UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS V - MINISTRO ALCIDES CARNEIRO
CENTRO DE CIÊNCIAS BIOLÓGICAS E SOCIAIS APLICADAS
CURSO DE RELAÇÕES INTERNACIONAIS

ALYNE RAYANNA DE SOUSA SALVADOR DA SILVA

CYBERSECURITY: A NOVA CONFIGURAÇÃO DE PODER NAS RELAÇÕES INTERNACIONAIS APÓS O CASO EDWARD SNOWDEN (2000-2018)

JOÃO PESSOA
2019

ALYNE RAYANNA DE SOUSA SALVADOR DA SILVA

CYBERSECURITY: A NOVA CONFIGURAÇÃO DE PODER NAS RELAÇÕES INTERNACIONAIS APÓS O CASO EDWARD SNOWDEN (2000-2018)

Trabalho de Conclusão de Curso apresentado ao Programa de Graduação da Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de Bacharel em Relações Internacionais.

Área de concentração: Política Externa.

Orientadora: Prof. Dra. Cristina Pacheco.

JOÃO PESSOA
2019

S586c Silva, Alyne Rayanna de Sousa Salvador da.

Cybersecurity [manuscrito] : a nova configuração de poder nas relações internacionais após o caso Edward Snowden (2000-2018) / Alyne Rayanna de Sousa Salvador da Silva. - 2019.

44 p. : il. colorido.

Digitado.

Trabalho de Conclusão de Curso (Graduação em Relações Internacionais) - Universidade Estadual da Paraíba, Centro de Ciências Biológicas e Sociais Aplicadas , 2019.

"Orientação : Profa. Dra. Cristina Carvalho Pacheco , Coordenação do Curso de Relações Internacionais - CCBSA."

1. Snowden. 2. Cibersecurity. 3. Relações russo-americanas. 4. Política cibernética. I. Título

21. ed. CDD 658.472

Elaborada por Elesbao S. Neto - CRB - 15/347 BSC5/UEPB

ALYNE RAYANNA DE SOUSA SALVADOR DA SILVA

CYBERSECURITY: A NOVA CONFIGURAÇÃO DE PODER NAS RELAÇÕES INTERNACIONAIS APÓS O CASO EDWARD SNOWDEN (2000-2018).

Monografia apresentada ao Curso de Relações Internacionais da Universidade Estadual da Paraíba.

Aprovado(a) em 25 / 04 / 2019.

Cristina Carvalho Pacheco /UEPB
Orientador(a)

Paulo Roberto Loyola Kuhlmann /UEPB
Examinador(a)

Fábio Rodrigo Ferreira Nobre/UEPB
Examinador(a)

A minha mãe, pela dedicação, amor, paciência,
companheirismo e zelo, DEDICO.

AGRADECIMENTOS

Eu sempre soube o que queria cursar, mas no dia que essa escolha chegou eu acabei não optando por ela. Nesse meio tempo, eu caí de paraquedas em um curso que eu não tinha a menor ideia do que se tratava, quais seriam as disciplinas lecionadas e principalmente, não passava pela minha cabeça como seria encarar essa nova realidade. Eu comecei a cursar Relações Internacionais em março de 2015 sem nem saber quais passos deveria dar, mas se concluo essa etapa hoje é porque pude contar com o apoio de várias pessoas, graças a Deus, a minha família e aos meus amigos pude chegar até aqui.

Dessa maneira, gostaria de agradecer a Universidade Estadual da Paraíba – UEPB, pele oportunidade de crescimento dentro da academia, em especial a professora Luiza Rosa B. de Lima, pela oportunidade de fazer parte do Programa Institucional de Bolsas de Iniciação Científica (PIBIC) e agregar ainda mais conhecimentos e valores; a professora Monica de Lourdes N. Santana, por acreditar em mim desde o quarto período e me convidar para ser a bolsista do Programa de Concessão de Bolsas de Extensão (PROBEX); e por último e não menos importante, a minha orientadora Cristina C. Pacheco por ter toda calma, paciência e leveza para comigo ao longo das orientações e por todo conhecimento compartilhado não só no âmbito acadêmico, mas conhecimentos para a vida.

Ademais, agradeço às pessoas que significam tudo em minha vida, que é a minha família, todos os que fazem parte do *Fat Family,* meus tios-irmãos Alice Salvador e Edilson Salvador, que sempre cuidaram de mim e puderam me ensinar o melhor, meus irmãos, Allana Dayanna e Alan Thyago que mesmo sendo como cão e rato, somos unidos, a minha tia Fidelina Albuquerque pelas palavras sábias, aos meus primos Anderson Meneses e Júnior Pires, por cada riso que me proporcionaram sem perceber. Em especial agradeço a minha mãe Sônia Maria, que é o meu tudo, me deu suporte, foi a minha fortaleza durante esses anos e nunca mediu esforços para dar o melhor para os seus filhos, a minha tia-irmã, Michelle Alice, por ser parte dessa conquista e sempre me incentivar e cuidar de mim, e a minha sobrinha, Ayla Maria, que é tão pequena e apesar de ainda não compreender esse universo foi capaz de me transmitir força e luz ao longo dessa jornada. Agradeço imensamente a vocês!

Minha gratidão aos meus colegas de classe e aqueles que conheci ao logo desses anos pelos momentos de amizade, apoio, diversão e companheirismo. Meu muito obrigada

à Rayssa Macena, Maria Beatriz, Heloísa Brito, Emilly Alves, Lídia Cavalcanti, Zé Luiz, Ananda Dourado, Ana Maura, Jerônimo Nóbrega, Ana Caroline, Maiko Gomes, Karla Sabryna, Dani Soares e um agradecimento especial para Gildércia Araújo, por ser como uma irmã mais velha, me apoiar, buscar sempre me aconselhar da melhor forma possível e sempre topar qualquer aventura; Paulo César, obrigada por ter estado comigo desde o Programa Youth@IGF, em 2015, e mesmo sem se conhecermos direito o interesse pela Cibersegurança permitiu que fôssemos amigos hoje.

As minhas amigas, Larissa, Jarbely e Mayara eu não tenho palavras suficientes que possam representar o que vocês foram/ fizeram/ representam para mim, vocês são os presentes que Deus me deu e espero preservar sempre essa amizade. Mayara, você foi uma irmã durante esses anos, partilhamos momentos, passamos por situações fortes e apesar de todas as brigas nossa amizade prevaleceu, obrigada!

Por último, gostaria de agradecer aos meus amigos *Os Gordinhos*, Laiz Cristina e Felipe Artur, por sempre terem estado comigo e por aprendermos a superar a distância do Norte e até mesmo de algumas horas até Alagoa Grande. Obrigada por sempre terem a pizza pronta quando chegava o final de semana, pelos momentos que precisávamos da força um do outro e por serem uma verdade pra abraçar pra sempre.

Agradeço a todos que fizeram e fazem parte da minha vida, que direta ou indiretamente contribuíram para o meu sucesso e meu crescimento pessoal, amo vocês!

"I don't want to live in a world where everything that I say, everything I do, everyone I talk to, every expression of creativity, or love, or friendship is recorded (…)".

Edward Snowden

SUMÁRIO

CYBERSECURITY: A NOVA CONFIGURAÇÃO DE PODER NAS RELAÇÕES INTERNACIONAIS APÓS O CASO EDWARD SNOWDEN (2000-2018)

Alyne Rayanna de Sousa Salvador da Silva[1]

RESUMO

O presente trabalho de conclusão de curso tem como objetivo geral avaliar como a cibersegurança tornou-se estratégia política dos Estados Unidos e da Rússia. Tendo em vista o advento da tecnologia no século XXI, torna-se necessário analisar como as relações internacionais foram afetadas por esse recurso, principalmente no que tange os problemas de política externa, como será analisado entre os Estados Unidos e a Rússia após o Caso Edward Snowden, uma vez que, o primeiro se refere ao país no qual Snowden foi um analista de sistemas da *Central Intelligence Agency* (CIA) e da *National Security Agency* (NSA) e o segundo corresponde ao país que ofereceu asilo ao ex-agente. Assim, pretende responder a problemática: Como as relações entre os Estados Unidos e a Federação Russa foram afetadas após o Caso Edward Snowden no período de 2013-2018? O trabalho foca nos objetivos específicos: i) Analisar o advento das tecnologias digitais voltando-se para as Relações Internacionais; ii) Verificar as políticas de Cybersecurity dos Estados Unidos e da Rússia no período de 2012-2018 e iii) Explorar os impactos nas relações entre os Estados Unidos e a Federação Russa após o asilo concedido a Edward Snowden. Logo, parte-se da hipótese de quanto maior for o advento da tecnologia, menor a estabilidade entre as relações dos Estados. Portanto, a pesquisa possui um caráter exploratório e a metodologia empregada é qualitativa utilizando de referencial teórico bibliográfico de periódicos especializados e documentos de segurança dos EUA e da Rússia.

Palavras-Chave: Snowden. Cibersecurity. Relações Russo-Americanas. Políticas Cibernéticas.

1 INTRODUÇÃO

Este artigo tem como proposta analisar as políticas de segurança cibernética dos Estados Unidos e da Rússia em decorrência do Caso Snowden em 2013. O estudo tem como guia a pergunta-problema: Como as relações entre os Estados Unidos e a Federação Russa foram afetadas após o Caso Edward Snowden no período de 2012-2018? Essa pergunta parte da premissa de que as relações russo-americanas foram afetadas pelo fato do primeiro referir-se ao país no qual Snowden foi um analista de sistemas da *Central Intelligence Agency* (CIA) e da *National Security Agency* (NSA) e o segundo corresponder ao país que ofereceu asilo ao ex-agente.

[1] Aluna de Graduação em Relações Internacionais na Universidade Estadual da Paraíba – CAMPUS V
E-mail: alyne.rayanna@gmail.com

Diante das mudanças causadas pelos avanços da tecnologia, os atores das relações internacionais têm a necessidade de adaptação para continuarem inseridos nesse novo sistema. Isso porque a tecnologia digital mudou a maneira como as empresas conduzem os negócios, como os indivíduos conduzem as relações sociais, as Forças Armadas conduzem suas estratégias de defesa e também como os Estados conduzem a governança interna e sua política externa (BJOLA; HOLMES, 2015).

Desta forma, é necessário que os Estados promovam políticas estratégicas de cibersegurança para proteção da sociedade e de suas instituições. Isso se deve ao fato de que o espaço cibernético desafia conceitos tradicionais, entre eles o de fronteiras geopolíticas ou mesmo organizacionais, constituindo um novo território, ainda inóspito, a ser desbravado pelos bandeirantes do século XXI (CARVALHO, 2016).

Diante do exposto, o objetivo geral desse trabalho consiste em avaliar como a cibersegurança tornou-se estratégia política dos Estados Unidos e da Rússia, buscando assim, verificar qual o impacto do Caso Snowden na relação entre as partes. Fazendo uso de uma pesquisa com caráter exploratório e metodologia qualitativa, utilizou-se de um referencial teórico bibliográfico, periódicos especializados e documentos de segurança dos EUA e da Rússia.

A fim de facilitar a compreensão da problemática, o trabalho estrutura-se em três partes: a primeira é teórica, e volta-se à apresentação do aparato conceitual e causal de como a tecnologia pode atribuir poder nas Relações Internacionais. A segunda seção trabalha com um aspecto descritivo do contexto que cerca a implementação das medidas estratégicas dos Estados Unidos e da Rússia a partir de documentos referentes à segurança cibernética. Na terceira seção, a pesquisa volta-se para a análise das relações entre os EUA e a Rússia após o asilo político obtido por Snowden.

2 TECNOLOGIA, PODER E RELAÇÕES INTERNACIONAIS

A Internet emergiu no contexto da Guerra Fria na década de 1960, a partir de um projeto do exército norte-americano, os principais propósitos eram: criar um sistema de informação e comunicação em rede que sobrevivesse a um ataque nuclear e dinamizar a troca de informações entre os centros de produção científica. Os militares pensaram que um único centro de computação centralizando toda informação era mais vulnerável a um ataque nuclear do que vários pontos conectados em rede, pois assim a informação estaria espalhada por inúmeros centros computacionais pelo país (GILES, 2010).

