ANAIS

III SIMPÓSIO

DE DEFESA E CIÊNCIA POLÍTICA

DA UNIVERSIDADE FEDERAL DE PERNAMBUCO

redectidc
.com.br

ANAIS

III Simpósio de Defesa e Ciência Política da Universidade Federal de Pernambuco

NATÁLIA DINIZ SCHWETHER

Organizadora

Recife

2021

UNIVERSIDADE FEDERAL DE PERNAMBUCO

Reitor Alfredo Macedo Gomes

Vice-Reitor Moacyr Cunha de Araújo Filho

Centro de Filosofia e Ciências Humanas

Diretora Maria da Conceição Lafaytte de Almeida

Vice-Diretor Ricardo Pinto de Medeiros

Núcleo de Estudos Americanos

Coordenador Marcos Aurélio Guedes de Oliveira (UFPE)

Rede CTIDC

Coordenador-Geral Marcos Aurélio Guedes de Oliveira (UFPE)

Coordenador-Regional Gills-Vilar Lopes (UNIFA)

Coordenadora-Regional Graciela de Conti Pagliari (UFSC)

Coordenador-Regional Luiz Rogério Franco Goldoni (ECEME)

Coordenador-Regional Pedro Linhares (UNIFA)

Coordenador-Regional Ricardo Borges Gama Neto (UFPE)

Comitê Científico do III Simpósio de Defesa e Ciência Política

Natália Diniz Schwether (coordenadora) – PPGCP/UFPE

Thays Felipe David de Oliveira – PPGCP/UFPE

Flávia Lessa

Luciana Belo Guedes

Pierre dos Santos

Simpósio de Defesa e Ciência Política da Universidade Federal de Pernambuco (3.: 2021 jul. 08 e 09 : Recife, PE).
Anais do III Simpósio de Defesa e Ciência Política da Universidade Federal de Pernambuco [recurso eletrônico] / organizadora : Natália Diniz Schwether.

Tema: "Ciberdefesa, cibersegurança e os novos desafios ao sistema internacional"
Inclui referências.
ISBN (online)

1. Ciência Política – Congressos. 2. Segurança nacional – Congressos. 3. Relações internacionais. 4. Cibernética – Medidas de segurança. I. Schwether, Natália Diniz (Org.). II. Universidade Federal de Pernambuco. III. Título.

SUMÁRIO

APRESENTAÇÃO

O III Simpósio de Defesa e Ciência Política da Universidade Federal de Pernambuco realizou-se nos dias 05 a 09 de julho de 2021, de modo remoto, com o auxílio de plataformas para videoconferência e a gravação de vídeos disponibilizados em nossas páginas *on-line*, com o tema: "Ciberdefesa, cibersegurança e os novos desafios ao sistema internacional".

O evento foi promovido pela *REDE Ciência, Tecnologia e Inovação em Defesa Cibernética* (REDE CTIDC) formada por pesquisadores dos temas de segurança e defesa cibernética de instituições civis e militares de diversas regiões do país, selecionados pelo Programa de Apoio ao Ensino e à Pesquisa Científica em Defesa Nacional – Pró Defesa IV, projeto apoiado pelo Ministério da Defesa e pela Coordenação de Aperfeiçoamento de Pessoal do Ensino Superior (CAPES).

A programação acadêmica do III Simpósio contou com cinco grandes seções – apresentação de trabalhos acadêmicos, apresentação de artigos publicados, documentários temáticos, depoimentos de parceiros e lançamentos –, nas quais participaram professores universitários, pesquisadores, coordenadores de centros de pesquisa, alunos de graduação e pós-graduação e militares de vários estados do Brasil.

O documentário "A Defesa Cibernética do Brasil" organizado pelo Prof. Dr. Gills Villar Lopes e convidados foi um dos vídeos com maior audiência e segue disponível em nossas páginas. Para além disso, foram realizados dois importantes lançamentos, o dossiê sobre Defesa Cibernética da Revista Brasileira de Estudos de Defesa e o número especial sobre Defesa e Segurança na Revista Política, ambas as edições contam com diversas publicações de nossos pesquisadores. Os artigos tratam de diferentes temáticas, com especial ênfase para a defesa e a segurança cibernética e foram brevemente comentados pelos autores em vídeos, também, acessíveis *on-line.*

Outrossim, foram apresentados doze trabalhos acadêmicos, tais comunicações foram reunidas e agrupadas em duas seções: 1. Trabalhos Completos e 2. Resumo Expandido para essa publicação.

A organizadora.

1. Trabalho Completo

GOVERNANÇA INTERNACIONAL NO MUNDO CIBERNÉTICO: Desafios para a defesa e segurança cibernética.

Georgia Maria Vasconcelos Pfeilsticker Ribas

Lucas Soares Portela

As primeiras fases da criação do que hoje chamamos de internet começou em 1960 no Estados Unidos da América, especificamente no Instituto de Tecnologia de Massachusetts (MIT) (KNIGHT, 2014). Os pesquisadores do MIT procuraram desenvolver uma espécie de comunicação através de "pacotes" entre alguns computadores. O conceito de computadores em redes conectados por roteamento de pacotes em vez de comutação por circuitos foi desenvolvido por Joseph Carl Robnett Licklider, do MIT, em agosto de 1962 (KNIGHT, 2014).

Por meio dessa criação e desenvolvimento dos pacotes, seria possível identificar a origem do dado até o ponto de chegada, permitindo o envio da informação de um local a outro. Naquela época, Licklider era o primeiro gerente do programa de pesquisa de computação da Defense Advanced Research Projects Agency (DARPA), conhecido atualmente como ARPA (KNIGHT, 2014).

Um segundo pioneiro, mas não menos importante para o desenvolvimento da internet, foi Paul Baran, que trabalhou como pesquisador financiado pela Força Aérea Americana na RAND Corporation na Califórnia (KNIGHT, 2014). Seu trabalho consistia em desenvolver um sistema que garantisse a resiliência da Força Aérea Americana após um ataque nuclear. A pesquisa de Baran consistia em criar uma comunicação descentralizado que em tese permitiria os militares de manter o comando e controles de aeronaves junto a mísseis nucleares mesmo depois de um ataque nuclear. Também considerado como um país da internet, Vincent Cerf que hoje é Vice- Presidente da Google explica o papel de Baran:

> Baran articulou a utilidade de empacotamento, embora tenha chamado as unidades como "Blocos de mensagem", seu sistema nunca foi construído. No entanto seu trabalho foi notado pelos especialistas de desenharam a ARPANET depois da conclusão do seu desenho básico. Enquanto eu estava dirigindo o programa da Internet tive como objetivo torná-la resistente a um ataque nuclear e, além disso, demonstrou sua capacidade de autorecuperação em cooperação com o Comando Aéreo Estratégico, utilizando rádios aéreos de comunicação por pacotes. Então, as ideias de Baran encontraram terra fértil na Internet, ainda que não na ARPANET. (KNIGHT, 2014, p. 18).

A comunicação por pacotes possibilitou a criação da ARPANET, através de pesquisas do Departamento de Defesa dos EUA. Tornando-se operacional em 1969, quando quatro computadores foram conectados. Esse projeto não foi criado para uso militar, mas sim para compartilhar recursos de comunicação entre universidades com o apoio de pesquisas do Pentágono. Eram elas a Universidade da Califórnia em Los Angeles, através de seu centro do desenvolvimento do "software"; o Stanford Research Institute; a Universidade da Califórnia em Santa Bárbara e a Universidade de Utah, todos beneficiários de contratos com a ARPA (KNIGHT, 2014).

Em seguida houve a criação do TPC/IP que viabilizou a arquitetura aberta de comunicações em rede, permitindo assim a interconexão entre rede de computadores onde quer que estejam localizados. Novas pesquisas para o pentágono conseguiram estender o conceito de pacotes de redes para rádio terrestre e satélite, que acabaram sendo interconectadas a ARPANET (KNIGHT, 2014).

Depois de 1980, a Internet começou a se disseminar em um ritmo muito alto; conectando redes locais, microcomputadores e estações de trabalho. Em 1986, a ARPANET foi conectada a uma nova rede acadêmica a National Science Foundation Network - NSFNET, assim desativando a ARPANET em 1990.

Já na Europa, outro grande avanço aconteceu, na Organização Europeia para Pesquisas Nucleares (CERN). Em 1089, Tim Berners-Lee, físico e cientista da computação, propôs o uso de hipertextos de uma forma distribuída, que basicamente seria um conjunto de documentos armazenados em locais distintos interligados entre si por meio de pontos não hierárquicos que estão vinculados uns aos outros (KNIGHT, 2014). Esses então documentos poderiam ser resgatados usando uma plataforma de navegação; o que possibilitaria o uso em massa da internet. Dessa forma Berners-Lee inventou e implementou a internet com o conceito de hipertexto, que hoje conhecemos com World Wide Web.

Outra criação que contribuiu para o que conhecemos como espaço cibernético hoje foi o sistema binário. A codificação das letras do alfabeto em uma sequência de dígitos binários foi devidamente aperfeiçoada pelo filósofo inglês Francis Bacon, em 1605. Segundo Bacon, qualquer "objeto" poderia ser codificado. Após meio século, o filósofo alemão Gottfried Leibniz criou o sistema binário a partir de numerais , como conhecemos hoje.

A partir de códigos criados através do sistema binário, os computadores realizam o processamento de dados, sendo que cada numeral, representa um bit . Sem eles não seria possível fazer a leitura das informações enviadas.

Após o advento das diferentes redes, surgiu um novo tipo de conflito, a "Guerra de Protocolos" (KNIGHT, 2014). Essa disputa surgiu entre o desenvolvimento da comunicação baseada no TCP/IP. Com parcerias internacionais cada vez mais frequentes e com o surgimento de novas políticas industriais e tecnológicas houve a necessidade da criação de uma única linguagem para que todos os envolvidos pudessem interpretar e entender as informações utilizadas.

Assim foi criado o chamado Hypertext Markup Language (HTML), um tipo de código básico utilizado para a viabilização da comunicação na Internet. Em 1993, houve um grande avanço tecnológico com a introdução de um dos primeiros navegadores gráficos que possuía uma ampla divulgação chamado de "Mosaic", que foi desenvolvido pelo National Center for supercomputing Applications (NCSA) da Universidade de Illinois nos Estados Unidos. Aquele momento abria a Internet ao público em geral.

Existiu também a formação do Hypertext Transfer Protocol (HTTP), o protocolo primordial que estabelece conexões de internet em todo o mundo. Esse aperfeiçoamento também permitiu a origem do primeiro navegador de internet, o WorldWideWeb (WWW), em 1990. Embora as grandes inovações tenham acontecido principalmente nos Estados Unidos, cada região do globo apresenta sua própria história de integração e territorialização do espaço cibernético, inclusive no Brasil.

Segurança Multidimensional E A Governança No Espaço Cibernético

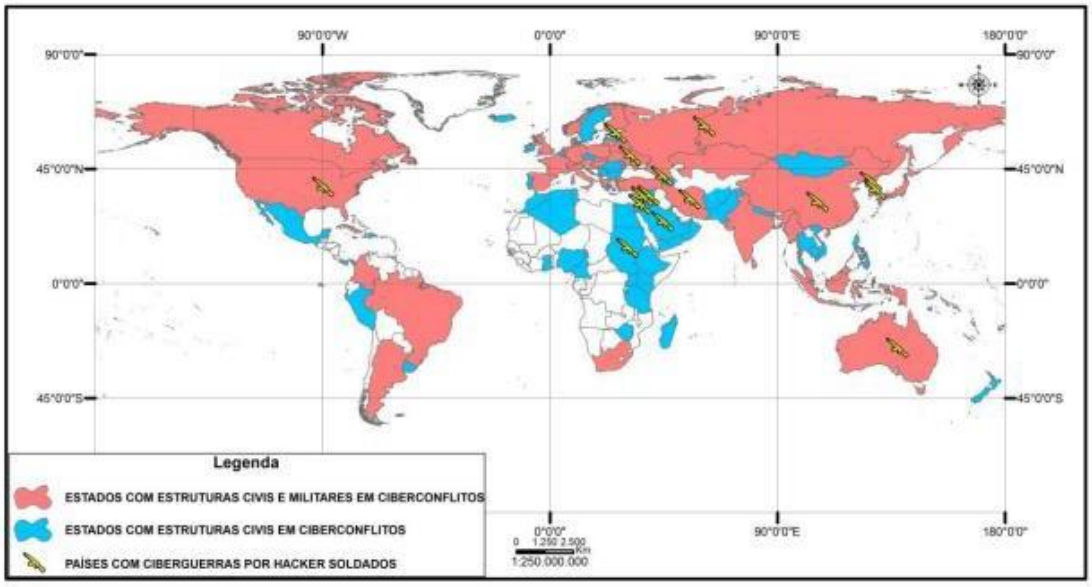
O conceito de Segurança Multidimensional foi definitivamente estabelecido na Conferência Especial sobre Segurança realizada na Cidade do México em 2003. Durante a conferência, o conceito de Segurança Multidimensional ajudou a entender como essa nova modalidade de guerra, como a ciberguerra, tem ganhado projeção entre os Estados. O espaço cibernético é um teatro de guerra caracterizado pela (in)segurança multidimensional, uma vez que ela possui tanto um caráter de ameaça tradicional interestatal quanto de nova ameaça. (RAMOS ,2015). Tendo em vista, que com a intensificação da globalização, não só os Estados e Organizações Internacionais tornam-se alvos, mas também os próprios indivíduos e empresas; A ciberguerra trata-se de uma questão de insegurança do sistema mundial como um todo.

A perspectiva de segurança multidimensional obtém relevância à medida que elucida porque a segurança cibernética antes de ser puramente e exclusivamente de uma ótica internacionalista, passa a ser então visualizada dentro de uma agenda multidimensional, com reverberação em agendas securitárias tênues de natureza civil e militar. (DAVID, 2001).

O grande dilema da segurança é que ele possui multidimensão, trazendo junto a ele uma diversidade de arenas e atores com fronteiras nem sempre convergentes. Percebe-se esse dilema em dois pontos, o primeiro sendo a indefinição de fronteiras dentro do espaço cibernético, separando o nacional do internacional, e o segundo sendo a indefinição de quais estruturas estatais atuariam no espaço cibernético, se seria as estruturas civis, de segurança pública, ou as estruturas militares, de defesa.

Com base na análise de cyber conflitos, na identificação e categorização de sua natureza e stakeholders envolvidos, mostra-se a possibilidade de uma apreensão da espacialização dos campos de poder dos ciber conflitos, de uma forma, a mostrar, tanto as forças descentralizadas dos ataques cibernéticos, quanto as forças centralizadas, dos meios civis e militares, conforme podemos vislumbrar:

Figura 1. Estruturas Civis e Militares da ciberguerra



Fonte: SENHORAS,2014.

A existência de estruturas civis e militares com ações realizadas principalmente por hackers soldados como observado nos Estados Unidos, Rússia, China, Coréia do Sul,

Coréia do Norte, Austrália, Estônia, Geórgia, Ucrânia, entre outros países gera ainda mais instabilidade no sistema internacional, pois dessa forma torna-se mais difícil o Estado ter controle sobre os ataques cibernéticos.

Há um regime de governança da Internet no plano internacional que vem sendo moldado nas quatro últimas décadas. Esse evolui conforme interesses de atores que, em contexto de competição tecnológica global, apresentam um diferencial de poder oriundo do conhecimento de que dispõem sobre novos padrões tecnológicos e de sua capacidade relativa de acompanhar e influir na própria evolução de tais padrões.

Por exemplo, o uso da língua inglesa como o padrão adotado para endereçamento dos sítios eletrônicos em escala global constituiria fator a preservar as vantagens iniciais dos Estados Unidos como "first movers" (CRUZ, 2006, p. 21). Esse tipo de diferencial habilitaria alguns atores a compreender melhor as implicações políticas e econômicas resultantes do regime em formação e, consequentemente, influir na definição das regras e na escolha dos padrões globalmente aplicáveis.

No intuito de delimitar a governança da Internet, faz-se necessário dar atenção ao significado e à extensão do termo governança e aos motivos do seu uso para designar o conjunto de mecanismos relacionados à gestão da Internet no plano global.

James Rosenau (2000) faz distinção entre governança e governo. Afirma que governo sugere um conjunto de atividades sustentadas por autoridade formal e poder de implementar decisões tomadas em determinado contexto político-institucional. Governança, por sua vez, estaria relacionada a atividades apoiadas em objetivos comuns, que podem ou não derivar de responsabilidades formais, porém não dependem do exercício de poder coercitivo para serem aceitas. Nessa perspectiva, o conceito de governança englobaria o de governo, mas a ele não se limitaria, abrangendo também um conjunto de decisões tomadas por atores não governamentais, aceitas e tacitamente seguidas pela maioria.

No contexto da difusão de poder numa economia globalizada, a emergência de novos atores internacionais, tais como empresas transnacionais e entidades não governamentais de atuação global, tenderia a limitar o exercício da soberania estatal. Essa diluição de poder não daria vazão, pelo menos em horizonte previsível, ao surgimento de governo global (STRANGE, 1996, p. 184), tendo em conta a resistência dos Estados nacionais em renunciar ao controle sobre três processos essenciais: o monopólio do uso da força, o poder de coletar tributos e a exclusividade em determinar o que é lícito e o que é criminoso.

Entretanto, quando falamos de espaço cibernético, esses processos essenciais não são puramente de controle do Estado. Embora esses atores continuem dominando o uso da força, os protocolos e tecnologias empreendidas no espaço cibernético dependem, em grande escala, da existência de uma constelação de empresas e grandes players do setor privado. Isso também é vislumbrado quando da coleta de tributos, que embora destinado para o Estado, perpassa pela cobrança pelo fornecimento de serviços dos grandes provedores de Internet.

Dessa forma, enquanto na geopolítica clássica, a governança é exclusiva dos Estados, no espaço cibernético o que observamos é uma governança de coexistência. Nesse ambiente, os processos tradicionais da geopolítica do poder, como securitização, defesa, segurança também são inseridos dentro da dinâmica empresarial. Nesse caso, devemos repensar cada um desses conceitos, como por exemplo, tratar dinâmicas securitária no lugar de securitização, segurança da informação invés de segurança pública, ou seja, repensar a governança do espaço cibernético dentro de um olhar teórico progressista.

Desafios Para A Defesa E Segurança Cibernética

Tanto no mundo, quanto no Brasil, há muitas instituições que lidam com a segurança e defesa cibernética, por esse motivo, a abordagem utilizada por elas, muitas vezes, transpassa a característica técnico-operacional, o que acaba refletindo no nível político e jurídico dos Estados. Essa diversificação criou uma série de desafios e oportunidades para cooperação e coordenação no meio cibernético.

Cabe ressaltar que a segurança cibernética se distingue do conceito de defesa cibernética em alguns países, como o próprio Brasil. O primeiro conceito está associado às mesmas fronteiras da segurança pública tradicional (MEDEIROS FILHO, 2014). Enquanto o segundo termo, conforme Oscar Medeiros Filho (2014) está vinculada às questões de guerra. Assim, conforme Oscar, as delimitações da segurança e defesa cibernética está vinculado com a ameaça que se debate.

Ainda sobre esses dois conceitos, há pelo menos quatro desafios que merecem destaque (LOBATO, 2018): (i) o risco de excessiva securitização e de uma acentuada militarização da segurança cibernética; (ii) o risco de exclusão de atores não-estatais da governança da segurança cibernética, desde a definição de prioridades até a elaboração e implementação de políticas; (iii) a preferência, cada vez maior, por soluções que buscam

o bloqueio de aplicações, remoção de conteúdo e criminalização de comportamentos na Internet; e (iv) problemas de coordenação e a transferência de tecnologia.

Os riscos da securitização e militarização é fruto de "megaeventos" no Brasil, a criação de órgãos especializados vinculados às forças armadas evidencia o esforço para lidar questões de segurança cibernética a partir da aplicação das competências de órgãos de aparato militar e de Inteligência do Estado. Esses esforços resultaram em uma maior alocação de recursos para combater ameaças, Terrorismo, Guerra cibernética e a Sabotagem industrial.

A ausência de canais para inclusão de atores não-estatais no processo de elaboração de políticas também resulta de processos de securitização e militarização, que acabam retirando da esfera do debate público determinados assuntos avaliados como estratégicos para o país.

Com isso, o processo de elaboração de políticas sobre o tema se torna mais restrito aos órgãos de segurança e inteligência. O tratamento e resposta a ameaças por meio de uma lógica de securitização, reacende o trade-off normativo entre a segurança e o respeito a liberdades e direitos fundamentais, colocando-os em polos opostos, ao invés de encará-los como princípios que devem caminhar conjuntamente no processo de elaboração de políticas para a segurança cibernética.

Diante desse contexto, representantes da academia e a sociedade civil chamaram a atenção para a importância da inclusão do multissetorial às diretrizes, a estruturação de órgãos pertencentes ao regime nacional de segurança cibernética, e para o processo de elaboração de políticas para o setor. (LOBATO, 2018).

Notou-se, também, uma tendência a responder aos desafios de segurança pelas vias do bloqueio, remoção de conteúdo e criminalização. A aprovação de leis que autoriza o bloqueio de aplicativos e websites, além da tentativa de criminalizar uma série de condutas, crimes autorais e o acesso indevido a computadores e sistemas, foram motivadas pela dificuldade e/ou imparcialidade de acessar dados criptografados de redes sociais e aplicativos de mensagens. Essas categorias de episódios contribuíram para elevar a tensão entre, de um lado, a abordagem com foco na criminalização de condutas e, do outro, aquelas com foco na proteção de direitos e garantias legais na internet.

Os desafios da coordenação são evidentes no âmbito da administração pública brasileira, em virtude da escassez de mecanismos que são efetivos de governança da segurança da informação e comunicação, somando a isso, encontra-se a dificuldade dos atores no meio internacional de "transferir conhecimento e tecnologia" uns para os outros,

onde no cenário em que vivemos é algo improvável de se acontecer, pelo simples fato de que esse ato de transferência possa abalar a estratégia e defesa de um país em relação a uma nação “amiga” ou não.

Conclusão

A internet e o espaço cibernético podem ser apresentado como um fenômeno tecnológico, que embora seja constituída como uma ferramenta pode apresentar atualmente um processo de construção de um regime global da governança da Internet. Essa surgiu nos Estados Unidos, no final dos anos 60, mas atualmente apresenta uma estrutura mais ampla e complexa, que abarca toda a dinâmica social do mundo, e consequentemente também das relações internacionais. A existência de acordos, tratados e estruturas internacionais comprova a existência desse regime global.

A criação dessa ferramenta acompanhou também a evolução política e os movimentos do poder nas relações internacionais. Isso impactou também na forma em que a internet passou a ser usada no mundo. Sendo criada dentro de instituições civis de caráter científico, suas engrenagens também foram aplicadas no contexto da segurança internacional, não no sentido estrito, mas na amplitude do que é a disputa de poder no mundo. Assim, ficou patente depois dessa pesquisa, que o espaço cibernético floresceu no contexto das estruturas hegemônicas de poder ao final do século XX.

Embora tenha sido notado um movimento em prol do que se chamou de governança global da Internet, não há tratado nem Organizações Internacionais que forneça uma base ou referência institucional definida para o regime de gestão da Internet. Logo, esse regime resulta da ação de governos, do setor privado, da sociedade civil e de organizações internacionais, de comunidades técnicas e principalmente dos usuários, sempre em um processo de interação ininterrupta que delineia a evolução e o uso da internet em todo o mundo, e que podemos melhor caracterizá-lo usando o termo “governança”.

A soma das interações dos mais diversos entes que contribuíram para o nascimento da internet tem contribuído para mantê-la em contínuo funcionamento. A pauta da Governança da Internet, contempla recorte histórico de surgimento e evolução da tecnologia e confirma a sua existência, que tende a afastar-se da concepção clássica multilateral com base em Organizações internacionais integradas por governos/Estados. Afinal, a concentração de poder nesse ambiente, somado com a difusão de poder para

atores não estatais, demanda uma configuração distinta de governança, que nesse caso, surgiu de forma natural.

Por mais que não possa ser compreendido como uma estrutura clássica, a governança da Internet pode ser enquadrada dentro de um espectro teórico. Por exemplo, no que se refere a autoridade formal, embora essa seja ausente ou inexistência, há princípios, normas, regras e processos decisórios específicos de um regime clássico, que nesse aspecto se mostra efetivo e vigoroso. Ainda assim, tentativas de criação de instâncias decisórias intergovernamental para o regime no meio cibernético chegaram a ser suscitadas em maior nível político. Entretanto, não houve alterações substanciais ao modelo vigente atualmente.

Assim, apesar de já considerarmos a existência de uma governança global, o regime internacional para a Internet continua em plena construção. Essa realidade impõe a diplomacia um desafio de adaptação em torno do regime vigente, tanto para identificar, sugerir e avançar pautas e temas de interesse nacional, quanto para influir na evolução institucional desse regime.

Por fim, a atual fase das relações internacionais é singular não somente por causa das mudanças sistêmicas, provocadas pelo processo de transformação na distribuição do poder mundial, mas principalmente pela aceleração e ampliação da interconectividade das sociedades e entre diferentes sociedades. São estabelecidas um conjunto de novas tecnologias digitais que pendem à universalização o que simultaneamente intensificam, importantes mudanças no padrão de interação social e, portanto, alterando a forma como as relações de poder são estabelecidas.

Referências

KNIGHT, Peter T. A Internet no Brasil: Origens, Estratégia, Desenvolvimento e Governança. Indiana: AuthorHouse, 2014.

LOBATO, Cruz Luiza. Uma Estratégia para a Governança da Segurança Cibernética no Brasil. Série: Segurança Cibernética e Liberdades digitais. Instituto Igarapé. Setembro 2018.

MEDEIROS FILHO, Oscar. “Em busca de ordem cibernética internacional”. In Segurança e Defesa Cibernética: da fronteira física aos muros virtuais, organized by Oscar Medeiros Filho, Walfredo B. Ferreira Neto and Selma Lúcia de Moura Gonzalez. Coleção I - Defesa e Fronteiras Cibernéticas Pernambuco: Editora UFPE, 2014.

SENHORAS, E. M. Mapas de ciber conflitos no mundo: relatório de pesquisa organizado para Congresso Acadêmico de Defesa Nacional. Boa Vista: UFRR, 2014.

SEGURANÇA CIBERNÉTICA INTERNACIONAL: O Terrorismo e a Internet das Coisas

Eduarda Maciel Travassos
Lucas Soares Portela

Greg Rattray (DENMARK E KAPLAN, 2010) menciona que o ciberespaço é fundamentalmente um ambiente físico, criado pela conexão de sistemas físicos e redes, e gerenciados por regras definidas em protocolos de software e comunicações - todos localizados nos limites soberanos de estados-nações, e que, embora muitas das informações no ciberespaço sejam consideradas públicas, os elementos físicos do ciberespaço - os desktops, os laptops, os servidores, as geladeiras habilitadas para Internet, os roteadores, os telefones, os celulares, cabos de LAN, cabos de fibra ótica - têm proprietários claros. A integração de componentes físicos de infraestrutura cibernética localizada dentro de um estado territorial para o "domínio global" do ciberespaço não pode ser interpretada como uma renúncia do exercício da soberania territorial. Os Estados têm enfatizado continuamente seu direito no ciberespaço, incluindo aqueles para exercer controle sobre a infraestrutura cibernética localizados em áreas de seu território soberano, para fazer valer sua jurisdição sobre atividades em seu território e para proteger sua infraestrutura cibernética contra interferência transfronteiriça por outros Estados ou por indivíduos. Na verdade, os Estados têm exercido, e continuarão a exercer, sua jurisdição sobre crimes cibernéticos e continuarão, também, a regular as atividades no ciberespaço, pois tal controle faz parte da natureza da soberania estatal. O significado jurídico do conceito de soberania moderna está contido na Carta das Nações Unidas de 1945, porém, para que o conceito seja aplicado no espaço cibernético é preciso, primeiramente, que os países entrem em um consenso sobre como e quais normas seriam aplicadas a essa realidade. Um exemplo de divergência de jurisprudências seria o caso do Brasil e Estados Unidos, enquanto em 2014 com a lei 12.965 - o Marco Civil da Internet - o Brasil garante a neutralidade da Internet no inciso IV do 3º artigo da referida lei, os Estados Unidos já não garantem a neutralidade da rede, permitindo que empresas privadas estipulem a distribuição de dados aos seus clientes (VALENTE, 2017).

