO, Yeli. A Three-Perspective Theoryof Cyber Sovereignty. **Institute For NationalStrategic Security**, __, v. 2, n. 7, p. 108-115, dez. 2017. Disponível em: https://www.jstor.org/stable/pdf/26470523.pdf?refreqid=excelsior%3A1fa6754821186be0e1256d92bf76df97. Acesso em: 25 nov. 2020.

HARDING, Luke. Os arquivos Snowden: A história secreta do homem mais procurado do mundo. São Paulo: LeYa Brasil, 2014. E-book.

HOBBES, Thomas. **Leviatã**: ou matéria, forma e poder de um estado eclesiástico e civil. __: Tradução Independente, . 230 p. Disponível em: http://www.dhnet.org.br/direitos/anthist/marcos/hdh_thomas_hobbes_leviatan.pdf. Acesso em: 08 dez. 2020.

HONG, Yu; GOODNIGHT, G. Thomas. Howtothinkabout cyber sovereignty: the case of china. **ChineseJournalOf Communication**, Hong Kong, v. 13, n. 1, p. 8-26, 12 nov. 2019. Informa UK Limited. http://dx.doi.org/10.1080/17544750.2019.1687536

http://dx.doi.org/10.18848/2327-0055/cgp/v15i01/1-12.

HU, Weixing. Xi Jinping’s ‘Big Power Diplomacy’ and China’s Central National Security Commission (CNSC). **Journal Of Contemporary China**, [S.L.], v. 25, n. 98, p. 163-177, 8 dez. 2015. Informa UK Limited. http://dx.doi.org/10.1080/10670564.2015.1075716.

HUNT, Katie. China tweaks Internet censorship. **CNN.** Disponível em: <https://edition.cnn.com/2013/10/07/world/asia/china-internet-monitors/index.html>. Acesso em: 26 Apr. 2021.

INDUSTRIA 4.0. **Industria 4.0**. Industria40.gov.br. Disponível em: <http://www.industria40.gov.br/>. Acesso em: 19 Apr. 2021.

INTERNATIONAL, Amnesty. LEGACY OF THE BEIJING OLYMPICS: china ⁚s choice. **Amnesty International**, Londres, v. 1, n. 1, p. 1-26, jan. 2007.

JI, You. China's National Security Commission: theory, evolution and operations. **Journal Of Contemporary China**, [S.L.], v. 25, n. 98, p. 178-196, dez. 2015. Informa UK Limited. http://dx.doi.org/10.1080/10670564.2015.1075717.

KANIA, Elsa B.; COSTELLO, John K.. The Strategic Support Force and the Future of Chinese Information Operations. **The Cyber Defense Review.** __, p. 105-122. abr. 2018.

KEMP, Simon. **Digital 2019: Global Internet Use Accelerates - We Are Social**, We Are Social, disponível em: <https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates>, acesso em: 30 Nov. 2020.

KEOHANE, Robert O.; NYE, Joseph S.. **Power andInterdependence**. 4. ed. __: Pearson, 2000. 365 p.

KOLTON, Michael. Interpreting China's Pursuit of Cyber Sovereignty and its Views on Cyber Deterrence. **The Cyber Defense Review: Army Cyber Institute.** __, p. 119-154. dez. 2017.

KREKEL, Bryan. Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation.**The US-China Economic and Security Review Commission**. oct, 2009

LAI, Linda S.L.; TO, Wai-Ming. Internet Diffusion in China: economic and social implications. **It Professional**, [S.L.], v. 14, n. 6, p. 16-21, nov. 2012. Institute of Electrical and Electronics Engineers (IEEE). http://dx.doi.org/10.1109/mitp.2012.65

LEVY, Pierre. **Cibercultura.** Ed. 34, 1° edição. São Paulo. 1999. Disponível em: https://mundonativodigital.files.wordpress.com/2016/03/cibercultura-pierre-levy.pdf. Acesso em: 12/07/2020

LEWIS, James. China's cyberpower International and domestic priorities. **Aspi: Australian Strategic Policy Institute.** --, p. 1-25. dez. 2014.

LI, Mingjiang. China Debates Soft Power. **ChineseJournalOfInternationalPolitics**, __, v. 2, n. 1, p. 287-308, 28 out. 2008.

LIANG, Qiao; XIANGSUI, Wang. Unrestricted Warfare. **PLA Literature and Arts Publishing House** Fev. 1999

LINDSAY, Jon R.. StuxnetandtheLimitsof Cyber Warfare. **Security Studies**, [S.L.], v. 22, n. 3, p. 365-404, jul. 2013. Informa UK Limited. http://dx.doi.org/10.1080/09636412.2013.816122

LOPES, Gills Vilar. **Relações Internacionais Cibernéticas (CiberRI):** uma defesa acadêmica a partir dos estudos de segurança internacional. Tese de doutorado apresentada como requisito obrigatório para a obtenção do título de Doutor em Ciência Política – Área de Concentração em Relações Internacionais – pelo programa de Pós-Graduação em Ciência Política da Universidade Federal de Pernambuco. Orientador Prof. Dr. Marcelo de Almeida Medeiros. Recife. 2016.