Na análise de Kohn e Moraes (2007), a sociedade do início do séc. XXI transita no que é qualificado como Era Digital, na qual os computadores ocupam espaços importantes na conjuntura atual em todos os setores da sociedade, sejam eles, comercial, política, serviços, entretenimento, informação e/ou relacionamentos. Logo, as transformações sociais estão diretamente ligadas às transformações tecnológicas das quais a sociedade se apropria para se desenvolver e se manter.

O espaço cibernético é um terreno no qual funciona a humanidade, hoje. É a instauração de uma rede de todas as memórias informatizadas e de todos os computadores. Com o espaço cibernético tem-se uma ferramenta de comunicação muito diferente da mídia clássica, porque é nesse espaço que todas as mensagens se tornam interativas, ganham espaço, e permitem maior transmissão da informação e têm uma possibilidade de metamorfose imediata, devido ao compartilhamento das informações (LEVY, 1994, p. 38).

A Internet e o computador passam a ser o suporte e o motor de uma cultura-mundo, e a conexão das pessoas, através das redes permite a comunicação além dos continentes, é possível além fronteiras "mostrar-se e ver-se pelos blogs e pela *webcam*, criar, vender, trocar, até mesmo inventar para si uma *second life*" (LIPOVETSKY, 2011, p.76). A própria cultura passa a se estabelecer através de um reino virtual tecnológico, em que as atividades humanas, das mais simples às mais complexas, são remodeladas e influenciadas pelas novas tecnologias e pela internet (LIPOVETSKY, 2011).

Qualquer informação pode ser obtida instantaneamente e de qualquer parte do mundo, a visibilidade dos fatos se tornou maior e mais rápida, na qual os dados são atualizados a todo segundo. Lévy (1993) expõe que a interface digital alarga o campo do visível, evidenciando a emergente evolução que diversificou, facilitou e transmitiu as informações de forma instantânea e ampla.

Na análise de Recuero (2012, p. 146) "um dos problemas mais comuns do contexto da internet é a fronteira entre o público e o privado". Em redes sociais, por exemplo, como o Facebook, muitos usuários sentem-se inseguros no que se refere a sua privacidade e intimidade, com medo de interferências na vida profissional, ou até mesmo de serem vítimas de alguma violência que as informações contidas no seu perfil online possam acarretar (ROSA; SANTOS, 2013).

A era da informação não proporcionou apenas transformações sociais, mas também reconfigurou as relações entre as nações, seja através de pagamento de licenças de uso, *royalties, leasing* ou o simples acesso, a aquisição e distribuição da informação têm implicações do ponto de vista do poder (SILVEIRA, 2000).

Segundo Matta (1980, p. 291), a informação está estreitamente vinculada à idéia de independência, quer seja econômica ou política. Observa-se um agravamento dos desníveis entre os países a partir da detenção de direitos intelectuais sobre tecnologias e da apropriação do conhecimento, por meio do controle do acesso à informação.

Na era da informação, as infraestruturas de redes e dados fazem parte do repertório de questões estratégicas (ibidem), constituindo, talvez, um novo *front* (LOPES; TEIXEIRA JR, 2010), pois, a informação é um produto importante no campo de batalha e até mesmo fora dela. Logo, Sheldon (2011) corrobora que é necessário se repensar estratégias cibernética com a finalidade de criar vantagens e influenciar eventos dentro de seu desenvolvimento operacional e por meio das estruturas tradicionais de poder.

Desta forma, é importante compreender que o papel da tecnologia atualmente está diretamente ligado a ideia de poder, uma vez que países com tal característica reforçam, por meio do uso combinado de forças convencionais e cibernéticas, seu *status quo* na estrutura de poder regional ou global (SHELDON, 2011).

2.1 Poder e Tecnologia: reconfiguração das Relações Internacionais

Max Weber (1999, p.33) apresenta um clássico conceito de poder ao asseverar que: "poder significa toda probabilidade de impor a vontade numa relação social, mesmo contra resistências, seja qual for o fundamento dessa probabilidade". Ou melhor, é a probabilidade de que uma ordem com um determinado conteúdo específico seja seguida por um dado grupo de pessoas. Segundo Bobbio (1996, p. 171), o poder classifica-se conforme o meio empregado para a sua manifestação, assim, existe o poder "econômico", cujo meio é a riqueza; o poder "ideológico", cuja moeda é o saber; e o poder "político", que se vale da força como último recurso para sua manifestação.

A evolução tecnológica preponderante a partir da segunda metade do século XX coaduna problemáticas de ordem política, econômica e social, ao passo que reordena as dinâmicas de poder no cenário internacional. O avanço da tecnologia e seus desdobramentos estimula a reflexão do papel do Estado como ator preponderante no sistema internacional, tal como a intensa atuação de atores não-estatais estratégicos e interessados, como as empresas transnacionais, na ampliação de mercados e investimentos nesse setor (ROCHA, 2017).

De acordo com Malik (2012, p. 4), a tecnologia é um dos fatores mais determinantes de interação entre as nações, ao lado das guerras e das mudanças econômicas. Por se tratar de um instrumento fundamental na promoção do desenvolvimento econômico e mais recentemente de forma pujante na segurança nacional, a tecnologia fundamentou a revolução

industrial e, desde então, vem exercendo sua influência e, em certa medida, hierarquizando as Nações.

Há uma correlação direta entre o *status,* o qual representar poder, de um país na hierarquia global e suas capacidades em termos tecnológicos. Todavia, a intenção, a forma e o ritmo de mudança da tecnologia nunca são uniformes, muitas das vezes, propositalmente. Dessa forma, adotar e/ou investir antecipadamente em novas tecnologias pode conferir novo status num futuro não tão distante. Stefan Fritsch (2014) enfatiza:

> Em um mundo globalizado, o acesso à tecnologia e a negação da tecnologia desempenham papéis-chave na determinação do destino das nações. As nações competem ou elevando-se a níveis mais altos de desempenho técnico-econômico ou mantendo os outros para baixo, tecnológica e economicamente. As nações tecnologicamente avançadas também desfrutam do poder de estabelecer as normas e padrões de comportamento na política internacional. As grandes potências, em particular, competem ferozmente para manter seu status de cão superior por meio de sua vantagem tecnológica. A maioria dos empreendimentos de alta tecnologia é impulsionada pela busca nacional competitiva de manter a superioridade tecnológica sobre os outros. (FRITSCH, 2014, p. 120)[2]

Apesar do impacto tecnológico gerado nas relações internacionais, o papel do Estado é fundamental como ator e agente dinamizador e estratégico. Ainda que não haja uma convergência entre os interesses e agendas dos atores internacionais, o campo tecnológico causa maior aproximação entre eles, devido ao caráter sensível e variado da tecnologia que reúne aspectos político-estratégicos, mas também, econômicos e comerciais que interessam fortemente ambos os lados (ROCHA, 2017).

Na análise de Weiss (2005, p.14), as Tecnologias da Informação e Comunicação (TIC), classificam-se por meio de quatro mecanismos: I) Influência na arquitetura do sistema internacional (SI), sua estrutura e organização; II) Alteração dos processos pelo quais o SI opera, como, a diplomacia, administração, política, guerra, finanças e outros; III) Criação de novas áreas temáticas, novas restrições no ambiente econômico, de política externa e restrições políticas no sistema internacional; e IV) Proporciona novas fontes de percepções, segurança, transmissão de informação tanto no funcionamento do sistema em si, quanto na criação de conceitos e ideias nas teorias das relações internacionais.

[2] In a globalized world, technology access and technology denial play key roles in determining the fate of nations. Nations compete either by raising themselves to higher levels of techno-economic performance or by keeping others down, technologically and economically. Technologically advanced nations also enjoy the power to set the norms and standards of behavior in international politics. Great powers, in particular, compete ferociously to maintain their top dog status through their edge in technology. Most high-tech developments are driven by the competitive national quest to maintain the technological superiority over others.

Diante de tais dimensões, é preciso lidar não apenas com os aspectos da informação de Estados, mas também com a garantia da segurança de sistemas, os quais têm como objetivo garantir a (SHAKARIAN; SHAKARIAN; RUEF, 2013, p. 7):

i) disponibilidade, a qual se refere ao fato das redes estarem aptas a ser utilizadas, ou seja, estão disponíveis aos usuários;

ii) integridade refere-se ao funcionamento sem interferências externas;

iii) confidencialidade se refere ao sigilo das informações, resguardando a privacidade dos usuários sem que terceiros as obtenham;

iv) autenticação se refere ao sigilo das informações, resguardando a privacidade dos usuários sem que terceiros as obtenham e o;

v) não repúdio, e que refere-se à garantia de que o remetente dos dados é fornecido com comprovante de entrega e o destinatário é fornecido com prova da identidade do remetente.

O poder está passando de "rico em capital" para "rico em informação". A informação está se tornando mais e mais abundante, mas a versatilidade de agir primeiro sobre nova informação é rara. A informação torna-se poder, especialmente depois que se espalha. Desse modo, a capacidade de resposta em tempo hábil à nova informação é um recurso de poder crítico. Com o aumento de uma economia baseada em informação, matérias-primas têm se tornado menos importantes, enquanto habilidades de organização e flexibilidade ocupam cada vez mais importância no cenário atual (NYE, 1990, p. 75).

A tecnologia é um vetor pioneiro nas relações internacionais, dessa forma é importante um planejamento estratégico dessa fonte de poder, uma vez que é evidente que o fator tecnológico é fonte e instrumento de poder nos acordos geopolíticos e uma variável determinante na hierarquia global (ROCHA, 2016). Logo, a cibersegurança coloca a informação como uma importante fonte de poder na contemporaneidade, o ciberespaço ganha fôlego na agenda internacional ao se transformar em um importante vetor para fins políticos e estratégicos de atores estatais e não-estatais (CEPIK; CANABARRO; BORNE, 2014; BUZAN, HANSEN; 2012).

Visto que a dependência tecnológica acarreta intensas repercussões no eixo das relações internacionais entende-se que o ciberespaço está totalmente interligado com a mesma, seja através de atores estatais e/ou não-estatais. Assim, pode-se perceber que a problemática atual está no cerne da segurança, mas não a segurança tradicional dos Estudos de Segurança Internacional (ESI), e sim o que se conhece por Segurança Cibernética, principalmente após os problemas levantados pelo caso que ficou conhecido em 2013, com as

informações sigilosas vazadas por Edward Snowden acerca de programas de vigilância que o país usava para espionar a população mundial.

2.2 O Caso Snowden

Edward Joseph Snowden foi um analista de sistema que iniciou sua carreira na *Central de Inteligência Americana* (CIA) e depois trabalhou em empresas privadas de inteligência que prestam serviços para a *National Security Agency* (NSA). Ficou conhecido por tornar público documentos referentes a programas de vigilância da NSA, em 2013, através dos jornais *The Guardian* e *The Washington Post*. Diante desse ato de espionagem, os EUA acusaram Snowden por violações do ato de espionagem, razão pela qual o americano solicitou asilo político a Rússia.

Em junho de 2013, o jornalista norte-americano Glenn Greenwald começou a publicar no jornal britânico *The Guardian*, as primeiras partes do que se tornaria o caso mais abrangente de vigilância internacional a partir da internet na história da rede. Isso se tornou público por se tratar de um país – os Estados Unidos – que sempre quis aparecer como um guardião da liberdade pessoal e da democracia, enquanto, na verdade, coletava secretamente dados pessoais de milhões de cidadãos de vários países, incluindo a comunicação de governos estrangeiros (OPPERMANN, 2014, p. 148).

Em 7 de junho de 2013, o *Washington Post*[3] e o *The Guardian US*[4] revelaram que os Estados Unidos da América tinham desenvolvido, em 2007, o programa de vigilância PRISM, através do qual a *National Security Agency* (NSA) tinha acesso aos servidores de empresas telefônicas e dos gigantes da internet (Microsoft, Yahoo, YouTube, Apple, Facebook, Skype, Twitter, Linkedln, PalTalk, AOL) e podia interceptar as mensagens dos internautas e supervisionar ações de rotina comuns à maior parte dos usuários de internet de todo o mundo (GELLMAN & POITRAS, 2013; GREENWALD & MASASKILL, 2013).