Uma vantagem da discussão ordenada desta forma é deixar claro os seguintes fatos: a igualdade internacional de soberania nacional é igualdade de diferentes níveis, ao invés de igualdade absoluta ou igualdade real; a utilização prática da soberania nacional depende mais da história da geopolítica, o ponto de vista da ordem mundial e a

constitucionalidade interna e externa de cada país. Em 1999 Tim Jordan, elaborou sistematicamente, pela primeira vez, o conceito de ciberpoder a partir das perspectivas da política e da sociologia: ciberpoder é a forma de poder da política e da cultura no ciberespaço e na Internet. O poder cibernético depende de uma série de recursos relacionados à eletrônicos e computadores utilizados para a criação de informações, controle e comunicação, incluindo infraestrutura de hardware, rede, software e habilidades humanas; quer sejam exageros, quer sejam realmente preocupantes, as ameaças cibernéticas alcançaram uma projeção indiscutível no pensamento de segurança no pós-Guerra Fria, particularmente entre os analistas e os formuladores de políticas de segurança e defesa. Enquanto as forças armadas convencionais e os orçamentos militares diminuíram com o fim da Guerra Fria, a nova ênfase dada na segurança da informação e nas ameaças cibernéticas foi uma exceção notável. Independentemente da perspectiva teórica, há uma lacuna óbvia a ser preenchida nos estudos de segurança: de abordar o impacto da revolução da informação para o entendimento geral da segurança no mundo contemporâneo, assim como para explicar a variação nas relações e políticas de segurança pelo mundo afora. Os realistas, presumivelmente, combateriam o desafio da revolução da informação da mesma forma como enfrentaram desafios anteriores, isto é, a transnacionalização, a interdependência complexa e a globalização. Assim, para essa corrente teórica, essas tendências são vistas como fenômenos secundários, que podem afetar as políticas e as estruturas domésticas dos Estados, mas que não enfraquecem o sistema anárquico da política internacional, e assim não afetam a primazia do Estado como a unidade política suprema. Os realistas podem considerar as ameaças de segurança relacionadas à tecnologia da informação como sendo uma questão econômica, não necessariamente afetando a segurança dos Estados e não sendo elas uma ameaça à segurança. Por sua vez, os construtivistas em Relações Internacionais, e nas Ciências Sociais como um todo, enfatizam a inevitabilidade da interpretação e, assim, a distorção da realidade, especialmente no que diz respeito à compreensão das atividades social e política. Diferentemente do realismo e do liberalismo, o construtivismo não busca uma teoria universal, mas sim generalizações condicionais, quer dizer, os construtivistas dão algumas orientações sobre o que as teorias de Relações Internacionais devem atentar. A securitização implica na identificação de uma "ameaça existencial", evidenciado por meio do ato da fala, que prioriza a questão na agenda política, legitimando medidas extraordinárias como confidencialidade, uso da força e a invasão da privacidade. A análise construtivista do poder e da segurança no mundo virtual implica enfatizar o

significado das imagens e dos símbolos em adição à realidade material dos computadores e cabos. O estudo da política simbólica, isto é, o uso e abuso de símbolos para manipular o discurso político e a opinião pública, é bastante relevante para estudar a segurança na idade digital.

Adentrando o lado prático do espaço cibernético e suas ameaças, Tong Zhang explica que muitos programas de software, como servidores da web, bancos de dados e sistemas operacionais, são frequentemente desenvolvidos usando linguagens de programação C/C++, que permitem manipulações arbitrárias de ponteiro e acessos de memória não gerenciados. Uma violação de segurança de memória espacial ocorre quando um programa acessa uma região de memória além do limite designado do objeto, conhecido como estouro de buffer, que consiste em um transbordamento de dados. Por meio dessas brechas, os cibercriminosos conseguem executar códigos maliciosos nos computadores e dispositivos da rede, o que pode levar à substituição de outro objeto ilegalmente ou à leitura de dados potencialmente confidenciais sem permissão. Cabe ressaltar também, que algumas programações são construídas com vulnerabilidade intencionais, utilizadas por diversos fins, algumas vezes para permitir uma intervenção do próprio programador em prol do programa, ou em outras por má fé, de forma a gerar defeitos no produto a ponto de ser requisitado um suporte técnico. Tratam-se, portanto, de atores estatais e não-estatais como espiões, hackers, criminosos e terroristas cibernéticos que atuam em esquemas altamente organizados, capazes de orquestrar ataques sofisticados sem que sua presença seja notada até que a ação tenha ocorrido e os danos causados.

Não é só uma questão de controle da máquina ou de informação, que por si só é por vezes ignorada pelo senso comum como um recurso de poder, mas também uma real ameaça a condição física do usuário. Exemplo dessa interação entre vulnerabilidades cibernéticas e ameaças físicas foi o ataque de 2017 ao hotel austríaco Romantik Seehotel Jaegerwirt, que teve seu sistema de fechaduras dos quartos e saguão hackeado, sequestrando todos os hóspedes e requerendo pagamento em moeda virtual para liberação (DEMARTINI, 2017). No que tange a segurança cibernética, nas últimas duas décadas a China, os Estados Unidos e a Rússia propuseram medidas substantivas como o aprimoramento das capacidades dos órgãos de comando e controle, o aumento do poder de serviços de inteligência, e a criação de novas divisões especializadas em segurança e defesa cibernética para conter esse tipo de ameaça. Os ciberataques estatais incluem ciberespionagem, guerra cibernética, interferência em eleições, campanhas de

desinformação, conhecidas como fake news, phishing, negação de serviço, malware, roubo de informações e outros tipos de interferências em governos, setores privados e civis. Stuxnet foi um ataque significativo porque mudou o cenário cibernético no que diz respeito aos atores do estado com o primeiro ataque direcionado como arma a um sistema que até então parecia estar isolado de ataques cibernéticos. Binxing Fang ainda observa que o ataque de 2017 "marcou a mudança em direção ao uso de nível militar armas, ferramentas de hacking que são poderosas o suficiente para uma agência nacional de defesa cibernética usar na ciberguerra internacional" (FANG, 2018 p.97). Turla é um grupo de ciberespionagem patrocinado pela Rússia que realiza campanhas contra instituições governamentais usando táticas criadas internamente, bem como táticas de exploração de código aberto em suas operações.

O FBI define o terrorismo internacional como "atos violentos e criminosos cometidos por indivíduos e/ou grupos que são inspirados por, ou associados a, designados estrangeiros organizações ou nações terroristas" e terrorismo doméstico como atos semelhantes para "promover objetivos ideológicos decorrentes de influências domésticas, como as de caráter político, religioso, natureza social, racial ou ambiental." Para os fins deste trabalho, a categorização não-estatais será alinhada com o National Intelligence Council, Journal of Military Science e FBI, que incluem hackers, hacktivistas, terroristas, cibercriminosos e organizações relacionadas, que agem de acordo com sua própria agenda e ideologias sem qualquer laço ou apoio de estados (JOSSELIN, WALLACE, 2001).

A Divisão Cibernética do FBI é a agência federal dos EUA líder na investigação de ataques cibernéticos e intrusões em redes governamentais e privadas por atores não estatais, como organizações criminosas, terroristas e outros adversários cibernéticos. Os simpatizantes de terroristas apelidaram o ato de "CyberCaliphate" e acessaram Servidores comerciais do CENTCOM por aproximadamente 30 minutos, postando uma foto de um lutador do ISIS com as palavras, "I love you isis" e "AMERICAN SOLDIERS, WE ARE COMING, WATCH YOUR BACK" (AWAN, 2017). O Departamento de Justiça dos EUA anunciou em dezembro de 2016 que sua Divisão Cibernética, juntamente com a Divisão Criminal do FBI, Western District of Pennsylvania U.S. Attorney's Office, Ministério Público da Alemanha e polícia local, Europol, investigadores e promotores de mais de 40 jurisdições globais, e várias outras entidades fizeram parceria para desmantelar uma infraestrutura criminosa — Avalanche — por meio de uma operação multinacional que resultou em prisões em quatro países. Era uma rede cibercriminosa, acessada através de fóruns on-line clandestinos, que forneciam uma infraestrutura segura para campanhas

e transações criminosas, como malware, esquemas de “mula de dinheiro”, lavagem de dinheiro fora do alcance da aplicação da lei (FANG, 2018). Desde 2010, quando o Avalanche se tornou operacional, a rede redirecionou, diariamente, dados financeiros e informações roubadas de até 500.000 computadores infectados pelo malware, causando em todo o mundo perdas monetárias estimadas em centenas de milhões de dólares. Em um nível técnico, arquiteturas de rede - uma malha flexível que pode redirecionar o tráfego a qualquer momento através de qualquer nó - parecia diametralmente oposto ao estado-nação e seus limites rígidos. Como escreveu Duggal (2018), essas leis transfronteiriças desafiam “os países a adaptarem os modos pré-digitais de soberania nacional e competição econômica para uma indústria digital que prospera na troca de informações sem fronteiras e contínua”. Na verdade, um dos aspectos centrais das leis transfronteiriças examinados por juristas são seus "efeitos”, as propriedades que especificam quais tipos de dados são cobertos e em que condições esses dados podem ser transferidos fora da nação. De acordo com o Artigo 37 da lei, “todas as informações pessoais e outros dados importantes produzidos e recolhidos pela CII operadores (e agora também operadores de rede) devem ser armazenados em servidores localizados na China continental” (FANG, 2018 p.362).

Métodos simples de geolocalização que dependem de autorrelatos não confiáveis ou da detecção mais confiável de endereços de protocolo de Internet (BASSETT, 2006) estão sendo substituídos por métodos avançados que combinam dados de várias fontes, como sinais de GPS e wi-fi para fornecer uma precisão significativamente maior com maior granularidade (FANG, 2018). As informações de localização podem ser usadas para coletar estatísticas para marketing e outros fins, fornece conteúdo localizado, apoiar a segurança cibernética medidas, dividir mercados a fim de discriminar preços e cumprir outros propósitos, como a instrumentos contra fraudes na compra de conteúdo, como ocorre com os jogos digitais. Em um estudo sobre as paralisações da Índia, Rydzak (2019) descobriu que eles encorajam os ativistas a substituir protesto não violento, que muitas vezes requer coordenação via comunicação online, com mais intervenções violentas ad hoc. Para Selva (2019), o uso crescente desta técnica pela Índia tem levado outras nações a "descobrir o interruptor de desligar", incluindo o Sudão, após uma brutal derrubada do governo protesto, e Benin e Malawi, coincidindo com parlamentares e eleições presidenciais.

Um dos exemplos mais recentes de filtragem é a “Lei Russa da Internet” aprovada em maio de 2019, uma lei que “exige provedores de serviços de internet para filtrar todo

o tráfego por meio de “nós” sob o controle de Roskomnadzor, o censor da Internet do Kremlin (FINANCIAL TIMES, 2019 np). Como Epivanova (2020) sugere, apesar da retórica da cibersegurança, o objetivo da emenda não é sobre defender a Rússia de ataques externos, “mas sim um passo proativo para separar seu próprio segmento nacional da infraestrutura da Internet global, a fim de ganhar a soberania do estado sobre ele” (EPIVANOVA, 2020 np). Quando a internet se torna uma caixa inflamável que pode instigar tensões - ou mais cinicamente, um site de contraprotesto ou constrangimento para o establishment político - então evidencia-se a busca pela capacidade de restringir essas comunicações.

Citando as paralisações na Índia discutidas anteriormente, o Estado alinhado ao Diário do Povo da China afirmou que tais medidas são um “Regulamentação necessária” da internet, uma “escolha razoável de países soberanos com base nos interesses nacionais, e uma natural extensão da soberania nacional no ciberespaço” (WANG, 2014 p.305). “Os governos quebraram a rede mundial de computadores", lamentou Mark Scott (2017), “criação de regras digitais regionais ameaça inviabilizar os avanços econômicos, sociais e políticos da era da Internet”. “Toda a Internet é uma coleção de links de longa distância entre redes discretas e conectadas localmente”, conforme Jack Goldsmith (2019, p.54), que nos lembra ainda que enquanto aparece “Suave e sem características, é na verdade um grupo de ilhas com ligações entre eles”. As redes nunca foram domínios onde vale tudo, mas, em vez disso, impuseram um conjunto estrito de controles sobre as solicitações de dados que foram atendidas, os usuários e portas que foram habilitadas, e as comunicações que poderiam ser divulgadas (MUELLER, 2019). “Ninguém questiona a autoridade e o direito de uma corporação para gerenciar, controlar e monitorar rigidamente da comunicação dentro e fora da rede de uma empresa”, documenta James Griffiths em sua história do Grande Firewall (2019, p.75), e continua: “essa tecnologia foi construída desde o início para atender o mercado de clientes corporativos. Embora os padrões e protocolos globais certamente devam ser respeitados, cada uma das redes é uma internet “nacionalizada” no sentido de que sua construção exigiu mão de obra de engenheiros nacionais, documentação na língua nacional e decisões particulares tomadas no interesse nacional. Para demonstrar essa dinâmica de uma forma mais concreta, volto à China - sem dúvida o exemplo mais forte de soberania cibernética - para examinar como as atividades além do firewall são capazes de ambos intensificar e minar a internet como espaço nacional.

A Internet é um ambiente único e desafiador no qual a radicalização e o recrutamento terrorista ocorrem com frequência, e que a compreensão e penetração neste ambiente é essencial para prevenir o terrorismo local (STEVENS, 2009). Terrorismo é um tema que vem pouco a pouco ganhando seu espaço na academia brasileira, seja pela crescente atenção que o país despertou no cenário internacional, sediando tanto a Copa do Mundo em 2014 como os Jogos Olímpicos em 2016, sendo que, no caso deste último evento, foi elaborada a Lei Brasileira Antiterror, em vigor desde sua publicação em 2016. Sendo assim, ainda é preciso certo amadurecimento da abordagem da matéria pelo poder público, tendo em vista que, infelizmente, verificou-se pouco amadurecimento desde a Lei de Segurança Nacional de 1983, com a repetição de erros conceituais e a ausência de um controle central para tais políticas públicas nacionais, como no exemplo das leis americanas e de Hong Kong (ROCHA e SCHUBERT, 2020). Gabriel Weimann (WEIMANN, Terror on the Internet: The New Arena, the New Challenge, 2006), distingue as ações terroristas entre atividades que visam construir, apoiam e gerar publicidade (comunicativa), e aquelas que facilitam atos de terrorismo (instrumental). o primeiro entre eles é que, no caso de grupos jihadistas militantes, como Al Qaeda, Boko Haram e outros passaram décadas espalhando suas ideologias e convencendo muitos de que o terrorismo suicida é um tipo de martírio islâmico, que construir um Califado, seria uma meta a ser alcançada posteriormente. Ademais, tentam convencer que fazer hijrah - isto é, viajar para terras regidas pela lei sharia - e participar na jihad militante são obrigações de todos os muçulmanos. Além disso, a internet tem evoluído a um ponto em que os mecanismos de feedback imediato das mídias sociais tornam possível para os terroristas cobrirem a internet com suas propagandas e mensagens de recrutamento e apenas esperar obterem respostas de usuários interessados.

Da mesma forma, a recém-descoberta intimidade em conexões de Internet, ao lado da possibilidade de criptografar a comunicação através de aplicativos como WhatsApp e Telegram, tornam as relações de recrutamento de terrorista baseado na Internet relações reais, vívidas e ocultas ao mesmo tempo (PYTHON, 2020). Similarmente, o Twitter tem em média 350.000 tweets enviados por minuto e 500 milhões de tweets por dia (TWITTER, 2014), enquanto o Facebook continua a ser a maior rede de mídia social com 500 milhões ativos usuários e 55 milhões de pessoas enviando atualizações (FIEGERMAN, 2014). Katz (2014) afirma que o Twitter permite que o Daesh mantenha um forte foco global que se estende além da Grã-Bretanha e da Europa. Awan (2017) propõe sete tipos de características do ofensor que podem facilmente serem encontradas

em usuários de redes sociais como o Twitter e o Facebook, tais características os tornam mais suscetíveis a radicalização. Internet e mídias sociais atuam como um banco de dados sobre como vídeos do YouTube da campanha de um bilhão promovem a violência e sua utilização como estratégia por meio da teoria do aprendizado social ou aprendizagem social (FREIBURGER E CRANE, 2008). Além disso, Tsfati e Weimann (2002) argumentam que grupos terroristas estão usando a Internet para preparar pessoas vulneráveis indivíduos justificando a violência contra civis inocentes como uma retribuição pelas invasões e crimes cometidos contra muçulmanos em todo o mundo (VERTON, 2003).

O cenário atual da industrialização, que pode ser considerado como a quarta revolução industrial ou Indústria 4.0, é composto por tendências atualizadas de tecnologias, mantendo a compatibilidade intacta para integrar sistemas inteligentes interativos com o conceito de big data. O principal objetivo da quarta revolução industrial em qualquer setor é servir sem riscos, operações sem esforço e entrega pontual de serviços, conforme definido anteriormente ao início da produção. Por exemplo, a casa inteligente pode ajustar as cortinas para economizar energia com base nas mudanças ambientais, abrir a porta da garagem automaticamente quando um veículo autorizado abordar sua entrada ou solicitar serviços médicos automaticamente quando emergências são detectadas. Se os dispositivos estiverem danificados, o impacto pode ser severo, por exemplo, o hackeamento bem-sucedido de fechaduras inteligentes permitirá que estranhos entrem em sua casa, ou como visto no primeiro capítulo deste trabalho, permite que um hacker te mantenha em cárcere em sua própria casa sem a necessidade do mesmo estar nela fisicamente; um hacker poderá assustar bebês remotamente por aparelhos de monitoramento ligados à internet ou conversar e dar ordens para crianças como foi detectado por diversos usuários de câmeras da Amazon que reportaram terem suas câmeras invadidas por hackers que conversavam e insultavam os proprietários dos aparelhos invadidos (THE GUARDIAN, 2020); o impacto da segurança cibernética na segurança do mundo físico é facilmente notado - os invasores obtêm acesso não autorizado a um sistema físico cibernético e o comandam a realizar qualquer tarefa danosa.

Reunindo estes exemplos de ataques ciberfísicos citados com os assuntos já abordados nos capítulos anteriores, principalmente nos capítulos 1 e 3, pode-se entender a gravidade que uma brecha de segurança significa no espaço cibernético. Desde roubo de dados aparentemente “insignificantes”, até ataques a estruturas estatais o espaço cibernético se

mostra de complexo manejo de segurança versus liberdade, adicionando o fator da Internet das Coisas estar cada vez mais presente no dia de cidadãos comuns é nítida a necessidade de uma legislação que acompanhe essa modernização de sistemas, casas inteligentes e até mesmo cidades inteligentes. Apesar da segurança em sistemas de rede tradicionais continuar sendo um desafio, os sistemas IdC apresentam aos pesquisadores desafios maiores e mais complexos devido aos diferentes recursos especiais dos sistemas IdC. diário The News colocam a segurança no topo das preocupações: vazamento de dados pessoais e econômicos, espionagem, infecção de sistemas informáticos confidenciais, roubo de identidade e receios sobre pagamentos com cartão são apenas alguns exemplos de ameaças (KOUICEM, BOUABDALLAH, LAKHLEF, 2018). Neste contexto, a tolerância a falhas - no sentido de, caso aconteça alguma falha no serviço de segurança ou no próprio software isso não comprometa os dados ou o próprio dispositivo - é essencial para a confiabilidade do serviço, mas qualquer solução deve ser especializada e leve para levar em conta o número limitado e facilmente acessível de dispositivos IdC. A primeira é proteger por padrão todos os objetos, para projetar protocolos e mecanismos seguros, os pesquisadores devem trabalhar na melhoria da qualidade da implementação do software, pois um patch de software pode não ser compatível para bilhões de dispositivos (ROMAN, NAJERA, LOPEZ, 2011).

Novos aplicativos emergentes baseados na IdC se beneficiarão de transações e mensagens seguras e privadas, descentralização de comunicações e privacidade de design, todos os quais são recursos muito importantes para a indústria e para a IdC em geral (BAHGA, MADISETTI, 2016). Blockchain é uma maneira eficiente de automatizar negócios e criar contatos inteligentes entre dispositivos inteligentes sem redirecioná-los para entidades centrais, além disso para gerenciamento de fluxo de dados mais dinâmico, em suma, todos os tipos de contatos digitais criam “contratos inteligentes”. Até agora, sua aplicação tem tido muito sucesso em aplicações financeiras e contratos inteligentes, mas alguns pesquisadores argumentam que vale a pena investigar até que ponto esta tecnologia eficaz pode melhorar significativamente a IdC e a segurança dos domínios. A pesquisa nesta área é muito necessária para resolver esses problemas de segurança e desafios da IdC em ambientes heterogêneos para que os usuários possam usar dispositivos IdC para se comunicar e compartilhar informações globalmente com garantia de segurança. Faz-se necessária tal segurança, também para que governos e entidades internacionais tenham a garantia de que documentos sensíveis e assuntos estatais não estejam sendo acessados por terceiros, visto que tecnologias conectadas a IdC estão cada

vez mais presentes não apenas nas casas, mas também em prédios governamentais, parlamentos etc.

Referências

AWAN, Imran. Cyber-extremism: Isis and the power of social media. Society, v. 54, n. 2, p. 138-149, 2017.

BAHGA, Arshdeep; MADISETTI, Vijay K. Blockchain platform for industrial internet of things. Journal of Software Engineering and Applications, v. 9, n. 10, p. 533-546, 2016.

DEMARTINI, Mariana. Hackers trancam quartos de hotel e exigem resgate em bitcoin. Exame. Disponível em: acessado em 20 de novembro de 2020.

DENMARK, Abraham M. Managing the global commons. The Washington Quarterly, v. 33, n. 3, p. 165-182, 2010.

FANG, Binxing; FANG; ZHANG. Cyberspace sovereignty. Springer Singapore, 2018.

GOLDSMITH, Jack; WU, Tim. How governments rule the net. In: Who Controls the Internet? Oxford University Press, 2006.

GRIFFITHS, James. The great firewall of China: How to build and control an alternative version of the internet. Zed Books Ltd., 2019.

JOSSELIN, Daphne; WALLACE, William. Non-state actors in world politics: a framework. In: Non-state actors in world politics. Palgrave Macmillan, London, 2001. p. 1-20.

KATZ, Stefan P. REFORMING THE COUNTER-TERRORISM WORKHORSE: ENSURING THE NATIONAL STRATEGY FOR THE NATIONAL NETWORK OF FUSION CENTERS. 2014.

KOUICEM, Djamel Eddine; BOUABDALLAH, Abdelmadjid; LAKHLEF, Hicham. Internet of things security: A top-down survey. Computer Networks, v. 141, p. 199-221, 2018.

MUELLER-BADY, Robin et al. An evolutionary hybrid search heuristic for monitor placement in communication networks. Journal of Heuristics, v. 25, n. 6, p. 861-899, 2019.

PYTHON, Andre. Debunking Seven Terrorism Myths Using Statistics. CRC Press, 2020.

ROMAN, Rodrigo; NAJERA, Pablo; LOPEZ, Javier. Securing the internet of things. Computer, v. 44, n. 9, p. 51-58, 2011.

SELVA RAJOO, Kukaneswaran. INTERNET OF THINGS IMPLEMENTATION IN HIGH FREQUENCY MEASUREMENTS. IRC. 2019

VALENTE, Junia; CARDENAS, Alvaro A. Security & privacy in smart toys. In: Proceedings of the 2017 Workshop on Internet of Things Security and Privacy. 2017. p. 19-24.

VERTON, Dan. Black ice: the invisible threat of cyber-terrorism. Osborne, 2003.

WALL, David. Policing the Virtual Community: The Internet, Cyberspace and Cyber-Crime. In: Policing futures. Palgrave Macmillan, London, 1997. p. 208-236.

WANG, Shiguang et al. Towards cyber-physical systems in social spaces: The data reliability challenge. In: 2014 IEEE Real-Time Systems Symposium. IEEE, 2014. p. 74-85.

WEIMANN, Gabriel. Terror on the Internet: The new arena, the new challenges. US Institute of Peace Press, 2006.

ESPIONAGEM CIBERNÉTICA E AS FAKE NEWS: análise do uso das Fake News como instrumento de poder.

Jacy Magalhães
Lucas Soares Portela

A prática de, secretamente, coletar dados e fornecer informações sigilosas sobre um grupo para outro, é conhecida como espionagem; e possui suas origens no mundo antigo, não se sabe ao certo como, nem quando. Mas, segundo arqueologistas, há evidências de espionagem primitiva (VOLKMAN, 2013). Ou seja, sabe-se que desde as primeiras guerras na história, a espionagem é vista como um instrumento crucial para a vitória, pois possibilita o conhecimento sobre o inimigo, suas habilidades, estratégias e qualquer perigo em potencial (VOLKMAN, 2013).

Com a informação obtida, o espião terá vantagem sobre o adversário. Com as informações certas, será possível, por meio de sabotagem, utilizada para prejudicar o inimigo (por meios físicos, materiais ou psicológicos), fazendo com que o lado do espião ganhe tempo e mais conhecimento sobre o inimigo (CARDOSO, 2017)

Segundo Farago (2018), a espionagem sempre teve um papel importante na história das guerras, mas apenas a partir da II Guerra Mundial, que a espionagem passou a ser considerada um "quarto estado da guerra". Uma outra esfera de batalha, lutando clandestinamente, em sua própria frente de batalha e seu próprio "exército". Já que a espionagem tem o objetivo de conhecer o inimigo e obter vantagem, por meio das informações coletadas e sabotagem, ela se torna um assunto de segurança e defesa (MARTINS, 2014).

> No século IV a.C., Sun Tzu, em "A arte da guerra", defendia que um líder vencedor seria aquele que baseasse sua razão na presciência, que não adviria de espíritos ou deuses, nem da analogia com ocorrências passadas ou de cálculo, mas, sim, por meio de homens espiões que conhecessem a situação do adversário. (MARTINS, 2014, pág. 14).

É importante, ao pensar espionagem, entender seu papel em relação à soberania e poder, assim como os fatores que estão em risco; tudo isso depende de uma estratégia. As técnicas de espionagem adaptaram-se às mudanças e desenvolvimento da humanidade, especialmente nos meios de comunicação (ex.: tecnologia, idiomas e diálogo), exigindo um aprimoramento das habilidades do "espião" (MARTINS, 2014).

Um exemplo clássico do uso de espionagem para a coleta de informações é o caso da "A Coisa", durante a Guerra Fria (1945 - 1991). Em 1945, a Organização Pioneira Jovem da União Soviética fez uma visita ao embaixador estadunidense, Averell Harriman, levando um selo cerimonial dos Estados Unidos esculpido a mão. Os agentes da embaixada revistaram o objeto cuidadosamente e não encontraram nenhum sinal de fios ou baterias, então consideraram o documento inofensivo.

Com o tempo, o presente passou a ser conhecido como "A Coisa", e ganhou lugar destaque no escritório de Averell Harriman. Após 7 anos, operadores de rádio estadunidenses captaram conversas do embaixador por meio de ondas radiofônicas e após inúmeras e minuciosas buscas no escritório, nada foi encontrado e o mistério permaneceu por um tempo.

O selo cerimonial foi criado por Leon Theremin, que desenvolveu um dispositivo de escuta, que se encontrava dentro do selo. A ideia foi bastante simples, o microfone que captava as conversas era, na verdade, uma "antena presa a uma cavidade com um diafragma prateado sobre ela, servindo como um microfone" (BBC Brasil, 2019). Excluindo a necessidade de qualquer fonte de energia (ex.: bateria). O microfone era ativado por meio de ondas de rádio enviadas pelos soviéticos para a embaixada e a energia do sinal impulsionava as transmissões para os soviéticos.

Outra forma de espionagem, pouco dita, mas muito impactante, é a inserção de informação. Antes mesmo da internet, a inserção de notícias falsas era um campo fértil para motivação política. Durante o império romano, uma notícia falsa bem implementada ajudou na ascensão do imperador Septímio Severo, que alegou ser irmão ilegítimo de Cômodo (herdeiro de Marco Aurélio), mesmo não sendo parente de verdade.

A disseminação de notícias falsas, para atender as necessidades políticas, era muito comum. O uso da imagem em Roma foi crucial para a disseminação de notícias, já que muitos não sabiam ler e escrever. Para reforçar sua "legitimidade", Septímio mandou fabricar moedas do império com traços parecidos com os de Marco Aurélio.

No século XVII, durante a inquisição, a elite, em especial o Clero, se alimentava de acusações e informações falsas, que incitavam violência, com objetivos políticos, que resultaram na perseguição, expulsão e morte de muitos judeus, mulçumanos e ciganos. Testemunhas e documentos falsos, até vítimas inventadas, foram parte de um jogo político para legitimar uma das maiores perseguições da história.

Com esses dois instrumentos de espionagem, o espião projeta poder e alcançar seus objetivos. Apesar do conceito de poder não ter um consenso e suas definições serem

muito genéricas, NYE (2010), descreve que a definição mais lógica é a do dicionário, que descreve o poder como a "capacidade de fazer coisas" (NYE, 2010, p. 2), ele completa essa definição explicando que se considerar a área política, o poder é "a capacidade de afetar/influenciar o outro, para conseguir um objetivo desejado" (NYE, 2010, p. 2).

