Centro Universitário de Brasília - UniCEUB
Faculdade de Ciências Jurídicas e Sociais - FAJS
Curso de Bacharelado em Direito / Relações Internacionais

JACY MAGALHÃES

ESPAÇO CIBERNÉTICO E A NOVA ESPIONAGEM: ANÁLISE DAS POLÍTICAS PÚBLICAS E A CAPACIDADE DEFENSIVA DO BRASIL

BRASÍLIA
2020

Centro Universitário de Brasília - UniCEUB
Faculdade de Ciências Jurídicas e Sociais - FAJS
Curso de Bacharelado em Direito / Relações Internacionais

JACY MAGALHÃES

ESPAÇO CIBERNÉTICO E A NOVA ESPIONAGEM: ANÁLISE DAS POLÍTICAS PÚBLICAS E A CAPACIDADE DEFENSIVA DO BRASIL

Relatório final de pesquisa de Iniciação apresentado à Assessoria de Pós-Graduação e Pesquisa

Orientação: Lucas Soares Portela

BRASÍLIA
2020

RESUMO

O presente trabalho busca investigar os meios de projeção de poder no espaço cibernético e como é explorado; assim como o seu impacto na política do sistema internacional. Essa pesquisa irá analisar os impactos do escândalo de espionagem de 2013 na política pública brasileira daquela época. Assim como considerar as formas de conexão e informação, legítimas ou não. No desenvolvimento do trabalho serão analisados impactos das políticas públicas brasileiras que tratam da defesa cibernética sobre as atividades de espionagem cibernética do século XXI, por meio de uma revisão histórica da evolução da espionagem da Guerra Fria até os dias atuais e análises dos impactos do espaço cibernético sobre as atividades de espionagem. Assim como entender as distinções das atividades de inteligência e espionagem, com ênfase em meios informais de coleta de informação, como as distâncias e embaixadas. Identificar, nas políticas públicas brasileiras para a segurança e defesa cibernéticas, pontos de mitigação das atividades de espionagem e avaliar o impacto da revelação de atividades de espionagem cibernética nas políticas públicas brasileiras.

Palavras-Chaves: ciberespaço; Brasil; fake news; espionagem cibernética.

SUMÁRIO

1 INTRODUÇÃO

A preocupação com a Segurança é uma prioridade de todos os Estados (STADNIK, 2017, p. 129), especialmente quando se trata do crescente avanço tecnológico dos dias atuais, o que permite um grande avanço das indústrias voltadas para a defesa nacional. Essa "insegurança" percebida ultrapassa o ator estatal, atingindo também atores não-estatais, inclusive indivíduos. Isso tornou-se mais crítico com a evolução das Tecnologias das Informações e Comunicações (TICs) e a difusão do poder para esses atores não estatais por meio do espaço cibernético.

A revolução na forma de se obter informações e fazer conexões facilitou a vida de muitas pessoas (físicas ou jurídicas) e a internet se tornou uma extensão na forma de se projetar poder, de se fazer política, de uma empresa expandir seus negócios e de uma pessoa mudar sua vida social. Mas, por outro lado, acabou tornando as coisas mais complexas no cenário internacional, já que não tem um regime internacional que governe o espaço cibernético (STADNIK, 2017, p. 130).

Para o Brasil, a situação não é muito diferente. A nossa política e capacidade de defesa não pode se manter estática perante as rápidas mudanças do espaço virtual. Por esse motivo, após as denúncias de Edward Snowden (2013) do maior escândalo de espionagem da história, o Brasil, assim como outros países, se viu com vulnerabilidades em sua capacidade de defesa e sua soberania afetada. O que agravou ainda mais a situação foi que, além da vulnerabilidade na defesa nacional, a sociedade civil brasileira se viu à mercê de um grande esquema de espionagem que violava seu direito à privacidade. Embora aparenta ser algo pontual, a espionagem cibernética pode apresentar diferentes vestimentas e se utiliza de diversos instrumentos, como a injeção de informações falsas, por meio da chamada "Fake News".