---

[3] **Edward Snowden comes forward as source of NSA leaks.** Disponível em: <https://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html?utm_term=.61f9b51eb70f>. Acesso em: 04 abr. 2019

NSA slides explain the PRISM data-collection program. Disponível em: < http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/>. >. Acesso em: 04 abr. 2019

[4] **Edward Snowden: the whistleblower behind the NSA surveillance revelations**. Disponível em: < https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>. Acesso em: 04 abr. 2019

Edward Snowden identifies himself as source of NSA leaks - as it happened. Disponível em: < https://www.theguardian.com/world/2013/jun/09/nsa-secret-surveillance-lawmakers-live>. Acesso em: 04 abr. 2019

A 29 de junho do mesmo ano, a alemã *Der Spiegel*[5] revelava um segundo escândalo: os Estados Unidos tinham também espiado os dirigentes europeus em Washington, na ONU e até em Bruxelas (POITRAS, ROSENBACH, SCHMID & STARK, 2013) algo que era revelado precisamente no momento em que se iniciavam as negociações do futuro acordo de comércio livre entre a União Europeia e os Estados-Unidos, que seriam suspensas por Paris, em 3 de julho (LE PARISIEN, 2013).

Desde junho de 2013, houve frequentes atualizações no programa de vigilância do governo dos EUA. Ficou claro que as agências de segurança na Austrália, Canadá, Nova Zelândia e Reino Unido também estiveram envolvidas, juntamente com os EUA, conhecidas como os *Five Eyes* (FVeY)[6]. Várias agências de inteligência destes países estariam gerenciando programas de cooperação e bancos de dados, dos quais alguns são chamados Prism, XKeyscore, Tempora e Boundless informant[7] (OPPERMANN, 2014, p. 148).

O Departamento de Justiça americano acusou Snowden de espionagem, roubo e utilização ilegal de instrumentos governamentais e pediu a sua detenção a Hong Kong, lugar em que iniciou as denúncias aos referidos jornais internacionais. Mas Snowden pediu asilo para a Rússia e para o Equador, como fizera o fundador do *Wikileaks*, Julian Assange. A 25 de junho, o presidente russo, Vladimir Putin, não cedeu a ameaças americanas para entregá-lo e garantiu a entrada de Snowden em seu país, o que gerou uma crise diplomática entre os dois países. (LE PARISIEN, 2013).

Conforme Yannakogeorgos (2012), apesar do papel central que a Internet desempenha nas questões relacionadas ao ciberespaço, somente quando Edward Snowden trouxe luz aos programas de espionagem digital liderados pelos americanos que as agendas de governança da Internet e segurança cibernética convergiram definitivamente. O caso Snowden aumentou a imprevisibilidade dentro do ecossistema mais amplo da Internet e reacendeu tensões políticas que giram em torno da proeminência dos EUA dentro da arena mais estreita de recursos críticos da Internet (CANABARRO; FERREIRA, 2015).

---

[5] **NSA Spied on European Union Offices.** Disponível em: < http://www.spiegel.de/international/europe/nsa-spied-on-european-union-offices-a-908590.html>. Acesso em: 04 abr. 2019
NSA Scandal: Germany Seeks Spying Concessions at White House. Disponível em: < http://www.spiegel.de/international/germany/nsa-scandal-germany-seeks-spying-concessions-at-white-house-a-930975.html>. Acesso em: 04 abr. 2019

[6] É um acordo multilateral de cooperação, chamado UKUSA, de inteligência firmada pelos países: Austrália, Canadá, Nova Zelândia, Reino Unido e Estados Unidos, que foi iniciado na Carta do Atlântico emitida em agosto de 1941 para colocar metas de vigilância aos seus aliados no pós segunda guerra mundial.

[7] São programa da NSA usado no sistema de vigilância mundial que permite aos funcionários da NSA, coletar os vários tipos de dados dos usuários, que estão em poder de serviços de Internet, incluindo histórico de pesquisas, conteúdo de e-mails, transferências de arquivos, vídeos, fotos, chamadas de voz e vídeo, detalhes de redes sociais, logins e quaisquer outros dados em poder das empresas de Internet.

A convicção de Snowden é que, devido à vigilância, "(...) o mundo de hoje é muito mais imprevisível e perigoso" do que George Orwell[8] poderia ter adivinhado. Isso representa também um verdadeiro desafio lançado por Snowden, não só para atualizar nossa compreensão de novas tecnologias, mas também para colocar todo e qualquer sistema tecnológico, em seus devidos contextos social, político-econômico e cultural (LYON, 2016)

O caso Snowden mostrou a necessidade de proteger pessoas que revelam informações acerca de assuntos que têm implicações nos direitos humanos, bem como a importância de assegurar o respeito pelo direito à privacidade. As pessoas precisam confiar que as suas comunicações privadas não serão indevidamente escrutinadas pelo Estado (UNITED NATIONS, 2013, p. 7-11).

Em um mundo hiperconectado, o ciberespaço é hoje palco de ataques lançados[9] contra indivíduos, empresas, redes públicas ou privadas, infraestruturas críticas ou mesmo contra os sistemas de governança eletrônica do Estado (NUNES, 2014, p. 146) e para isso é primordial que os Estados busquem por medidas que zelem pela sua proteção e segurança. Pois, com o caso Snowden, indivíduos, empresas e atores governamentais puderam perceber que a espionagem através da internet é muito mais comum do que a maioria das pessoas podem pensar, e está provado que vem também daqueles que pretendem proteger seus aliados através de seu avanço tecnológico, enquanto, na realidade, eles também são capazes de criar um ambiente de insegurança e desconfiança (OPPERMANN, 2014, p. 149).

2.3 Segurança Cibernética: conceituação e prática

De acordo com Cruz (2012), o domínio do espaço cibernético constitui-se em grande desafio no presente século, tornando-se uma nova fronteira a ser desbravada em razão do ineditismo e da assimetria. O ineditismo é devido à falta de modelos e de referências, bem como da ausência de marcos legais. A assimetria está relacionada à diferença de poder, onde o mais forte pode ter vantagens, ou seja, estar à frente dos demais países em termos da segurança do seu espaço cibernético.

---

[8] George Orwell é o pseudônimo de Eric Arthur Blair, escritor e jornalista, que escreveu um livro no qual descreve uma sociedade em que o governo controla estritamente a informação, onde a tecnologia contribui para ampliar o controle dos cidadãos e a perda da privacidade.

[9] 1. Ataque de *ransomware* força empresa de alumínio a paralisar sistemas no mundo todo. Disponível em: < https://mundohacker.net.br/ataque-de-ransomware-forca-empresa-de-aluminio-a-paralisar-sistemas-no-mundo-todo/> Acesso em 22 de mar. 2019

2. O ataque cibernético que fez um território americano voltar no tempo. Disponível em: < https://www.bbc.com/portuguese/vert-fut-47296609> Acesso em: 22 de mar. 2019

3. Partidos políticos da Austrália sofrem ataque de hacker estrangeiro. Disponível em: < https://mundohacker.net.br/partidos-politicos-da-australia-sofrem-ataque-de-hacker-estrangeiro/> Acesso em: 22 mar. 2019

É inevitável a prestação de apoio aos esforços internacionais de desenvolvimento e implantação de um regime de governança global cibernética, para melhorar nossa segurança interna e externa, no sentido de ajudar a construir a capacidade de segurança cibernética de estados menos desenvolvidos e parceiros estrangeiros. Essas medidas podem ajudar a evitar que adversários explorem elos fracos na defesa cibernética globais (SOUZA JR, 2013).

O conceito de segurança cibernética emergiu no final dos anos 1980, momento em que o ciberespaço passou a ser parte da agenda de governos e organizações internacionais (LOPES, 2016). Como apontam Hansen e Nissenbaum (2009, p. 1155), o conceito de segurança cibernética surgiu como resposta a uma mistura de inovações tecnológicas e mudanças nas condições geopolíticas.

A *International Telecommunication Union* (ITU)[10], em 2018, definiu a segurança cibernética como a coleção de ferramentas, políticas, conceitos de segurança, proteções de segurança, guias, metodologias de gestão de riscos, ações, treinamentos, melhores práticas e tecnologias que podem ser utilizadas para proteger o ambiente cibernético e os ativos da organização e de seus usuários.

> Os objetivos gerais de segurança cibernética são os seguintes: disponibilidade, integridade e confidencialidade. A primeira se refere ao sistema estar apto para uso; a integridade significa que nenhum dado tenha sido alterado sem autorização. E por último, a confidencialidade se refere a manter os dados privados, uma vez que a informação tem valor no mundo digital; portanto, protegê-la é de suma importância (SINGER; FRIEDMAN, 2014).

A *Information Systems Audit and Control Association* (ISACA)[11] definiu em 2013 que: Segurança cibernética engloba tudo que protege organizações e indivíduos de ataques intencionais, falhas e incidentes assim como suas consequências. Na prática, segurança cibernética refere-se primariamente a tipos de ataque, falhas e incidentes que são visados, sofisticados e difíceis de detectar ou gerenciar.

Nos últimos anos, *policymakers* e especialistas demonstraram a preocupação a respeito da proteção das Tecnologias de Informação e Comunicação (TIC) contra ataques cibernéticos, e muitos deles esperam o aumento do número e da gravidade desses ataques (FISCHER, 2016).

De acordo com Singer e Friedman (2014), a segurança não é apenas a noção de estar livre de perigo, mas também se associa à presença de um adversário, isto é, a questão

[10] É uma agência da Organização das Nações Unidas (ONU) especializada em tecnologias de informação e comunicação, destinada a padronizar e regular as ondas de rádio e telecomunicações internacionais.
[11] É uma associação internacional que suporta e patrocina o desenvolvimento de metodologias e certificações para o desempenho das atividades de auditoria e controle em sistemas de informação.

cibernética torna-se um problema de segurança em vista de um adversário que busca ganhar algo em decorrência de sua atividade, seja para obter informação privada, seja para prevenir o seu uso legítimo.

Para Pimentel (2014, p. 4), a segurança cibernética fornece a informação como uma fonte de poder na contemporaneidade, ganhando fôlego na pauta internacional, uma vez que o ciberespaço se transforma em "um importante vetor para fins políticos e estratégicos de atores estatais e não estatais". Assim, como fonte de poder estrutural, a tecnologia será objeto de disputa entre os Estados, na atual ordem internacional, sua possessão significa, para uma potência dominante, a perpetuação do atual estado de coisas, porque age como freio ao desenvolvimento interno e como aumento da autonomia relativa dos demais países (CARPES, 2006).

Deste modo, quanto mais conectada ao ciberespaço uma nação é, maior é a vantagem que esta pode tirar da Internet, entretanto, quanto maior essa conexão, maiores as chances de ser potencialmente prejudicada pelo uso malicioso da Internet (SINGER; FRIEDMAN, 2014). Ou seja, enquanto as nações estiverem dependentes de redes de computadores como base para seu poder econômico e militar e estas puderem ser acessadas pelo exterior, elas estarão em risco (LIBICKI, 2009).

A segurança cibernética necessitaria de um arcabouço baseado na resiliência e preparação, ligados à gestão de risco e práticas de governança antecipatória (preventiva) (MUNK, 2015, p. 46). Dessa forma, a resistência aos ataques cobriria a cooperação de aspectos operacionais e políticos de organizações governamentais, harmonização via cooperação, legislação internacional e o envolvimento de atores não-estatais (MUNK, 2015, p. 178).

O controle da informação representa uma mudança significativa no mundo atual, o qual mostra o papel que a informação passou a ter não só no dia a dia das pessoas, mas como nas estratégias políticas de uma nação (CASTILHO, 2013). Logo, a cibersegurança se torna um objeto especial de estudo por suas características inovadoras que distinguem o ciberespaço dos domínios tradicionais do pensamento estratégico, especialmente devido a sua virtualidade transfronteiriça (GRAY, 2013).

Desta forma, é importante que os Estados passem a entender as normas legais e a importância que a Segurança Cibernética tem nos debates e pesquisas da atualidade, uma vez que a mesma vem ganhando destaque a nível internacional, através dos diversos episódios de ataques cibernéticos e de espionagem internacional, para que então possam colocar em prática as suas estratégias.