O alcance do poder cibernético é muito amplo, especialmente quando se trata de guerra comercial. Para entender melhor como o poder cibernético se projeta, NYE (2010), dividiu o poder cibernético em dimensões (NYE, 2010, p. 5):

Quadro 1. Dimensões Físicas e Virtuais do Poder Cibernético

Alvos do Poder Cibernético	***Intra Cyber Space***	***Extra Cyber Space***
Instrumentos de Informação	**Hard**: Negação de serviço de ataques. **Soft**: Definir normas e padrões	**Hard**: Ataque em sistema SCADA [1](O controle de supervisão e aquisição de dados) **Soft**: Campanha de diplomacia pública para influenciar a opinião
Instrumentos Físicos	**Hard**: Controle governamental sobre companhias. **Soft**: Infraestrutura para auxiliar ativistas de direitos humanos.	**Hard**: Roteadores de bombas ou cabos cortados. **Soft**: Protestos para nomear e envergonhar fornecedores cibernéticos

Assim, para Nye (2014), é preciso lembrar o quão recente são as formas de projeção de poder no espaço cibernético e que apesar da espionagem ser uma prática antiga, não é contra nenhuma lei internacional (NYE, 2014, p.10). O *Poder Cibernético* se concentra na criação, controle e comunicação de informações de computadores ou qualquer meio eletrônico (NYE, 2010, p. 4). E o ciberespaço possui as mudanças mais rápidas do que qualquer outra área de domínio (marítimo, aéreo e terrestre). O ciberespaço é bastante referido como um benefício para os objetivos comuns ou globais. O que, segundo NYE (2010, p. 15), é algo contraditório. Já que um bem comum é quando todos se beneficiam de algo, e a internet não é frequentemente usada para o bem de todos.

[1] Supervisory Control and Data Acquisition.

Espionagem Cibernética

Atualmente, a internet tornou-se a mais importante forma de processamento de informações no mundo (KNIGHT, 2013), esta compõe dados dos diversos nichos sociais, desde sistemas financeiros, governos digitais, segurança e defesa, bem como das relações sociais de cada pessoa. Ademais, a internet tem capacidade de remodelar a sociedade e transformar todos os ambientes em que ela está conectada. Assim, um ator pode usar esse recurso para modelagem intencional do ambiente que está inserido.

Com o crescente avanço da tecnologia e o aumento em seus investimentos (em especial, na área de segurança cibernética), por parte de Estados, de empresas e organizações internacionais, as ameaças globais chegam cada vez de forma tão sutil por meio do ambiente digital. Ambiente propício para uma ação de espionagem, haja vista a característica inerente do anonimato. Dessa forma, Estados, empresas, organizações e sociedade civil estão expostos aos perigos pertencentes ao espaço cibernético, ainda mais por ser um espaço incapaz de ser completamente analisado e controlado, ao menos, não no momento.

Aparentemente, a limitação do espaço cibernético é o próprio imaginário humano, sendo que as ações dentro desse ambiente também são limitadas apenas pela imaginação. Essas características provocam uma falsa sensação de segurança a Estados, empresas, organizações e indivíduos, que podem não perceber ou não conseguir evitar ataques cibernéticos. Esses litígios cibernéticos podem acontecer das mais variadas formas, presencial ou não. A possibilidade de se realizar esse ato a distância pode conceder anonimato e mais segurança ao executor.

Dentro do espaço cibernético há três formas de se fazer guerra, segundo Mandarino (2010), pode ser definida como um confronto que busca a coleta de informações. Assim, por meio dos meios de inteligência, quem conseguir maior quantidade de informações será detentor de maior vantagem. (LIBICKI, 1995):

Quadro 2. Conceitos de Guerras Tecnológicas

Guerra Eletrônica	**Guerra Cibernética**	**Guerra da Informação**
Tem como alvo o controle da área eletromagnética, que protege, previne ou reduz, ataques contra seu país, empresa e pessoas, por meio cibernético (Política de Guerra	Guerra sem território, que pode acontecer em qualquer espaço do globo sem que atinja, necessariamente, um espaço físico. Repercute em todas as áreas -	Confronto que busca a coleta de informações. Ou seja, através dos meios de inteligência, quem conseguir maior quantidade de informações (relevantes para as

Eletrônica de Defesa do Ministério da Defesa, 2004).	econômica, bélica, política e psicológica (LESSA et. alli, 2002).	partes) será detentor de maior vantagem. (LIBICKI, 1995).

Fonte: Elaboração própria com base em Mandarino (2010)

Segundo a teoria da "guerra além dos limites" do livro Unrestricted Warfare,escrito pelos coronéis Qiao Liang e Wang Xiangsui (apud MANDARINO, 2010, p.22), a guerra se adaptou conforme os avanços tecnológicos e do sistema de mercado, tornando ela ainda mais imprevisível. Essa teoria também afirma que a violência militar pode ser inversamente proporcional à violência política, econômica e tecnológica.

> Podemos entender que as infraestruturas críticas de um país são os alvos preferenciais de uma guerra da informação. Deflagrada contra a infraestrutura crítica financeira de um país, por exemplo, ela será percebida nas atividades típicas da sociedade da informação, pois deliberadamente atrapalha o fluxo das transações comerciais feitas por intermédio da internet e, se perdurar, causará como consequência um recuo das atividades econômicas do Estado sob ataque. (MANDARINO, 2010, p.22)

Na última década, o Brasil ganhou, gradativamente, um protagonismo no cenário internacional, chamando a atenção de outros países em relação ao seu potencial nas agendas econômica, política, ambiental e cultural. No que se refere à defesa e segurança da informação, o Brasil está alguns passos atrás de muitos países. Mesmo que possua alguns órgãos dos governos com funções no setor de segurança da informação e defesa cibernética, é uma área pouco explorada.

> A atual situação permite dizer que não se tem uma estrutura brasileira consistente que possa fazer frente a um possível cenário de ameaças reais ou de conflito no espaço cibernético, pois a situação ainda é de definição de 6 responsabilidades desde o mais alto nível de governo até as esferas governamentais mais simples, o que dificulta, em muito, qualquer ação geral de maneira integrada. (HOSANG, 2011, p. 5)

No Brasil, a falta de medidas de proteção e o pobre investimento em infraestruturas tecnológicas por parte das entidades públicas e privadas se dá por ficarem apenas, segundo Mandarino (2010), em medidas de proteção em suas próprias redes de sistemas; fragilizando o Estado e a sociedade ao buscarem por proteção e coordenação de redes de forma individualizada. A necessidade da criação de políticas públicas que solucionem a carência em segurança e defesa cibernética no Brasil, pode ser superada na criação de um "grupo especial de trabalho" (MANDARINO, 2010, p.14) integrado pelo setor público e privado, que invistam e usufruam das infraestruturas da informação.

Compreendendo que o espaço cibernético tem como uma de suas características a integração de ambientes, a necessidade de dinâmicas civil-militar e público-privado, são essenciais. No ambiente clássico do poder, é tangível a distinção dos territórios militares e civis, bem como das áreas pública e privada, mas no espaço cibernético a rede que sustenta um campo também sustenta o outro. Assim, as fragilidades das redes civis também geram fragilidades nos ambientes militares. Igualmente, o desenvolvimento de uma área favorece a outra, o que justifica a necessidade de integração entre civis e militares, entre setor público e privado.

Com base na teoria da “guerra além dos limites” (LIANG; XIANGSUI, 1999) é importante enfatizar a necessidade de estudar as ameaças do espaço cibernético para, assim, desenvolver uma estratégia e metodologia capazes de guiar as organizações brasileiras, especialmente a Administração Pública Federal, na adoção de posturas rigorosas de defesa cibernética, que proteja os ativos de informação do Estado e seus dependentes, físicos ou jurídicos, de possíveis ataques cibernéticos.

Para garantir a inviolabilidade da segurança nacional, é necessária a criação (por meio de decisões políticas) de um sistema bem estruturado, eficaz e de rápida ação, que deve ser composto por leis, investimentos e incentivos na área cibernética. Um sistema organizado e utilizado por todos os órgãos, garantirá uma postura adequada em relação às ameaças inerentes ao espaço cibernético, o que evitará que acontecimentos como os de julho de 2013, venham a se repetir.

Fake News Como Abertura À Espionagem Cibernética

A espionagem não pode ser limitada apenas à "retirada" de informação. A inserção de informações, especialmente no espaço cibernético e na “era das redes sociais”, possui um grande papel. A plataforma oferecida pelas redes sociais oferece “poucas” consequências para aqueles com “más intenções” em relação ao que publicam; não há uma “proteção” oferecida pelos meios tradicionais de notícias. Ainda sim, essa mesma plataforma fornece voz para muitos que não tinham, o que resulta em uma diminuição não só no espaço/tempo, mas nas distâncias políticas e sociais. A opinião popular tem uma forte influência nos processos de tomada de decisão e jogo político.

As *fake news* são um famoso instrumento de inserção de informações por meio do espaço cibernético, elas possuem uma grande influência na tomada de decisão por

envolver a opinião pública. Ou seja, possuem a capacidade de incitar determinados comportamentos, por meio de notícias falsas ou informações descontextualizadas.

As eleições estadunidenses de 2016 podem ser consideradas um exemplo, já que foi nesse contexto que nasceu o conceito de fake news. Os serviços de inteligência estadunidenses acreditam que a eleição de Donald Trump teve interferência russa. A inteligência russa conseguiu informações sobre várias juntas eleitorais dos Estados Unidos (estaduais e locais).

O Kremlin focou, segundo a inteligência dos EUA, na opinião pública, ao acessar dados e divulgá-los, por meio de operações cibernéticas que invadiram contas de e-mails dos Democratas. O volume de informações extraídas e inseridas em redes sociais em campanhas pró-Trump foi enorme. O governo russo não tinha interesse na vitória de Hillary Clinton. Vladmir Putin criticou Clinton publicamente por sua influência em protestos contra o governo russo no final de 2011 e 2012.

As redes sociais (Facebook e Twitter) foram os principais meios de propagação de fake news. Durante as investigações de inteligência dos EUA, até 126 milhões de usuários do Facebook e 3.814 contas no Twitter estavam ligados ao Kremlin, pela empresa Internet Research Agency. Moscou foi citada diretamente pela inteligência estadunidense, acusada por ser responsável pela invasão dos e-mails do Partido Democrata, e pela disseminação de fake news, para favorecer Donald Trump.

O impacto das fake news varia de acordo com cada local e sua realidade. Sua força é maior em países com menor acesso à informação e com níveis desiguais de educação entre a população, diminuindo a capacidade da população em discernir informações relevantes de informações de baixa qualidade e até falsas.

O Brasil ocupa a terceira posição entre os países que mais são afetados pelas fake news, onde ao menos 73,3 milhões de pessoas (35% da população) declara ter consumido notícias fabricadas (FORBES,2018). Segundo o relatório Reuters Digital News Report, o Brasil lidera o ranking de pessoas preocupadas com as fake news, com 84% da população insegura em relação às notícias fabricadas e seus impactos.

Políticos são vistos como os maiores disseminadores de fake news pela população, especialmente pelo espaço cibernético. Brasil e Estados Unidos são protagonistas quando se trata de disseminação de fake news por membros eleitos. As fake news podem ser vistas como um risco a democracia, especialmente por sua origem de má fé, fraudes e pela eleição de pessoas incapacitadas que se apoiaram na disseminação de notícias falsas para chegar ao poder.

No Brasil, ainda não há leis de combate efetivo as fake news, mas em junho de 2020, um projeto foi aprovado pela Câmara e será votado ainda neste ano de 2020. A PL2.630/2020 se trata de medidas que combatem a disseminação de fake news e impõe regras de transparência em servidores de redes sociais, como o WhatsApp, Facebook e Twitter, especialmente as fake news divulgadas em anonimato ou com perfis falsos. A PL não busca agredir a liberdade de expressão, mas sim garantir a legitimidade das informações que chegam nas mãos da população.

A *deepfake* é conhecida como uma inteligência artificial capaz de alterar rostos e vozes de pessoas, de forma realista. O realismo que a deepfake cria, gera um debate sobre a linha tênue entre "diversão" e "ameaça à democracia" ou "ameaça a moral e integridade". Esse software proporcionou de vídeos divertidos até fake news de discursos falsos de políticos e famosos em supostos vídeos pornôs.

As *deepfake* ficaram tão comuns que o Facebook baniu da rede social, para evitar maior disseminação de fake news. Um exemplo da repercussão desse deepfakes no Brasil, foi o caso do governador de São Paulo, João Doria, que teve um vídeo vazado onde, supostamente, estava em uma orgia. Doria alegou ser vítima do software, usado para prejudicar sua imagem. Até o momento, o caso não teve conclusão e não se sabe se foi o software ou não.

Considerações Finais

A guerra cibernética não é algo especulativo, e se provou (inúmeras vezes) real e muito eficaz na hora de fazer estragos. A globalização evidencia, cada vez mais que o confronto no espaço físico já não é a única opção para imposição e neutralização do inimigo e segundo o coronel Éric Cólen, representante do Comando da Aeronáutica, o espaço cibernético pode ser considerado uma arma de guerra, que será cada vez mais presente em conflitos internacionais (SENADO FEDERAL, 2019).

Os acontecimentos de 2013 influenciaram nas decisões políticas em relação à segurança cibernética, e mesmo que as medidas ainda não sejam as ideais ou as mais eficientes, os repasses públicos para a defesa cibernética aumentam a cada ano. Ainda que essa agenda esteja presente na Estratégia Nacional de Defesa, desde 2008, foi só a partir do escândalo de espionagem, que o Brasil passou a prestar mais atenção para o espaço cibernético.

A empresa de segurança cibernética Fortinet, que levantou dados por meio de clientes e entidades de classe, afirmou que o Brasil é um alvo mundial e o número de

ataques aumentaram e se aprimoraram. Devido à falta de correções e atualizações em sistemas de empresas no Brasil, o número de tentativas de ataques cibernéticos chegou a 15 bilhões (O GLOBO, 2019), no segundo trimestre de 2019. E mesmo que a postura brasileira tenha mudado com o passar dos anos, os prejuízos causados por ataques cibernéticos levaram a uma autorização do aumento no orçamento para defesa cibernética, já para 2020-2023. A partir de 2021, os repasses devem alcançar a quantia de R$ 150 milhões.

Ainda que medidas preventivas e defensivas tenham sido providenciadas, o Brasil não está conseguindo acompanhar a velocidade dos ataques cibernéticos que vem sofrendo. O que é preocupante para a defesa nacional, colocando o Brasil em uma posição de fragilidade muito grande, diante desses ataques, exigindo uma nova e mais intensa postura por parte da defesa brasileira, assim como uma presença mais forte por parte do Congresso Nacional se faz necessária, ações rápidas e precisas, são cruciais para garantir a proteção nacional.

Referências

HOSANG, Alexandre. **Política Nacional de Segurança Cibernética**: uma necessidade para o Brasil. Rio de Janeiro: ESG, 2011. Disponível em <https://abeic.org.br/Admin/Publicacoes/29/PolNacSegCib.pdf> Acessado em 15 abr 2019.

KNIGHT, Peter T. **A Internet no Brasil**. Braudel Pares. 2013. Instituto Fernand Braudel de Economia Mundial. Associado à Fundação Armando Alvares Penteado - N. 48. São Paulo. Disponível em <http://en.braudel.org.br/publications/braudel-papers/downloads/portugues/bp48_pt_internet.pdf>. Acessado em 9 out 2019.

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

LIBICKI, Martin C. **What is Information Warfare?**. National Defense University Press, Estados Unidos: 1995.

MANDARINO JUNIOR, Raphael. **Segurança e defesa do espaço cibernético brasileiro**. Recife: Cubzac, 2010

NYE, Joseph S. 2014. **The Regime Complex for Managing Global Cyber Activities**. Global Commission on Internet Governance Paper Series, 1. Massachucets: Harvard, 2014. Disponível em < https://dash.harvard.edu/bitstream/handle/1/12308565/Nye-GlobalCommission.pdf?sequence=1&isAllowed=y > Acessado em 06 abr 2019.

NYE, Joseph S. **Cyber Power**. Massachussetts: Harvard, 2010. Disponível em <https://www.belfercenter.org/sites/default/files/files/publication/cyber-power.pdf> Acessado em 20 set 2020.

O GLOBO. Brasil foi alvo de 15 bilhões de ataques cibernéticos no 2º trimestre, diz estudo. **O Globo**. Seção: Economia. 06 ago 2019. Disponível em <https://oglobo.globo.com/economia/brasil-foi-alvo-de-15-bilhoes-de-ataques-ciberneticos-no-2-trimestre-diz-estudo-23858547> Acessado em 15 abr 2020.

Fronteiras Cibernéticas e a desinformação: analise acerca da Pandemia da COVID-19

Lucas Soares Portela

Introdução

A pandemia da COVID-19 ocorreu em um mundo que já vinha lidando com outros desafios, crises econômicas, guerras, instabilidade política, competição, imersão tecnológica, entre outros. Uma das questões que já estava em foco, em especial devido aos impactos que causava na política e na vida cotidiana eram as chamadas *Fake News*. Apesar da pandemia, a disseminação dessas notícias falsas deixou de ocorrer.

Entretanto, cabe ressaltar que os fenômenos das *Fake News* não é algo novo. O uso de informações falsas dentro de uma estratégia de desinformação já era algo utilizada a anos na humanidade, mas era conhecida com o nome de "pós-verdade", que tem como definição no dicionário de Oxford "um adjetivo definido como relacionando ou denotando circunstâncias em que fatos objetivos são menos influentes na formação de opinião pública do que apelos à emoção e crença pessoal" [tradução nossa][2] (Oxford, 2020, n. p.).

Cabe ressaltar que por trabalhar o emocional e as crenças pessoais, as pós-verdades não são ao acaso, mas intencionais, principal diferença de uma simples desinformação. De acordo com Rucuero e Gruzd (2019, p. 32), "[...] não se trata apenas de uma informação pela metade ou mal apurada, mas de uma informação falsa intencionalmente divulgada, para atingir interesses de indivíduos ou grupos". Assim, não se pode dizer que são apenas formas de poluir o ambiente cercado pelas fronteiras cibernéticas, mas tem um objetivo concreto, por vezes, inclusive políticos, uma forma de movimentar uma das forças da politização, a sociedade como um todo.

O presente artigo tem como objetivo discutir a necessidade de controle sobre as pós-verdades no espaço cibernético, como uma questão de segurança cibernética e de saúde. Encontrando na figura das fronteiras cibernéticas uma saída para limitação dessas *Fake News.* Assim, utilizando de pesquisa bibliográfica, o texto ele foi dividido em duas etapas, cujo primeira trabalha as fronteiras cibernéticas e a segunda debate o espaço cibernético brasileiro e a necessidade de regulamentação e controle das fronteiras cibernéticas como mitigantes da disseminação das *Fake News*.

[2] Post-truth is an adjective defined as 'relating to or denoting circumstances in which objective facts are less influential in shaping public opinion than appeals to emotion and personal belief'.

Fronteiras Cibernéticas E As Fake News

Embora a pós-verdade não seja algo tão recente, o fato de sua disseminação utilizar instrumentos de Tecnologia e Comunicação é o que inova esse fenômeno, tornando-o no que chamamos hoje de *Fake News*. Isso é possível devido a capacidade de multiplicar, disseminar, difundir e atingir mais pessoas que a Internet, por exemplo, permite.

A difusão dessa desinformação não está vinculada a velocidade da comunicação da Internet. A características instantânea esteve presente no mundo desde o início do século XX, com a utilização de equipamentos de comunicação como código Morse, que já enviava informações a longas distâncias em tempo real. O que pode ser considerado realmente como um fator inovador nas tecnologias de comunicação é o volume de informação que o espaço cibernético permite.

Esse fluxo de informação em pouco espaço de tempo gera o ambiente ideal para a troca de informações. Entretanto, o espaço cibernético é sempre paradoxal, por exemplo, quando maior é o número de pessoas com acessos a Internet em um país, melhor também é o acesso à informação, entretanto, mais comprometido é a segurança, já que os pontos de vulnerabilidades aumentam. Da mesma forma, há um paradoxo em relação ao fluxo de informação que se dissipa no espaço cibernético. Enquanto esse ambiente é propicio para a difusão de informação, ele também abre margem para a disseminação das *Fake News*, haja vista que as pós-verdades também se apropriam das facilidades disponibilizadas pela Internet.

Ademais, as características do espaço cibernético proporcionam um ambiente adequado a disseminação das *Fake News*. As características desse domínio virtual são pontuadas por Maziero e Pinto (2018):

Quadro 1. Características do espaço cibernético

Características	**Significância**
Temporalidade	Modifica a nossa noção de tempo, a torna mais instantânea, devido a velocidade da troca de informação;
Fisicalidade	Através do espaço cibernético é possível ultrapassar as barreiras geográficas sem sair do seu local;
Permeação	É possível se infiltrar em fronteiras e jurisdições;
Fluidez	Está em constante alteração;
Participação	Devido ao fato de aumentar a possibilidade de ativismos políticos;

Atribuição	Em alguns casos, como a Dark Web, é difícil identificar os atores responsáveis;
Responsabilidade	Conectada, especialmente, com a sexta característica, devido à dificuldade, em alguns casos, de conectar o crime com o responsável, possibilita evitar mecanismos de responsabilidade.

Fonte: Arthur C. Maziero e Danielle J. Ayres Pinto,2018.

A instantaneidade oriunda da temporalidade garante que a pós-verdade seja disseminada rapidamente. A fisicalidade permite que um apelo emocional não fique restrito a um único local, também angariando replicadores da *Fake News* em outros países, que por sua vez não conseguem impedir a entrada no território, devido a permeação do espaço cibernético. Embora esforços sejam feitos no sentido de eliminar cada vez mais as pós-verdades do ambiente cibernético, a fluidez permite que a disseminação das *Fake News* se adapte a novas estruturas, se reinventando e burlando as barreiras criadas e dificuldades que historicamente limitavam as pós-verdades, a saber:

Quadro 2. Dificuldade para a propagação das Pós-Verdades

Obstáculos	**Descrição**
Custo Alto	Praticamente todo material precisava ser produzido e distribuído de maneira impressa. Os custos para criação de estações de rádios, por exemplo, também eram elevados e retiravam do indivíduo isolado, em regra, a possibilidade de alcançar uma audiência expressiva.
Falta de flexibilidade	O material precisava ser pensado no formato ideal para papel, depois impresso e distribuído. A modificação de alguns conteúdos era inviável.
Falta de conhecimento sobre o leitor	Entender como o público pensa, seus argumentos e principais pontos de radicalização é fundamental para a difusão de notícias falsas. Nunca houve tanto acesso a essas informações quanto hoje.
Ausência de contexto ideal	Um fator importante para a eficácia de uma notícia falsa é a impressão de credibilidade de sua origem. Panfletos distribuídos por um avião, prática comum durante a Segunda Guerra Mundial, levantavam suspeitas sobre sua origem, por exemplo. Mas o que fazer na Internet quando qualquer pessoa pode criar uma página e chamá-la imediatamente de “jornal”, começando a compartilhar o seu conteúdo?

Fonte: Elaboração própria baseada em Itagiba (2017, p. 03).

Ressalta-se que as pós-verdades não podem ser confundidas com desinformações ou simples mentiras, pois apresentam uma motivação por detrás, na maioria das vezes políticas, o que é potencializado pelo espaço cibernético, haja vista que aumenta a possibilidade de ativismo político. Ademais, tais ações são instigadas pelas características da atribuição, que permite uma difícil identificação dos atores responsáveis do espaço cibernético, ou seja, um anonimato. Isso evita, por exemplo, a punição de

geradores de *Fake News*, ou seja, próprio da última característica do espaço cibernético, a responsabilidade.

Assim, as dificuldades que limitavam a disseminação de uma pós-verdade podem ser superadas. O alto-custo de se disseminar uma *Fake News*, por exemplo, é reduzido a praticamente nada em virtude das características da temporalidade e fisicalidade do espaço cibernético. Ademais, as faltas de flexibilidade e de conhecimento acerca do leitor da pós-verdade é superada pelas características da fluidez, participação e permeação. Dessa forma, embora as pós-verdades sejam um fenômeno antigo, as *Fake News* somente têm atingindo um nível de poder informacional, em virtude das estruturas que compõe o espaço cibernético.

Ao realizar essa pesquisa, e refletir sobre as *Fake News*, notou-se uma relação entre alcance internacional das pós-verdades e reconhecimento do objeto também como algo internacional. Tal relação converte-se em força, ou seja, quanto maior o alcance internacional o objeto fonte da pós-verdade têm, maior será o apelo gerado. Assim, compreendendo que as pós-verdades possam surgir de criações nacionais e internacionais, e que seu alcance permeia fronteiras, observa-se uma característica transnacionalista que deve ser observada em seu combate. Em especial, quando o apelo emocional produzido diz respeito a um elemento também transnacional, como é o caso da Covid-19.

Assim, não somente esse vírus burlou fronteiras, como o apelo emocional causado por ele, que por vezes surge em um dado país, também se torna transnacional, fortalecendo as *Fake News* criadas. Dessa forma, as fronteiras cibernéticas se tornam bastante relevantes como instrumentos de controle para a contenção das pós-verdade, afinal, nas palavras de Raffestin (1993), a territorialização é uma forma de controle.

Diante disso, como combater as pós-verdades que penetram nas dinâmicas sociais. A resposta pode estar na própria estrutura do espaço cibernético e em como o controle se dá. Embora não haja ainda uma conceituação universal sobre o que são as fronteiras cibernéticas, cada estudo já proposto pode auxiliar em compreender como se controla ou restringe a disseminação das *Fake News*. Isso porque, em um ambiente geográfico clássico, a compreensão dos limites do Estado permite a aplicação de instrumentos de controle que auxiliam no combate aos litígios internacionais.

No quadro abaixo, o autor tentou uma síntese desses diversos estudos, observando como cada pesquisador observa as fronteiras cibernéticas. Esse foi o ponto de partida do pensamento proposto nesse artigo:

Quadro 3. Conceituações acerca das Fronteiras Cibernéticas

CATEGORIA	AUTOR	DEFINIÇÃO	EXEMPLO	MONITORAMENTO
Fronteiras Cibernéticas Imateriais	John & Post (1996)	As informações são a própria fronteira do espaço cibernético; assim proteger a informação é proteger o espaço cibernético em questão.	Pacotes de dados; E-mails; arquivos.	Defesa por meio de softwares
	Barros (2010)	As fronteiras cibernéticas são caracterizadas pela competência dos responsáveis pela rede em questão.	Domínios como os ".com"; ".gov"; ".br".	Defesa por meio de softwares
	Finklea (2013)			
Fronteiras Cibernéticas Materiais	Hare (2009)	As fronteiras cibernéticas equivalem às estruturas físicas que conectam as redes entre os países.	Cabos ultramarinos; e sinal dos satélites.	Filtros ligados juntamente aos cabos para monitorar os dados
	Mandarino Jr (2010)			Fronteiras simultâneas das quais as interconexões são feitas
	Hosang (2011)	Assim como o espaço cibernético, as fronteiras cibernéticas resultam dos sistemas das próprias máquinas.	Computadores e servidores.	Ferramentas de segurança dos equipamentos por meio de softwares e das estruturas físicas
	Ferreira Neto (2014)	Pontos de conexões da rede (nós) em que trafegam os pacotes de informações.	Roteadores; Pontos de Trocas de Dados	Filtros ligados juntamente aos pontos de conexões

Fonte: Portela (2015, p. 44-45).

Conforme exposto, cada fronteira apresenta uma característica específica que demanda um controle específico, típico do ambiente multifacetário que o espaço

cibernético é. No entanto, cabe ressaltar que embora haja uma discordância dentro do debate das fronteiras cibernéticas, os conceitos apresentados não se anulam, assim, o conjunto de ações para o controle do ambiente cibernético é o mais desejado. Assim, considera-se aqui que o espaço cibernético é formado por uma fronteira tida como hibrida, em que há aspectos materiais e imateriais. Além disso, se o poder possibilita moldar comportamento, podemos afirmar que ter poder é também ter controle, assim, quanto maior o poder cibernético do Estado sobre as fronteiras, melhor será o combate as *Fake News*.

Ressalta-se aqui que não estamos discursando contra qualquer tipo de alegação a favor da liberdade no espaço cibernético. Pelo contrário, a repreensão da liberdade no ambiente cibernético pode fragilizar a legitimidade das fronteiras cibernéticas, haja vista que se trata de um ambiente em que a participação, atribuição e responsabilidade são altas e permitem a difusão de poder ao nível do indivíduo. Pelo contrário, o controle aqui defendido visa a proteção da liberdade do indivíduo e sua segurança, ao garantir a redução de poder dos criadores e difusores das *Fake News*.