2 DA ESPIONAGEM À ATIVIDADE DE INTELIGÊNCIA

A distinção entre os conceitos de espionagem e inteligência permite uma clareza sobre a compreensão da influência do espaço cibernético na prática dessas atividades. Isso requer uma

abordagem inicial desses termos para compreensão e propósito deste artigo. Para Dra. Ursula M. Wilder (2017), psicóloga e ex-funcionária da Agência Central de Inteligência[1] (CIA) espionagem pode ser definida como uma prática na qual pessoas, chamadas de espiões, secretamente entregam informações sigilosas sobre um grupo no qual os mesmos trabalham, disfarçadamente, com o objetivo de coletar dados.

> Espiões engajados em espionagem para entregar, secretamente, informações sigilosas a um grupo que o espião acredita estar trabalhando diretamente contra o seu próprio país. Normalmente, isso envolve um intermediário - um manipulador - que geralmente é um Oficial de serviços de inteligência treinado em gerenciar agentes de maneira segura e produtiva. O objetivo de um intermediário é manter o espião indetectável e transferir informações secretas. Por questões de segurança e veracidade, os oficiais de inteligência raramente lidam com fontes anônimas por um longo período. (WILDER, 2017, p. 2) [tradução nossa].[2]

Um outro ponto de vista interessante sobre a espionagem se encontra na definição de Kevin Mitnick (2001), conhecido mundialmente como um hacker estadunidense, que conceituou espionagem como “habilidade de manipular pessoas para obter informações”. Ou seja, pode-se também inferir que a atividade de espionagem seria a “arte de enganar” (MITNICK, 2001).

A espionagem é uma prática antiga e, mesmo assim, há limitação de leis internacionais específicas em relação a ela (NYE, 2014). Mesmo que antiga, ainda hoje essa atividade possui a capacidade de afetar Estados soberanos, empresas e organizações internacionais. A baixa sensibilidade quanto a sua existência ocorre em virtude dessa atividade ter impulsionado e aprofundado algumas guerras e conflitos, com alto custo de vidas humanas. Assim, o termo espionagem é hoje observado como uma trapaça, já que não permite ao espionado um direito de se defender de forma digna.

---

[1] Central Intelligence Agency

[2] Spies engaged in espionage secretly deliver classified information to a party the spy understands is working directly against his or her own country. This typically involves an intermediary—a handler—who usually is a foreign intelligence service officer trained in managing agents safely and productively. The aim of a handler is to keep the spy undetected and the transfer of information ongoing and secret. For reasons of security and veracity, professional intelligence officers rarely handle anonymous sources for long periods. (WILDER, 2017, p. 2)

Chamamos atenção ainda a fala de Wilder (2017) que insere uma atividade de suporte a espionagem, chamada de inteligência. Enquanto espionagem é considerada uma prática “antiética” e “ilegal”, a inteligência é reconhecida como uma atividade moralmente aceita. A inteligência pode ser definida como uma forma de obter informações e dados convenientes que possam fornecer vantagens, por um meio legal, ético e controlado, como explica Eugênio Moretzsohn (2018).

Dessa forma, há atualmente uma “aparente” desvinculação entre espionagem e inteligência. De forma legítima, o agente de inteligência, antes um intermediário da atividade, busca por meio de outros meios adquirir as informações que antes eram fornecidas pelos espiões, principalmente por meio de observações. Entretanto, seria imprudente tomar como verdade o fim da atividade de espionagem, já que tal conclusão evidencia, por si só, a atividade fim do intermediário em manter o espião indetectável.

O que se percebe é que as atuais agências de inteligência não mais dependem apenas do espião, mas utilizam de suas organizações para conseguir contatos e informações. A globalização permite uma transação de informações de grande fluxo sem uma amplitude restrita de espaço, ou seja, a captação da informação está mais facilitada pelas TICs, rompendo um pouco com a dependência de uma agente espião de campo. Dessa forma, não há uma extinção da atividade de espionagem, mas um redesenho diante dessas novas tecnologias.

No século anterior, principalmente durante a Guerra Fria, o objetivo da espionagem era a coleta de informações sobre a capacidade militar do inimigo. Quanto maior o número de informações obtidas sobre o inimigo, maior seria a vantagem (LLEWELLYN; THOMPSON, 2018). As informações, em sua maioria, eram obtidas por meio de atos de espionagem, ou seja, por grampos telefônicos, aparelhos de vigilância, documentos roubados e agentes duplos (LLEWELLYN; THOMPSON, 2018). Além disso, a atividade de espionagem não se limitava a coleta de informação, podendo também englobar missões de assassinato, sabotagem, sequestro, roubos etc. Missões essas, delegadas por agências dedicadas exclusivamente à inteligência (LLEWELLYN; THOMPSON, 2018).