3 AS POLÍTICAS CIBERNÉTICAS DAS POTÊNCIAS MUNDIAIS: ESTADOS UNIDOS E RÚSSIA

Diante da necessidade que os países sentiram em desenvolver políticas de segurança cibernética, as discussões a respeito da temática intensificaram-se e se tornaram mais do que uma mera discussão acadêmica e conceitual. A pauta da cibersegurança está presente nas estratégias nacionais de defesa e no orçamento dos principais *players* globais, mais de 40 países[12] possuíam doutrinas, políticas ou organizações militares devotadas a cibersegurança em 2009 (UNIDIR, 2009), entre eles os Estados Unidos e a Rússia.

Na visão de Geers (2015), o avanço da tecnologia da informação e a vulnerabilidade dos sistemas informacionais à ataques externos impõem novos desafios aos Estados modernos. O principal desafio passa a ser a garantia da segurança cibernética em um sistema internacional repleto de inseguranças, uma vez que a segurança é o movimento que conduz a política (*politics*) para além das regras já estabelecidas do jogo e enquadra uma questão como um tipo especial de política (BUZAN, WAEVER, WILDE, 1998, p. 23).

De acordo com Buzan, Waever e Wilde (1998, p. 21, 27,46), a segurança do contexto internacional é bem diferente da nacional, ela lida com elementos realistas tradicionais da política do poder e da sobrevivência do Estado. Logo, num sistema rodeado de inseguranças, a função de Estado é a de se manter enquanto tal, em um mundo cujas relações de força e poder não devem ser desprezadas, pelo contrário, elas devem ser realçadas quando da análise (ACÁCIO, 2016, p. 40). Em um sistema internacional anárquico no qual prevalecem as relações de poder, a insegurança é um elemento chave, e cada ator potencialmente experimenta diversos tipos de ameaças advindos do nível sistêmico. Ou seja, há maior necessidade de cada Estado zelar por sua própria segurança através de políticas e estratégicas contra ameaças nacionais advindas de ciberespaço (ACÁCIO, 2016, p. 41).

Vale salientar que as ameaças à segurança cibernética não surgem apenas de agentes internacionais, mas também de ameaças sistêmicas (HANSEN; NISSENBAUM, 2009, p. 1160) que devem-se em grande parte ao início conturbado da Internet. Deste modo, estes perigos desencadeiam maior preocupação por parte de governos, uma vez que podem causar danos a sistemas, colocar a população geral em perigo, causar danos severos à economia e às

[12] África do Sul, Albânia, Alemanha, Argentina, Austrália, Áustria, Bielorússia, Brasil, Canadá, Cazaquistão, China, Cingapura, Colômbia, Croácia, Cuba, Coréia do Norte, Coréia do Sul, Dinamarca, Eslováquia, Espanha, Estados Unidos, Estônia, Fiji, Finlândia, França, Georgia, Grécia, Holanda, Hungria, Índia, Indonésia, Irã, Israel, Itália, Japão, Lituânia, Malásia, Mianmar, Noruega, Polônia, Rússia, Sri Lanka, Suíça, Turquia, Ucrânia, Reino Unido e Vietnã.

infraestruturas públicas, constituindo uma ameaça existencial para o objeto referente. Logo, a evolução do caráter das ameaças sistêmicas contribuiu para que fossem planejadas e elaboradas criações de estratégias de segurança cibernética.

Clarke e Knake (2010, p. 81) consideram que os Estados Unidos é atualmente um dos Estados mais conectados a sistemas de informações e redes, porém a preocupação com as consequências da evolução tecnológica vem desde a década de 1990, uma vez que houve uma crescente adoção da Internet e de ciberespaço por parte das indústrias estadunidenses.

Os EUA têm a mais sofisticada capacidade cibernética, seguidos pela Rússia; em segundo nível, encontram-se a China e a França. Segundo Clarke e Knake (2010), na questão de capacidade ofensiva cibernética, o país se encontra em primeiro lugar, mas merece destaque a questão de que, em uma guerra cibernética, é necessária mais do que uma ofensiva cibernética, já que deve se levar em conta também a sua dependência deste meio. Em outras palavras, o grau de dependência de uma nação está relacionado à quantidade de sistemas controlados ciberneticamente. Os Estados Unidos, embora possuam uma ótima capacidade ofensiva, têm suas deficiências na questão da defesa cibernética, pois sua grande dependência traz consigo também grandes vulnerabilidades.

3.1 Estratégias de Segurança Cibernética dos Estados Unidos

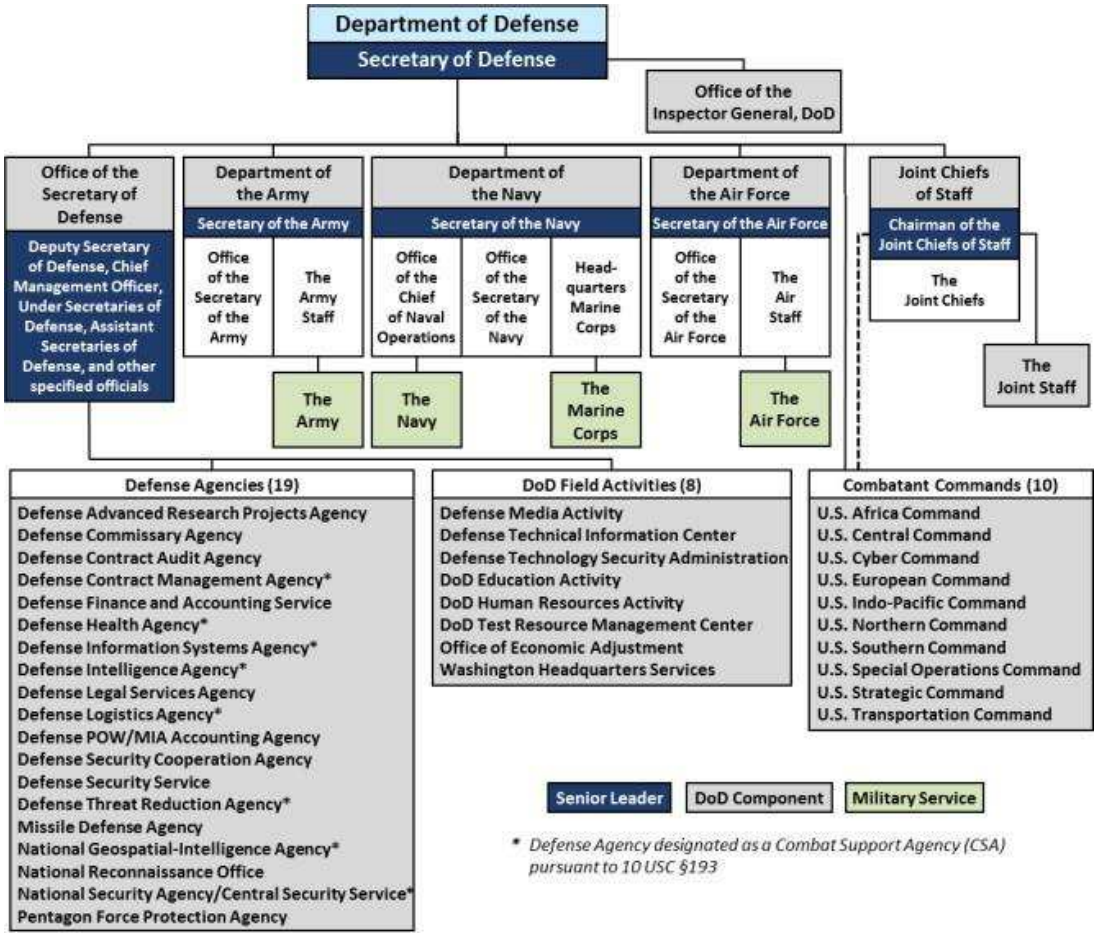
Tirreel (2012) considera a estrutura organizacional cibernética dos Estados Unidos vasta e complexa, devido a grande variedade de entidades e componentes. De acordo com o autor, existem três entidades primárias que são: *Departament of Defense* (DOD), *Departament of Homeland Security* (DHS) e o *Departament of Justice* (DOJ), uma vez que se limita a órgãos federais. Na área secundária, existem seis centros nacionais de segurança cibernética, que são o *Computer Emergency Readiness Team* (US-CERT), *United States Cyber Command* (USCYBERCOM), *National Cyber Investigative Joint Task Force* (NCIJTF), *National Security Agency/Central Security Service Threat Operations Center* (NTOC), *Defense Cyber Crime Center* (DC3) e o *Intelligence Community–Incident Response Center* (IC-IRC).

O DHS, criado em 2002, pelo *The Homeland Security Act*, tem a função de coordenar os esforços nacionais relativos à proteção de infraestrutura crítica nos setores de TIC, assim como também compartilhar informações sobre ameaças, avaliações de vulnerabilidades e desenvolvimento de ações apropriadas para tais planos de contingência (PERNIK; WOJTKWIAK, VERSHOOR-KIRSS, 2012, p. 11).

O DoJ tem a função de executar as leis relativas à segurança cibernética. Ele é responsável, então, por investigar e processar em casos de invasões, juntamente da Inteligência como suporte, além de prover suporte legal e de política para outros departamentos. Lida com crimes cibernéticos, investigações e atributos sob sua jurisdição (PERNIK; WOJTKWIAK; VERSHOOR-KIRSS, 2012). O líder para investigações criminais dentro do Departamento de Justiça é o FBI, o qual tem competência sobre questões de aplicação da lei relacionadas ao cibercrime, incluindo criminosos, adversários estrangeiros e terroristas (TIRREEL, 2012, p. 60).

Por último, o DoD – que é o foco principal – além de ser responsável pela proteção do domínio ".mil" e de sua infraestrutura de informação global de ataques, é encarregado também de reunir informações a respeito de ameaças cibernéticas estrangeiras e garantir a segurança de sistemas de segurança nacional e militares (PERNIK; WOJTKWIAK, VERSHOOR-KIRSS, 2012). De modo a esclarecer a organização de vários níveis desta entidade, segue abaixo o quadro organizacional desse departamento.

Figura 1 - Estrutura Organizacional do Departamento de Defesa



Fonte: *Department of Defense (2018)*[13].

A era digital criou desafios para o Departamento de Defesa (DoD) e para os EUA. A natureza aberta, transnacional e descentralizada da Internet que procuramos proteger cria vulnerabilidades significativas. O Departamento deve agir no ciberespaço durante a competição do dia-a-dia para preservar o país, as vantagens militares e defender os interesses dos EUA.

As atenções do governo norte americano no espaço cibernético começaram a partir do governo de Ronald Reagan (1981-1989), o qual buscava evitar divulgações prejudiciais de informações confidenciais. Porém, foi no governo de Bill Clinton (1993 – 2001) foi possível perceber que as ameaças cibernéticas seriam um dos perigos do século XXI. E precisamente no governo George W. Bush (2001 – 2009), que esse tema passou a ter um foco muito forte. (CAVELTY, 2007, p. 44- 92).

No ano de 2003, os Estados Unidos lançou sua primeira estratégia de cibersegurança, denominada *The National Strategy to Secure Cyberspace*. Era parte constitutiva da *National Strategy for Homeland Security* e complementada pela *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Tinha como principal objetivo envolver e capacitar os americanos para garantir o controle no ciberespaço que eles possuem e operam, o que requer, na visão do governo dos EUA, um esforço coordenado e focado de toda sociedade, o governo federal, os governos estaduais e municipais, o setor privado e o povo americano (UNITED STATES, 2003).

A estratégia descreve uma estrutura inicial para organização e priorização de esforços. Fornece direção aos departamentos do governo federal e agências que têm papéis em segurança do ciberespaço, identificando etapas que governos estaduais e municipais, empresas privadas e organizações e americanos individuais pode levar para melhorar a segurança cibernética coletiva ao longo do tempo (UNITED STATES, 2003).

Logo, os objetivos estratégicos são para:

I. Evitar ataques cibernéticos contra as infraestruturas críticas;

II. Reduzir a vulnerabilidade nacional ao cyberataques; e

III. Minimizar o dano e tempo de recuperação de ataques cibernéticos que ocorrem.

O documento traz consigo cinco prioridades estratégicas a serem cumpridas, a primeira prioridade era um Sistema Nacional de Resposta à Segurança do Ciberespaço, na qual se fosse

[13] **U.S. Department of Defense Agency Financial Report for FY 2018**. Disponível em:<https://comptroller.defense.gov/Portals/45/Documents/afr/fy2018/2-Managements_Discussion_and_Analysis_MDA.pdf>

possível uma rápida identificação, troca de informações e remediação pode mitigar o dano causadas pela atividade maliciosa do ciberespaço, deste modo, era necessário parceria entre o governo e a indústria para realizar análises, emitir avisos e coordenar os esforços de resposta (UNITED STATES, 2003, p. 10).