Espaço Cibernético Brasileiro E O Combate A Pandemia

O maior desafio de se combater as *Fake News* é agir dentro do limite para não comprometer a liberdade do usuário no espaço cibernético. Isso porque as pós-verdades são propagadas principalmente dentro dos ambientes sociais, ou seja, ações para endurecer esses ambientes também podem comprometer o espaço do indivíduo. Tal debate acompanha a questão das Fake News desde as eleições americanas de 2016, quando esse fenômeno se demonstrou um recurso de poder explorado.

No Brasil, a preocupação em lidar com as *Fake News* ganhou força no período anterior as eleições de 2018. Isso em decorrência do aumento da sensibilidade e reconhecimento de que o problema que afetou os EUA também seria uma questão no território brasileiro, conforme verificou-se pelo cuidado apresentado pelo Tribunal Superior Eleitoral (TSE) sobre a temática (AVELAR, 2018). Como estratégias para lidar com o problema, o TSE se empenhou no lançamento de um site com vistas ao combate da propagação da *Fake News* (AVELAR, 2018).

Ainda sobre o combate, durante a pesquisa do Instituto Brasileiro de Opinião Pública e Estatística (Ibope), encomendada pela ONG Avaaz, 90% dos respondentes afirmaram que acreditam que a solução para o combate das *Fake News* passa pela regulamentação do espaço cibernético (UOL, 2020). Tal sentimento também é observado

por especialistas dessa temática, pois entende-se que as empresas de tecnologias provedoras dessas redes sociais também apresentam responsabilidade na gestão das pós-verdades. Por exemplo, conforme documento da organização Konrad Adenauer Stiftung (2018), para o combate das Fake News é imperativo a cooperação entre empresas de tecnologias, governos, mercado e sociedade civil.

No que diz respeito a regulação brasileira que é utilizada ao combate da prática de disseminação de *Fake News*, o arcabouço é composto por:

Quadro 4. Exemplos de normas brasileiras que auxiliam no combate a *Fake News*

Norma	Como auxilia ao combate das *Fake News*
Lei n.º 5.250, de 09/02/1967 (Lei de Imprensa)	Art. 16 trata da publicação e divulgação de falsas notícias e fatos verdadeiros truncados ou deturpados que provoquem perturbação ou alarme social, desconfiança sobre instituições entre outras. Prevendo inclusive punição e detenção. Entretanto, devido sua idade não aborda diretamente as *Fake News*, se limitando a generalização das pós-verdades.
Lei de nº 12.965/14 (Marco Civil da Internet)	Além dos princípios gerais, como da neutralidade na rede, em seu artigo 19, determina que os provedores e aplicações de Internet somente poderão ser responsabilizados civilmente por dados, após ordem judicial. Embora não trate diretamente, tal instrumento também se refere ao combate à disseminação de *Fake News*, em especial a responsabilidade do setor privado.
Projeto de Lei n° 2630, de 2020 (Lei das Fake News)	Estabelece normas relativas à transparência de redes sociais e de serviços de mensagens privadas, sobretudo no tocante à responsabilidade dos provedores pelo combate à desinformação e pelo aumento da transparência na internet, à transparência em relação a conteúdos patrocinados e à atuação do poder público, bem como estabelece sanções para o descumprimento da lei.

Fonte: Elaboração própria baseado em BRASIL (1967; 2014; 2020).

Como demostrado no quadro, a Lei da Imprensa limita-se a proibição das notícias falsas e distorcidas, imputando culpa aos publicadores e disseminadores, mas não adentra no problema das *Fake News* em si. De forma semelhante é o Marco Civil da Internet, que limita a responsabilidade do setor privado, vinculando sua punição a uma decisão judicial. Embora cria uma previsão legal, essa norma também protege de certa forma as empresas da responsabilidade de controlar as pós-verdades. Por último a PL das *Fake News* tem se

dedicado a temática, entretanto apresenta diversos entraves que podem dificultar sua tramitação, como por exemplo, o descontentamento do setor privado em relação os instrumentos apresentados, que de acordo com ofícios anexos ao processo de tramitação, consideram uma lei férrea para o setor.

Tais fragilidades legais não são próprias da temática *Fake News*. De acordo com relatórios da União Internacional de Telecomunicação (2018), o Brasil apresenta fragilidades no arcabouço regulatório que comprometem a segurança cibernética do país. Tal posicionamento reflete as já mencionadas preocupações com a questão normativa como ponto focal para o combate das *Fake News*. Cabe enfatizar que a solução regulatória tem sido comum nos principais países do mundo, não somente no âmbito governamental, mas também dentro da sociedade civil.

Apesar disso, a dificuldade de combate continua emergencialmente aumentando, em especial, devido ao desafio de lidar com a ação de programações destinadas a propagação das *Fake News*. Também chamados por alguns especialistas nesse fenômeno de robôs, tais linhas de códigos destinam-se a criação de falsos perfis nos mais diversos ambientes de redes sociais para reprodução e envio de *Fake News*. Assim, embora seja o ponto inicial no combate aos crimes cibernéticos em geral, outro braço que deve ser explorado pelo Brasil é a capacidade técnica e tecnológica.

De acordo com Joseph Nye Jr (2012) existem três faces em que o poder cibernético é projetado:

Quadro 5. As três faces do poder no domínio cibernético

PRIMEIRA FACE **(A induz B a fazer o que B inicialmente não faria)** Duro: ataques de negação de serviços, inserção de malwares, interrupções de sistema Scala, prisões de bloggers. Brando: campanha de informação para mudar as preferências iniciais dos hackers, recrutamento de membros de organizações terroristas.
SEGUNDA FACE **(A impede a escolha de B excluindo as estratégias de B)** Duro: firewalls, filtros e pressão sobre as companhias para excluir algumas ideias. Brando: automonitoramento de ISPs e sites de busca, regras do ICANN sobre os nomes de domínios padrões de software amplamente aceitos.
TERCEIRA FACE **(A molda as preferências de B para que algumas estratégias não sejam nunca consideradas)** Duro: ameaças de punir bloggers que disseminam material censurado.

Brando: informações para criar preferências (como estimulação do nacionalismo e hackers patrióticos), desenvolvimento de normas de repulsa (como o caso da pornografia infantil)

Fonte: Nye Jr (2012, p. 171)

De acordo com o quadro acima, podemos encaixar as *Fake News* como uma projeção de poder Brando da primeira e/ou terceira face do domínio cibernético. Principalmente porque, como já comentado, há um proposito por de trás das pós-verdades, que pode ser influenciar alguém a fazer algo que não faria ou evitar que uma estratégia seja considerada. Infere-se, ainda da tabela, embora as pós-verdades sejam uma projeção branda de poder, tal ação pode ser contrabalanceada pela projeção dura.

Dessa forma, além das normatizações, o Estado brasileiro pode adotar medidas tecnológicas e técnicas para excluir a intenção dos produtores de *Fake News*. Também pode usar de investigações cibernéticas de forma a tentar reduzir o campo de atuação do produtor, uso dos robôs e por fim, encontrar o ciber criminoso por detrás da pós-verdade. Entretanto, ressalta-se que esses mecanismos, dependem da relação entre setor público e privado, haja vista que podem ser confundidos com interferência pública. Por fim, encontra-se na relação público-privada outra ferramenta que deve ser explorada com vistas ao controle das *Fake News*.

Considerações Finais

O poder informacional tem cada vez mais se demonstrado presente e impactando nas relações sociais e políticas no mundo. Com a evolução constante do espaço cibernético e a possibilidade de difusão do poder, um instrumento que era pouco conhecido, as pós-verdades, se transvestiram com o termo *Fake News* e tem cada vez mais impacto nas relações de poder. Chegou a tal modo que não influencia apenas questões políticas, mas chega a ameaçar a segurança do país, pois impacta também na gestão da pandemia da COVID-19, afinal, o poder nada mais é do que o uso de recursos, a informação, para moldar comportamentos, a sociedade.

O grande problema das *Fake News* no mundo está no seu poder de disseminação, resultado inclusive das características do espaço cibernético, que permite que as pós-verdade superem barreiras que antigamente as limitavam, como por exemplo, o custo de divulgação. Atualmente, com o uso do anonimato e linhas de programação, criam-se reprodutores da informação, garantindo a impunidade e mais ainda a propagação do apelo emocional. Assim, observou-se que há necessidades de criação de regulamentações que

possam auxiliar no combate, atribuindo responsabilidade não somente ao publicador e propagador das *Fake News*, mas também as empresas responsáveis pelo espaço cibernético correspondente a parte do território cibernético.

Ao estado também há parcela de responsabilidade, já que as fronteiras cibernéticas que delimitam seu território estão sob sua jurisdição. A constante atualização dessas normas também garante que o problema transnacional não afete de tal forma o território nacional. Assim, é necessária uma cooperação público-privada em prol dos controles das *Fake News*. A pesquisa em questão também compreende que o controle das fronteiras cibernéticas com vistas a mitigação dessas pós-verdades também deve passar pela aplicação de técnicas de segurança cibernética e tecnologia de controle, ou seja, aplicação de poder bruto, de tal forma e dissuadir ações que visam as *Fake News*.

No entanto, tanto a regulamentação, quanto o uso do poder bruto, são aspectos sensíveis e que devem ser tratados com muita cautela. Embora a emergência da COVID-19 requeira uma ação mais taxativa, ações no espaço cibernética podem limitar a liberdade do usuário, bem como prejudicar empresas, o que revela o carácter paradoxal do espaço cibernético. Isso ficou patente ao observar as tramitações, por exemplo, da chamada "PL das *Fake News"* que tem provocado divisões dentro sociedade civil e do próprio setor privado. Ademais, tem prejudicado as relações público-privado de controle desse fenômeno.

Por fim, entende-se que a compreensão dos aspectos das fronteiras hibridas do ambiente cibernético pode auxiliar no reconhecimento da responsabilidade sobre as parcelas do espaço cibernético. Quando bem delimitada, pode principalmente auxiliar nos debates de regulamentos e mecanismos de controle apropriados, que respeitem a liberdade da rede a atuação das empresas. Afinal, cachorro com muitos donos morre de fome, por isso, é necessário compreender os fluxos de poder e como de fato o espaço cibernético é delimitado para determinar os donos das pós-verdades contemporâneas, ou seja, as chamadas *Fake News.*

Referências

Aristóteles (2004). **Política**. São Paulo: Nova Cultura.

Avelar, José Ricardo Cabral (2018). **A Guerra Cibernética e seus Desafios para o Brasil**. Rio de Janeiro: ECEME.

Bourdie, Pierre (1989). **O poder simbólico**. Rio de Janeiro: Bertrand.

Braman, Sarah (2006). **Change of state**: information, policy and power. Cambridge: MIT Press.

Bobbio, Norberto (1998). **Dicionário de Política**. Brasília: Ed. Universidade de Brasília.

Foucault, Michel (2014). **Microfísica do Poder**. Rio de Janeiro: Ed. Paz & Terra.

IBOPE: 90% apoia regulamentação das redes sociais para combater fake news. **UOL Notícias.** São Paulo, 02 de junho de 2020. Disponível em <https://noticias.uol.com.br/politica/ultimas-noticias/2020/06/02/ibope-fake-news.htm>. Acessado em 10 de fev de 2021.

Itagiba, Gabriel (2017). **Fake News e Internet:** esquemas, bots e a disputa pela atenção. Rio de Janeiro: Its.

ITU (2018). **Global Cybersecurity Index (GCI)**. Studies & Research. Genebra: ITU Publications.

Konrad Adenauer Stiftung (2018). **Segurança Cibernética e Interesse Nacional durante Período de Campanha.** COLEÇÃO DE POLICY PAPERS. Rio de Janeiro: CEBRI.

Nye Jr., Joseph (2012). **The future of power**. New York: PublicAffairs.

Oxford (2017). **Word of The Year 2016**. Inglaterra: Oxford Language. Disponível em <https://languages.oup.com/word-of-the-year/2016/>. Acessado em 30 dez. 2020.

Maziero, Arthur C; Pinto, Danielle J. Ayres (2018). P**oder Cibernético e o espaço Internacional**: uma Perspectiva a partir das Teorias das Relações Internacionais. Segurança Internacional, Estudos Estratégicos e Política de Defesa.

Montalvão Neto, A. L; Rocha, G. G; Simas Filho, J. P; Machado, R. (2020). **Ciência, Fake News e Pós-Verdade:** a produção de efeitos de verdade em tempos de pandemia. XIV Congresso Internacional de Linguagem e Tecnologia. Minas Gerais: Texto Livre.

Portela, Lucas Soares (2018). **Geopolítica do espaço cibernético e o poder:** o exercício da soberania por meio do controle. Revista Brasileira de Estudos de Defesa, v.5, n. 1. Santa Catarina: ABED.

_____(2015). **Movimentos Centrais e Subjacentes no Espaço Cibernético do século XXI**. Dissertação [Mestrado em Ciências Militares. Rio de Janeiro: ECEME.

Raffestin, Claude (1993). **Por uma Geografia do Poder.** Paris: Ed. Ática.

Recuero, Raquel; Gruzd, Anatoliy (2019). Cascatas de Fake News Políticas: um estudo de caso no Twitter. **Galaxia** (São Paulo, online), n. 41, mai-ago.

Um Estudo À Luz De Geoffrey Till Acerca Da Estratégia Naval E O Submarino Nuclear Brasileiro (Sn-Br)

Gustavo Henrique Barbosa da Silva

Introdução

O presente trabalho versa sobre a importância da criação nacional de uma estratégia naval voltada para a pós-modernidade (conceito calcado por Geoffrey Till - 2007) ainda que, aparentemente esteja imersa em um contexto de modernidade, que vise o compartilhamento e a cooperação entre pares. Deste modo, o estudo é pautado em doutrinas sobre as temáticas propostas, com vista a entender qual é o real objetivo por detrás da aquisição de um submarino com propulsão nuclear no Estado brasileiro. No primeiro momento, conceitua-se, através de Geoffrey Till (2007), as questões latentes quanto a modernidade e pós-modernidade em face a estratégia naval que pode ou não ser adotada pelos Estados. Os parâmetros traçados por Till (2007) distingue-se sumariamente dos que por exemplo Alfred T. Mahan (2004) traçou por alguns anos e que foi premissa fulcral na vida naval dos Estados.

Faz-se preciso mencionar Klein (2011), que traz em seu trabalho a concepção de inclusivismos e exclusivismos quanto a detenção dos espaços marítimos, sendo esta uma opção a ser tomada pelos Estados. Em síntese, um Estado inclusivista, tende ao pós-modernismo quanto a sua segurança, já um exclusivista, ao modernismo, todavia são vertentes que por serem de tudo novas acabam misturando-se e são confundidas no âmbito prático.

Hugo Grotius (1609), ao disseminar o conceito de *mare liberum*, permitiu a ideia de que não haveria nenhum tipo de restrição quanto a utilização dos espaços marítimos, com o decorrer dos anos, essa premissa tornou-se um escudo que protegia a todos os Estados. Na contemporâneidade, devido a globalização e aos novos mecanismos de governança dos oceanos, os Estados passaram a não mais aceitarem essa liberdade como máxima. A questão central na vida dos Estados liga-se intimamente a ideia de insegurança de suas áreas marítimas, o que pode por em risco os espaços terrestres. Entretanto, com base no que Till (2007) defende enquanto um conceito pós-moderno de estratégia naval, a utilização dos mares teria tonalidades de liberdade como as de outrora, mas a salvaguarda desses espaços, dar-se-á por uma preocupação de todos. Para Till ainda, a segurança tende a ser um ato cooperativo, onde todos trabalham em prol de um único objetivo, mesmo que se utilizem de artefatos distintos.

Para a pós-modernidade a cooperação e a inclusão tende a ser benéfica para a manutenção da vida estatal. Todavia, é necessário ressaltar que os denominados modernistas vivem de modo cauteloso, isto é, suas ações tendem a ser mais protecionistas, ainda que essa atitude não seja a melhor, com vista a salvaguardar os interesses nacionais. Mas, são os mesmos que sofrem mais riscos e tendem a ter mais gastos reais quanto a essa escolha. O Submarino Nuclear Brasileiro (SN-Br) ainda que em processo de execução visa fomentar a segurança, não só aos espaços brasileiros, mas a todo o Atlântico Sul, embebido assim desse caráter pós-moderno.

O advento da globalização exige dos Estados certa flexibilidade quanto ao domínio de ferramentas de defesa, ou seja, defesa não pode mais ser pensada dentro de uma única esfera da sociedade, ela tende a ser vista em todas possíveis para evitar-se equívocos mais sérios. Em resumo, a defesa não pode mais ser vista como apenas uma preocupação militar, mas tende a ser colocada inclusive no âmbito da política. Para Till (2007) a globalização portanto, passa a ser um agente catalisador por meio do qual os Estados vão tomar decisões e responderão por elas quando as consequências chegarem. O intento aqui, será o de averiguar a maneira com que o Estado brasileiro está interagindo com seu entorno, a fim de tornar a segurança viável não mais como ato unilateral.

Trabalha-se aqui com o que para Till (2007) é visto como os quatro pilares fundamentais para a manutenção dos espaços marítimos e que tende a cercear diversos outros documentos nacionais e internacionais sobre essa manutenção. Deste modo, aborda-se que é necessário um efetivo controle do mar, as operações expedicionárias, boa ordem no mar e a manutenção de um consenso marítimo compartilhado. Isso significa dizer que é preciso ordem eficaz dentro do sistema internacional que produza bons resultados para alcançar esses objetivos.

O objetivo central desse trabalho consiste em analisar quais os principais motivos que levaram ao Brasil a tamanha aquisição e os pressupostos envoltos aos acordos com a França para tal empreitada. A partir disso, estuda-se como ocorreu a adequação dos projetos no nível nacional, onde perpasar-se-á na maneira como deram-se as capacitações tanto na França quanto no Brasil e far-se-á uma análise acerca dos objetivo por detrás de tamanha parceria estratégica. Com base no entendimento acerca da interdependência entre os Estados, percebe-se o quanto decisões como as tomadas por um, pode atuar e gerar impactos a níveis altos como o dessa aquisição em todo o globo terrestre.

Till (2007) afirma portanto, que a guerra é uma tendência humana, caracterizada por essa circularidade, em outras palavras, o denominado vai e vem. Preparar-se para

qualquer ataque se torna fulcral para a vida e manutenção do Estado enquanto ente soberano e dotado de riquezas. Assim, o trabalho discorre sobre como o submarino nuclear poderá criar essa imagem nacional e, por conseguinte promover essa segurança compartilhada.

Barry Buzan (2004), afirma que segurança deve ser pensada dentro de cinco dimensões: a política, a social, a militar, a econômica e a ambiental. Onde o entrelaçamento dessas tornam o Estado seguro, mas a falha em qualquer uma, pode gerar um caos. A globalização causa espanto na vida dos Estados, visto as inúmeras incertezas que a cerca. De algum modo, não há estabilidade, o mundo evolui muito rápido e alguns Estados não conseguem alcançar tal desenvolvimento. Entretanto, o medo pelo colapso dessa globalização mundial não deve e nem pode afetar a ocorrência de agentes externos que comprometam a vida do Estado.

O trabalho tem como objetivo final, entender o quão importante esse projeto se faz, e fará mesmo após o seu término para a vida do Estado brasileiro como um todo. Levando o Brasil a alinhar-se com algumas das grandes potências mundiais e crescer militarmente dando um salto grande de sua condição anterior para a atual. Por fim, averiguar-se-á que as vantagens desse projeto inovador e de proporções gigantescas provam ao mundo que o Brasil sabe trabalhar em parceria com outros países e obtém sucesso nessas parcerias.

Estratégia Naval em Geoffrey Till

Geoffrey Till (2007), propõe um estudo sobre a importância do domínio do mar em parâmetros distintos daqueles propostos por Mahan (2004) o estrategista naval inglês. Entende-se assim, que há uma necessidade iminente no presente século de interação comercial entre o globo terrestre e a segurança destes espaços interativos. Para Eric Grove (2003), o Poder Naval tem diversas funções dentre as quais estão elencadas as de tarefas militares relacionadas a guerra, a diplomacia e as relacionadas ao cumprimento da lei e regulamento do mar. Ainda que as marinhas sejam pensadas para os tempos de guerra, sua utilização maior dá-se em tempos de paz sendo importante elemento de dissuasão, fomentando apoio a política externa, tal como na fiscalização do cumprimento das normas e regulamentos marítimos.

As questões econômicas sempre foram e não há resquícios evidentes de que deixaram de ser, nucleares para vida da humanidade, assim sendo é possível entender que a interdependência dos Estados seguirá com ou sem a ideia de pós-modernidade. Deste

modo, o individualismo estatal que por tempos foi visto como fundamental, tende a ser deixado de lado para que passem a cooperar e lograr bons resultados para a segurança internacional. Ainda que seja notória as diferenças sobre os interesses de segurança, é necessário destacar que um dos maiores riscos é compartilhado entre todos e diz respeito a questões relacionadas ao comercio, isto é, econômicas. A segurança marítima global passou por mudanças radicais nos últimos anos, muitas foram necessárias e ao mesmo tempo muito atrasadas.

Geoffrey Till (2007) afirma que para entender o contexto atual faz-se necessário conhecer o passado que o cerca, assim expõe em seu trabalho de modo sintético, mas nuclear o período pré-moderno, moderno e pós-moderno. Entretanto, expõe que o mundo pós-moderno tende a ser mais cooperativo e o mundo moderno competitivo, assim o pré-moderno não tem repercussões marcantes para a humanidade, visto ser um período de consciência desenvolvimentista que não alcança grandes postos. Todavia, a ideia globalização é o tema que difere os modernistas dos pós-modernistas, motivo esse que levam os Estados modernistas em suas ações a serem mais cautelosos e protecionistas. Logo, a globalização torna-se o catalisador de ações para a estratégia naval dos Estados, perpassa-se assim por diversas esferas que antes não tomavam parte para promover segurança. Assim, os Estados passam a perceber que segurança não era mais uma questão unilateral e sim multilateral, do mesmo modo como a globalização é feita de um sistema dinâmico, a segurança precisa fundamentar-se na mesma perspectiva.

As ameaças à segurança são diversificadas, todavia Till (2007) afirma que a guerra do petróleo tende a ser a mais preocupante, entretanto faz-se necessário entender o que é a segurança. Desse modo, propõe que existem quatro pilares nucleares para a manutenção dos espaços marítimos enquanto um lugar integrado, sendo essas: controle do mar, operações expedicionárias, boa ordem no mar e manutenção de um consenso marítimo. É fundamental que os oceanos seja um espaço seguro para todos e a boa ordem no mar é o meio mais eficaz para a paz e a segurança deste espaço.

Portanto, paradigma moderno e pós-moderno de desenvolvimento naval estão intimamente ligados à ideia de globalização, no qual cada um encontra-se numa posição em relação a esta. O primeiro é um modelo tradicional de papeis e capacidades navais, que as vezes tenderá a manter certa desconfiança em relação a globalização. Neste estado, o poder naval reflete as preocupações nacionais com uma visão da sociedade internacional centrada no Estado-nação. Já o paradigma pós-moderno, deriva parcialmente de aspirações positivas com relação a globalização. Entretanto esta

abordagem enfoca-se no sistema internacional e consequentemente no lugar em que ocupa o Estado dentro desse sistema. Till afirma em sua introdução que:

o paradigma moderno do desenvolvimento naval prevê a competição entre as marinhas, enquanto o pós-moderno é mais cooperativo e colaborativo por natureza, talvez voltado contra algum adversário comum no mar ou na terra. (2007, p.01, tradução nossa)

A vulnerabilidade do sistema é consequência da globalização, que inevitavelmente impulsiona diversas ameaças. Chocando-se com a insurgência de vários grupos que poderiam explorar essa crescente vulnerabilidade. Tais ameaças incluem, entre tantas outras, ataque direto por grupos ou Estados hostis aos valores e resultados que o sistema encoraja. O crime marítimo internacional em suas múltiplas formas (pirataria, drogas e contrabando de pessoas) e o saque insustentável dos recursos marinhos, são ameaças constantes. Tais ameaças podem minar a boa ordem de que depende a passagem segura e oportuna do transporte marítimo.

Além do mais, entende-se que o conflito e a instabilidade em terra podem ter efeitos destrutivos nos mares vizinhos. Muitas destas ameaças podem ser alocadas diretamente contra o próprio comercio marítimo, o que pode gerar um caos em todos os âmbitos. Portanto, vale destacar que as ameaças são globais. Assim, Daniel Coulter sengundo Till (2007) observa que:

Manter a segurança da globalização, portanto, é um papel do qual as marinhas não ousam encolher. É a razão de ser das marinhas e das marinhas que entendem que, em primeiro lugar, aquelas que apresentam a estratégia mais coerente, credível e imaginativa para persegui-la, são as marinhas que justificarão sua existência e estarão firmemente sintonizadas com seu mestre, o público (p.167)

Com a finalidade de cobrir este espectro necessário de risco, ameaça e conflito, as marinhas pós-modernas necessitam desenvolver forças e estratégias para produzir resultados plausíveis. Till (2007) declara, que os efeitos das marinhas serão quatro, os dois primeiros intimamente ligados as aspirações tradicionais da marinha. Sendo estes: a) controle do mar; b) operações expedicionárias; c) boa ordem no mar; e d) manutenção de um consenso marítimo.

Destarte, entende-se que a globalização encoraja o desenvolvimento nos Estados pós-modernos tornando-os voltados para o exterior em termos econômicos, políticos e militares. Esses últimos contentam-se em abrir suas economias para os outros e ver a realocação em outras partes de suas indústrias manufatureiras. Geoffrey Till (2007) reitera que governos adotam atitudes clássicas de *laissez-faire* em relação à defesa das

economias nacionais, tanto quanto podem, e não dão grande ênfase à criação ou manutenção de uma base industrial de defesa independente. Todavia, orgulham-se de desenvolver formas de governo abertas e responsáveis, nas quais a informação é livremente disponível como base para a inovação contínua.

Os Estados pós-modernos desse tipo adotam políticas de defesa que provavelmente produzirão marinhas cujo foco é a manutenção da segurança internacional em vez da nacional, muitas vezes preza-se pelo bloco regional em que se insere, onde busca desse modo, uma inserção mais significativa. Estados pós-modernos adotarão atitudes inclusivistas, isto é, trabalharão para que todos tenham acesso aos espaços marítimos de modo seguro, contrário as exclusivistas, sobretudo com relação ao controle do mar. Assim, entende-se que os pós-modernos dão menor prioridade a competição entre pares como possíveis rivais de segurança, em outros termos, compartilham suas estratégias ao invés de utilizarem essas apenas como mecanismos de disputas, tendo um grau de competição menor que nos Estados modernos.

Contudo, Geoffrey Till (2007) em seu trabalho organiza suas ideias em poucas palavras que aqui sintetizou-se em uma tabela para o melhor esclarecimento, na qual expõe-se a esquerda as características de um Estado moderno e a direita o pós-moderno. Ao centro da tabela tem-se os objetos comparativos para cada qual, que criou-se com base nos dados encontrados no trabalho de Till (2007) e Klein (2011).

<table>
<tr><th colspan="2">MODELOS COMPETITIVOS DO DESENVOLVIMENTO NAVAL</th></tr>
<tr><td>MODERNA</td><td>PÓS-MODERNA</td></tr>
<tr><td>Tradicional</td><td>Não tradicional</td></tr>
<tr><th colspan="2">SUPOSIÇÕES DE GLOBALIZAÇÃO</th></tr>
<tr><td>Sistema centralizado</td><td rowspan="2">Centrado no Estado de Westifália</td></tr>
<tr><td>Mercantilismo Liberal</td></tr>
<tr><th colspan="2">FOCO POLÍTICO</th></tr>
<tr><td>Regional</td><td>Global Nacional</td></tr>
<tr><th colspan="2">FUNÇÕES E FUNÇÕES NAVAIS</th></tr>
<tr><th colspan="2">CONTROLE DO MAR</th></tr>
<tr><td>Operações expedicionárias para o litoral</td><td rowspan="2">Destinado a outras marinhas</td></tr>
<tr><td>Supervisão</td></tr>
<tr><th colspan="2">EXPEDICIONÁRIO</th></tr>
</table>

Prioridade central, terra	Baixa prioridade
Guerra anfíbia	
BOA ORDEM NO MAR	
Exclusivo/Interno	Inclusivo/Externo
DESENVOLVIMENTO DE CONSENSO MARÍTIMO	
Bilateral	Alta prioridade/Especifica
MEIOS E HABILIDADES	
FORMA DE FROTA	
Equilibrada/Autônoma	Contributiva/Especializada
INTEROPERABILIDADE	
Baixa Prioridades	Alta prioridade
BASE INDUSTRIAL DE DEFESA	
Fechada	Aberto protegido

Geoffrey Till (2007) indaga que Estados tradicionalmente nacionalistas, modernos e mais independentes poderiam ser um pouco menos afetados pelo colapso ou pela deterioração da globalização; Estados com características pós-modernas, isto é, aqueles que tem em sua política ideais de cooperação e estão imersos na globalização, por outro lado, enfrentariam uma grande reviravolta. De qualquer forma, parece que todos precisam protegerem-se contra as consequências do colapso da globalização. Com isso, entende-se o segundo paradigma mais moderno de comportamento estatal e naval, que procede claramente com base em um conjunto bastante diferente de pressupostos sobre os papéis e as capacidades necessárias das marinhas, nas quais as preocupações nacionais prevalecem sobre as cooperativas. Esses são, portanto, em muitos aspectos, bastante distintos e às vezes o oposto dos pressupostos navais dos pós-modernistas. No presente estudo, Till (2007) afirma que o mundo global é algo que urge de ações conjuntas e cooperativas. Em contrapartida, os riscos a serem assumidos devem ter as mesmas dimensões e serem encarados por todos de modo equitativo, a proteção conjunta requer responsabilidades e isso demanda recursos internos.