Por ser considerada ilegal e antiética, a espionagem não só coloca Estados em uma situação de vulnerabilidade, mas a própria sociedade civil fica à mercê desse jogo de coleta de

informações e tem seu direito de liberdade violado. O cenário dos anos 1945 a 1991 representava o medo e incerteza das pessoas, causados pelo próprio Estado nacional ou por um Estado rival, do qual as mesmas escolheram sacrificar a própria liberdade por qualquer garantia de segurança.

Independente do objetivo que essas missões atribuíam a seus agentes, o foco central das atividades de espionagem eram as informações. Por exemplo, a neutralização de uma figura poderia ser uma forma de se "queimar arquivo", ou seja, eliminar a fonte de uma informação, evitando sua propagação. No mesmo sentido, o assassinato de uma pessoa poderia permitir o acesso a uma informação que até então era restrita.

Assim, as informações possuem importância e finalidade (DRUCKER, 1996), o que se diferencia dos dados brutos, que apenas fazem parte da informação, mas que apenas representam algo de forma isolado. Quando coletados e organizados propriamente dentro de um contexto, esses dados ganham relevância e se tornam uma informação (MCGEE; PRUZAK, 1995, p. 24). A compilação desses dados dentro informação que pode ser utilizada para moldar uma tomada de decisão também foi impactada com a evolução tecnológica, tornando a quantidade de dados processados maior em um menor tempo. Tal evolução também contribuiu para que a coleta fosse realizada por meios cada vez mais anônimos, como no espaço cibernético.

Por exemplo, em 2013, a NSA foi acusada de coordenar operações de inteligência para adquirir informações sigilosas, por meio de ex-diretores e especialistas da Petrobrás, sobre segredos industriais que fosse de interesse dos Estados Unidos. Inclusive, tecnologias sobre perfuração de petróleo em alto mar. As informações eram muito vantajosas para a competitividade das companhias de petróleo estadunidenses e de seus parceiros comerciais.

Tal ação não seria percebida se não fosse pelas revelações de Edward Snowden, ex-funcionário da NSA. Ele denunciou esse e outros atos de espionagem, o que impactou todo o cenário internacional. Após o estouro desse escândalo, o diretor de inteligência nacional, James Clapper, disse que não era um segredo o fato de que a comunidade de inteligência coleta informações sobre economia e assuntos financeiros, e financiamentos de terrorismo (WATTS, THE GUARDIAN, 2013):

> Quando se trata de coleta de inteligência intencionalmente, nosso foco é o combate ao terrorismo, armas de destruição em massa, ciberterrorismo - principal interesse dos Estados Unidos. Eu posso garantir para a população da Europa e ao redor do mundo que nós não saímos bisbilhotando os e-mails ou escutando os telefonemas das pessoas. Estamos focando em áreas específicas que nos preocupam. Barack Obama (WATTS, 2013) (tradução nossa).[3]

A possibilidade de espionar por meio do espaço cibernético é um resultado da sua incessante evolução. Apesar dos incontáveis benefícios que todas as áreas adquirem com esse ambiente, sua evolução também aumenta fragilidades, ao permitir mais pontos de coletas de informações por meio dos seus usuários. A falsa sensação de segurança que o ambiente cibernético causa no usuário, que imagina estar seguro atrás da tela do computador, pode ser explorada pelos espiões cibernéticos para obter informações adicionais, como por exemplo, fotos de uma área privada e estratégia, sem a necessidade de infiltração presencial.

Além disso, a quebra de barreiras e diminuição das fronteiras, por meio da globalização, redesenhou o cenário internacional. Ainda que com benefícios e maravilhas incontáveis, aumentou a imprevisibilidade das políticas frente ao surgimento de novos atores nesse novo cenário político internacional do século XXI. Devido a contribuição tecnológica para a disseminação de informações, os Estados deixaram se ser os principais detentores do controle de informações e como as mesmas são repassadas para o resto do mundo, inclusive pelos ciber espiões, que por sua vez, não somente coletam as informações como também podem fazer injeção de informações para manipular uma questão.