MARTINS, Elaine. O que é TCP/IP? Tecmundo.com.br. Disponível em: <https://www.tecmundo.com.br/o-que-e/780-o-que-e-tcp-ip-.htm>. Acesso em: 9 Dec. 2020.

MAUDE, Hon Francis. **The UK Cyber Security Strategy**: protectingandpromotingtheuk in a digital world. Protectingandpromotingthe UK in a digital world. 2011. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf. Acesso em: 01 out. 2020.

MEARSHEIMER, John J..China'sUnpeacefulRise. **CurrentHistory**, [*s. l*], v. 105, n. 160, p. 160-162, jan. 2006. Disponível em: https://online.ucpress.edu/currenthistory/article/105/690/160/108268/China-s-Unpeaceful-Rise. Acesso em: 17 nov. 2020.

MEDEIROS, Breno Pauli; GOLDONI, Luiz Rogério Franco. The Fundamental Conceptual Trinity of Cyberspace. **Contexto Internacional**, [S.L.], v. 42, n. 1, p.

MILARÉ, Luís Felipe Lopes; DIEGUES, Antônio Carlos. CONTRIBUIÇÕES DA ERA MAO TSÉ-TUNG PARA A INDUSTRIALIZAÇÃO CHINESA. **Revista Economia Contemporânea.** Rio de Janeiro, p. 1-22. maio 2012.

MULVENNEY, Nick. **IOC admits Internet censorship deal with China**. U.S. Disponível em: <https://www.reuters.com/article/us-olympics-idUSN3039947420080730>. Acesso em: 14 Apr. 2021.

MULVENON, James C.. **Chinese Responses to U.S. Military Transformation and Implications for the Department of Defense**. __: Rand, 2006.

NEGRO, Gianluigi. A historyofChinese global Internet governanceand its relationswith ITU and ICANN. **ChineseJournalOf Communication.** _, p. 104-121. 12 ago. 2019. Disponível em: https://doi.org/10.1080/17544750.2019.1650789. Acesso em: 17 out. 2020.

NETO, Walfredo Bento. Territorializando o “novo” e (re) territorializando os tradicionais: a cibernética como espaço e recurso de poder. In: MEDEIROS FILHO, Oscar; FERREIRA NETO, Walfredo Bento; GONZALES, Selma Lúcia de Moura (org.). **Segurança e defesa CIBERNÉTICA**: da fronteira física aos muros virtuais. Recife: Ufpe, 2014. p. 67-98

NUNES, Danilo Henrique; LEHFELD, Lucas Souza; SILVA, Jonatas Santos. CIBERTERRORISMO: a internet como meio de propagação do terror. **Revista Húmus**, [*s. l*], v. 10, n. 29, p. 209-234, 2020. Disponível em: http://www.periodicoseletronicos.ufma.br/index.php/revistahumus/article/view/13837/7843. Acesso em: 25 nov. 2020.

NYE, Joseph. Soft power: theoriginsandpoliticalprogressof a concept. **Palgrave Communications**, [S.L.], v. 3, n. 1, p. 1-3, 21 fev. 2017. Springer Science and Business Media LLC. http://dx.doi.org/10.1057/palcomms.2017.8.

NYE JR., Joseph S. Difusão e Poder Cibernético. In: _____. (org.). O Futuro do Poder. Benvirá, 2012.

OLIVEIRA, Marcos Fábio Martins de; MOTA, Sarah Dantas Rabelo. DESENVOLVIMENTO ECONÔMICO NA CHINA PÓS 1978: ANÁLISE DAS VOCAÇÕES DESENVOLVIMENTISTA E SOCIAL. **V Congresso em Desenvolvimento Social.** __, p. 1-24. jun. 2016.

O que é DoS e DDoS? Canaltech. Disponível em: <https://canaltech.com.br/produtos/o-que-e-dos-e-ddos/>. Acesso em: 27 Apr. 2021.

OWENS, Yvonne. William Gibson andthe World ofTomorrow: digital dystopias in futuristfiction. **The InternationalJournalOfCritical Cultural Studies**, [S.L.], v. 15, n. 1, p. 1-12, jan. 2017. Common GroundResearch Networks.