O Submarino Nuclear Brasileiro (SN-Br)

O Programa de Desenvolvimento de Submarinos (PROSUB), é um dos mais importantes empreendimentos da história militar nacional, coloca o país no mesmo

patamar que algumas outras potências mundiais. A entrelinha dessa aquisição dá-se relacionado ao progresso tecnológico e cientifico nacional, que até então estava limitado aos conhecimentos tradicionais. O histórico nacional quanto a desenvolvimentos voltados a marinha vem de muito tempo, desde a colonização feita pelos portugueses, porém só neste século que presencia-se tamanho acordo. Barão do Rio Branco (1845-1912) foi peça fundamental na história dos desenvolvimentos de defesa, sendo um grande nome quando pensa-se nos primórdios de um desenvolvimento mais autônomo.

Ao longo de sua história o Brasil sempre buscou por parcerias estratégicas que fossem eficientes para os seus interesses, isto é, a parceria dura enquanto meu interesse é atendido, após isso, tudo muda. Os EUA foi um parceiro importante, que de algum modo investiu esforços para que o Brasil ocupasse um cargo hegemônico quanto a defesa do Atlântico Sul, ainda que houvesse outras parcerias. Em dado momento da história, a Marinha do Brasil precisou aproximar-se das universidades para que conseguisse desenvolver tecnologias marítimas nacionais e a Universidade de São Paulo (USP) foi a escolhida.

Segundo a Doutrina Básica da Marinha:

> Os espaços marítimos brasileiros atingem aproximadamente 3,6 milhões de km². O Brasil está pleiteando, junto à Comissão de Limites da Plataforma Continental (CLPC) da ONU, a extensão dos limites de sua Plataforma Continental, além das 200 milhas marítimas, o que acrescentará uma área de cerca de 900 mil km². Após serem aceitas as recomendações da CLPC pelo Brasil, os espaços marítimos brasileiros poderão atingir uma área de 4,5 milhões de km², que é um pouco menor do que a Amazônia Verde (5,2 milhões de km²) (BRASIL, 2014, p. 1-2).

Os Submarinos são meios extremamente estratégicos de qualquer Estado, por possuir uma grande capacidade de ocultação, segundo Machado (2009). Conforme Pesce (1999) os submarinos convencionais necessitam vir a superfície de forma periódica para utilizar o ar atmosférico mesmo sem aparecerem completamente por conta do esnórquel e para recarregar por utilizarem um conjunto diesel-gerador como propulsor.

Por outro lado, os submarinos desenvolvem velocidades reduzidas e estão limitados pela condução de transporte de óleo como combustível. Já os submarinos nucleares por sua vez, ao utilizarem energia advinda da fissão nuclear não precisam do ar atmosférico para seu sistema de propulsão, caracterizando-se por uma maior capacidade de ocultamento e ainda índices de velocidades superiores (PESCE, 1999). Tal singularidade de ocultação garante uma grande vantagem, pois se entende que sua simples

presença em territórios do exterior acaba produzindo desconfiança e insegurança mesmo que não desejados (MACHADO, 2009).

Dentre um dos objetivos primordiais da Estratégia Nacional de Defesa (END) destaca-se a estratégia de segurança marítima "a dissuasão com a negação do uso do mar ao inimigo que se aproxime, por meio do mar, do Brasil" (BRASIL, 2008). A parceria estratégica firmada entre Brasil e França em 2008 possibilitará a construção de quatro submarinos convencionais, do tipo *Scorpène*, além da transferência de tecnologia que capacitará ainda mais o Brasil na produção de submarinos com reatores nuclear inteiramente nacional. O acordo ainda prevê a construção em Itaguaí, do Estaleiro e Base Naval (EBN) e da Unidade de Fabricação de Estruturas Metálicas (UFEM), além de possibilitar também a qualificação para os profissionais brasileiros que contribuirão para a construção dos submarinos (REMONDEAU, 2014).

A parceria firmada com a França foi regulamentada sob a condição de compensação direta, em que a compensação está diretamente relacionada com o objeto central do contrato de formalização. A prática compensatória é exigida por um comprador estrangeiro, como condição para a importação de bens e serviços, com a intenção de gerar benefícios de natureza industrial, tecnológica e comercial e apesar de ser pouco difundida no Brasil denomina-se pelo conceito de *offset*. Relacionando tal conceito com o PROSUB, entende-se que toda a transferência de tecnologia visa promover que as empresas brasileiras dominem o *know-how* para desenvolver futuros projetos de cunho integralmente nacional (TAVARES et al, 2014).

A troca de conhecimentos permitida pelo acordo entre Brasil e França evidencia o quanto essas parcerias são fundamentais para a saúde econômica do Estado, visto a economia feita em divisas e também em tempo. Além do mais, a autonomia do Estado em quesitos estratégicos é fundamental para as relações internacionais que este pretende executar e fomentar. Dentre diversas oportunidades geradas para a nação brasileira, o PROSUB produziu a qualificação de diversos níveis de técnicos e cientistas, o que ficará marcado e perpetuará no âmbito nacional para todo o sempre.

O PROSUB dentre todas as vantagens para o âmbito interno do Estado brasileiro, fomenta por sua imponência, o posicionamento brasileiro no âmbito de suas relações internacionais. Assim, Lana declara que: "Nos cinco continentes, a notícia desperta atenção – quase todos os países acompanham a evolução do programa que poderá tornar o Brasil independente em tecnologias sensíveis. Uma conquista que representa desenvolvimento e soberania. " (2014, p. 20).

Com a descoberta dos campos de petróleo do pré-sal, o país passa a perceber que há uma necessidade ainda maior por segurança, visto a diversas especulações internacionais e o destaque do Brasil dentro do cenário internacional como um todo. O pré-sal torna-se por essa via uma das questões estratégicas mais importantes do Estado brasileiro, onde entende-se que a expectativa da Petrobrás é de que, até 2020, a produção do pré-sal chegue a 2 milhões de barris/dia, o que representaria 53% da produção nacional, segundo Lana.

Para Bitencourt e Vaz:

> Fica claro que esses dois novos itens colocam o Brasil dentro de um contexto estratégico distinto. Embora esses feitos sejam ainda notícias novas que reverberam em toda a arena internacional, é fácil antecipar que irão criar consideráveis demandas e, assim, pressões, para definições mais ousadas diante da segurança e da defesa. [...] As descobertas de petróleo aumentarão as pressões por "capacidades de defesa" proporcionais à vulnerabilidade dos novos espaços estratégicos (2009, p. 29).

Segundo o Centro Tecnológico da Marinha em São Paulo (CTMSP), a qual cunhou o lema de que "Tecnologia Própria é Independência":

> Desde o final da década de 1970, a Marinha do Brasil desenvolve, nas dependências de seu Centro Tecnológico da Marinha em São Paulo (CTMSP), um programa de desenvolvimento e tecnologia nuclear, visando, por um lado, o domínio do ciclo do combustível nuclear, que logrou êxito em 1982, com a divulgação do enriquecimento do urânio com tecnologia desenvolvida pela MB. Por outro, o desenvolvimento de um protótipo de reator nuclear capaz de gerar energia para fazer funcionar a planta de propulsão de um submarino nuclear. (CTMSP, 2014)

Portanto, após longos atos de negociação e por detrás de anos de anseio, o Brasil finalmente consegue um parceiro estratégico a altura de seus desejos para a defesa naval. Ainda que seja uma nação com identidade pacífica declarada a todo o mundo, necessita-se estar preparada para a defesa do território e das riquezas naturais as quais é dotado. Portanto, à medida que o submarino for se desenvolvendo, o Brasil não apenas contará com o submarino em si, mas com a capacidade tecnológica e cientifica de criar outros mais e mais que isso, será capaz de vender esse tipo de tecnologia a outros Estados. Os contratos para que o submarino fosse possível foram minuciosamente pensados para que o país ao final tivesse autonomia suficiente para a projeção e construção de outros. Como visto, ao longo da história nacional, diversos personagens foram importantes para que o submarino fosse um projeto palpável, que paulatinamente tem ganhado forma e se nacionalizado por inteiro. Um projeto ambicioso, que está abrindo e abrirá outras grandes portas ao Estado brasileiro.

Com vista ao desenvolvimento de uma estratégia naval de dissuasão o SN-Br chega em um momento de extrema necessidade nacional, visto aos grandes desenvolvimentos econômicos e os enfoques mundiais. O conceito de Amazônia Azul começou a ganhar forma e o Brasil enquanto um país de dimensões continentais passa a entender a importância desses espaços, onde o submarino virá para salvaguardá-los. Os efeitos dessa aquisição que ainda não está completa já são notórios no âmbito interno e no externo do Brasil. As dimensões políticos, militar, econômico e científica ganham tonalidades novas com essa aquisição.

O Estado passa a ter mais autonomia com o acordo feito, ou seja, tem a propriedade intelectual, que pode vir a gerar ainda mais benefícios para o país no decorrer dos próximos anos. Ainda que o submarino tenha previsão de conclusão para 2025, o Brasil tem se capacitado em diversos quesitos e isso gerará muitas outras mudanças positivas. Essa troca de conhecimentos entre o Brasil e a França tem sido importante para ambas as partes. O Estado brasileiro tem se destacado por consegue trabalhar em cooperação e integração, onde há a promoção de um projeto totalmente diferenciado e consciente de suas atribuições.

A abertura de empregos e a promoção de capacitação profissional a todos os possíveis funcionários faz toda a diferença nas localidades em que se encontra o PROSUB, sendo esse um projeto complexo, de dimensões muito abrangentes e que tem dado certo. Os desenvolvimentos promovidos por esse projeto são grandes e marcantes para a história nacional, a necessidade de diversos trabalhadores com as mais diferentes especialidades e mesmo sem nenhum tipo de capacitação, permitiu-se o aprimoramento de técnicas aos interessados.

Essas aquisições de conhecimentos vão perdurar por longos anos e enriquecerá a nação de um modo muito maior que a própria aquisição do submarino nuclear. Vale destacar sobretudo, a preocupação com o meio ambiente que tornou-se um marco e exemplo para todo o mundo, visto a urgência de obras responsáveis para com o meio ambiente, e o PROSUB mostra-se um excelente marco para construções numa estrutura assim. Os ganhos nacionais ultrapassam os tangíveis, alcançam níveis mais profundos, os investimentos feitos são pequenos quando comparados aos ganhos adquiridos em termos de capacitações.

Considerações Finais

O desenvolvimento do presente estudo possibilitou uma breve análise das relações internacionais advindas de políticas de defesa do Estado brasileiro. Além disso, também permitiu compreender alguns dos diversos benefícios correlatos a essa parceria entre o Brasil e França para o desenvolvimento do SN-Br. Pode-se mencionar como exemplos, a economia de tempo e recursos que essa parceria estratégica gera para o Brasil, além dos outros diversos benefícios que o PROSUB acarretou ao Estado brasileiro em quesitos de capacitação profissional e técnica. Dentre as diversas contribuições que esse projeto traz, vale destacar as inúmeras oportunidades envoltas a um projeto que promove o desenvolvimento social nas localidades em que se insere.

Visando um embasamento teórico para o tema aqui apresentado, calcou-se um estudo alicerçado na ótica de Geoffrey Till que argumenta sobre a importância de uma estratégia naval pós-moderna. O primeiro objetivo relaciona-se a entender quais são os parâmetros da teoria de Till sobre estratégia naval, a partir disso, parte-se para os documentos oficiais sobre o PROSUB para entendermos como ele se insere nesse contexto, onde chega a fim de ser um importante elemento dissuasivo no espaço que denominou-se Amazônia Azul.

O segundo objetivo, foi de analisar e demonstrar o histórico da Marinha do Brasil quanto a aquisição e projeção de submarinos. Percebeu-se com isso que os acordos que atualmente findam com a aquisição de tecnologia para o SN-Br é um projeto longínquo que apenas com o governo Lula saiu do papel e começou a tomar vida efetivamente. A partir disso, percebe-se também que os efeitos correlatos a esse projeto têm sido observados em todos os âmbitos nacionais e internacionais, devido a importância dada a tal aquisição. O Brasil ao se beneficiar de um submarino nuclear, garante para si a propriedade intelectual de projetar outros submarinos desse porte e consequentemente de vender essa tecnologia a outros Estados. Esse ponto torna-se importante ao Estado brasileiro, sobretudo quando se pensa nas parcerias futuras que surgirão por meio do que está sendo executado agora.

Por fim, o terceiro objetivo relacionou-se com a busca por entender como foram feitas as negociações para tamanha parceria e como esse projeto tem se encaminhado no dia a dia, quais os desdobramentos e os reflexos no cenário brasileiro. Onde aferiu-se que os impactos do projeto foram super positivos tanto para as populações locais, que puderam se capacitar e desenvolver novas habilidades, quanto para a imagem internacional do Brasil.

Observou-se assim, que cooperações deste tipo são benéficas para a relação dos Estados que a fazem. Dentre os efeitos gerados, percebe-se uma harmonia que gera a integração entre os Estados, visto os trabalhos cooperativos diários e os sucessos obtidos a cada novo passo dado dentro do projeto. O PROSUB como foi outrora relatado tem sido um grande espaço de troca de conhecimentos e experiências entre os dois países, com a geração de benefícios mútuos e contínuos.

O trabalho aqui proposto tem sua análise até meados de 2018, logo, aferiu-se que com vista ao engrandecimento econômico que o Brasil vinha tendo e a ascensão da consciência sobre a Amazônia Azul, o submarino chegaria em um momento propício. Desse modo, a cooperação mais uma vez resulta em benefícios ao Estado brasileiro, pois auxilia esse a expor para o mundo que o seu desenvolvimento econômico vem acompanhado de avanços tecnológicos, de modo mais preciso os voltados para a defesa. Isso é possibilitado por meio da interdependência existente entre os países que cooperam, que promove um auxílio mútuo com assistência recíproca, nos setores estratégicos e de defesa. E em partes, pode se dizer que o setor econômico entra nessa interdependência visto as movimentações fomentadas por tal parceria, e por tabela o desenvolvimento econômico voltado as regiões onde se encontram os estaleiros do PROSUB. Portanto, fica evidente que este convênio entre Brasil e França gera confiança entre os Estados e vantagens a cada um.

Por essa via, a hipótese inicial foi confirmada. Logo, o Brasil tem conseguido a aquisição desse equipamento que promove mais e melhor sua imagem internacional, e com isso a aquisição da propriedade intelectual. Considera-se também em relação a conceituação de Till, o SN-Br chega como um meio de cooperação regional, como proposto nas políticas de defesa nacional, constituídas em meados de 2005. Os benefícios dessa aquisição se repercutirão por muito tempo na história nacional, isto significa que o Brasil alcançou um novo patamar para o que diz respeito a sua defesa e ninguém lhe pode tirar isso. Porém, é de suma importância destacar que os benefícios para o Brasil são diferentes dos obtidos pela França, todavia, ambos os Estados ganham com essa cooperação.

Por fim, dada a importância do assunto, torna-se necessários outros estudos sobre as questões de defesa no Brasil, voltadas para as agendas de defesa nacional, em especial para a Marinha do Brasil. Além disso, o Brasil necessita promover mais conversas entre política e defesa, ou seja, há uma grande necessidade de outros trabalhos que promovam essa interação entre as áreas mencionadas. No atual momento, o Brasil

precisa continuar investindo seus esforços para a finalização desse projeto do SN-Br.

Neste momento, o grande desafio encontra-se em continuar mantendo esse projeto e tomando as melhores escolhas que preservem tudo o que já foi construído. Com base nisso, há inúmeras possibilidades de pesquisas cientificas voltadas aos desdobramentos ocorridos a partir daqui. Assim também, torna-se válido entender como o imperialismo do Brasil em relação a outros países devido ao seu potencial econômico e sua diplomacia integracionista vai desdobrar-se com a finalização desse projeto.

Referências

BITENCOURT, L; VAZ, A. C. **Brazilian strategic culture**. Miami: Florida International University, Applied Research Center, Latin American and Caribbean Center, 2009.

BRASIL, Agência Brasileira de Desenvolvimento Industrial. **Diagnóstico**: Base Indstrial de Defesa. 2011. Disponível em: < http://www.abdi.com.br/Estudo/relatorio_neit_04-defesa_ 01b.indd.pdf>. Acesso em: 06 out. 2018.

BRASIL, Instituto Brasileiro de Geografia e Estatística. **Resolução Nº 2. 21 jun. 2016**. Publicada no Diário de 22 jun. 2016, nº 118, Seção 1, p. 87.

BRASIL, Ministério da Defesa. **Livro Branco de Defesa Nacional**. Disponível em: <http://www.defesa.gov.br/estado-e-defesa/livro-branco-de-defesa-nacional>. Acesso em: 16 jun. 2018.

BRASIL, Ministério da Defesa. **Marinha do Brasil. Doutrina Básica da Marinha**. 2º Revisão. Brasília, 2014.

BRASIL, Presidência da República. **Constituição da República Federativa do Brasil de 1988**. 1988.

BRASIL. **Decreto no 7.546, de 2 de agosto de 2011**. Regulamenta o disposto nos §§ 5o a 12 do art. 3o da Lei no 8.666, de 21 de junho de 1993, e institui a Comissão Interministerial de Compras Públicas. Diário Oficial da União, Brasília, 2011.

BRASIL, Ministério da Defesa. **Estratégia Nacional de Defesa**. Brasília, 2008. Disponível em: <http://www. planalto.gov.br/ccivil_03/_ato2007-2010/2008/Decreto/D6703.htm>. Acesso em: 23 de ago. 2018.

BRASIL. **Lei nº 10.303, de 31 de outubro de 2001**. Altera e acrescenta dispositivos na Lei no 6.404, de 15 de dezembro de 1976, que dispõe sobre as Sociedades por Ações, e na Lei no 6.385, de 7 de dezembro de 1976, que dispõe sobre o mercado de valores mobiliários e cria a Comissão de Valores Mobiliários. Disponível em:< http://www.planalto.gov.br/ ccivil_03/leis/LEIS_2001/L10303.htm>. Acesso em: 22 de jun. 2018.

BRASIL. **Lei nº 12.598, de 21 de março de 2012**. Estabelece normas especiais para as compras, as contratações e o desenvolvimento de produtos e de sistemas de defesa. Disponível em:<http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/Lei/L12598.htm>. Acesso em: 09 de set. 2018.

BRASIL, Ministério da Defesa. **Livro Branco de Defesa**. Brasília, 2012. Disponível em: <http://www.defesa. gov.br/arquivos/2012/mes07/lbdn.pdf>. Acesso em: 20 ago. 2018.

BRASIL. Ministério da Defesa. **Estratégia de Defesa Nacional**. Paz e Segurança para o Brasil. MD, 2008.

BUZAN, Barry (Jul. 1991), "**New Patterns of Global Security in the Twenty-first Century**" in International Affairs, Vol. 67, Nº. 3, pp. 431-451.
GROVE, Eric. **The Future of Sea Power**. Naval Institute Press, Annapolis, 2003.
KOLTZ, A.; Prakash, D. (eds) **Qualitative Methods in International Relations**. Palgrave Macmillan, 2008. Cap 05 e 10.
KLEIN, Natalie. **Maritime Security and the Law of the Sea**. 1. Ed. Oxford: Editora Oxford University, 2011. 377 p. Law of the Sea. New Haven Press, New Haven 1987.
LANA, Luciana. **Submarinos**: Defesa e desenvolvimento para o Brasil. Editora VersalEditores. Rio de Janeiro, 2014.
MACHADO, Roberto Loiola. **A Necessidade de Construção do Submarino Nuclear Brasileiro**. Revista Marítima Brasileira. Rio de Janeiro, v. 129, n. 7/9, p. 163-191, 2009.
MAHAN, Alfred T. (2004) "**The influence of Sea Power upon History, 1660-1783**". Project Gutenberg. Disponível em:< www.gutenberg.org/files/13529/13529.txt.> Acessado em: 20 de jul. de 2018.
MAHAN, Alfred T. **Retrospect and Prospect**. London: Sampson, Low, Marston, 1902.
MARINHA DO BRASIL. **Programa de Desenvolvimento de Submarinos (PROSUB).** 2017.Disponível em: <https://www.mar.mil.br/hotsites/sala_imprensa/pdf/temas/snbr.pdf>. Acesso em 13 jul. 2018.
PESCE, Eduardo Italo. **Submarinos de ataque**: Nucleares ou Diesel-Elétricos? Revista Marítima Brasileira. Rio de Janeiro, v. 119, n. 7/9, p. 127-130, 1999.
REMONDEAU, Camille Regina Jacqueline. **Parceria Estratégica Brasil-França**: A construção do Submarino Nuclear Brasileiro. Porto Alegre, 2014. Disponível em: < http://hdl.handle.net/10183/116318>. Acesso em 09 out. 2018.
TAVARES, Daniel de Mello Barreiro et. al. **Offset**: Os Impactos da Lei nº 12.598/2012 nas Importações de Produtos e Sistemas de Defesa pela Marinha do Brasil. Rio de janeiro, 2014. Disponível em: < http://jornalggn.com.br/sites/default/files/documentos/os_impactos_ da_lei_n_12.598_nas_importacooes_de_produtos_e_sistemas.pdf>. Acesso em: 09 out. 2018.
TILL, Geoffrey**. Globalization**: Implications of and for the Modern / Post-modern Navies of the Asia Pacific. Londres, 2007.

Transformações, alcances e limitações do acordo de paz na Colômbia

Luciano Alexandrino dos Santos Junior

Introdução

Após décadas de negociações e tentativas de negociações de Paz fracassadas, o governo nacional finalmente concretizou um acordo final em 2016 liderado pelo então mandatário Juan Manoel Santos (2010-2018). Não obstante, para compreender este complexo conflito e o posterior processo de paz faz-se necessário retomar às suas origens e o contexto nacional e internacional em que ocorreram, estabelecendo ponderações tanto conceituais como epistemológicas das origens do conflito, identificando a importância de cada um dos atores nele presente e examinando as motivações tanto para o conflito como para a paz negociada.

O período que abrangeu e acirrou o conflito colombiano foi a Guerra Fria (1945-1991), marcado por uma disputa ideológica bipolar entre os Estados Unidos da América e a União das Repúblicas Socialistas Soviéticas (URSS) que dividiu o mundo em dois grandes blocos ideológicos, o capitalista e o socialista/comunista (KEOHANE; NYE, 2008). Apesar de não ter havido conflito armado direto entre as potências, o reflexo dessa disputa refletiu notadamente nos países em desenvolvimento, em especial na América Latina. Nesse período surgiram também muitos movimentos extremistas revolucionários representados pelas duas ideologias. Nesse sentido, observa-se a forte presença estadunidense continental cada vez mais significativa para consolidar sua ideologia e influência, ora patrocinando as mais perversas ditaduras, ora apoiando financeiramente os regimes e políticos que defendiam seus interesses para "vencer" a ideologia e a influência socialista (BORBA, 2010).

Como agravantes para o surgimento da FARC enquanto movimento revolucionário, no nível internacional destaca-se também a revolução Cubana (1956) que contribuiu para o fortalecimento e aspiração das FARC contra o governo e a subserviência do país à intervenção externa. O fortalecimento das FARC não está somente relacionado com a conjuntura internacional, mas também ao conturbado cenário político interno do país que sempre foi tomado por oligarquias que não cediam nenhum espaço de inclusão a quaisquer outras classes que não fosse as pertencentes ao partido Liberal ou Conservador. Ademais, por ser caracterizada como uma política externa de alinhamento pragmático com os EUA (GUÁQUETA, 2006) a Colômbia foi um dos poucos países em que não houve uma ditadura civil-militar direta, ao contrário do que ocorreu nos demais países da América Latina como o Chile, Uruguai, Paraguai, Argentina e Brasil.

Em muitos países da América Latina a desigualdade social, corrupção e acumulação de riquezas têm origens desde seus processos de independência (GALEANO, 2000). Na Colômbia, desde 1819, dois grupos dominaram a política nacional, sendo eles os conservadores que se originaram dos grandes proprietários de terra, herdeiros do regime colonial e os liberais, representados pela burguesia (SILVEIRA, 2014). Estes dois grupos se intercalaram no poder político e econômico com alguns momentos de coalizão e outros de conflitos de interesses.

A origem do grupo guerrilheiro também remonta-se à insatisfação das pessoas e principalmente de campesinos pela tomada de poder dos liberais e conservadores. Um importante fato que antecede sua criação oficial aconteceu em 1928, que ficou denominado como o "massacre dos bananeiros" em que trabalhadores da companhia estadunidense *United Fruit Company*, em Barrancabermeja, estabeleceram uma greve para demandar melhores condições de trabalho (SILVEIRA, 2014).

Diante da ameaça dos Estados Unidos de intervir no país caso o governo colombiano não atuasse em defesa dos interesses da empresa o então presidente conservador Miguel Abadia Méndez (1926-1930) ordenou a repressão militar aos trabalhadores colocando fim na greve e iniciando um massacre contra a classe trabalhadora (LOZANO, 2006; OSPINA, 2010).O dirigente do partido liberal Jorge Eliécer Gaitán se tornou uma figura de grande importância no ano de 1940, sua postura de preocupação sobre as oligarquias afirmando que "o povo não tem dois partidos, mas sim está dividido em dois" (OSPINA, 2010, p. 61) referindo-se a que ambos partidos, o conservador e o liberal se opõem aos interesses nacionais e da população.

Nesse emblemático contexto, Gaitán, candidato à presidência é assassinado em nove de abril de 1948. A versão oficial do governo e da opinião pública acusa os comunistas e como prova de sua veracidade, rompe relações diplomáticas com a União Soviética (SILVEIRA, 2014). Com a morte do parlamentar, o povo se rebela, ataca símbolos do poder e em todo o país ocorrem revoltas populares. Com o temor de que poderia haver uma grande revolução do povo e da classe trabalhadora, os liberais se unem aos conservadores na figura do presidente, assim como as forças armadas e a igreja católica para solucionarem o caótico cenário de instabilidade do país.

Segundo Silveira (2014) a elite colombiana, ou seja, os grandes proprietários de terra, empresários e burgueses vinculados aos grupos estratégicos da economia foram percebendo que nenhum dos partidos conseguia acalmar a população e reprimir os movimentos armados e por isso começaram a colocar suas expectativas nas forças

armadas. Então, em 1953, o general Gustavo Rojas Pinilla (1953-1957) assumiu o poder por um golpe apoiado pelos grupos da elite colombiana. Contrário ao que se esperava Rojas Pinilla propôs aos grupos armados que estes abandonassem pacificamente as armas, concedendo anistia a todos e a proteção das forças armadas para sua inserção social. Com isso, os interesses da oligarquia não estavam sendo correspondidos e estes trataram de tirar do poder quem eles mesmos haviam colocado. Conservadores e Liberais vinculados à oligarquia, com o apoio da igreja se coligaram ao "Frente Nacional" derrubando Pinilla do poder e formulando um discurso ideal de que estavam fazendo com que a Colômbia "retomasse" ao caminho democrático (SILVEIRA, 2014).

Como estratégia para adentrar no mundo político surgiram movimentos insurgentes como as FARC, o M-19 (Movimento 19 de Abril) e o ELN (Exército de Liberação Nacional) insatisfeitos com o cenário nacional e convictos de que a única maneira de mudar tal conjuntura seria com as armas, ou em outras palavras, a revolução. Assim como expõe Silveira (2014) por outro lado, ao longo das décadas, pela incapacidade do governo de combater as ações criminosas de tais grupos como sequestros e ligação com o narcotráfico surgem também movimentos de extrema direita, os paramilitares, como o Grupo Autodefesas Unidas da Colômbia (UDC), que possuíam conhecimento técnico militar e objetivavam combater as guerrilhas de esquerda fazendo "justiça com as próprias mãos" (SILVEIRA, 2014, p. 29), o que intensificou e dificultou ainda mais o conflito.