A segunda prioridade, diz respeito a um programa nacional de redução de vulnerabilidades e ameaças à segurança do ciberespaço, no qual, é necessário explorar as vulnerabilidades em nosso ciberespaço, uma vez que um ataque organizado pode pôr em risco a infraestrutura crítica da nação (UNITED STATES, 2003, p. 11).

A terceira prioridade era um programa nacional de conscientização e treinamento em segurança cibernética, devido a falta de pessoal treinado e ausência de níveis multi-amplamente aceitos de programas de certificação para segurança cibernética, os profissionais por não terem experiência acabar por complicar tarefa de abordar vulnerabilidades cibernéticas (UNITED STATES, 2003, p. 11).

A quarta prioridade era assegurar o ciberespaço dos governos, visando assegurar e promover um mercado mais seguro para tecnologias através da sua aquisição. Por último, a quinta prioridade era a chamada Segurança Nacional e Cooperação Internacional em Segurança do Ciberespaço, uma vez que uma rede de redes abrange o planeta, permitindo que atores maliciosos de um continente possam atuar em sistemas de milhares de milhas de distância é necessário um sistema de cooperação internacional para facilitar o compartilhamento de informações e reduzir vulnerabilidades (UNITED STATES, 2003, p. 12).

Depois de oito anos, em 2011, é lançada uma nova estratégia denominada como *DoD's Strategy for Operating in Cyberspace.*, com foco nos aspectos centrais da ameaça cibernética, que incluem ameaças externas de atores, ameaças internas, vulnerabilidades da cadeia e ameaças com uma atuação mais específica do Departamento de Defesa no ciberespaço e traçando cinco iniciativas estratégicas que lhe complementam e são voltadas para questões operacionais (UNITED STATES, 2011).

A primeira iniciativa estratégica refere-se ao tratamento do espaço cibernético como um domínio operacional para organizar, treinar, e equipar para que o DoD possa tirar total vantagem do potencial do ciberespaço. A segunda iniciativa é sobre o emprego pelo DoD de novos conceitos operacionais de defesa para proteger redes e sistemas do departamento, para isso primeiro é necessário um aprimoramento das práticas para melhorar a segurança cibernética, depois é necessário fortalecer as comunicações de força de trabalho, assim como o monitoramento e gerenciamento de informações para garantir o desenvolvimento de novos

conceitos operacionais de defesa e arquiteturas de computação (UNITED STATES, 2011, p. 5-7).

A terceira iniciativa diz respeito a fazer parcerias com outros departamentos e agências do governo dos EUA e com o setor privado para permitir uma segurança cibernética de "todo o governo". A quarta tem a perspectiva de construir relacionamentos robustos com aliados dos EUA e parceiros internacionais para fortalecer a segurança cibernética coletiva. E a última, busca aumentar a engenhosidade da nação por meio de uma força tarefa excepcional e rápida de inovação tecnológica (UNITED STATES, 2011, p. 8-12)

A última estratégia foi a *The DoD Cyber Strategy* (2015), a mesma é baseada nas decisões anteriores relativas à força de missão cibernética do DoD e ao desenvolvimento da força de trabalho cibernético. Dessa maneira, seu primeiro objetivo era construir e manter forças de prontidão e capacidades de conduzir operações no ciberespaço, para desenvolver uma pronta Força Missão Cibernética e força de trabalho cibernética associada. Esta força de trabalho será construída em três pilares fundamentais: treinamento aprimorado; melhoria militar e civil, recrutamento e retenção; e apoio do setor privado mais forte (UNITED STATES, 2015, p. 17-19).

O segundo objetivo é defender a rede de informação do DoD, assegurar dados e mitigar riscos para as missões do DoD, procurando identificar, priorizar e defender as redes e dados mais importantes. O terceiro objetivo busca pela preparação para defender a pátria e os interesses vitais dos EUA dos ataques cibernéticos destrutivos de consequência significante. O quarto buscar construir e manter opções cibernéticas viáveis e planejar o uso destas para controlar escalas de conflito e moldar o ambiente de conflito em todos os estágios. E o último, almeja construir e manter alianças e parcerias internacionais robustas para deter ameaças compartilhadas e melhorar a segurança e estabilidade internacional (UNITED STATES, 2015, p. 19-28).

No final do ano de 2018, a *White House* lançou a *National Cyber Strategy,* delineando os passos que o governo federal estava tomando para promover um ciberespaço aberto, seguro e confiável. Esta estratégia representa a visão do Departamento de abordar as questões referentes às ameaças e implementar as prioridades das estratégias anteriores, porém, esta substitui a *estratégia do The DoD Cyber Strategy* de 2015 (UNITED STATES, 2018).

Primeiro, deve-se garantir a capacidade dos militares dos EUA de lutar e vencer guerras em qualquer domínio, incluindo ciberespaço. Este é um requisito fundamental para a segurança nacional dos EUA e uma chave para garantir que possam dissuadir à agressão,

incluindo ataques cibernéticos que constituem um uso da força, contra os Estados Unidos (UNITED STATES, 2018).

Em segundo lugar, o Departamento procurará antecipar, derrotar ou impedir a segmentação por atividades cibernéticas maliciosas à infra-estrutura crítica dos EUA que poderia causar um incidente cibernético significativo, independentemente de incidente teria impacto na prontidão ou capacidade de combate do DoD. E por último, o Departamento trabalhará com aliados e parceiros dos EUA para fortalecer a capacidade cibernética, expandir as operações combinadas do ciberespaço e aumentar o compartilhamento bidirecional a fim de promover os interesses mútuos (UNITED STATES, 2018).

Desta forma, os Estados Unidos (2018), pontua em seu documento que a chegada da era cibernética criou novas oportunidades e desafios para o Departamento e para a Nação. O acesso aberto e confiável à informação é um interesse vital dos EUA e que os aliados e concorrentes tanto deve entender que irão defendê-lo assertivamente. A estratégia lançada em 2018 dar abertura para o Departamento de Defesa moldar a competição do dia-a-dia, e se preparar para a guerra através da construção de uma força mais letal, expandindo alianças e parcerias.

3.2 Estratégias de Segurança Cibernética da Rússia

De acordo com Maurer e Hinck (2018), em 2009 Timothy Thomas[14], declarou que a Rússia, mais do que qualquer outro país, está alarmada com os aspectos cognitivos das questões cibernéticas e seus aspectos técnicos. Moscou adotou uma abordagem diferente, mais abrangente e integrada à segurança da informação, comparada ao foco das capitais ocidentais na segurança cibernética mais centrada na rede. Descrito explicitamente em doutrinas e estratégias nas últimas duas décadas, está se tornando cada vez mais claro como a Rússia está implementando essa perspectiva na prática - com bastante sucesso até agora, pode-se acrescentar.

O governo russo - como contido em documentos oficiais como a Doutrina de Segurança da Informação de 2000 - ligou a segurança da informação à estabilidade interna, argumentando que o Estado deveria assumir um papel forte na proteção contra interferências externas. A doutrina define segurança da informação como “proteção dos interesses nacionais [da Rússia] na esfera da informação definida pela totalidade dos interesses equilibrados do indivíduo, da sociedade e do estado” (THOMAS, 2009, p. 40).

[14] Um especialista russo no Escritório de Estudos Militares Estrangeiros em Ford Leavensforth, nos EUA.

Na análise de Thomas (2009, p. 40) internacionalmente, as iniciativas diplomáticas da Rússia refletem preocupações domésticas sobre o livre fluxo de informações e a abordagem militar para operações de informação e segurança cibernética. Em meados da década de 1990, o Kremlin se aproximou da Casa Branca com uma proposta de tratado internacional para segurança da informação. Embora o governo dos EUA tenha rejeitado a proposta, não impediu o governo russo de perseguir e promover a ideia globalmente. A visão de que a informação descontrolada representa uma ameaça para o governo e a sociedade tem informado a estratégia da Rússia na diplomacia internacional sobre as tecnologias da informação e comunicação (TICs) e na sua doutrina militar.

A Federação Russa há muito considera como usar a informação como arma, além de explorar o uso de ataques cibernéticos para causar danos físicos a fim de conduzir a guerra de informação para apoiar seus interesses nacionais, contando com as Operações cibernéticas ofensivas (OCOs). Com base na definição do Estado-Maior Conjunto, os OCOs são operações que visam "projetar energia no ciberespaço ou através dele". A Rússia utiliza OCOs para promover seu estado final estratégico desejado: ser percebida como uma grande potência em um policêntrico na ordem mundial e exercer maior influência nos assuntos internacionais.

Osnos, Remnick e Yaffa (2017) consideram que tais operações não são uma nova tática para a Rússia, mas uma manifestação contemporânea das técnicas de implementação Komitet Gosudarstvennoy Bezopasnosti (KGB) da era soviética, "aktivniye meropriyatiya" ou "medidas ativas". Essas medidas visam "[influenciar] eventos" e "[enfraquecer] um poder rival com falsificações", agora através da incorporação do domínio cibernético.

Entre os principais documentos que definem atualmente as abordagens fundamentais para garantir a Segurança da Informação da Federação Russa, pode ser elencados os seguintes (LEONIDOVICH, 2013):

1. Lei da Federação Russa 07.07.2006 № 149-ФЗ "Informação, Tecnologias de Informação e Proteção das informações";
2. Doutrina de Segurança da Informação da Federação Russa;
3. Estratégia Nacional de Segurança da Federação Russa.

A primeira, Lei da Federação Russa 07.07.2006 № 149-ФЗ "Informação, Tecnologias de Informação e Proteção das informações", remete-se a Responsabilidade por Ofensas, como corrobora o "Artigo 17. […] Quando a disseminação de determinada informação é restrita ou proibida nos termos de leis federais, a responsabilidade civil pela disseminação dessa informação não será suportada pelo provedor de serviços quando diga respeito a: 1) transferência de informação fornecida por terceiro, na condição de que tenha sido transferida

sem modificações ou correções; 2) ou armazenamento de informação e provisão de acesso, contanto que o provedor não tivesse como estar ciente da ilegalidade da disseminação da informação" (RÚSSIA, 2006).

A segunda estratégia é a Doutrina de Segurança da Informação da Federação Russa, é um documento de planejamento estratégico que desenvolve as cláusulas da Estratégia de Segurança Nacional da Federação da Rússia aprovada pelo Decreto 683 do Presidente da Federação da Rússia em 31 de dezembro de 2015, e também por outros documentos de planejamento estratégico nesta área (RÚSSIA, 2015).

Nesta Doutrina, utilizam-se os seguintes conceitos básicos:

a. Espaço de informação - um campo de atividade relacionado formando, criando, transformando, transmitindo, usando, armazenamento de informações fornecendo impacto, incluindo consciência individual e pública, infra-estrutura de informação e informação adequada;
b. Segurança da informação - o estado da segurança pessoal, organizações e o Estado e seus interesses de ameaças, destrutivas e outras impactos negativos no espaço da informação;
c. Ciberespaço - o campo de atividade na informação espaço formado por um conjunto de canais de comunicação A internet e outro telecomunicação redes, tecnológico infraestrutura, garantindo seu funcionamento, e quaisquer realizado através do uso da atividade humana (indivíduos, organizações, estados);
d. Cibersegurança - um conjunto de condições sob as quais todos componentes do ciberespaço são protegidos do maior número possível ameaças e impactos com consequências indesejáveis.

A terceira denominada de Estratégia Nacional de Segurança da Federação Russa, a qual busca garantir a segurança cibernética do indivíduo organizações e estados da Federação Russa, definindo um sistema prioridades, princípios e medidas no domínio da política interna e externa. De acordo com a Estratégia Nacional de Segurança da Federação Russa, o impacto negativo das tecnologias na garantia da segurança nacional tomam a dependência da infraestrutura de estado, de poder e de controle, fornecendo abordagens de força nas relações internacionais (ALEXANDROVICH, 2015).