3 ESPIONAGEM E A PROJEÇÃO DE PODER

Como explicado, a prática de, secretamente, coletar dados e fornecer informações sigilosas sobre um grupo para outro, é conhecida como espionagem; e possui suas origens no

[3] "When it comes to intelligence gathering internationally, our focus is on counter terrorism, weapons of mass destruction, cybersecurity – core national interest of the United States, I can give assurances to the publics in Europe and around the world that we are not going around snooping at peoples emails or listening to phone calls. We are targeting very specifically areas of concern." Barack Obama (THE GUARDIAN, 2013)

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 da humanidade, 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).

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.

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):

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 [4](O controle de supervisão e aquisição de dados) **Soft**: Campanha de diplomacia

[4] Supervisory Control And Data Acquisition

		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

Nye considera três faces/aspectos nas relações de poder, na hora de analisar a configuração de poder no espaço cibernético (NYE, 2010, p. 7). Segue, abaixo uma tabela com explicações e exemplos:

Quadro - Três Faces do Poder no Espaço Cibernético

1ª Face	O poder de fazer com que outros se portem ou façam algo que eles inicialmente não planejavam fazer. Por meio do *Soft Power*, é visto como um um ato de persuasão de um indivíduo (jurídico ou físico) em relação ao comportamento do outro (NYE, 2010, p. 7). "***A** induz **B** a fazer o que **B** inicialmente não faria de outra forma*" **Hard Power**: ataques de negação de serviço, inserção de malware, interrupções SCADA, prisões de blogueiros. **Soft Powe**r: campanha de informação para mudar as preferências iniciais dos hackers, recrutamento de membros de organizações terroristas
2ª Face	É o poder que um ator tem de impedir as escolhas de outro, eliminando suas estratégias. Caso essa exclusão seja algo forçado e contra a vontade de outro agente, é um aspecto do *hard power*; caso aceita de forma persuasiva e/ou legítima, é um aspecto de *soft power* (NYE, 2010, p. 8). "***Controle de agenda**: **A** impede a escolha de **B** por exclusão das estratégias de **B***" **Hard Power**: firewalls, filtros e pressão sobre as empresas para excluir algumas ideias. **Soft Power**: ISPs [5](Código Internacional para Segurança de Navios e Instalações

[5] International Ship and Port Facility Security Code.

	Portuárias) e mecanismos de pesquisa auto monitoram, regras da ICANN[6] (Corporação da Internet para Atribuição de Nomes e Números) sobre nomes de domínio, padrões de software amplamente aceitos.
3ª Face	Trata-se de um indivíduo (jurídico ou físico) que influencia e/ou molda os planos iniciais de outro para que algumas estratégias nem mesmo sejam consideradas (NYE, 2010, p. 8). "***A*** *modela as preferências de* ***B*** *para que algumas estratégias nunca sejam consideradas*" **Hard Power**: ameaças de punir blogueiros que disseminam material censurado. **Soft Power**: informações para criar preferências (por exemplo, estimular o nacionalismo e "*hackers patrióticos*", desenvolver normas de repulsa (por exemplo, pornografia infantil)

Fonte: Elaboração própria baseada em Nye (2010).

4 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

[6] Internet Corporation for Assigned Names and Numbers

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 1.1 – 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 Eletrônica de Defesa do Ministério da Defesa, 2004).	Guerra sem território, que pode acontecer em qualquer espaço do globo sem que atinja, necessariamente, um espaço físico. Repercute em todas as áreas - econômica, bélica, política e psicológica (LESSA et. alli, 2002).	Confronto que busca a coleta de informações. Ou seja, através dos meios de inteligência, quem conseguir maior quantidade de informações (relevantes para as 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.

5 FAKE NEWS COMO ABERTURA À ESPIONAGEM CIBERNÉTICA

A espionagem não pode ser limitada apenas em "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.

6 CONSIDERAÇÕES FINAIS

As revelações de Snowden fizeram com que o sistema internacional voltasse os olhos para o espaço cibernético e que essa agenda ganhasse cada vez mais relevância. O que evidenciou ainda mais a necessidade da cooperação internacional para a segurança cibernética, por meio de tratados, acordos e políticas de informação para a sociedade civil.

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.

REFERENCIAL BIBLIOGRÁFICO

BRASIL, Congresso Nacional. Senado Federal. **Brasil é 2º no mundo em perdas por ataques cibernéticos, aponta audiência**. Seção: Notícias - Matérias. 05 set 2019. Disponível em <https://www12.senado.leg.br/noticias/materias/2019/09/05/brasil-e-2o-no-mundo-em-perdas-por-ataques-ciberneticos-aponta-audiencia> Acessado em 8 abr 2020.