Os primeiros indícios de negociação de paz do governo com as forças insurgentes começaram em 1980. Nesta época, um dos acordos seria a formação de um partido político, a União Patriótica (UP) que posteriormente viria a fracassar na tentativa de representá-los oficialmente (SILVEIRA, 2014). O governo justificou o fracasso culpando a guerrilha de usar essa tentativa de firmar a paz para se fortalecer militarmente. Em contrapartida não só o M-19 como as outras guerrilhas acusavam a ineficiência do governo de reintegrar os ex-guerrilheiros na sociedade e de protegê-los, pois, após a dissolução da guerrilha M-19 os ex-combatentes foram perseguidos e mortos. Este fato marcou uma profunda desconfiança em qualquer outra iniciativa de acordo para a paz.

A segunda tentativa de negociação da paz ocorreu em 1998. O presidente Andrés Pastrana (1998-2002) destinou à guerrilha uma área desmilitarizada ao sul do país para iniciar o fim dos combates armados, mas tal iniciativa não funcionou devido a negativa do governo para a liberação de guerrilheiros das FARC ao narcotráfico e a pressão

exterior, principalmente dos Estados Unidos da América (EUA), seus desdobramentos impediram a consecução da paz nacional.

Anos mais tarde, baseado nos insucessos de acordos anteriores e com uma nova postura securitária, o governo de Álvaro Uribe (2002-2010) impôs uma política de forte enfrentamento armado direto, com isso, as forças militares das FARC diminuíram consideravelmente e as ações do governo, mesmo que violentas satisfizeram a vontade popular (SILVEIRA, 2014). Após o "11 de setembro de 2001" surge o conceito de "terrorismo" nas Relações Internacionais, definição esta que se enquadrou aos membros das FARC. Portanto, a partir do entendimento de que as FARC eram um grupo terrorista, nota-se a perda de parte do apoio popular e intelectual. Devido à repercussão dos sequestros e assassinatos noticiados na comunidade internacional, marcada pela campanha antiterrorista mundial liderada pelos EUA.

Diante desse complexo cenário e após a morte de milhares de vítimas, uma cultura de violência alastrou-se pelo país, desacreditando qualquer processo de paz. Contudo, após um longo processo de negociação, disputas, conflitos e cooperação, o país consolidou um acordo efetivo e um definitivo cessar fogo com um amplo apoio da comunidade internacional como a União Europeia (UE), Organização dos Estados Americanos (OEA), Organização das Nações Unidas (ONU) e dos Estados Unidos da América (EUA), visando um cessar-fogo e uma paz estável (ECHANDÍA, 1999).

Metodologia

Para o desenvolvimento e elaboração do presente estudo utilizou-se o raciocínio dedutivo como procedimento metodológico que permeia os dois tipos de pesquisa a serem desenvolvidos: a pesquisa bibliográfica sobre as transformações do acordo de paz nos primeiros anos do pós-conflito e a pesquisa documental. Como obtenção de fontes primárias foi utilizado pesquisa documental oficial através das resoluções da Missão de Paz da ONU para a Colômbia (Resolução CSNU 2261/2016), do Instituto Kroc da Universidade de Notre Dame (EUA), Centro de Resolução de Conflitos da Noruega (NOREF), entre outras instituições educacionais e sociais imbuídas de analisar e acompanhar a implementação da paz.

Fim do conflito ou início das transformações? Aprendizados, inovações e avanços

As duas partes buscaram compreender acertos e erros de tentativas de negociações anteriores, que ultrapassaram o simples cessar fogo para incluírem discussões de

problemas históricos que motivaram o início do conflito. A preparação antes da negociação configura-se como uma inovação do processo de paz. A partir de Herbolzheimer (2016) antes da etapa exploratória e ainda em meio aos diálogos em Havana, as equipes negociadoras já estudavam o pós-conflito e todos os principais fatores que sempre empacavam as negociações, pois, como lição de processos anteriores ao redor do mundo a simples assinatura de um acordo não significa necessariamente que a violência cessaria, por isso, estabeleceram uma sólida concepção de distinguir a diferença entre o término do conflito e a transformação dele.

Colocar as vítimas do conflito armado no centro das negociações foi também uma inovação deste acordo, através da participação efetiva em painéis, delegações, exposições e mecanismos de reparação presentes na Justiça de Transição, além da comissão da verdade e aparatos jurídicos de garantia de não repetição. Por exemplo, em meio às negociações finais do acordo de paz 12 vítimas foram cuidadosamente escolhidas para representarem as todas vítimas e viajaram até Havana, Cuba. Tal ocasião foi desafiadora, mas vital para a consolidação simbólica da paz ao colocar as vítimas cara a cara com os perpetradores de crimes contra elas. O impacto dessas participações das vítimas foi fortemente percebido para ambos os lados da negociação, mas também para as vítimas, que tiveram o direito à verdade sobre o que ocorreu e garantias de reparação financeira, psicológica, entre outras.

Ainda que a reforma agrária tenha sido uma das causas para guerras civis e o surgimento de movimentos revolucionários em diversos conflitos ao redor do mundo, geralmente tal tema não é amplamente discutido ou sequer incluído em um acordo de paz. Contudo, no acordo de paz da Colômbia tal tema recebeu um tratamento e atenção peculiar se comparado com outras resoluções de conflitos, pois "foi o primeiro acordo entre o governo colombiano e as FARC com qualquer avance político substancial neste tema" (HERBOLZHEIER, 2016, p. 5). Analisando o conteúdo do primeiro ponto que foi discutido, a "reforma rural integral", o Estado assume o compromisso de realizar uma distribuição justa de terra, conceder uma ajuda financeira para pequenos fazendeiros e donos de propriedade rural e promover o amplo desenvolvimento de Estados e municípios com preponderância agroindustrial.

A inovação neste ponto do acordo se reflete justamente em tratar do campo colombiano muito além da reforma rural, mas em um enfoque no desenvolvimento estrutural, social e econômico destas localidades. Nota-se que, ao invés de tratar publicamente o tema com os tradicionais discursos de "reforma agrária", sendo esta

expressão muito pouco ou sequer utilizada pelas equipes negociadoras do governo nem por apoiadores do acordo, enfatizou-se a "coexistência entre a comunidade rural e o agronegócio" (HERBOLZHEIMER, 2016, p.5).

Segundo Pécault (2010, p. 70) "a economia da droga alimenta de fato todos os atores armados e está, portanto, bem no coração do conflito" e este também teve atenção especial nos pontos discutidos durante as rodadas de negociação. A Colômbia é a maior exportadora de cocaína do mundo, ao longo dos anos a economia ilegal, um negócio altamente lucrativo para comunidades locais rurais se entrelaçou com o conflito, servindo como financiamento das guerrilhas, paramilitares, narcotráfico, corrupção e deterioração do Estado colombiano (PÉCAULT, 2010). Enquanto as FARC admitiram que protegia, organizava, controlava e aplicava taxas aos fazendeiros produtores de cocaína o governo acusava a guerrilha de ser o principal cartel de droga no país. Dessa forma, este exigiu que as FARC retornassem ao Estado seu aparato financeiro advindo do narcotráfico, bem como seu controle nas áreas de produção de coca. Ademais, criou mecanismos jurídicos e suporte financeiro para a substituição da produção de coca por parte dos fazendeiros que não possuíam outra forma de renda.

Apesar de muitas recomendações e um considerável número de resoluções da ONU enfatizando a importância da participação de mulheres nas negociações de paz e resolução de conflitos, elas dificilmente obtêm um assento nas mesas de negociações ou tampouco são contempladas com cargos de protagonismo nos processos de paz. Porém, na Colômbia criou-se uma subcomissão de gêneros para consolidar o acordo e quatro mulheres tiveram um importante papel como membras das delegações nas mesas de negociações. Na equipe negociadora do governo faziam parte a Sra. María Angela Holguín, a Sra. María Paulina Riveros e a Srta. Nigeria Rentería, por parte da delegação das FARC possuiu um assento a Sra. Victoria Sandino (GOBIERNO NACIONAL DE COLÔMBIA, 2017).

Herbolzheimer (2016) aponta que o governo teve que seguir uma significante pressão das organizações de mulheres e em setembro de 2014 o governo e as FARC concordaram em criar uma subcomissão de mulheres, imbuídas da tarefa de revisar todos os documentos relativos aos pontos acordados, garantindo que as mulheres se sentissem contempladas e que os documentos tivessem providências relacionadas ao respeito e direito das mulheres. A comissão foi composta por uma diversidade de mulheres das duas partes e três delegadas internacionais. As mulheres desta subcomissão criaram o primeiro espaço permanente entre a sociedade civil e o setor militar. Por fim, é importante destacar

que a Colômbia é provavelmente o primeiro país ao incluir direitos da comunidade LGBTQI em uma negociação de paz, além da participação de mulheres representantes de diferentes tribos indígenas.

Socialmente, diferente de acordos anteriores o governo promoveu iniciativas sociais significativas por meio da educação para a paz para preparar para a implementação antes mesmo do término das negociações. A legislação em 2015 tornou obrigatório para todas as instituições educacionais públicas e privadas (da pré-escola à escola secundária) ajustar seus currículos "com o propósito de criar e fortalecer uma cultura de paz na Colômbia" (HERBOLZHEIMER, 2016, p. 7). Em paralelo, o governo lançou um processo denominado de "a maior conversa do mundo" para fomentar discussões públicas durante a transição para o cenário pós-conflito.

Por sua vez, as FARC pararam todo o treinamento militar a partir de outubro de 2015, e em vez disso, começou a preparar seus combatentes para a transição da organização para uma política de movimento. O governo também foi muito ativo no *Twitter* e *Facebook*, com uma transmissão semanal de notícias de televisão e rebatendo críticas feitas pela oposição (HERBOLZHEIMER, 2016, p. 9).

Considerações Finais

Constatou-se que o acordo de paz, firmado na Colômbia em 2016 representa uma vitória tanto paras as forças armadas e para o Estado quanto para as organizações revolucionárias, pois ambas as partes conseguiram alcançar algumas demandas e interesses em certa medida. A antiga guerrilha em conseguir adentrar oficialmente na política e o Estado, por aprender um enorme arsenal de armas, desmobilizar guerrilheiros e reduzir o índice de violência relacionado com o conflito FARC- Estado.

Os impactos sociais de um acordo de paz podem ser mensurados através da análise da mudança ou não de determinadas áreas, se as demandas de ambas as partes foram atendidas e estão sendo implementadas e se houve ou não alguma mudança estrutural urbana, econômica, jurídica e social. No caso colombiano, do acordo de paz entre as FARC e o Estado é possível identificar a presença destes pontos, pois o acordo perpassa da reforma rural, incorporação política, narcotráfico e mecanismos jurídicos de implementação. No âmbito econômico é possível vislumbrar diferenças significativas relacionadas ao cenário antes do acordo, através de grupos, comissões e mecanismos que transferência de renda para comunidades camponesas e financiamentos de infraestrutura urbana, de internet, saneamento básico e estrutura elétrica, em regiões que o Estado foi

historicamente omisso. Ademais, elaborou-se incentivos monetários para a substituição da produção de coca e drogas ilícitas.

A limitação de um acordo de paz e sua implementação se dá pela dependência da atuação da gestão do governo, ou por seu líder, o presidente da República, de promover, incentivar e aplicar a paz. Além disso, destaca-se também a ausência de uma pressão popular para fazer cumprir os pontos formalizados no acordo, em outras palavras, a indiferença. Estes fatores são fundamentais para que o país não se afunde e se desgaste novamente na guerra e luta armada com as FARC, podendo atuar e desenvolver outros problemas como a relação e crimes de outras guerrilhas, a corrupção e o narcotráfico.

Referências

ALTO COMISIONADO PARA LA PAZ. Publicaciones e informaciones sobre el acurdo de paz. 2017. Disponível em: <http://www.altocomisionadoparalapaz.gov.co/herramientas/Paginas/Todo-lo-que-necesita-saber-sobre-el-proceso-de-paz.aspx>. Acesso em 10 de julho de 2021.

ANTUNES, D. F. B. Capacidades para a Paz: Estudo Comparativo dos processos de paz entre o governo colombiano e as FARC nas gestões Andrés Pastrana (1998-2002) e Juan Manuel Santos (2010-2016). Dissertação de Mestrado em Ciência Política da Universidade Federal do Rio Grande do Sul. Porto Alegre: UFRGS, 2018.

BORBA, P.S. **Drogas ilegais, Crime organizado e insegurança no México:** Uma reflexão crítica a partir da experiência colombiana. Monografia apresentada ao Departamento de Economia da Universidade Federal do Rio Grande do Sul. Porto Alegre: UFRGS, 2010.

COLÔMBIA. **Acuerdo Final para la Terminación del Conflicto y la Construcción de Una Paz Estable y Duradera**. Bogotá, 24 nov. 2016. Disponível em: <https://goo.gl/YbUAIk>. Acesso em 10 de julho de 2021.

CORTES, G. Colômbia: acordo é ponto de partida, ressalvam especialistas. **Jornal online da PUC RIO**. Rio de Janeiro, 16 de dez de 2016. Disponível em <http://jornaldapuc.vrc.pucrio.br/cgi/cgilua.exe/sys/start.htm?infoid=5052&sid=49>. Acesso em 10 de julho de 2021.

GALEANO, E. **As veias abertas da América Latina**. Tradução de Galeno de Freitas. 39ª ed. Rio de Janeiro: Paz e Terra, 2000, 307p.

GUÁQUETA, A. Transformación y efectos de la cooperación antidrogas entre Colombia y Estados Unidos (1970-2000). In: CAMACHO GUIZADO, Álvaro (org.). **Narcotráfico: Europa, EEUU, América Latina**. Observatorio Relaciones UE-América Latina (OBREAL). Barcelona: Publicacins i edicins de la Universitat de Barcelona, 2006, p. 185-225.

HERBOLZHEIMER, K. Innovations in the Colombian peace process. **Norwegian Peacebuilding Resource Centre**, 2016. Disponível em: < https://www.c-r.org/downloads/NOREF_CR_Report_Colombia%20Innovations_final.pdf>. Acesso em 05 de julho de 2021.

KEOHANE, R. NYE, J**.** Power and Interdependence. In: BETTS, Richard. **Conflict After the Cold War.** Nova York: Pearson, 2008.

LOAIZA, A G. L. **Negociaciones de paz em Colombia, 1982-2009**. Un estado del arte. Medellin: Universidad de Antioquia, 2012.

LOZANO, C. G. **Guerra o paz en Colombia?** Cincuenta años de un conflicto sin solución. Bogotá: Izquierda Viva, 2006.
NASI, C. **Cuando callan los fusiles**. Impacto de la paz negociada en Colombia y en Centroamérica, Norma, Ciencia Política, Universidad de los Andes, CESO, Bogotá, 2007.
ONU. **Missão de Paz da ONU na Colômbia.** 2017. Disponível em: <https://unmc.unmissions.org/documentos>. Acesso em 10 de julho de 2021.
PÉCAUT, D. **As FARC:** uma guerrilha sem fins? Tradução de Ivone Castilho Benedetti. São Paulo, SP: Paz e Terra, 2010.
SANTOS, J. M. **La batalla por la paz.** Bogotá: Ediciones Peninsula, 2019.
SANTOS, M. Passado e presente nas relações Colômbia-Estados Unidos: a estratégia de internacionalização do conflito armado colombiano e as diretrizes da política externa norte-americana. In**: Revista Brasileira Política Internacional**, 53, 1, p. 67-88, 2010.
SILVEIRA, W. A. **As FARC- EP, o Plano Colômbia e seus desdobramentos nas Relações Internacionais**. Trabalho de conclusão do curso de Graduação de Relações Internacionais da UFRGS. Porto Alegre: UFRGS, 2014.
OSPINA, H. C.**O terrorismo de Estado na Colômbia**. Florianópolis: INSULAR, 2010.

Sistema Eleitoral Brasileiro, Cibersegurança Das Urnas E Reflexões Sobre A Necessidade De Implementação Do Voto Impressso.

David Victor de Melo Chaves
Camila Bezerra
Priscila Serafim de Andrade

Introdução

São as urnas de votação brasileiras, e consequentemente seu sistema eleitoral, seguros de ataques cibernéticos e/ou de crackers, ao ponto de ser necessária a implementação do comprovante de votação/voto impresso como camada de proteção de cibersegurança? Na última eleição municipal, em 2020, ressurgiu o ceticismo na opinião pública sobre a confiabilidade do Sistema Eletrônico de Votação Brasileiro. Tal fato está correlacionado com as inúmeras declarações feitas pelo Presidente Jair Bolsonaro, em suas redes sociais e à mídia, no que tange à segurança das urnas eletrônicas, que de acordo com seu ponto de vista não seriam passíveis de auditoria após o término da votação. Haja vista que o voto não é impresso depois de ser gravado no "*chip-set*" das urnas eletrônicas. E por esse motivo, não seria possível conferir a posteriori se o resultado da votação representa de fato o montante de votos recebidos pelos candidatos. Consoante a opinião do Presidente, a contagem dos comprovantes de votos seria uma forma de auditar e assegurar a integridade dos resultados das eleições.

O Tribunal Superior Eleitoral (TSE), órgão responsável por impedir fraudes eleitorais, portanto assegurar que as eleições sejam livres e justas, atestou que nunca houve indícios de fraudes que comprometesse a integridade do Sistema Eletrônico de Votação Brasileiro desde sua gênese, em 1996. Desse modo, o risco de fraude ínfimo não anularia a eficiência e o avanço tecnológico que foram fomentados pela informatização do sistema de votação no Brasil.

A revisão de literatura sobre Sistemas Eleitorais e Segurança Cibernética guiará a discussão deste artigo a fim de responder a seguinte questão de pesquisa: *"São as urnas de votação brasileiras, e consequentemente seu sistema eleitoral, seguros de ataques cibernéticos e/ou de crackers?*" Primeiro o tema será analisado sob a ótica da literatura sobre sistemas eleitorais (NICOLAU, 2015) (BLAIS et al, 2012), (BOIX, 1999), (DUVERGER,1951), (MARENCO, 2012). Posteriormente as discussões acerca dos Poderes Executivo e Judiciário lançam luz sobre a confiabilidade e segurança do Sistema Eleitoral Brasileiro. Por fim, analise-se as normas de Segurança Cibernética para as votações brasileiras que lastreiam o voto nas urnas eletrônicas e a transmissão de dados desses votos para o TSE.

Fundamentado pela revisão de literatura, conclui-se que a adição do comprovante de voto, popularmente conhecido como "voto impresso", no Sistema Eletrônico de Votação Brasileiro tornaria a votação onerosa e mais dispendiosa. Uma vez que, este não tornaria o Sistema Eleitoral mais seguro e não contribuiria para que as eleições fossem livres e justas, em verdade, aumentaria o custo do processo eleitoral, além de torná-lo mais complexo.

Da Discussão sobre Sistemas Eleitorais

Existem três tipos de sistemas eleitorais principais: proporcional, misto e majoritário. Este último é o sistema mais antigo do mundo e o mais simples. Em cada disputa é eleito apenas um candidato, o critério pode ser a regra do "*first-past-the-post*", "*plurality*", ou seja, dentre os candidatos que estão disputando aquela eleição, quem obtiver o maior número de votos é eleito, por isso é também conhecido como "*first-past-the-post*" (FPTP). Ou pode ser pela regra da maioria absoluta, o candidato só será eleito se obtiver mais do que 50% dos votos, se ninguém conseguir ultrapassar o "*threshold*", se realiza um segundo turno com os candidatos melhor posicionados no primeiro turno (BLAIS et al, 2012).

No sistema proporcional existe mais do que um vencedor, os assentos são divididos entre os partidos de acordo com o número de votos que cada um conseguiu. Portanto, só pode ser aplicado em distritos com vários assentos, porque é impossível distribuir um único assento entre vários partidos. Existem dois tipos principais de sistema proporcional, o de lista (aberta ou fechada) e o de '*single transferable vote*' (que está apenas em vigor na Irlanda) (BLAIS et al, *idem*).

No misto, os eleitores geralmente têm dois votos, um para eleger um candidato segundo a regra do sistema majoritário e o outro de acordo com o proporcional. Ou seja, é um sistema que se caracteriza pela junção de diferentes fórmulas para converter votos em assentos numa mesma eleição.

Regras eleitorais são instituições formais que encorajam o comportamento estratégico de ambas as elites e eleitores que forçam a coordenação deles em volta de um conjunto de candidatos (BOIX, 1999). De acordo com Duverger (1951), o psicológico antecede o voto, isto é, influência como o eleitor vota e quais candidatos os partidos escolhem para concorrer às eleições. O mecânico sucede o voto, pois são aqueles oriundos das regras eleitorais que convertem votos em assentos e o segundo de mecânico. Efeitos

psicológicos afetam o voto, efeitos mecânicos afetam o resultado da eleição (BLAIS et al, 2012).

O efeito psicológico atua também sobre as elites partidárias. Elas podem priorizar candidatos mais tradicionais à medida que a magnitude do distrito diminui. Desse modo, nos sistemas majoritários esse efeito seria maior, porque apenas um candidato seria eleito naquela eleição.

No psicológico, os eleitores decidem se votarão no seu candidato preferido, ou em outro que lhe agrada mais, mas que tem mais chances de ser eleito, para não "desperdiçar" seu voto. Se os eleitores agem estrategicamente dessa forma, esse efeito é mais forte no sistema majoritário, porque apenas um candidato seria eleito. Desse modo, iria se penalizar as minorias, inclusive as mulheres, na disputa, pois elas seriam mais competitivas do que os candidatos mais tradicionais.

Como resultado desses dois processos, eleitores e recursos fluem para candidatos mais "fortes". A extensão do comportamento estratégico entre eleitores e elites varia dentro de efeitos constrangedores das regras eleitorais. Ou seja, maior a barreira de entrada colocado pela regra eleitoral, maior a extensão do comportamento estratégico será (BOIX, 1999)

As principais divagações acerca do sistema eleitoral brasileiro estão inseridas na lapidar obra "*Sistemas Eleitorais*" de Jairo Nicolau, 2015. Em seus argumentos o autor aponta que existem três componentes principais para classificar os distintos tipos de sistemas no mundo. O primeiro componente, *Fórmula Eleitoral*, determina a distribuição das cadeiras eleitorais proporcionais de acordo com a coleta do voto, desta forma, cria-se um mecanismo matemático para distribuir a quantidade de vagas em dado colégio eleitoral de acordo com a quantidade de votação dos pleiteadores e/ou dos partidos. O segundo componente de importância é a *Magnitude dos Distritos,* este componente é essencial para designar através de distribuição matemática a quantidade de cadeiras que cada distrito, estado, município terão de acordo com o sistema eleitoral em seu caráter federativo e/ou unitário, o terceiro componente citado por Jairo, *Estrutura do Voto*, dá conta de como os eleitores podem, dentro de um sistema eleitoral demonstrar suas preferências. (NICOLAU, 2015)

Destarte, o autor classifica as distintas *Fórmulas Eleitorais*, podendo estas estarem dispostas entre: I - Majoritárias; II - Proporcionais e III Mistas. *Na Fórmula Eleitoral Majoritária,* o vencedor que angariar mais votos em seu distrito terá a vaga para si, desta forma, apenas um vencedor terá sua representação garantida, aquele que obtiver o maior

quantitativo de votos. Esta Fórmula pode ser resumida na lapidar frase de "*The Winner Takes It All*" (LIJPHART, 2003) (NICOLAU, 2015)

Outrossim, a *Fórmula Eleitoral Proporcional*, é deveras complexa em sua implementação, haja vista sua variedade de formas e cálculos. Neste tipo, os partidos apresentam previamente à entidade judiciária eleitoral uma lista de candidatos pré-selecionados para o pleito, as cadeiras eletivas são distribuídas de acordo com a quantidade de votos válidos para cada partido, tendo assim o *Quociente Eleitoral*; denota-se também nesta seara a importância do *Quociente Partidário*, tratando-se da divisão do quantitativo total de votos do partido pelo quociente eleitoral - *Quota Hare*. A fórmula do tipo proporcional, pode ser entendida também pela sua dicotomia de listas. em eleições proporcionais de lista aberta os eleitores estão aptos para votar em quaisquer dos candidatos das listas enviadas pelos partidos, em eleições proporcionais de lista fechada o eleitor vota apenas no partido, os ocupantes das cadeiras serão àqueles que estiverem no topo da lista de acordo com a quantidade de votos. As *Fórmulas Eleitorais Mistas* são aquelas que mesclam parte do modelo majoritário com o proporcional (NICOLAU, *Idem*).

Especialmente no Caso Brasileiro, cujo Sistema Eleitoral é classificado como *Proporcional de Lista Aberta*, existe o fenômeno da "*Sobras de Voto*", uma vez que, por ser lista aberta, nem todos os partidos conseguiram fazer o quociente eleitoral em sua totalidade, havendo desproporcionalidades, uma vez que não existe a possibilidade do cálculo ser exato e fechado. O sistema de sobras é feito pela seguinte equação: votos do partido/ vagas conquistas + 1. Faz-se esse mecanismo até que a quantidade de vagas - *Fórmula D Hondt.* (NICOLAU, *Idem*).

O sistema brasileiro de Lista Aberta possibilita ao eleitor escolher exclusivamente o candidato político que irá dar seu voto. A principal vantagem dessa modalidade é que existe um maior grau de escolha eleitoral favorecendo a renovação política, como principal desvantagem tem-se a competição entre candidatos do mesmo partido, o personalismo dos políticos e a falta de coordenação dos dirigentes partidários (NICOLAU, *Idem*). Assim, o supracitado autor nos apresenta de forma ampla como está formulado o Sistema Eleitoral Brasileiro. Complexo, multifacetado, multiinstitucional, *multiplayers* e multidimensional.

O sistema proporcional de lista fechada e aberta se diferenciam sobre como o eleitor expressa sua preferência. No primeiro, o partido apresenta ao Tribunal Eleitoral do país uma lista com a ordenação hierárquica dos candidatos. Cabe aos eleitores um voto

impessoal na lista do partido de sua escolha. Desse modo, o voto é no partido e são eleitos os candidatos que estão nas primeiras posições da lista do partido, mediante a quantidade de votos total que o partido recebeu. Por outro lado, no segundo tipo, em outros termos, voto preferencial, a lista do partido não é ordenada e são os eleitores que ranqueiam os candidatos através do voto nominal, diante disso, o voto é pessoal (MARENCO, 2012).

Aprofundamentos: A Guerra entre Executivo Federal e Tribunal Superior Eleitoral sobre a Confiabilidade do Sistema Eleitoral Brasileiro

Sem dúvidas, o principal tema que marcou as eleições de 2020 foi a COVID-19, em um país onde o número de abstenções já vinha em crescente vertiginosa, os brasileiros ficaram preocupados no ato de registrar seus votos, com medo de serem infectados pelo vírus que assolou o mundo neste ano pandêmico. Segundo informações obtidas pela Agência do Senado, 29,5% dos eleitores, aptos a votar, preferiram justificar seu voto, sendo a maior abstenção na recente história da redemocratização brasileira. Embora a discussão entre abstenções e obrigatoriedade do voto sejam pertinentes no quadro político nacional, não se tratará delas aqui, uma vez que nos interessa neste artigo a segurança de um outro tipo de vírus que pode adoecer a democracia brasileira, a Segurança Cibernética, dos eleitores que foram às urnas. (SENADO, AGÊNCIA, 2020)

Destarte, logo após votar em segundo turno, em sua seção eleitoral no Rio de Janeiro, em 29 de novembro de 2020, o Presidente Jair Bolsonaro voltou a defender o voto impresso como forma mais segura para garantir uma apuração presidencial justa e que seja auditável, em suas palavras, defendendo o mérito da questão, o citado afirmou:

> "Está até na própria Constituição. A apuração tem que ser pública". Além disso, estabeleceu duras críticas ao sistema eleitoral atual, atacando defronte o Tribunal Superior Eleitoral; "Vou mostrar pra vocês [jornalistas]. A apuração minuto a minuto que acontecia no TSE [eleição geral de 2018]. Era alternado: em duas horas, no 1º minuto, eu ganhei, no 2º minuto, o Haddad ganhou, e assim intercalando. Estatisticamente, isso é impossível. Mesma coisa que eu contar as areias da praia de Copacabana agora, quantos grãos de areia têm lá (…). Não podemos continuar votando e não sabendo, não tendo a certeza daquele voto que foi dado para aquela pessoa"(BOLSONARO, JAIR MESSIAS, 2020)

Ainda diante dos jornalistas, Bolsonaro afirmou que faria de tudo para que a reforma no processo eleitoral ocorresse para que nas eleições de 2022 o sistema de voto impresso seja implementado. Pelas redes sociais, um de seus filhos, o deputado federal Eduardo Bolsonaro, também se manifestou a favor do voto impresso.