De acordo com Lopes (2017, p. 58), o sistema de planejamento estratégico russo, a "Стратегия национальной безопасности Российской Федерации" ou Estratégia de Segurança Nacional da Federação da Russa (СНБРФ – ESNFR) é atualizada uma vez a cada seis anos. E representa o documento básico para o sistema de planejamento e

desenvolvimento da Federação Russa que visa garantir a segurança nacional até o ano de 2020. A implementação da Estratégia de Segurança Nacional Russa tem por objetivos básicos contribuir para o desenvolvimento da economia nacional, melhorar a qualidade de vida dos cidadãos, reforçar a estabilidade política, assegurar a defesa nacional, a segurança pública, a competitividade e o prestígio internacional da Federação Russa.

O texto da Estratégia de Segurança Nacional Russa está dividido em seis grandes áreas de interesse estratégico. A primeira diz respeito às Disposições Gerais, do artigo 1º ao 6º. Nestes artigos encontra-se a premissa da Estratégia – relação de simbiose e interdependência de segurança nacional da Federação Russa e o desenvolvimento socioeconômico do país. Na segunda, é apresentada a visão da Rússia no mundo moderno, na qual é nítida a preocupação em definir o "futuro incerto" (RÚSSIA, 2015).

Na terceira área são apresentados os interesses nacionais e prioridades estratégicas russos de longo prazo com a finalidade de reforçar a defesa nacional. A quarta área, denominada de "Garantindo a Segurança Nacional" é composta por subáreas correspondendo às Ações Estratégicas e Diretrizes Governamentais para a consecução dos OE. A quinta área é dedicada à Implementação de Estrutura Organizacional, Legal e Informativa da estratégia. E a última, busca identificar os Principais Indicadores de Segurança Nacional, como, o grau de satisfação dos cidadãos na proteção dos seus direitos e liberdades, no nível pessoal e nos interesses de propriedade, incluindo contra ações criminosas; andamento dos modernos projetos de modelos de armas, entre outros (RÚSSIA, 2015).

4 CONTROLE VERSUS PODER: RESULTADO DA RELAÇÃO RUSSO-ESTADUNIDENSE PÓS SNOWDEN

A evolução das relações entre a Rússia e os Estados Unidos é marcada por um longo ciclo histórico que se estruturou por meio de uma dinâmica pendular de aproximações e distanciamentos que se manifestaram em determinadas periodizações, com tendências, tanto, de cooperação, quanto, de conflito, entre os países na garantia de interesses nacionais (SENHORAS, 2014).

O confronto indireto entre Estados Unidos e União Soviética, como superpotências pela disputa da ampliação do seu poder e dos espaços de influência no mundo, ficou conhecido como "Guerra Fria" frente à inviabilidade de um confronto direto e aberto de natureza nuclear entre os países, motivo pelo qual é possível identificar diferentes fases

evolutivas das relações EUA-URSS e guerras regionais com o apoio de um dos lados (LAFEBER, 1997; HOBSBAWN, 1995).

Jubran (2015, p. 18) corrobora que as relações entre a URSS e os EUA no início do século XX estavam em uma fase bastante negativa, em função do cumprimento da promessa de expansão da Organização do Tratado do Atlântico Norte (OTAN) para Leste e do bombardeio da OTAN contra a então Iugoslávia, com a qual Moscou tinha relações próximas, ainda que tensas. Assim, a Rússia, criticava a falta de reciprocidade por parte do Ocidente e dos EUA, na promoção de gestos amistosos, inclusive no apoio à modernização econômica russa. Houve uma significativa melhora das relações com os Estados Unidos, entretanto, após os atentados terroristas de 11 de setembro de 2001 (SELEZNEVA, 2002; KORTUNOV, 2009).

Nos últimos anos, a dinâmica da cooperação internacional e do conflito no ciberespaço tornou-se o foco de intenso interesse por parte dos governos nacionais e comunidade especializada em todo o mundo, não foi diferente com a Rússia e os EUA. Os mesmos tendem a abordar o problema da segurança cibernética de diferentes perspectivas, o governo russo geralmente enfatiza o princípio de controle soberano sobre todo o domínio de informação e comunicação, já os Estados Unidos rejeitam a "segurança da informação" como um princípio fundamental e defende a idéia de que a Internet deveria ser "aberta, seguro, interoperável e confiável" (REMINGTON *et all*, 2016).

Em 17 de Junho de 2013, a Rússia e os Estados Unidos finalmente chegaram a um acordo assinado na cúpula do G-8 na Irlanda do Norte que cobria "questões de ameaças à ou no uso de TICs no contexto da segurança internacional". Em uma declaração conjunta Obama e Putin garantem:

> "Reconhecemos que as ameaças e o uso das TICs incluem ameaças político-militares e criminosas, bem como ameaças de natureza terrorista, e são alguns dos mais sérios desafios de segurança nacionais e internacionais que enfrentamos no século XXI. Afirmamos a importância da cooperação entre os Estados Unidos da América e a Federação Russa com o propósito de melhorar o entendimento bilateral nesta área. Consideramos essa cooperação essencial para salvaguardar a segurança de nossos países e para obter segurança e confiabilidade no uso de TICs essenciais à inovação e à interoperabilidade global." (OBAMA, PUTIN, 2013)[15]

Os dois países concordaram em (DEMIDOV, 2014):

[15] We recognize that threats to or in the use of ICTs include political-military and criminal threats, as well as threats of a terrorist nature, and are some of the most serious national and international security challenges we face in the 21st Century. We affirm the importance of cooperation between the United States of America and the Russian Federation for the purpose of enhancing bilateral understanding in this area. We view this cooperation as essential to safeguarding the security of our countries, and to achieving security and reliability in the use of ICTs that are essential to innovation and global interoperability.

a) estabelecer um vínculo de comunicação de voz seguro e direto entre Moscou e Washington, para ser usado em caso de ameaças à segurança envolvendo TICs; o qual autorizaria o contato direto entre o Serviço Federal de Segurança (SFS) da Rússia e a Agência Central de Inteligência dos Estados Unidos (CIA) em relação às ameaças cibernéticas;

b) permitir que a "linha direta" nuclear (os Centros de Redução de Risco Nuclear dos EUA-Rússia) seja usada para comunicações sobre ameaças cibernéticas, incluindo avisos sobre cybers-exercício futuros ou ciberataques em andamento; e

c) vislumbrar a coordenação entre os Centros de Estudos, Resposta e Tratamento de Incidentes de Segurança (CERTs) dos dois países - isto é, as equipes de especialistas que investigam e abordam os ataques a infraestruturas críticas de TIC.

Figura 2 - Presidente dos EUA, Barack Obama com o presidente russo, Vladimir Putin durante a cimeira do G8 em Enniskillen, Irlanda do Norte, em 2013.

Fonte: *BBC (2013)*[16]

No entanto, a melhoria das relações entre os Estados Unidos e a Rússia foi apenas temporária. Pois, pouco tempo depois do acordo ser assinado, as revelações de vigilância dos EUA começaram a ser liberadas e com a decisão da Federação Russa de conceder a Edward Snowden asilo temporário por um ano, um muro foi traçado em relação ao relacionamento

[16] **G8 meeting: Obama and Putin push for Syria summit.** Disponível em: < https://www.bbc.com/news/world-europe-22930266>

futuro entre a Rússia e os Estados Unidos, pois, na sequência da decisão da Rússia de oferecer a Snowden asilo temporário, as relações entre os dois países deterioraram-se rapidamente (GORST, 2014).

De acordo com Herrington (2015), apenas um mês depois da Rússia conceder o referido asilo, os Estados Unidos e a Rússia organizaram uma cúpula do G8 na Irlanda do Norte, previstas para setembro de 2013. No entanto, as autoridades americanas cancelaram a cimeira e políticos americanos pediram um boicote aos Jogos Olímpicos de Inverno de 2014, realizados em Sochi, Rússia. Além disso, pela primeira vez desde as Olimpíadas de Sydney em 2000, os Estados Unidos não enviou um Presidente, Primeira Dama, Vice-Presidente, ou ex-presidente para representar os Estados Unidos na cerimônia de abertura de uma Olimpíada.

Ao invés de comparecer a Olimpíada os Estados Unidos enviaram Billie Jean King, uma ex-tenista, Brian Boitano, ex-patinador, e Caitlin Cahow, uma jogadora de hóquei no gelo, todos abertamente gays, para representar os Estados Unidos na abertura cerimônia. A decisão de Obama de incluir os acima mencionados atletas da delegação dos EUA provavelmente foi feito para responder publicamente a aprovação de uma Lei Russa de 2013 "que estigmatiza os gays e proíbe dar às crianças qualquer informação sobre a homossexualidade" (WHITESIDE, 2013).

No contexto das relações internacionais, as potências têm estado em conflito sobre os interesses econômicos, geopolíticos, militares e tecnológicos, de práticas tradicionais de espionagem usados na Guerra Fria, e que hoje são desenvolvidos por agências de segurança e inteligência, com grandes avanços em tecnologia; fornecendo um controle mais eficaz da informação, onde o ciberespionagem torna-se uma arma poderosa, silenciosa e eficaz (USECHE, 2014).

A tecnologia possibilitou uma mudança dinâmica no sistema de relações internacionais, na forma como corporações transnacionais, organizações não-governamentais, organizações intergovernamentais, grupos sociais e outros atores ganham potencial de informação e tornam-se mais poderoso - uma forma de poder com base em recursos de informação - do que os governos tradicionais, eles às vezes possuem mais instrumentos de influência internacional do que os estados, criando um sistema policêntrico de relações (NYE, 2011).

Os Estados Unidos têm um papel especial no ciberespaço. Devido a circunstâncias históricas, o mesmo lidera na maioria dos indicadores de produção relevantes (participação global de patentes, tecnologia educação, serviços de consultoria, etc.) e na exportação de bens e serviços de informação e também controlam muitos dos mecanismos para governar o

domínio cibernético global. A importância dos Estados Unidos no ciberespaço é uma das razões pelas quais os interesses russos nessa área são interconectados com as relações bilaterais russo-americanas, bem como com as relações internacionais estratégia (CENTRE FOR ANALYSIS OF STRATEGIES AND TECHNOLOGIES, 2012).

Desde o início do século XXI, a Rússia tem tentado iniciar uma resolução na Assembléia Geral da ONU, sobre "Desenvolvimentos no campo da informação e Telecomunicações no Contexto da Segurança Internacional", visando abordar tais preocupações. A resolução criaria um marco legal internacional, baseado nos princípios de não uso da força, não-interferência nos assuntos domésticos e respeito pelos direitos humanos e liberdades fundamentais, e visaria impedir o uso da informação e das telecomunicações em violação da Carta da ONU (UNITED NATIONS, 2001).

No entanto, os EUA sempre se opuseram à resolução em parte porque "falta entendimento compartilhado sobre as normas internacionais relativas ao comportamento do Estado ciberespaço". Essa falta de compreensão, acredita os EUA, defende a elaboração de medidas destinadas a reforçar a cooperação e reforçar a confiança, reduzir os riscos ou reforçar transparência e estabilidade (SHARIKOV, 2013).

Desta forma, Sharikov (2013) corrobora que uma maneira possível de a Rússia e os Estados Unidos cooperarem na segurança cibernética seria o estabelecimento de normas internacionais que efetivamente impediriam outros atores de se engajarem em comportamentos disruptivos, destrutivos ou ilegais no ciberespaço. Tomadores de decisão russos e americanos enfrentam junto o desafio de se adaptar à natureza em constante evolução da política internacional. Garantir a segurança nacional e manter a estabilidade internacional é cada vez mais fatores como o papel das tecnologias da informação.

É, pelo menos, a terceira vez nos últimos dois anos que a Rússia solicitou alguma forma de cooperação com os Estados Unidos em questões cibernéticas. Em 2017, em reunião do G20, realizada na Alemanha, Vladimir Putin propôs a criação do grupo de trabalho cibernético EUA-Rússia, que o presidente Trump chamou de "uma unidade impenetrável de segurança cibernética". Em dezembro do mesmo ano, o *BuzzFeed* informou que o vice-ministro das Relações Exteriores da Rússia havia proposto um acordo segundo o qual ambos os países concordariam em não interferir na política interna de cada um, porém as autoridades dos EUA rejeitaram esse acordo (GRIGSBY, 2018).