DRUCKER, Peter. **Administrando em tempos de grandes mudanças**. 4 ed. São Paulo: Pioneira, 1996.

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.

INTITUTE FOR INFORMATION LAW. **A crises of Accountability:** a global analysis of the impact of the Snowden revelations. Bruxelas: Privacy Surgeon, 2014. Disponível <http://www.privacysurgeon.org/blog/wp content/uploads/2014/06/Snowden-final-report-for-publication.pdf> Acessado em 06 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.

LLEWELYN, Jennifer; THOMPSON, Steve. **Cold War espionage**. Alpha History, Austrália, 22 set 2018. Disponível em: <https://alphahistory.com/coldwar/espionage/>. Acesso em: 05 out 2019.

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

McGEE, T.; PRUSAK, L. **Gerenciamento estratégico da informação**. Rio de Janeiro: Campus, 1995

MENDES, Pricilla. Relatório final da CPI da Espionagem aponta que o Brasil está vulnerável. **G1**. Seção: Política. 09 abr 2014. Disponível em <http://g1.globo.com/politica/noticia/2014/04/relatorio-final-da-cpi-da-espionagem-aponta-que-brasil-esta-vulneravel.html> Acessado em 31 mar 2019.

Ministério da Defesa. **Política de Guerra Eletrônica de Defesa**. Brasil: 2004. Disponível em <https://www.defesa.gov.br/arquivos/File/legislacao/emcfa/publicacoes/md32_p_01_polguerraeletrdef_1a_ed_2004.pdf>. Acessado em 13 out 2019.

MITNICK, Kevin; SIMON William L. **A Arte de Enganar**. Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação. São Paulo: Pearson Education do Brasil Ltda, 2003.

MORETZSOHN, Eugênio. **Técnicas de Contraespionagem para a Proteção de Projetos em Tecnologias Inovadoras.** Palestra para Abepro. Rio de Janeiro: ABEPRO, 2018.

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.

PARKS, Raymon C.; DUGGAN, David P. **Principles of Cyber-warfare**. Proceedings of the IEEE Workshop on Information Assurance, West Point, NY, p 122 – 125, 2001.

RIVER, Charles. **A KGB: A História e Legado da Notória Agência de Espionagem da União Soviética**. Charles River Editors, 17 de dez. 2018. Disponível em <https://www.academia.edu/38935685/A_KGB_A_Hist%C3%B3ria_e_Legado_da_Not%C3%B3ria_Ag%C3%AAncia_de_Espionagem_da_Uni%C3%A3o_Sovi%C3%A9tica_Por_Charles_River_Editors_Emblema_da_KGB> Acessado em 18 nov 2019.

SNOWDEN, Edward. **Edward Snowden's 'open letter to the Brazilian people'** – in full. **The Guardian**. Seção: World – Americas. 17 dec 2013. Disponível em < https://www.theguardian.com/world/2013/dec/17/edward-snowden-letter-brazilian-people > Acessado em 19 abr 2019

STADNIK, Ilona. **What is an international cybersecurity regime and how can we achieve it?** República Tcheca: Masaryk University, 2017. Disponível em < https://journals.muni.cz/mujlt/article/view/6483/6401 > Acessado em 15 abr 2019.

VALENTE, Jonas. Especialistas discutem necessidade de lei para crimes cibernéticos. **Agência Brasil**. 25 abr 2018. Disponível em <http://agenciabrasil.ebc.com.br/justica/noticia/2018-

04/especialistas-discutem-necessidade-de- ei-para-crimes-ciberneticos> Acessado em 20 abr 2019.

WATTS, JONATHAN. **NSA accused of spying on Brazilian oil company Petrobras**. The Guardian. World. Reino Unido. 2013. Disponível em <https://www.theguardian.com/world/2013/sep/09/nsa-spying-brazil-oil-petrobras>. Acessado em 12 out 2019.

WILDER, Ursula M. **The Psychology of Espionage and Leaking in the Digital Age**. Estados Unidos: Studies in Intelligence vol 61, CIA, 2017. Disponível em <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-61-no-2/pdfs/why-spy-why-leak.pdf> .