Recentemente, em suas aparições ao público, como a ocorrida em primeiro de julho de 2021, o Presidente voltou a defender a utilização do voto impresso, afirmando que só aceitaria uma possível derrota nas presidenciais de 2022 se o método em questão fosse aplicado. Em suas palavras: "Eu entrego a faixa presidencial para qualquer um que ganhar de mim na urna de forma limpa. Na fraude, não" (BOLSONARO, JAIR MESSIAS, 2021).

A resposta a seus apoiadores e ao Presidente não demorou muito a chegar, em coletiva de imprensa após-divulgação dos resultados das eleições em segundo turno, na noite de 29 de novembro de 2020, o Ministro do Supremo Tribunal Federal (STF) e então Presidente do TSE, Luís Roberto Barroso, afirmou que a volta do voto impresso traria o caos ao Sistema Eleitoral, ao poder Judiciário e a própria democracia brasileira. Defendeu com unhas e dentes a confiabilidade da urna eletrônica e lembrou que o STF já firmou jurisprudência, com a maioria de votantes, sobre a inconstitucionalidade de votar com uma caneta. Em suas palavras:

> "O presidente da República merece todo o respeito institucional e tem o direito de manifestar sua opinião. A verdade, porém, é que o STF já entendeu pela inconstitucionalidade do voto impresso. E não só pelo gasto, mas porque representaria um risco real para o sigilo de voto. Não existe hoje a possibilidade de voto impresso. Respeitando a opinião de todos, o voto impresso causaria grande tumulto, porque todo derrotado ia pedir recontagem, haveria impugnações, alegações de nulidade e judicialização do processo. Considero que traria um grande tumulto. Se o presidente tiver alguma comprovação de fraude de 1996 para cá, imediatamente designarei diligências para apurá-la. Mas quero lembrar que sou juiz, não posso me impressionar com retórica política" (BARROSO, LUÍS ROBERTO, 2020).

Continuando, com suas críticas ao líder do Executivo, de maneira ainda mais densa e com tons de ironia, Barroso referiu-se que "Na farmacologia" não existiria nenhum remédio para fazer qualquer pessoa parar de duvidar que é possível fraudar as urnas brasileiras. Para isso, argumentou que as urnas não são conectadas em rede e por isso não podem ser "*crackeados*"; sendo carregadas individualmente e com seu programa operacional submetido a conferências de todos partidos políticos, Ministério Público, da Ordem dos Advogados do Brasil (OAB) e de outras entidades civis.

Depois da conferência, em suas palavras, as urnas são lacradas em um cofre, que trava sob quaisquer tentativas de alteração e arrombamento, no final das votações cada urna emite um boletim com o resultado impresso, sendo ele entregue a todos os fiscais de partidos e colados nas paredes das seções eleitorais para que qualquer cidadão as veja. Ainda segundo Barroso; "*Nunca, desde 1996, quando começou o voto eletrônico,*

ninguém demonstrou nenhum caso de fraude", informou ainda que, a Organização dos Estados Americanos (OEA) considera o sistema de apuração brasileira, em suas palavras *"o mais ágil e seguro das Américas"*.A convicção sobre a segurança do sistema eleitoral é tanta que na próxima seção discutirei, em profundidade, como o TSE elaborou as chamadas "Camadas de Proteção" das urnas eletrônicas brasileiras e como funciona a transmissão dos dados de cada Tribunal Regional Eleitoral (TRE), de cada estado da federação para o TSE em Brasília.

As Camadas De Proteção Contra Ataques Cibernéticos Do Tse

Uma complexa rede de sistemas *on-line* e *off-line,* com fases de segurança mecânicas e virtuais, em várias camadas de proteção fazem do sistema de segurança eleitoral brasileiro um dos mais difíceis de ser "*crackeados*" do mundo, fato que também contribui para a rápida divulgação dos resultados, correspondendo, com alto grau de paridade às pesquisas de boca de urna formuladas por cientistas políticos e institutos de pesquisas, destinados ao próprio TSE. Desta forma, explica-se aqui, por partes, para que fique mais compreensível ao leitor, o funcionamento deste complexo sistema, cuja fonte foi obtida através do site do próprio Tribunal Superior Eleitoral. (ELEITORAL, 2014)

O uso da criptografia.

A criptografia é essencial em todas as etapas das transmissões dos dados para o sistema que vai contabilizar, depois de encerrada a votação, o resultado dos pleitos. O conceito de criptografar dados foi inventado por Júlio César, o grande líder romano, que usava em suas mensagens militares a troca de posições de três letras, a cada letra escrita, para que um possível interceptor da mensagem não soubera de seu conteúdo. Tão somente o receptor real saberia o código para descriptografar, refazer o texto substituído por 3 letras anteriores, para ter acesso ao conteúdo do qual César quisera que apenas o destinatário tivera. Evidentemente, com a evolução para um mundo globalizado, interconectado por redes, as formas de criptografias são muito mais avançadas e dificultosas para um possível interceptor, *Hacker* ou *Cracker* do que a forma apresentada pela Cifra de César (ELEITORAL, *Idem*).

O TSE utiliza a criptografia através de assinaturas digitais para que seja garantido que os dados possam ser verificados, enquanto a sua integridade, buscando saber se estes não foram alterados ou modificados de forma intencional ou não, perdendo assim suas

características originais, por falha de gravação ou de leitura. Garantindo que o arquivo não foi modificado em seu tráfego.(ELEITORAL, *Idem*)

Da mesma forma, o Resumo Digital, ou *hash*, também feito por meio de criptografia, assemelha-se a um dígito verificador, que tem como função dos arquivos enviados por um conjunto de sistemas trabalhando em paralelo, em um algoritmo público, onde todas as pessoas podem ver as parciais das apurações de seus candidatos.(ELEITORAL, *Idem*)

Ecossistema das Urnas.

O funcionamento de uma Urna eletrônica é totalmente *off-line,* com diversas camadas de proteção. Essas camadas são físicas e não físicas. Por camadas físicas entende-se todos os tipos de lacres, vedos, e proteção de cabeamento da urna. Por camadas não físicas, também conhecido como ecossistema da urna, define-se pelo conjunto de programas autônomos entre si, cada um com sua função específica para que a urna funcione. Caso exista algum tipo de falha em qualquer um desses programas a urna para sua atuação no exato momento, mas os votos que até então foram computados não se perdem, uma vez que estão armazenados na memória física de cada urna, em seu chipset, uma espécie de caixa-preta. Após isso, são substituídas por urnas novas. (ELEITORAL, *Idem*)

Registro Digital do Voto.

Depois que o eleitor digita os números de seus candidatos e aperta o botão de confirma são gerados dois arquivos, o primeiro é destinado para o sistema que vai processar os dados totais e dar os resultados das eleições já o segundo, permanece armazenado dentro da própria urna, sendo emitido no final como comprovante de total de votos, vale lembrar que neste comprovante também faz-se uso da criptografia, uma vez que dentro da urna existe um sistema que embaralha o nome do eleitor e se interessa apenas no quantitativo de dígitos registrados iguais, ou mais detalhadamente, no quantitativo de votos que cada candidato deteve.(ELEITORAL, *Idem*)

Cerimônia de Assinatura Digital.

Antes das urnas serem lacradas, representantes dos partidos políticos, e da sociedade civil, são convidados para checarem os equipamentos e o processo de assinatura digital.(ELEITORAL, *Idem*)

Votação Paralela e Auditoria pela sociedade Civil.

Por votação paralela entende-se o ato de simular uma eleição previamente para constatar se todo o sistema está funcionando em harmonia, verifica-se também se o número digitado nas urnas, foram os mesmos computados e impressos nos boletins de final de expediente. A auditoria pela sociedade surgiu em 2018, trata- se de mais uma etapa de verificação dos equipamentos por setores da sociedade, antes do início da eleição, qualquer eleitor poder ser apto a ser auditor. (ELEITORAL, *Idem*)

Auditorias

Em 17 anos de utilização do sistema, inúmeras auditorias e perícias já foram realizadas, destacam-se as realizadas pela Unicamp em 2002, que concluiu que *"o sistema eletrônico de votação atende às exigências fundamentais do processo eleitoral, ou seja, o respeito à expressão do voto do eleitor e a garantia do seu sigilo".* e a da Polícia Federal de 2008 que em laudo técnico nas eleições municipais de Caxias (MA), descartou qualquer suspeita de fraude, ou enviesamento de dados das urnas.(ELEITORAL, *Idem*)

Também em 2008, o TSE contratou a Fundação de Apoio à Capacitação em Tecnologia da Informação (FACT) para prestação de serviços especializado e de suporte na especificação de programas para garantir ainda mais segurança ao sistema eletrônico brasileiro. Garantindo às urnas, características ergonômicas, de interferência eletromagnética e confiabilidade do *hardware,* gerando assim economia na compra de novas plataformas cada vez mais seguras. (ELEITORAL, *Idem*)

Testes de Segurança

Os testes de segurança são espécies de *hackathon* – Junção de *hackers* em um mesmo espaço físico para tentar hackear os sistemas de segurança de determinada empresa ou instituição, com objetivo de aperfeiçoá-los – demonstrando a importância dada pelo TSE ao melhoramento contínuo do sistema. (ELEITORAL, *Idem*)

Nas ocasiões os investigadores inscritos, em grupo ou individualmente, apresentam planos de ataque e os executam, concernentes a componentes externos e internos das urnas. No primeiro teste, em 2009, nenhum especialista conseguiu adentrar o sistema, entretanto as ideias apresentadas ali ajudaram o TSE a aperfeiçoá-lo, na segunda edição em 2012 e na Terceira edição em 2016, os especialistas tiveram acesso prévio ao código fonte. Já em 2017, dos 14 participantes dos testes, 10 conseguiram burlar

o sistema de alguma maneira, ajudando o TSE a ampliar a segurança cibernética de seu sistema de votação. (ELEITORAL, *Idem*)

Com a eficiência no melhoramento do processo com os testes, através da Resolução-TSE nº 23.444/2015, ficou determinado que os testes públicos de segurança sejam realizados antes de cada eleição ordinária, preferencialmente no segundo semestre dos anos que antecedem os pleitos eleitorais.(ELEITORAL, *Idem*)

Votação Paralela.

Os TREs designam um local após sorteio de duas a quatro urnas eletrônicas nas vésperas das eleições. A auditoria acontece simultaneamente à votação oficial sendo apresentada a verificação do funcionamento das urnas sorteadas. Anteriormente à votação, o mínimo de 500 cédulas é entregue aos representantes dos partidos políticos que comparecerão ao evento, que deverão preenchê-las e em seguida depositá-las em urnas de lona lacrada. A comissão de votação paralela deve estar atenta ao caso de algum partido não entregar todas as cédulas, neste momento será pedido que representantes de outros partidos preencham as cédulas restantes. Os participantes recolhem uma cédula da lona lacrada, revelam aos fiscais e demais presentes os candidatos escolhidos e em seguida digitar os números correspondentes no Sistema de Apoio a Votação Paralela e na Urna Eletrônica. Sendo todo o processo filmado e fiscalizado.(ELEITORAL, *Idem*)

Os objetivos da votação paralela são: I – Verificação de assinatura digital; II – Verificação de resumo digital; III – Comparação do resultado da votação por cédula com o resultado do boletim da urna; IV – Verificação da filmagem do procedimento e do registro do sistema e V – Verificação do registro digital do voto. (ELEITORAL, *Idem*)

Reflexões sobre o uso do Voto Impresso, suas Consequência e a Confiabilidade do Sistema Eletrônico de Votação.

Embora, costumeiramente, o Presidente Jair Bolsonaro venha batendo na tecla de que o voto impresso seria uma forma de garantir a confiabilidade das eleições brasileiras, um discurso mais político do que técnico, sua tese é respaldada por alguns cientistas políticos, que embora não defendam o voto impresso, assumem que não exista no Brasil uma maneira de se fazer um contrafactual, auditoria, acerca dos resultados obtidos na urna eletrônica.

Os autores deste artigo se colocam na ala contrária ao voto impresso, pelas inúmeras ineficiências que este pode trazer ao Sistema, já tão complexo, Eleitoral

Brasileiro. O sistema eleitoral brasileiro pode ser reconhecido como um dos mais avançados e seguros, devido ao desenvolvimento de softwares, que contém processos que vão do planejamento do TSE à integração do sistema. Destarte, através da técnica de projeções de cenário, citam-se em sequência, os seus argumentos dos autores acerca das desvantagens da implementação e do uso do voto impresso.

Aumento dos Gastos com Compra de Papel e Tinta pelo TSE.

De fato, o voto impresso já é inconstitucional, mas se fosse adotado aumentariam em alguns milhões de reais os custos totais com a votação, uma vez que cada voto demandaria a impressão e o uso de papéis e tintas para serem registrados. Devido também ao histórico de corrupção aderente à política brasileira, os retrocessos que podem vir a ser compactuados com o voto impresso, transmite uma insegurança tanto para os eleitores quanto para o próprio Sistema Eleitoral.

Falhas na Impressão dos votos e possíveis erros de dados registrados nos folhetins.

O voto impresso daria margem para que possíveis erros de impressão acontecessem, sendo essas cédulas invalidadas. Exemplificando, em um segundo turno em que o eleitor deve votar entre os números 11 e 17, que são muito parecidos em termos estéticos, qualquer falha de impressão nestes números fariam por exemplo que os eleitores que votaram no número 17, tenham seu voto impresso registrado o número 11, gerando ainda mais transtorno quando comparados aos números da urna eletrônica.

Dificuldades Logísticas de Deslocamentos e Contagem dos Votos.

Em uma República Federativa continental como o Brasil, cercada de cantões com densos vazios demográficos e regiões com difícil acesso de chegada, como seria o transporte desses votos impressos para cada Tribunal Regional Eleitoral (TRE), ou melhor, como todos esses votos impressos chegariam à Brasília? Teriam que sair comitivas de caminhões cercados de carros da polícia federal para deixarem os milhões de votos armazenados em algum lugar. Aumentando ainda mais os gastos com o sistema eleitoral. Além disso, a contagem dos votos impressos, demoraria deverás e custaria contratação de recursos humanos aos cofres públicos, além de deter uma margem de erro considerável, pois humanos são mais falhos do que computadores em atividades repetitivas.

Facilitação de Fraudes.

Ao contrário do que afirma o Presidente, com o voto impresso, ficará mais fácil fraudar o Sistema Eleitoral, uma vez que se abrange as possibilidades mecânicas de viagens dos dados. Imaginem que um grupo político consiga trocar um pacote de determinada zona eleitoral com votos impressos, com um resultado que beneficie o candidato que eles apoiem, ou que os caminhões que carreguem os votos sofram qualquer tipo de troca de malotes ou sejam até mesmo assaltados, roubando-lhes os votos. Como proceder nestas situações?

Aumento de pedidos de recontagem de votos, contestações do resultado de eleições e acúmulo de trabalho para um Judiciário que já caminha lento.

Com centenas de milhares de processos travados, o voto impresso, traria ainda mais demanda ao Judiciário, uma vez que vasta maioria dos partidos e candidatos derrotados recorreram ao TSE para tentar a recontagem dos votos impressos, gerando ineficácia, lentidão e acúmulo de trabalhos à justiça. Existiu em 2020, o caso de pedido de recontagem de votos do presidente Donald Trump, nos Estados Unidos em uma tentativa de reeleição, teve-se a confirmação da derrota, porém a o pedido de recontagem foi feito mais de uma vez, e então ratificou-se que:

> O estado no sudeste americano deu vitória ao presidente eleito Joe Biden. Porém, como a margem foi inferior a 0,5 ponto percentual, as cédulas foram contadas manualmente uma segunda vez. A nova contagem não viu mudanças significativas no resultado e manteve a vitória do democrata — que foi, inclusive, oficialmente certificada. (G1, 2020).

Dessa forma, se verifica problemáticas insurgentes da insegurança transmitida pelo voto impresso, além de que fere a própria noção de Estado democrático Brasileiro.

Estímulo ao Clientelismo, Coronelismo e Voto de Cabresto.

Chama-se em Ciência Política clientelismo, o fenômeno pelo qual os candidatos compram votos a seus eleitores, como se estes fossem seus clientes. Entretanto, a compra de voto não é garantia de que este candidato ganhará, tendo em vista que o voto é secreto, o eleitor pode pegar o dinheiro e votar em outro candidato, ou até mesmo nem ir votar. Com o voto impresso, a quebra do sigilo do voto ficaria em cheque, facilitando que os compradores de votos confiram quem, dos que foram pagos, realmente os votaram. Os mesmos argumentos são válidos para o coronelismo e para o voto de cabresto.

Entretanto, embora o sistema de votação brasileira seja, inviolável e não *"Hackeável"* como afirma o ministro Barroso, vislumbrou-se pós eleição, o acesso ao sistema do TSE, antes do primeiro turno, pelo grupo de *Crakers* portugueses denominados *CyberTeam*, cujo chefe corresponde pelo codinome *Zambrius*. Segundo, Barroso o episódio acontecera por motivação política para desacreditar o sistema eleitoral brasileiro, ainda sobre o episódio o ministro destacou que não houve acesso aos programas relativos às eleições de 2020, uma vez que as urnas não ficam conectadas à internet e a transmissão para a totalização dos votos é feita por uma rede própria do tribunal e o processo da soma é feito por um supercomputador exclusivamente dedicado a esse processo.

Todavia, uma máxima que existe na informática, é "Tudo pode ser decodificado, "hackeável" ou acessado, basta a pessoa que estiver tentado fazê-lo deter mais conhecimento do que a que está sendo vítima". Neste trabalho, utiliza-se dessa máxima para reafirmar a necessidade de investimentos ainda mais sisudos na área de cibernética, no que diz respeito ao sistema informatizado do TSE. Argumento ainda, que seja necessário uma aproximação maior do TSE com o Comando de Defesa Cibernética do Exército Brasileiro, ComDCiber, ligado ao gabinete de segurança institucional e por último, abrir para a participação de testes mais rotineiros em parcerias com universidades brasileira renomadas no assunto de segurança da informação, para uma constante evolução do código e possíveis alterações de segurança.

À Guisa de Conclusão

Desta forma, na revisão de literatura aponta-se a complexidade do Sistema Eleitoral Brasileiro, classificado por (NICOLAU, 2015) como Proporcional de Lista Aberta. Tamanho enredamento se dá pelas proporções da grandeza da democracia brasileira, inserida em um sistema federativo com 26 estados e um Distrito Federal. Outra importante variável nesse sistema está na divisão dos entes federativos, divididos entre União Estados e Munícipio.

Vislumbra-se, neste artigo, no jogo dos Poderes brasileiros um constante embate acerca da implementação do dispositivo de Voto Impresso. Denotando-se principalmente entre os embates de retórica do Presidente do Executivo para com o Presidente do Supremo Tribunal Eleitoral (TSE), autarquia do poder Judiciário.

Analisou-se nesse trabalho, as etapas estabelecidas pelo TSE, tanto em processos *offline* e *online* e estruturas de *softwares* e *hardwares*, a magnitude do Sistema de Votação

brasileira, demostrando sua funcionalidade, eficácia e aptidão para garantir aos Cidadãos Brasileiros Eleições Livres e Justas, no que concerne aos requisitos de *Cyber Security*. Enumerou-se I - O uso da criptografia; II - O Ecossistema das Urnas; III - O Registro Digital do Voto; IV - A Cerimônia de Assinatura Digital; V - A Votação Paralela e Auditoria pela sociedade Civil; VI As Auditorias; VII - Os Testes de Segurança e a VIII - A Votação Paralela, como principais argumentos para garantir a confiabilidade em termos de Segurança Cibernética do Sistema Eleitoral Vigente. Deste modo, responde-se com um sim! a pergunta de pesquisa supracitada neste artigo. "São as urnas de votação brasileiras, e consequentemente seu sistema eleitoral, seguros de ataques cibernéticos e/ou de crackers?"

Outrossim, assim como projetado pelos autores, o possível cenário da implementação do comprovante de votação, ou voto impresso, geraria transtornos logísticos, financeiros e democráticos ao atual sistema. Tais quais: I Aumento dos Gastos com Compra de Papel e Tinta pelo TSE; II - Falhas na Impressão dos votos e possíveis erros de dados registrados nos folhetins; III - Dificuldades Logísticas de Deslocamentos e Contagem dos Votos; IV - Facilitação de Fraudes; V- Aumento de pedidos de recontagem de votos, contestações do resultado de eleições e acúmulo de trabalho para um Judiciário que já caminha lento e V - Estímulo ao Clientelismo, Coronelismo e Voto de Cabresto. Destarte conclui-se como desnecessária, onerosa, infundada, impertinente, inoportuna e infeliz o argumento levantado pelo Presidente da República, de que o Comprovante de votação deixaria as eleições mais livres e justas. Ao contrário, com esta retórica o Presidente brasileiro faz um desvia o foco da opinião pública brasileira população brasileira, fazendo com que estes desconfiem de seu Sistema Eleitoral. Mais do que isso, o Presidente põe em *checkmate* o *Status* de Estado Democrático de Direito, garantido pela Carta Magna de 1988. Da mesma forma, concluímos que os arroubos de retórica levantados pelo Chefe do Executivo nesta questão, estão relacionados a sua estratégia política de reeleição, utilizado muitas vezes como "cortina de fumaça" em episódios está o Governo Federal está em desvantagem no jogo político.

Referências

APÓS derrota, Trump pede nova recontagem de votos na Geórgia. **G1.** 2020. Disponível em: https://g1.globo.com/mundo/eleicoes-nos-eua/2020/noticia/2020/11/22/apos-derrota-trump-pede-nova-recontagem-de-votos-na-georgia.ghtml. Acesso em: 02 mar. 2021.

BLAIS, André et al. Assessing the psychological and mechanical impact of electoral rules: A quasi-experiment. **Electoral Studies**, v. 31, n. 4, p. 829-837, 2012.

BOIX, Carles. Setting the rules of the game: the choice of electoral systems in advanced democracies. **American political science review**, v. 93, n. 3, p. 609-624, 1999.
BOLSONARO diz que só passa faixa presidencial com voto impresso. Estado de Minas, Minas Gerais, 01 de jul. de 2021. Disponível em : https://www.em.com.br/app/noticia/politica/2021/07/01/interna_politica,1282721/bolsonaro-diz-que-so-passa-faixa-presidencial-com-voto-impresso.shtml. Acesso em 01 de jul. de 2020
DUVERGER, Maurice. **Political parties: Their organization and activity in the modern state**. Metheun & Co. Ltd., 1959.
ELEIÇÕES/Urna eletrônica/Segurança, **Tribunal superior eleitoral**, Brasília, **[s.d.]** Disponível em: https://www.tse.jus.br/eleicoes/urna-eletronica/seguranca. Acesso em : 16 de dez. de 2020.
ELEITORAL, Brasil Tribunal Superior et al. **Eleições no Brasil:** uma história de 500 anos. 2014.
LIJPHART, Arend et al. **Modelos de democracia**. Planeta, 2003.
MARENCO, André. Reformas eleitorais na América Latina: grandes expectativas, poucos casos, resultados perversos. **Sociologias**, v. 14, p. 238-268, 2012.
NATHAN, Victor, Bolsonaro volta a defender voto impresso depois de votar no 2º turno do Rio. **Poder 360**, Rio de Janeiro, 29 de Nov. de 2020.Disponível em: https://www.poder360.com.br/governo/bolsonaro-volta- a-defender-voto-impresso-depois-de-votar-no-2o-turno-do-rio/. Acesso em: 13 de Dez. de 2020.
NICOLAU, Jairo. **Sistemas eleitorais**. Editora fgv, 2015.
PRESIDENTE do TSE diz que volta do voto impresso traria o caos às eleições. **Jovem Pan,** São Paulo, 29 de nov. de 2020. Disponível em:https://jovempan.com.br/noticias/politica/eleicoes-2020/presidente-do-tse-diz- que-volta-do-voto-impresso-traria-o-caos-as-eleicoes.html . Acesso em: 13 de Dez. de 2020.
SUSPEITO de ataque hacker ao sistema do TSE é preso em Portugal. **Uol**, Brasília, 28 de nov. de 2020. Disponível em: https://noticias.uol.com.br/eleicoes/2020/11/28/pf-ataque-hacker-sistema-do-tse.htm. Acesso em: 12 de dez. de 2020.
TSE- Mecanismos de segurança da urna eletrônica, **Tribunal superior eleitoral**, Brasília, **[s.d.]** Disponível em: https://www.tse.jus.br/videos/tse-mecanismos-de-seguranca-da-urna-eletronica. Acesso em : 13 de Dez. de 2020

Ciber Pandemonium: A Estratégia Chinesa de Utilização do Ciberespaço para Projeção de Poder Nacional (2010-2021)

Fernando Henrique Casalunga

Introdução

Este trabalho pretende analisar as vantagens estratégicas que a utilização do ciberespaço oferece aos Estados contemporâneos para projetação de poder no cenário internacional. Com intuito de identificar se este novo domínio de guerra contribui para um aumento da assimetria de poder entre os países, verifica seu emprego nas disputas regionais desencadeadas entre China e Índia (2010-2020). A fim de evidenciar como esse novo engenho de força tornou-se chave para a compreensão dos conflitos desencadeados neste século, intenta correlacionar as mudanças nos principais documentos oficiais que versam sobre a Política de Defesa e Segurança à complexidade das operações e sofisticação tática das principais ameaças cibernéticas utilizadas por forças convencionais e não-convencionais a serviço do Estado chinês.

Nesse ensejo, busca identificar se as condições que sustentam a projeção de poder nacional da China frente à Índia, resultam do funcionamento do mecanismo de ação tática coordenada entre a agência estatal e não-estatal, fator que reflete o processo de mudança na estratégia de atuação dos Estados contemporâneos em disputas regionais. Para tanto, utiliza a análise qualitativa, aplicando as técnicas de rastreamento de processos e dependência da trajetória, para responder ao seguinte questionamento: Por que a China utiliza o ciberespaço para conquistar seus objetivos estratégicos? A contribuição para os estudos de Defesa é marcada pela análise inovadora do impacto da tecnologia de informação na estratégia de ação dos Estados.

Na medida em que o avanço da tecnologia da informação impõe novos desafios aos Estados contemporâneos cresce a preocupação dos atores políticos e entidades privadas com questões concernentes à vulnerabilidade dos sistemas de informação. Este artigo procura compreender a estratégia de atuação da República Popular da China a partir da análise das vantagens que a utilização do ciberespaço oferece aos Estados contemporâneos para projetação de poder no cenário internacional.

Com especial atenção aos eventos que se sucederam após o embate na fronteira sino-indiana, onde se localiza o Vale de Galwan (2020), objetiva demonstrar a relevância do ciberespaço enquanto um novo engenho de força capaz de oferecer vantagens assimétricas aos Estados que se encontram na vanguarda do desenvolvimento da tecnologia da informação.

Para tanto, propõe identificar as principais ameaças cibernéticas à segurança da informação utilizadas nas operações levadas a cabo pela China contra os sistemas de tecnologia da informação da Índia, e, assim, identificar se a atuação conjunta de atores estatais e não-estatais é capaz de produzir sinergia para ampliar o poder nacional da China frente a um adversário regional.

A relevância do ciberespaço: o conflito sino-indiano (2020-2021)

Na medida em que os dois Estados mais populosos do globo, China e Índia, se desenvolvem, aumentam também suas ambições geoestratégicas para ampliar seus domínios regionais. Separados por uma zona de fronteira que se estende por 3.440km, esses gigantes estiveram envolvidos em disputas territoriais durante boa parte do século passado que só arrefeceram com a assinatura de um acordo, em 1996, o qual estabeleceu medidas de confiança para manutenção pacífica das áreas controladas pelos dois países.

No entanto, recentemente a escalada de tensão na região do Himalaia reavivou os embates, culminando em um confronto físico rudimentar desencadeado dentro do território indiano, numa área de entroncamento na zona fronteiriça do Vale de Galwan, em Ladakh, que se localiza ao longo do setor oeste da Linha de Controle Atual (LCA), perto de Aksai Chin, área reivindicada pela Índia, mas controlada pela China (BBC, 2020).

O território de Galwan é estratégico, pois é considerado o local de pouso para aeronaves militares mais alto do mundo, uma área com cumes de até 14.000 pés, na qual, em 2019, a Índia construiu uma estrada para conectar a base aérea militar reativada de Daulat beg Oldi à região de Ladakh, ampliando as capacidades de transporte de homens e materiais de modo eficaz e rápido em caso de conflito, a ação despertou a vigilância das forças chinesas (BBC, 2020)

O confronto que se iniciou na noite de 15 de junho de 2020 e ocasionou baixas entre soldados indianos e chineses, pode ser considerado o mais grave na fronteira terrestre instável mais longa do mundo em quase meio século. Embora, o número preciso dessas baixas permaneça sob escrutínio, é inegável que o retorno do conflito sino-indiano abalou as relações diplomáticas e econômicas entre esses Estados (THE PRINT, 2021).