Na opinião de Grigsby (2018), a oportunidade mais promissora para a cooperação cibernética EUA-Rússia viria no outono de 2018 nas Nações Unidas, na qual a Rússia proporia uma resolução buscando o endosso da Assembléia Geral de um código de conduta

para a atividade do Estado no ciberespaço. Mas, em novembro de 2018 no Fórum da Paz de Paris, o presidente francês Emmanuel Macron lançou um acordo internacional para fortalecer a cibersegurança, com o objetivo de garantir com que os signatários respeitem uma série de princípios comuns para proteger o espaço digital, para combater o roubo de propriedade intelectual online e impedir governos de usar ciberataques para esconder esforços de espiar ou influenciar processos eleitorais outros países, no entanto os Estados Unidos e a Rússia não assinaram o documento (FRANÇA, 2018).

Desta forma, há fortes indícios de que as relações entre os Estados Unidos e a Rússia pós Snowden não foram afetadas significativamente, uma vez que sua relação sempre passou por momentos de aproximação e distanciamento. Mas, vale destacar que a informação é e sempre será um elemento de importância vital para os atores mais importantes do Sistema Internacional, uma vez que as relações entre os Estados estão condicionadas aos seus interesses e a tecnologia está na vanguarda e é uma ferramenta essencial dos Estados (USECHE, 2014).

5 CONSIDERAÇÕES FINAIS

Como exposto, o objetivo geral deste artigo é avaliar como a cibersegurança tornou-se estratégia política dos Estados Unidos e da Rússia no marco temporal de 2000 a 2018, visto que em 2000, foi o ano de ascensão da tecnologia e 2018 foi o ano da última estratégia dos Estados Unidos, baseando-se no questionamento: Como as relações entre os Estados Unidos e a Federação Russa foram afetadas após o Caso Edward Snowden no período de 2013-2018?

O avanço da tecnologia foi o *gap* que os Estados precisavam para se desenvolver, tanto economicamente, quanto politicamente e militarmente. Pois, possibilitou uma reconfiguração nas relações de poder entre os países, logo, ao mesmo tempo em que a tecnologia gerou independência de alguns Estados, a mesma também gerou dependência por parte de outros.

A informação, com a ascensão tecnológica, tomou proporções ainda maiores e inimagináveis, através da difusão das redes, ou seja, a informação passou a ser alcançada em qualquer parte do mundo, por qualquer pessoa, por qualquer Estado. Contudo, ao mesmo tempo em que o desenvolvimento tecnológico contribuiu positivamente, ele também contribui negativamente, no que cerne as relações e as mudanças no cenário internacional.

Quando o poder informacional alcança uma alta escala de importância no sistema internacional, a sociedade, as empresas, organizações e Estados devem se questionar sobre do

que o outro é capaz de fazer com os seus dados e a proporção que esse compartilhamento pode causar nacionalmente e internacionalmente, pois, o avanço tecnológico cria um cenário de insegurança e desconfiança.

A problemática da inovação tecnológica está no cerne da segurança, posto que existe uma necessidade de proteção e de garantia de direitos fundamentais, como a privacidade. Para isso, é primordial que os Estados possam proporcionar políticas e estratégias de segurança, visto que o ciberespaço é atualmente um cenário de ataques cibernéticos e de espionagem, mas e quando são os Estados que promovem os ataques e a espionagem, o que fazer?

Foi a partir do Caso Snowden que tivemos conhecimento dos documentos pertinentes a programas de vigilância por parte dos Estados Unidos, e através do ocorrido à pauta de segurança cibernética ganhou espaço na agenda internacional, porém provocando tensões entre algumas nações, entre eles, Rússia e Estados Unidos, houve uma necessidade por parte dos mesmos de zelar pela sua segurança contra ameaças proveniente do ciberespaço.

As estratégias dos Estados Unidos e da Rússia buscaram de diferentes formas, mas com o mesmo objetivo, garantir a sobrevivência do seu *status quo* no cenário internacional, porém a estrutura cibernética dos Estados Unidos é um pouco mais complexa do que a da Rússia, devido a sua organização e ao encargo das funções de cada entidade.

Os Estados Unidos desenvolveram ao longo de quinze anos, quatro estratégias – a *The National Strategy to Secure Cyberspace* em 2003, a *DoD's Strategy for Operating in Cyberspace* em 2011, a *The DoD Cyber Strategy* em 2015 e a última, *National Cyber Strategy* em 2018 – as quais buscaram o envolvimento e a capacitação dos americanos no desempenho do espaço cibernético, com o objetivo de fazer uma colaboração conjunta entre os diversos setores da sociedade. As estratégias ao longo dos anos foram apenas se adaptando e complementando, a única que mostrou um caráter mais realista e ofensivo foi a de 2018, quando deu abertura para uma moldagem de competição e possível uso da guerra e da construção de uma força letal para alcançar os objetivos nacionais.

A Rússia adotou uma abordagem diferente com foco na segurança da informação e a estabilidade interna, na qual buscou com que o Estado assumisse o papel de proteção contra as ameaças externas. Ao logo de quinze anos, desenvolveu duas estratégias, a Estratégia Nacional de Segurança da Federação Russa e a Doutrina de Segurança da Informação da Federação Russa – ambas em 2015 – e sancionou a Lei da Federação Russa 07.07.2006 № 149-ФЗ "Informação, Tecnologias de Informação e Proteção das informações", em 2006. A Rússia tem a visão de que a informação ela pode ser considerada uma arma, principalmente se tratando das Operações cibernéticas ofensivas (OCOs), pois pode ser considerada como um

meio para alcançar a influência no meio internacional. Não explicitamente, como deixou claro os Estados Unidos, a Rússia também busca garantir a defesa nacional e o prestígio a âmbito internacional.

Em 2013, os dois países assinaram um acordo o qual criaria um vínculo na comunicação direta entre Moscou e Washington nos assuntos pertinentes a segurança, porém após o acordo as revelações de Snowden começaram a serem liberadas e logo em seguida Vladimir Putin – Presidente da Rússia – concedeu asilo temporário a Snowden, por conseqüência disto, as relações que até o momento esta harmoniosa foram alteradas pelo acontecimento.

A relação russo-americana sempre foi marcada por inconstâncias, pois, ambas buscam ser a potência internacional mais temida e influente, a qual visa apenas os seus interesses nacionais desde a Guerra Fria. No meio cibernético não é diferente, é uma contínua disputa por poder tecnológico, a melhoria das relações entre ambos são apenas temporária, até onde lhe convém ou até onde quem está ganhando mais.

Desde 2013, a Rússia vem tentando criar um acordo de cooperação com os Estados Unidos e os mesmos sempre se opõem a resolução devido a falta de entendimento das normas do Estado no ciberespaço. Portanto, o desafio da cibersegurança se dá devido à falta de marcos legais e de regimes internacionais que tenham em vista a necessidade de uma cooperação que regulamente o cenário cibernético, e não a criação de um ambiente de disputa por poder das nações independentes.

Desta forma, é plausível considerar que as medidas tomadas por Snowden tiveram uma grande repercussão no ambiente internacional que fizeram com que os Estados voltassem a olhar o âmbito nacional e analisassem suas estratégias de Cibersegurança a nível internacional. Porém, a relação entre Estados Unidos e Rússia sempre passou por uma agitação, o Caso Snowden foi apenas mais um acontecimento para balancear a instabilidade da relação russo-americana, a qual sempre foi medida por interesses que podem ser condizentes e acordados agora, mas que futuramente podem sofrer alterações, uma vez que cada potência busca pela ampliação do seu poder e dos espaços de influência no mundo.

CYBERSECURITY: THE NEW CONFIGURATION OF POWER IN INTERNATIONAL RELATIONS AFTER EDWARD SNOWDEN (2000-2018)

ABSTRACT

The present work of course completion has as a general objective to evaluate how cybersecurity has become the political strategy of the United States and Russia. In view of the advent of technology in the 21st century, it is necessary to analyze how international relations have been affected by this resource, especially with regard to foreign policy problems, as will be analyzed between the United States and Russia after the Edward Case Snowden, since the first refers to the country in which Snowden was a systems analyst for the Central Intelligence Agency (CIA) and the National Security Agency (NSA) and the second one for the country that offered asylum to the former agent. So how do relations between the United States and the Russian Federation have been affected after the Edward Snowden Case in the period 2013-2018? The work focuses on the specific objectives: i) Analyze the advent of technologies by turning to International Relations; (ii) To review the Cybersecurity policies of the United States and Russia in the period 2012-2018; and (iii) To explore the impacts on relations between the United States and the Russian Federation after the asylum granted to Edward Snowden. Therefore, the hypothesis of the greater the advent of technology, the lower the stability between the relations of the States. Lastly, the research has an exploratory character and the methodology used is qualitative using a bibliographic theoretical reference of specialized periodicals and security documents from the USA and Russia.

Keywords: Snowden. Cibersecurity. Russian-American relations. Cyber Policies.

6 REFERÊNCIAS

ACÁCIO, Igor Daniel Palhares. **Segurança Internacional no século XXI: o que as teorias de Relações Internacionais têm a dizer sobre o ciberespaço?** In: OLIVEIRA, Marcos Aurélio Guedes de; GAMA NETO, Ricardo Borges; LOPES, Gills Vilar (Org.). Relações Internacionais Cibernéticas (CiberRI): Oportunidades e desafios para os Estudos Estratégicos e de Segurança Internacional. 23. ed. Recife: Ufpe, 2016. p. 40-41

BJOLA, Corneliu; HOLMES, Marcus**. Digital Diplomacy**. 1. ed. Routledge, 2015

BOBBIO, Norberto. **O futuro da democracia: uma defesa das regras de jogo**. Tradução de Marco Aurélio Nogueira. Rio de Janeiro: Paz e Terra, 1996.

BUZAN, B; HANSEN, L. **A Evolução dos Estudos de Segurança Internacional.** São Paulo: Unesp, 2012.

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

CANABARRO, Diego R.; FERREIRA, Thiago B. **As reações brasileira ao Caso Snowden: Implicações para o Estudo das Relações Internacionais em um mundo interconectado**. V. 6, n. 30 (2015). Disponível em: <https://seer.ufrgs.br/ConjunturaAustral/article/view/54617>. Acesso em 10 fev. 2019

CARPES, Mariana. **A política nuclear brasileira no contexto das relações internacionais contemporâneas.** Domínio tecnológico como estratégia de inserção internacional. PPGRI/PUC-RJ, 2006. Disponível em: <

http://www.iaea.org/inis/collection/NCLCollectionStore/_Public/40/073/40073553.pdf > Acesso: 05 fev 2019

CARVALHO, Paulo S. M. de. **A defesa cibernética e as infraestruturas críticas nacionais**. Disponível em: <http://www.nee.cms.eb.mil.br/index.php/biblioteca/101-a-defesa-cibernetica-e-as-infraestruturas-criticas-nacionais>. Acesso em: 22 mar. 2019

CASTILHO, C. **A diplomacia (ou guerra) da informação**, 2013. Disponível em: < http://observatoriodaimprensa.com.br/codigoaberto/post/a_diplomacia_ou_guerra_da _informacao>. Acesso em 12 fev. 2019

CAVELTY, Myriam Dunn. **Cyber-security and threat politics: US efforts to secure the information age.** Routledge, 2007.

CENTRE FOR ANALYSIS OF STRATEGIES AND TECHNOLOGIES (CAST). **"We Help Russian Companies to Enter New Markets"**, interview with Sergey Ryabkov, Deputy Minister of Foreign Affairs in Russia. March 14-20, 2012. Disponível em: <http://cast.3ebra.com/eng/journal/2010/> Acesso em: 18 mar. 2019

CEPIK, M; CANABARRO, D; BORNE, T. **A securitização do ciberespaço e terrorismo: uma abordagem crítica.** In: SOUZA, A; NASSER, R; MORAES, R. Do 11 de Setembro de 2001 à Guerra ao Terror: Reflexões sobre o terrorismo no século XXI. Brasília: IPEA, 2014. cap. 7.

CLARKE, Richard A.; KNAKE, Robert K. **Guerra Cibernética: a próxima ameaça à segurança e o que fazer a respeito.** Brasport: Rio de Janeiro, 2010.