Pequim. Full Text: China's National Defense in the New Era. Www.gov.cn. Disponível em: <http://english.www.gov.cn/archive/whitepaper/201907/24/content_WS5d3941ddc6d08408f502283d.html>. Acesso em: 26 Apr. 2021.

PEREIRA, Bernardo Futscher. **Waltz Revisado**. Disponível em: http://www.ipris.org/files/19/B_19_Waltz_revisitado.pdf. Acesso em: 19 nov. 2020.

PRC State Council. The regulations of safety protection for computer information systems. Order No.147, Feb. 18, 1994; Disponível em <http://www.cernet.edu.cn/LAW/qry_law2. html>

QIN, Liwen. Securing the "China Dream": What Xi Jinping wants to achieve with the National Security Commission (NSC). **Merics: Mercator Institute for China Studies.** --, p. 1-8. abr. 2014.

QUINN, Ben. **Google services blocked in China**. the Guardian. Disponível em: <https://www.theguardian.com/technology/2012/nov/09/google-services-blocked-china-gmail>. Acesso em: 15 Apr. 2021.

RAHUL, Anshuman.O Jogo pela Hegemonia Regional: A OBOR Chinesa e a Resposta Estratégica Indiana Austral: **Revista Brasileira de Estratégia e Relações Internacionais** v.7, n.13, Jan./Jun. 2018

ROHR, Altieres. **Saiba como age o vírus que invadiu usinas nucleares no Irã e na Índia.** Tecnologia e Games. Disponível em: <http://g1.globo.com/tecnologia/noticia/2010/10/saiba-como-age-o-virus-que-invadiu-usinas-nucleares-no-ira-e-na-india.html>. Acesso em: 14 May 2021

RONCONI, Giordano Bruno Antoniazzi. Poder, Relações Internacionais e mudança tecnológica: Contextualizações da Indústria de Defesa sob um Marco Realista, 1., 2015, São Paulo. **Simpósio de Pós-Graduação em Relações Internacionais do Programa "San Tiago Dantas" (Unesp, Unicamp, PUC-SP) "Governança Global: transformações, dilemas e perspectivas":** Contextualizações da Indústria de Defesa sob um Marco Realista. São Paulo: Santiago Dantas, 2015. 26 p. Disponível em: https://d1wqtxts1xzle7.cloudfront.net/46369480/RONCONI_Industria.pdf?1465511136=&response-content-disposition=inline%3B+filename%3DPoder_Relacoes_Internacionais_e_Mudanca.pdf&Expires=1607426131&Signature=ea7nTELBtKvpoYK5WCShoZz7eXHI5vEsZ5L-M1GET3J839RePy1amTuP5~onvbv9z3ziTcyZjiwHav4AmSB7jUrxIGWysTCbFw77EJ64iZXC-IwaQ15YTd8mjOgsyqjYfkIKciiLW12rgDETfFKJRyVwz3AK44O7QR4PkSVoWC~NU7zmBlDgzjNynUUdpJAbBTFbARYpHi5pqCC202T-89MVXm6veV~C9hRiw8cTvZ1O11RVBGfjyxDYHESF9T3mGQ2EQ6W~9UQFKA1yNv4UylPRmOSR1TLXloFxZo6M2EoNq87wtk8zKu5smtH6hlfW41hfPVjFWQ4Dwn7uMyZOsQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA. Acesso em: 09 nov. 2015.

SEGAL, Adam. China's Pursuit of Cyberpower. **Asia Policy**, [S.L.], v. 27, n. 2, p. 60-66, 2020. Project Muse. http://dx.doi.org/10.1353/asp.2020.0034.

SEGEV, Hiddai. The Ban on TikTok: The US Struggle against China Spreads to Apps. **Institute For National Security Studies**, __, p. 1-4, abr. 2020.

SHELDON, John B.. DecipheringCyberpower: strategicpurpose in peaceandwar. **StrategicStudiesQuarterly**, __, v. 1, n. 1, p. 95-117, jan. 2011. Disponível em: https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-05_Issue-2/Sheldon.pdf. Acesso em: 25 nov. 2020.

SHEN, Hong. China and global internet governance: toward an alternative analytical framework. **Chinese Journal Of Communication**, [S.L.], v. 9, n. 3, p. 304-324, 2 jul. 2016. Informa UK Limited. http://dx.doi.org/10.1080/17544750.2016.1206028.

SILVA, Jorge Tavares da; BREDA, Zélia.O dragão chinês e o elefante indiano: traços de similitude e de divergência nos processos de abertura e reforma econômica. Revista Economia Global e Gestão, v.14. Lisboa, 2009

SPIRI, Raquel Torrecilha. **CIBERSEGURANÇA NO BRASIL:** uma análise de seus desdobramentos à luz da securitização. 2020. 202 f. Dissertação (Mestrado) - Curso

de Ciências Sociais, A Faculdade de Filosofia e Ciências, Unesp, Marília, 2020. Disponível em: https://repositorio.unesp.br/handle/11449/194103. Acesso em: 27 nov. 2020.