Destarte, ambos os países tenham iniciado tratativas diplomáticas para reestabelecer as relações de confiança mútua na região, medidas coercitivas foram tomadas em diversos segmentos econômicos, dentre as quais, se destacam o banimento de mais de duzentos aplicativos de origem chinesa, sob alegação do governo de que

estariam sendo utilizados para coletar dados dos cidadãos indianos (RECORDED FUTURE, 2021).

A resposta chinesa foi dada no mesmo ano via ciberespaço, em 13 de outubro de 2020, com a invasão de *softwares* maliciosos na rede elétrica da Índia, o que causou danos ao sistema financeiro e de transporte ferroviário. Vinte milhões de indianos ficaram sem energia elétrica em suas casas, outros milhares foram impedidos de se locomover, além disso, geradores de emergência necessitaram ser ligados para garantir o funcionamento de energia nos hospitais em Mumbai (THE NEW YORK TIMES, 2021).

Em fevereiro de 2021, na medida em que as investidas cibernéticas da China sobre a Índia continuaram a ganhar relevo, um relatório do Insikt Group, publicado pela Record Future, identificou os agentes responsáveis pela série de operações de infiltração aos setores de infraestrutura crítica da Índia, sendo detectados *malwares* em quatro centros regionais de distribuição de energia e dois portos marítimos. De acordo com o relatório a operação foi conduzida pela Ameaça Persistente Avançada (APT) 41, também denominada RedEcho (RECORDED FUTURE, 2021).

A análise, realizada em conjunto com empresas especializadas em segurança cibernética, empregou técnicas de verificação de registro de domínio, tráfego de rede automatizadas e de componentes e código aberto, para identificar o modus operandi das ameaças e estabelecer a ligação entre a ação dos hackers e o governo chinês, revelando o envolvimento do Ministério de Segurança do Estado (MSE) e de departamentos ligados ao Exército de Libertação do Povo da China (PLA) (RECORDED FUTURE, 2021):

> [...] fomos capazes de determinar um padrão claro e consistente das organizações indianas visadas nesta campanha por meio do perfil comportamental do tráfego de rede para atingir a infraestrutura do adversário (RECORDED FUTURE, 2021).

O Relatório (2021) identificou que a APT41, especializada em espionagem cibernética, utilizou os malwares ‘PlugX’ e ‘ShadowPad’ para invadir sites do governo, setor público e organizações de defesa e do setor privado indianos, movendo-se lateralmente nesses sistemas por cerca de nove meses antes do ataque que comprometeu setores de comando e controle (C2) de infraestrutura crítica (RECORDED FUTURE, 2021). As ações via ciberespaço representam uma forte evidência das capacidades chinesas de utilização deste domínio para causar danos físicos, inéditas até então:

> [...] à medida que as tensões bilaterais continuam a aumentar, esperamos ver um aumento contínuo nas operações cibernéticas conduzidas por grupos vinculados à China, como a RedEcho, de acordo com os interesses estratégicos nacionais (INSIKT GROUP, 2021).

De acordo com artigo publicado pelo jornal norte americano The New York Times (2021), os ataques às instalações elétricas fizeram parte de uma campanha cibernética chinesa que serviu de alerta para os indianos sobre as capacidades de utilização do ciberespaço para conter as divergências territoriais entre os dois países. Embora, os analistas reconheçam que a ligação entre a interrupção de energia e o malware ainda não tenha sido comprovada por fontes oficiais, existem fortes evidências que apontam para o envolvimento da China neste evento. Razão pela qual, especialistas em segurança cibernética foram enfáticos ao afirmar:

> [...] a sinalização está sendo feita [pela China] para indicar que podemos e temos a capacidade de fazer isso em tempos de crise [...] é como enviar um aviso à Índia de que temos [chineses] essa capacidade" (THE NEW YORK TIMES, 2021).

A despeito de que ambos os Estados possam recorrer ao domínio cibernético em caso de conflito, as capacidades da China para utilizar este novo engenho de força provavelmente serão desproporcionalmente superiores às da Índia, em razão de que os *hardwares* utilizados no setor de energia indiano, bem como no sistema ferroviário, são de origem chinesa, fator que preocupa as autoridades indianas que após os ataques anunciaram a intenção de revisar os contratos de tecnologia da informação do país. Entretanto é pouco provável que conseguirão eliminar a dependência de tecnologia de sistemas estrangeira em um curto espaço de tempo (THE NEW YORK TIMES, 2021).

Por essa lógica, Estados que detêm o monopólio da produção e comercialização de tecnologias empregadas em sistemas operacionais de infraestrutura crítica obtêm larga vantagem no uso do ciberespaço para consecução de objetivos estratégicos em conflitos contemporâneos, uma vez que os ataques cibernéticos representam uma ação de menor potencial de impacto quando comparado, por exemplo, ao potencial destrutivo dos arsenais nucleares de que dispõem ambos os países.

Sem embargo, especialistas em segurança cibernética alegaram que as incursões da China contra alvos indianos cresceram exponencialmente no último ano, após o conflito no Vale de Galwan (REUTERS, 2021).

Senão vejamos, em dezembro de 2020, a Cyber Peace Foundation, verificou outra tentativa de ataque cibernéticos que utilizou spear phishing e-mails contendo informações sobre os feridos indianos no conflito do Vale de Galwan para subtrair senhas de acesso ao setor de energia, refinarias de petróleo e uma usina nuclear. As operações cibernéticas, provenientes do território chinês de Guangdong e Henan, foram atribuídas à organização Fang Xiao Qing, e, reportados como tentativa de infiltração para ataques disruptivos futuros (THE NEW YORK TIMES, 2021).

> Yashasvi Yadav, oficial de polícia encarregado da unidade de inteligência cibernética de Maharashtra, disse que as autoridades encontraram 'atividades suspeitas' que sugeriram a intervenção de um ator estatal [...] mas Yadav se recusou a entrar em detalhes, dizendo que o relatório completo da investigação seria divulgado em março [2021] [...] Até agora, o foco da China era o roubo de informações. Mas Pequim está cada vez mais ativa na inserção de códigos em sistemas de infraestrutura, sabendo que, quando descoberto, o medo de um ataque poder ser uma ferramenta tão poderosa quanto o próprio ataque (THE NEW YORK TIMES, 2021).

Já em 2021, outra ameaça vinculada à China, denominada APT10 ou Stone Panda/MenuPass, foi detectada tentando acessar as redes de infraestrutura de tecnologia da Informação da empresa Bharat Biotech e do instituto Serum da Índia (SII), em uma tentativa de obter dados de propriedade intelectual vinculada à produção da vacina AstraZeneca, desenvolvida para combater o novo coronavírus (COVID-19) (REUTERS, 2021).

As atividades cibernéticas da APT10 estavam sendo monitoradas há mais de uma década por empresas especializadas em cibersegurança (FIREEYE, 2017; CROWDSTRIKE, 2018; CYFIRMA 2020a; 2020b).

O relatório do FireEye (2017) indica que a presença do Stone Panda já havia sido registrada e estava sendo acompanhada desde o ano de 2009, sendo as operações do grupo associadas ao Ministério da Segurança de Estado (MSE) e ao Centro de Avaliação de Tecnologia da Informação (CNITSEC) da China (CROWDSTRIKE, 2018).

De acordo com o Relatório (2017), as operações cibernéticas tinham por objetivo coletar informações militares e de inteligência, bem como subtrair dados comerciais, que pudessem contribuir com o desenvolvimento tecnológico das forças armadas e corporações chinesas. Dentre os principais alvos atingidos inicialmente, figuravam empresas de construção e engenharia aeroespacial, telecomunicações e instituições dos governos norte americano, europeu e japonês. Contudo, em 2016, as operações ganharam

maior visibilidade e se expandiram, atingindo setores de tecnologia da informação em diversos países, incluindo empresas de manufatura da Índia (FIREEYE, 2017).

As principais armas cibernéticas identificadas para invasão dos sistemas foram o 'Haymaker' e o 'Snugride' utilizados na primeira fase de intrusão e o 'Bugjuice' e 'QuasarRat' na segunda fase de aquisição, por fim, o 'SOGU' na terceira fase, trata-se de *backdoors* altamente sofisticados que demandam forte investimento para seu desenvolvimento, fator que indica a presença de um ente com alta capacidade de empregar recursos em sua construção (FYREEYE, 2017).

O modus operandi da Stone Panda inclui ataques *spear phising* e o uso de provedores de serviços globais para acesso às redes de sistemas corporativos operados pelas vítimas. De tal modo que ao se movimentar lateralmente pelos sistemas infectados, mediante o estabelecimento da comunicação entre servidores de Comando e Controle (C2) das vítimas e do provedor de serviços remoto, utilizado como um 'proxy' para instalação dos malwares, o grupo obtém acesso a dados confidenciais sem que possa ser detectado, tática que serve para mascarar a ameaça e permitir o roubo das informações (FYREEYE, 2017).

No que tange a ligação entre a Stone Panda e o Estado da China, o relatório publicado pela Crowdstrike (2018) corroborou a veracidade das informações publicados pelo blog anônimo 'Intrusion Truth', que expôs imagens fotográficas, de satélite, e, recibos de aplicativos de transporte, mostrando dois hackers associados ao grupo viajando regularmente para o complexo do MSE, em Tianjin, como evidências da ligação entre as instituições chinesas e esses hackers (CROWDSTRIKE, 2018; FCW, 2018). De acordo com Adam Meyers, vice-presidente de inteligência da Crowdstrike, os dados publicados pelo 'Intrusion Truth', combinados com a pesquisa do instituto revelaram evidências confiáveis da ação conjunta entre os hackers e o governo chinês:

> [...] embora pesquisadores e governos suspeitem há muito tempo que o Stone Panda está ligado à China, evidências que ligam membros do grupo de hackers a um escritório de campo específico do Ministério de Segurança do Estado chinês podem permitir que os legisladores decretem sanções criminais, diplomáticas ou econômicas contra Pequim (FCW, 2018, p ?).

Outros dois relatórios publicados pelo Cyfirma (2020a; 2020b) reforçam o envolvimento entre o governo chinês e os hackers em operações de ciberespionagem contra a Índia. O primeiro (2020a) descreve as ações cibernéticas do Stone Panda para subtrair dados comerciais e informações sobre cadeia de suprimentos de empresas

indianas; o segundo, (2020b) identifica uma série de tentativas de invasão aos sistemas de informação de setores diversos (automotivo, aviação, educação, energia, finanças, saúde, manufatura de alta tecnologia, produtos farmacêuticos e telecomunicações) de adversários comerciais, sendo as redes corporativas indianas alvo de tentativa de extração de dados de propriedade intelectual vinculadas a projetos de Pesquisa e Desenvolvimento de tecnologia com alto valor agregado (CYFIRMA, 2020a; 2020b).

Há pelo menos uma década as atividades de espionagem cibernética da China envolvendo atores não-estatais privados e órgãos institucionais vem sendo motivo de preocupação da comunidade internacional de segurança. Nesse ensejo, em 2016, o setor de inteligência do Pentágono norte americano reportou uma possível ligação entre empresas de segurança cibernética e o serviço de inteligência do Ministério de Segurança do Estado (MSE) da China em operações de espionagem cibernética (THE WASHINGTON FREE BEACON, 2016).

O Documento (2016) indica que as operações cibernéticas tinham como objetivo favorecer empresas chinesas do setor de telecomunicações que atuam como vetores para produção de produtos de segurança alta tecnologia de uso dual que seriam empregados no setor privado e pelas forças militares chinesas (THE WASHINGTON FREE BEACON, 2016). As suspeitas do governo norte americano foram comprovadas no ano seguinte por analistas do Insikt Group em relatório publicado pelo Recorded Future (2017) que estabelece com algo grau de confiança, a primeira ligação entre uma Ameaça Persistente Avançada (APT) e um órgão institucional do Estado chinês atuando em conjunto com setores empresariais.

A denominada APT3, também conhecida como Gothic Panda/TG-011/UPS, vinha sendo monitorada desde 2010, e, foi atribuída ao Ministério da Segurança do Estado (MSE) da China em associação com a empresa Boyu Information Technology Company (Boyusec), localizada em Ghanzhou. Em 2015 a Boyusec e o escritório de segurança da informação da China criaram um laboratório conjunto para teste de softwares para desenvolvimento de defesas cibernéticas (THE WASHINGTON FREE BEACON, 2016). A diretoria de inteligência J-2 do Estado-Maior Conjunto do Pentágono afirmou:

> Boyusec e Huawei estão trabalhando juntos para produzir produtos de segurança que serão carregados em computadores e equipamentos telefônicos de fabricação chinesa. Os produtos adulterados permitirão que a inteligência chinesa capture dados e controle computadores e equipamentos de telecomunicações (THE WASHINGTON FREE BEACON, 2016).

O Relatório (2017) revela que a Boyusec atua em parceria com a Huawei Technologies e a rede nacional de centros de avaliação de segurança Guangdong Information Technology Security Evaluation Center (Ghangdong ITSEC) sendo este administrado pelo China Information Technology Evaluation Center (CNITSEC), instituição vinculada ao MSE, responsável pelo desenvolvimento de produtos de defesa desde e comandar operações de inteligência cibernética desde 2014 (RECORDED FUTURE, 2017).

Nesse ensejo, o Relatório (2017) revela uma forte ligação entre instituições governamentais chinesas, a Boyusec e suas parceiras com as operações da Gothic Panda, um modelo de ação orquestrado pelo Estado da China para mobilizar agentes não-estatais em missões de espionagem cibernética que serviram de cobertura para as operações de inteligência do MSE (RECORDED FUTURE, 2017).

No que toca às táticas de infiltração utilizadas, de acordo com o relatório publicado pelo FireEye (2015), dentre as armas cibernéticas atribuídas à Gothic Panda durante as operações, verificam-se técnicas de invasão tradicionais via spear phishings e ferramentas de acesso remoto (RAT), bem como o uso de ferramentas mais sofisticadas capazes de causar ataques de ‘zero-day’ atingindo empresas do setor de defesa, transporte, alta tecnologia, telecomunicações e departamentos governamentais em diversos países ao redor do mundo.

Ao acessar os e-mails, as vítimas eram redirecionadas para um servidor com ‘scripts’ de criação de perfil em modelo ‘Java’ que continha arquivos maliciosos em formato Adobe Flash Player (SWF) e de Flash Video (FLV) carregados com um ‘backdoor’ chamado ‘ShotPut’. O relatório aprofunda os detalhes técnicos das táticas de intrusão empregadas, uma vez que o sistema esteja infectado os hackers o exploram lateralmente para conseguir as informações que procuram, então, em um segundo momento, utilizam ‘backdoors’ para descartar as credenciais de acesso adquiridas movendo-se para hosts adicionais, instalando novos ‘backdoors’ personalizados, o uso de uma robusta infraestrutura de comando e controle (C2) torna seu rastreio de difícil identificação (FIREEYE, 2015).

Desde 2009, o Pentágono já havia publicado relatórios apontando para a ligação entre a Huawei e as forças armadas da China (PLA) na área de pesquisa e desenvolvimento (P&D). Dois anos depois, a agência central de inteligência norte americana (CIA) revelou que o presidente da empresa Sun Yafang era funcionário do departamento de comunicações do MSE, sendo o responsável por estabelecer a ligação

entre o serviço de inteligência chinês e a Huawei (THE WASHINGTON FREE BEACON, 2016).

Frente a essa conjuntura, analistas indicam que existe um padrão no uso por Estados como China e Rússia de empresas de segurança cibernética como fachada para coleta de inteligência, de modo que softwares de segurança para redes de controle industrial poderiam ser criados com vulnerabilidades cibernéticas específicas que possam ser utilizadas em momentos oportunos de modo estratégico por esses Estados (THE WASHINGTON FREE BEACON, 2016).

Conclusões Parciais

A pesquisa, ainda em estágio exploratório inicial, procurou coletar evidências que corroborem a relevância do ciberespaço para compreensão dos conflitos contemporâneos mediante ao rastreamento das operações cibernéticas e dos efeitos causados no mundo físico por Ameaças Persistentes Avançadas (APT). Foram identificadas três delas: RedEcho (APT41), Stone Panda (APT10) e Gothic Panda (AP3), bem como alguns *softwares* maliciosos utilizados em ataques aos sistemas de informação da Índia.

Ao explorarmos como a China utiliza o ciberespaço enquanto novo engenho de força para consecução de seus objetivos estratégicos, utilizamos fontes jornalísticas, relatórios produzidos por instituições governamentais e empresas especializadas em segurança cibernética que permitiram verificar uma forte relação entre atores estatais e não-estatais do setor privado atuando para produção de força sinérgica capaz de oferecer vantagens à República Popular da China em confrontos regionais como o desencadeado contra a Índia (2020-21).

De modo parcial, em razão de nossos achados, podemos admitir com alguma segurança analítica que as possibilidades de uso do ciberespaço para aquisição de informação sigilosa ou mesmo para infligir danos físicos às infraestruturas críticas por potências como a China parecem crescer exponencialmente, facilitadas, no caso da Índia, em função de que grande parte dos hardwares utilizados nos sistemas de informação tem origem chinesa. Por essa lógica, é bem provável que os chineses continuem a utilizar este domínio para obter vantagens estratégicas sobre seus adversários regionais.

Até o momento, acreditamos ser plausível sustentar a tese de que Estados detentores de monopólio na produção e comercialização de tecnologias empregadas em sistemas operacionais de infraestrutura crítica podem obter larga vantagem estratégica ao

fazer uso do ciberespaço para consecução de objetivos regionais em conflitos contemporâneos.

Uma das razões do porquê atuam dessa forma, questionamento central do artigo, parece residir na ideia de que ataques cibernéticos representem uma ação de menor potencial de impacto se comparado, por exemplo, ao potencial destrutivo dos arsenais nucleares de que dispõem os Estados contemporâneos como Índia e China, mas possuem um alto potencial para dissuadir o inimigo a tomar determinadas ações coercitivas sejam políticas ou econômicas em função da possibilidade de colocar em risco a segurança nacional de setores críticos fundamentais para a sociedade, aparentemente o ciber pandemonium continuará intrigando a comunidade internacional durante este século.

Referências

BBC. Galwan Valley: China and India clash on freezing and inhospitable battlefield. Jun. 2020. Disponível em https://theprint.in/defence/4-9-or-14-even-china-isnt-sure-how-many-pla-soldiers-died-in-galwan-valley/613372/. Acesso em 15.03.2021.

CROWDSTRIKE. Two Birds, One Stone Panda. Ago. 2018 Disponível em https://www.crowdstrike.com/blog/two-birds-one-stone-panda/. Acesso em 08.09.2019.

CYFIRMAb. RISING CYBER ATTACKS DUE TO CHINA-INDIA BORDER CONFLICT Jun. 2020. Disponível em https://www.cyfirma.com/early-warning/rising-cyber-attacks-due-to-china-india-border-conflict/. Acesso em 13.07.2020.

CYFIRMAa. Cyber espionage and the Asia Threat Landscape. Set. 2018. Disponível em https://www.cyfirma.com/news/cyber-espionage-and-the-asia-threat-landscape/ Acesso em 02.09.2019.

FCW. Chinese hacker group targets tech supply chain, report says. Set. 2018. Disponível em https://fcw.com/articles/2018/08/31/china-supply-chain-hack.aspx. Acesso em 10.09.2019.

FIREEYE. APT10 (MenuPass Group): New Tools, Global Campaign Latest Manifestation of Longstanding Threat. Abr. 2017. Disponível em https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html Acesso em 26.08.2019.

RECORDED FUTURE. Recorded Future research concludes Chinese Ministry of State Security Behind APT3. Mai. 2017. Disponível em https://www.recordedfuture.com/chinese-mss-behind-apt3/. Acesso em 20.08.2019.

RECORDED FUTURE. China-lined Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions. Fev. 2021. Disponível em https://www.recordedfuture.com/redecho-targeting-indian-power-sector/. Acesso em 02.03.2021.

REUTERS. Chinese hackers target Indian vaccine makers SII, Bharat Biotech, says security firm. Mar. 2021. Disponível em https://www.reuters.com/article/health-coronavirus-india-china-idINKCN2AT21O. Acesso em 09.03.2021.

THE NEW YORK TIMES. China Appears to Warn India: Push Too Hard and the Lights Could go out. Fev. 2021. Disponível em https://www.nytimes.com/2021/02/28/us/politics/china-india-hacking-electricity.html Acesso em 04.03.2021.

THE WASHINGTON FREE BEACON. Pentagon Links Chinese Cyber Security Firm to Beijin Spy Service. Nov. 2016. Disponível em https://freebeacon.com/national-security/pentagon-links-chinese-cyber-security-firm-beijing-spy-service/. Acesso em 08.08.2019.
THE PRINT. 4, 9 or 14? Even China ‘isn’t sure’ how many PLA soldiers died in Galwan Valley. Mar. 2021. Disponível em https://theprint.in/defence/4-9-or-14-even-china-isnt-sure-how-many-pla-soldiers-died-in-galwan-valley/613372/. Acesso em 12.03.2021.

2. Resumo Expandido

Letalidade dos recursos cibernéticos diante de conflitos no ciberespaço

Jéssica Maria Grassi
Danielle Jacon Ayres Pinto

O ciberespaço tem passado por um processo de securitização - e, até mesmo, militarização - sendo considerado um novo domínio para a ocorrência de guerras. No entanto, há divergências entre os pesquisadores quanto à existência ou possibilidades de ocorrência de uma guerra cibernética, bem como no que diz respeito à proposição de que essa nova modalidade de guerra seria menos violenta ou letal. Isso ocorre, em grande parte, pela falta de definições objetivas ou consensuais dos termos que envolvem o ciberespaço, já que existe uma complexa lista de conceitos que permeiam o contexto cibernético. Nessa perspectiva, existem diferentes definições de guerra cibernética, resultando em diferentes graus de abrangência e a utilização frequentemente confusa do termo, como sinônimo de qualquer ato de invasão hacker ou ataque a redes de computadores.

No entanto, propor a definição de guerra cibernética exige a retomada e compreensão dos elementos que caracterizam a ocorrência de guerras. Clausewitz (2010) é autor central na discussão sobre a definição da guerra, uma vez que - apesar de sua teoria ter sido construída um século antes do surgimento do ciberespaço - as proposições do autor ainda parecem ser essenciais na análise dos conflitos contemporâneos. Clausewitz (2010) apontava que, para a caracterização de uma guerra, três fatores devem ser observados concomitantemente: 1) o caráter violento; 2) o caráter instrumental; e 3) a natureza política.

Ao discutir sobre as possibilidades de ocorrência de uma guerra cibernética nesses termos, Rid (2012) afirma que nenhuma ação cibernética ofensiva até hoje congregou esses três fatores simultaneamente e argumenta que ciberataques não tem o potencial de letalidade. Portanto, a tendência não seria a realização de uma guerra autônoma no ciberespaço, com o código como a arma principal, porém, tendo em vista que a última década testemunhou atos cada vez mais sofisticados de sabotagem, espionagem e subversão através do ciberespaço, essas ações podem apoiar operações militares, sendo utilizadas como ferramentas auxiliares (RID, 2012). Por outro lado, Stone (2013) o

contra-argumenta afirmando que, apesar de ainda não ter ocorrido, é possível que uma ciberguerra venha a ocorrer no futuro, divergindo de Rid (2012) principalmente na proposição de violência deste último, uma vez que afirma que Clausewitz (2010) não conecta a ideia da força física ou a violência da guerra com a letalidade, como o faz Rid (2012).

Convergimos com a proposição sobre a baixa probabilidade de uma guerra autônoma vir a ocorrer no ciberespaço, porém os recursos cibernéticos estão sendo e serão utilizados, conjuntamente com ferramentas cinéticas, em operações de guerra. Defendemos, contudo, ser equivocada a argumentação de que ataques cibernéticos não tem potencial de causar violência física ou letalidade. Nessa perspectiva, e independente do impasse acerca da possibilidade de uma ciberguerra vir ou não a ocorrer, cabe perguntar se ataques cibernéticos têm ou não o potencial de causar grande força física ou violência, ou ainda, se possuem o potencial de causar letalidade. Isso porque, mesmo que não provoquem violências diretamente às pessoas - e sim às infraestruturas -, ataques cibernéticos, como a sabotagem cibernética, podem causar danos efetivamente sérios às sociedades e aos Estados, os quais podem ser compreendidos como atos de força física ou violência. Sobre isso, Stone (2013) ressalta que a tecnologia, de forma particularmente eficiente, pode fazer com que pequenas quantidades de força se traduzam em grandes quantidades de violência.

Partindo dessa lógica, ataques cibernéticos poderiam vir a provocar perdas de vidas humanas. Duas considerações podem ser postas diante dessa asserção. Primeiro, deve-se levar em consideração que o espaço cibernético possui, entre suas particularidades, a característica da transversalidade, ou seja, permite a projeção de poder e seus reflexos nos demais domínios espaciais (FERREIRA NETO, 2014). Em segundo lugar, importa mencionar a impossibilidade de dimensionar os efeitos e as consequências de um ciberataque; ou seja, por um lado, este pode não surtir o resultado desejado por parte do agressor ou, por outro lado, trazer danos muito maiores do que os previstos inicialmente. Da mesma forma, há dificuldades por parte do país atacado de indicar os danos causados e, frequentemente, até mesmo identificar que está sofrendo um ataque (MARQUES, 2018; MEDEIROS; GOLDONI, 2020).

Ataques cibernéticos têm sido direcionados a infraestruturas críticas e podem ter um efeito cascata – ou seja, uma operação cibernética contra um sistema específico pode ter repercussões em outros sistemas, paralisando vários serviços essenciais –, causando danos reais às populações civis. Importa refletir também sobre a eventualidade de ataques

cibernéticos serem realizados em locais que, em condições de guerra tradicional, seriam proibidos pelas legislações internacionais , como a hospitais (MARQUES, 2018; RODENHÄUSER; MAČÁK, 2021). Ataques também poderiam ser efetuados contra sistemas de tráfego aéreo, deixando centenas de aviões voando sem comunicação, ou em sistemas de usinas nucleares, que poderiam levar à perda de resfriamento, derretimento e contaminação ou explosão (RID, 2012) - e o Stuxnet foi um importante exemplo do nível alcançado por uma sabotagem cibernética.

Assim, é um paradoxo ainda pouco claro se podemos utilizar de forma efetiva o conceito de guerra cibernética para determinar a conflitualidade que hoje ocorre no mundo virtual, todavia, é fato que as práticas lesivas nesse espaço podem, dependendo do teor e alcance do ataque, produzir uma letalidade indireta, onde o resultado do dano causado a uma determinada infraestrutura crítica pode reverberar em violência e até morte de indivíduos. Porém, quando pensamos em letalidade direta, nos parece que o meio digital é um recurso acessório, um meio para comandar recursos tradicionais (cinéticos) que produzem violência e letalidade, mas não um fator central para a produção do efeito lesivo e letal do ataque.

Referências

CLAUSEWITZ, Carl Von. Da guerra. 3. ed. [S.l.]: Martins Fontes WMF, 2010.
FERNANDES, José Pedro Teixeira. A ciberguerra como nova dimensão de conflitos do século XXI. Relações Internacionais, v. 33, p. 17, 2012.
FERREIRA NETO, Walfredo Bento. Territorializando o “Novo” e (Re)territorializando os Tradicionais: a Cibernética como Espaço e Recurso de Poder. Revista das Ciências Militares, Coleção Meira Mattos, v. 31, n. 8, p. 07–18, 2014.
MARQUES, Rafael. O ambiente cibernético e o direito internacional dos conflitos armados: uma proposta de adequação doutrinária. Doutrina Militar Terrestre em Revista, v. 1, n. 15, p. 6–19, 2018. Disponível em: <http://ebrevistas.eb.mil.br/index.php/DMT/article/view/1811>.
MEDEIROS, Breno Pauli; GOLDONI, Luiz Rogério Franco. The Fundamental Conceptual Trinity of Cyberspace. Contexto Internacional, v. 42, n. 1, p. 31–54, 2020.
RID, Thomas. Cyber War Will Not Take Place. Journal of Strategic Studies, v. 35, n. 1, p. 5–32, 2012.
RODENHÄUSER, Tilman e MAČÁK, Kubo. Even ‘cyber wars’ have limits. But what if they didn’t? EJIL: Talk! - Blog of European Journal of International Law, 2021. Disponível em: <https://www.ejiltalk.org/even-cyber-wars-have-limits-but-what-if-they-didnt/?utm_source=mailpoet&utm_medium=email&utm_campaign=ejil-talk-n…>. Acesso em: 12 jun 2021.
STONE, John. Cyber War Will Take Place! Journal of Strategic Studies, v. 36, n. 1, p. 101–108, 2013.