STOVER, Christine M.. Network Neutrality: A Thematic Analysis of Policy Perspectives Across the Globe. **Global Media Journal**: Canadian Edition, [*s. l*], v. 1, n. 3, p. 75-86, dez. 2018.

STOVER, Christine M.. Network Neutrality: A Thematic Analysis of Policy Perspectives Across the Globe. **Global Media Journal**: Canadian Edition, [*s. l*], v. 1, n. 3, p. 75-86, dez. 2018.

TAI, Zixue. Casting the Ubiquitous Net of Information Control. **International Journal Of Advanced Pervasive And Ubiquitous Computing**, [S.L.], v. 2, n. 1, p. 53-70, jan. 2010. IGI Global. http://dx.doi.org/10.4018/japuc.2010010104.

TAN, Zixiang Alex; MUELLER, Milton; FOSTER, Will. *China's new Internet regulations: two steps forward, one step back.* **Communications of the ACM***, 40(12), 11–16.* doi:10.1145/265563.265565

TANEJA, Harsh; WU, Angela Xiao. Does the Great Firewall Really Isolate the Chinese? Integrating Access Blockage With Cultural Factors to Explain Web User Behavior,. **The Information Society**, [*s. l*], v. 5, n. 30, p. 297-309, jan. 2014.

TAUBMAN, Geoffry. A Not-So World Wide Web: The Internet, China, and the Challenges to Nondemocratic Rule. **Political Communication**, __, v. 2, n. 15, p. 255-272, jan. 1998

TERHOCH, Nadjine. **O Que é e Para que Serve um Endereço de IP?** - Blog. Blog GoDaddy Brasil. Disponível em: <https://br.godaddy.com/blog/o-que-e-e-para-que-serve-um-endereco-de-ip/>. Acesso em: 2 Dec. 2020.

THOMPSON, Clive. Google's China Problem: (and china's google problem. **Nwe York Times**, [*s. l*], v. -, n. -, p. 1-7, abr. 2006.

TRIGO, Virgínia. Os Empreendedores Chineses e o Processo de Transformação Económica na China. Cadernos de Estudos Africanos, [S.L.], n. 11/12, p. 153-174, 1 jun. 2007. OpenEdition. http://dx.doi.org/10.4000/cea.941.

WAGNER, Christian. From Hard Power to Soft Power?:ideas, interaction, institutions, andimages in india⁚⁚ssouthasiapolicy. **Heidelberg Papers In South AsianAndComparativePolitics**, Heidelberg, v. 1, n. 1, p. 1-17, mar. 2005. Disponível em: http://archiv.ub.uni-heidelberg.de/volltextserver/5436/1/hpsacp26.pdf. Acesso em: 25 nov. 2020.

WALTZ, Kenneth N.. **O Homem, o Estado e a Guerra**: uma análise teórica. São Paulo: Martins Fontes, 2004. 124 p.

WORTZEL, Larry M. **THE CHINESE PEOPLE'S LIBERATION ARMY AND INFORMATION WARFARE**. Strategic Studies Institute and U.S. Army War College Press. Mar. 2014

WU, Chris. An Overview of the Research and Development of Information Warfare in China. **Cyberwar, Netwar And The Revolution In Military Affairs.** __, p. 173-195. maio 2006.

WU, Tim. Etwork Neutrality, Broadband Discrimination. **Technology Law**, __, v. 2, n. -, p. 1-43, jan. 2003.

WÜBBEKE, Jost. **Made in China 2025**: the making of a high-tech superpower and consequences for industrial countries. __: Merics, 2016. 75 p.

WUTHNOW, Joel; SAUNDERS, Phillip C.. Chinese Military Reforms in the Age of Xi Jinping: Drivers, Challenges, and Implications. **Center For The Study Of Chinese Military Affairs Institute For National Strategic Studies National Defense University.** __, p. 1-98. out. 2013.

YEO, Shin Joung. Geopolitics of search: Google versus China? **University London, Uk Media, Culture & Society**, [*s. l*], v. 4, n. 38, p. 591-605, jan. 2016.

互联网论坛社区服务管理规定. China Law Translate. Disponível em: <https://www.chinalawtranslate.com/en/provisions-on-the-management-of-internet-forum-community-services/>. Acesso em: 26 Apr. 2021.

谱写网信事业新篇章-中共中央网络安全和信息化委员会办公室. Cac.gov.cn. Disponível em: <http://www.cac.gov.cn/2017-04/14/c_1120802183.htm>. Acesso em: 18 Apr. 2021.