COMPUTERWORLD. **Estados Unidos e Rússia em acordo de cibersegurança.** 2013. Disponível em: <https://www.computerworld.com.pt/2013/06/18/estados-unidos-e-russia-em-acordo-de-ciberseguranca/> Acesso em: 18 mar. 2019

CRUZ, Ricardo Henrique Paulino da. **SETOR CIBERNÉTICO NO EXÉRCITO BRASILEIRO**, 2012 . Disponível em: <http://www.eceme.ensino.eb.br/ciclodeestudosestrategicos/index.php/CEE/XICEE/paper/vie >. Acesso em 12 fev. 2019

DEMIDOV, Oleg. "**U.S.-Russian CBMS in the Use of ICTS: A Breakthrough with an Unclear Future,**" *Security Index*, vol. 20 nos. 3–4 (108–9) (2014), pp. 69–80

ESPOSITO, Richard; COLE, Matthew; SCHONE, Mark. **Exclusive: Edward Snowden gives wide-ranging interview to Brian Williams**. NBC News. 2014. Disponível em: <https://www.nbcnews.com/storyline/nsasnooping/exclusive-edward-snowden-gives-wide-ranging-interview-brian-williams-n110351>. Acesso em 10 fev. 2019

FISHER, Eric A. **Cybersecurity Issue and Challenges: In Brief**. Congressional Research Service: s.l., August, 2016. Disponível em: < https://fas.org/sgp/crs/misc/R43831.pdf> Acesso em 12 fev. 2019

FRANÇA. **Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace**. Disponível em: <https://www.diplomatie.gouv.fr/en/french-foreign-

policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in> Acesso em: 20 mar. 2019

FRITSH, Stefan. **Conceptualizing the Ambivalent Role of Technology in International Relations: Between Systemic Change and Continuity**. IN MAYER, Maximilian. Et al. The Global Politics of Science and Technology – vol.1 – Concepts from international relations and other disciplines, Springer, 2014. Disponível em: < http://www.springer.com/us/book/9783642550065> Acesso em 05 fev. 2019

GEERS, K. **Cyber War in Perspective: Russian Aggression Against Ukraine**. NATO CCDCOE Publications: Tallinn, 2015.

GELLMAN, B.; POITRAS, L. (2013). **U.S. British Intelligence mining data from nine U.S. Internet companies in broad secret program.** Washington Post. Disponível em: <https://www.washingtonpost.com/investigations/usintelligence-mining-data-from-nine-us-internet-companies-in-broad-secretprogram/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html>. Acesso em 11 fev. 2019

GILES, D. (2010). **Psychology of the media**. New York: Palgrave Macmillan.

GREENWALD, Glenn; MACASKILL, Ewen; POITRAS, Laura. **The 29-year-old source behind the biggest intelligence leak in the NSA's history explains his motives, his uncertain future and why he never intended on hiding in the shadows**. The Guardian. 2013. Disponível em <https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>. Acesso em 10 fev. 2019

GORST, Isabel. **Russia Gives Edward Snowden Asylum for Three More Years**, L.A. TIMES (Aug. 7, 2014, 10:37AM), Disponível em: <http://www.latimes.com/world/europe/la-fg-russia-snowdenasylum-20140807-story.html> Acesso em: 18 mar. 2019

GRAY, C**. Making Sense of Cyber Power: Why the Sky is Not Falling.** S Army War College Strategic Studies Institute, 2013.

GREENWALD, G. **NSA collecting phone records of millions of Verizon customers daily.** *The Guardian*. 6 jun. 2013.

GRIGSBY, Alex. Russia Wants a Deal with the United States on Cyber Issues. Why Does Washington Keep Saying No? 2018. Disponível em: < https://www.cfr.org/blog/russia-wants-deal-united-states-cyber-issues-why-does-washington-keep-saying-no> Acesso em: 20 mar. 2019

HANSEN, Lene; NISSENBAUM, Helen. (2009) **Digital Disaster, Cyber Security e a Escola de Copenhague. Estudos Internacionais Quarterly,** vol. 53, p. 1155-75 [1155-75] Disponível em: <http://www.nyu.edu/projects/nissenbaum/papers/digital%20disaster.pdf>. Acesso em 09 fev. 2019

HERRINGTON, William C.*"**Snowed In" na Rússia: uma análise histórica da extradição americana e russa e como a saga de Snowden pode impactar o futuro***, 48 W ASH . UJL & P OL'Y 321 (2015), Disponível em: <https://openscholarship.wustl.edu/law_journal_law_policy/vol48/iss1/16>

Acesso em: 19 mar. 2019

HOBSBAWN, E. **Era dos extremos: o breve século XX**. 2ª edição. São Paulo: Companhia das Letras, 1995.

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION (ISACA), (2013). **Transforming Cybersecurity.** Rolling Meadows: ISACA.

JUBRAN, Bruno Mariotto. **A Política de Grandeza da Rússia em Formação: uma síntese do período pós-soviético.** REVISTA PARANAENSE DE DESENVOLVIMENTO, Curitiba, v.36, n.129, p.71-98, jul./dez. 2015

KOHN, Karen; MORAES, Cláudia H. de. **O impacto das novas tecnologias na sociedade: conceitos e características da Sociedade da Informação e da Sociedade Digital**. Disponível em: <https://www.intercom.org.br/papers/nacionais/2007/resumos/R1533-1.pdf>. Acesso em 05 fev. 2019

KORTUNOV, S. V**. A atual política externa da Rússia: estratégia de envolvimento seletivo**. Moscou: HSE, 2009. Título original: Sovremennaya vneshnyaya politika Rossii: strategiya izbiratel'nosti vovlechenosti.

LAFEBER, W. **America, Russia and the Cold War**, 1945-1996. 8th edition. New York:McGraw-Hill, 1997.

LE PARISIEN. (2013, 3 de julho). **L'affaire Snowden, un scandale mondial**. Le Parisien. Disponível em: <http://www.leparisien.fr/international/chronologieinteractive-l-affaire-snowden-un-scandale-mondial-03-07-2013-2950953.php#xtref=https%3A%2F%2Fwww.google.pt%2F>. Acesso em 11 fev. 2019

LEONIDOVICH, Tsirlov Valentin de**. Quadro jurídico segurança cibernética Federação Russa.** Disponível em: <https://cyberleninka.ru/article/n/pravovye-osnovy-kiberbezopasnosti-rossiyskoy-federatsii.pdf> Acesso em: 21 fev. 2019

LEVY, P. **As tecnologias da inteligência.** Rio de Janeiro: Ed. 34, 1993.

_____. A **EMERGÊNCIA DO CYBERSPACE E AS MUTAÇÕES CULTURAIS**. Festival Usina de Arte e Cultura, em Outubro, 1994 Prefeitura Municipal de Porto Alegre. Disponível em: <http://www1.portoweb.com.br/pierrelevy/aemergen.html.>. Acesso em 12 fev. 2019

LIBICKI, Martin C. **Cyberdeterrence and Cyber War**. Santa Monica: RAND, 2009.

LIPOVETSKY, Gilles. **A cultura-mundo: resposta a uma sociedade desorientada**. São Paulo, 2011, p. 76.

LOPES, Gills V. **Relações Internacionais Cibernéticas (CiberRI): Uma defesa acadêmica a partir dos estudos de segurança internacional**. Recife: UFPE, 2016. Disponível em: <https://www.academia.edu/31120775/_TESE_DE_DOUTORADO_Rela%C3%A7%C3%B5es_Internacionais_Cibern%C3%A9ticas_CiberRI_uma_defesa_acad%C3%AAmica_a_partir_dos_Estudos_de_Seguran%C3%A7a_Internacional>. Acesso em 09 fev. 2019

LOPES, Gills; TEIXEIRA JR, Augusto. **O Ciberespaço é o novo front: implicações para o pensamento estratégico.** Trabalho apresentado na I Conferência Nacional da ILA (*International Law Associations*)-Brasil. João Pessoa: ILA-Brasil, 2010.

LOPES, João R. da C. C, **A Estratégia de Segurança Nacional da Federação Russa até o ano de 2020.** PADECEME, Rio de Janeiro, v. 10, n. 19, p. 05, 02/2017. Disponível em:<http://www.eceme.eb.mil.br/images/docs/PADECEME_v10_n19_Edicao_2017.pdf> Acesso em: 5 mar. 2019

LYON, David. **As apostas de Snowden: desafios para entendimento de vigilância hoje**. Cienc. Cult., São Paulo, v. 68, n. 1, p. 25-34, Mar. 2016. Disponível em: <http://cienciaecultura.bvs.br/scielo.php?script=sci_arttext&pid=S0009-67252016000100011&lng=en&nrm=iso>. Acesso em 10 fev. 2019

MALIK, Mohan. **Technopolitics: how technology shapes relations among nations.** In: The interface of science, Techonology and Security: Areas of most concern, now and ahead. 2012. Disponível em: <http://apcss.org/wp-content/uploads/2012/12/Mohan-Malik.pdf> Acesso em 05 fev. 2019

MATTA, Fernando Reyes. A **informação na nova ordem internacional.** Rio de Janeiro: Paz e Terra, 1980.

MAURER, Tim. HINCK, Garret**. Parts of this are based and include extracts from "Russia: Information Security Meets Cyber Security**", in Confronting an "Axis of Cyber?" edited by Fabio Rugge, ISPI, October 25, 2018, 39-58. Disponível em: <https://www.ispionline.it/sites/default/files/pubblicazioni/cyber_def_web2.pdf> Acesso em: 12 fev. 2019

MUNK, Tine Hojsgaard.**Cyber Security in the European Region: Antecipatory Governance and Practice.** 2015. Thesis (Doctor of Philosophy). University of Manchester, Manchester.

NUNES, Paulo Viegas. **Ciberespaço, ciberviolência e o uso organizado da força**. Janus 2014 - Metamorfoses da violência (1914-2014), p. 146. Disponível em: <http://repositorio.ual.pt/bitstream/11144/2902/1/3.33_PauloVNunes_Ciberespaco.pdf>. Acesso em 15 dez. 2018

NYE, Joseph S. Jr. **"Cyber Power"** em O futuro do poder no século XXI (New York: Public Affairs Press, 2011)

NYE Jr, Joseph S Jr. **Soft Power. Foreign Policy**, v. Twentieh Anniversary, n. 80, p. 153-171, 1990e. In: NYE,Joseph S. Jr. Power in the Global Information Age. New York: Routledge, 2004b, pp 68-80

OBAMA, B. PUTIN, V. **Joint Statement by the Presidents of the United States of America and the Russian Federation on a New Field of Cooperation in Confidence Building**. 2013. Disponível em: <https://obamawhitehouse.archives.gov/the-press-office/2013/06/17/joint-statement-presidents-united-states-america-and-russian-federatio-0>. Acesso em: 16 mar. 2019

OPPERMANN, Daniel. **O cenário de cibersegurança depois de Snowden e consequências no Brasil.** OBSERVARE - JANUS 2014 - Metamorfoses da violência (1914-2014). p. 148-149 Disponível em: <http://repositorio.ual.pt/bitstream/11144/2903/1/3.34_DanielOppermann_Ciberseguranca.pdf>. Acesso em 15 dez. 2018

OSNOS, Evan, REMNICK, David, YAFFA, Joshua. (2017) **"Trump, Putin e a Nova Guerra Fria".** Disponível em: <https://www.newyorker.com/magazine/2017/03/06/trump-putin-and-the-new-cold-war> Acesso em: 17 fev. 2019

PERNIK, Piret; WOJTKWIAK, Jesse, VERSHOOR-KIRSS, Alexander. **National Cyber Security Organisation: United States.** CCDCOE: Tallin, 2012 Dísponível em: <https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_USA_122015.pdf> Acesso em 10 fev. 2019

PIMENTEL, Cauê. **Notas Analíticas Sobre o Conceito de Dissuasão Aplicado ao Fenômeno da Cibersegurança.** XI Encontro da ABCP: Brasília, agosto, 2014. Disponível em: <http://conferencias.fflch.usp.br/sdpscp/IVsem/paper/download/175/129> Acesso em 09 fev. 2019

POITRAS, L., ROSENBACH, M., SCHMID, F. & STARK, H. (2013, 29 de junho). **Attacks from America: nsa spied on European Union offices. Der Spiegel.** Disponível em: <http://www.spiegel.de/international/europe/nsa-spied-on-european-unionoffices-a-908590.html>. Acesso em 11 fev. 2019

RECUERO, Raquel. **Redes sociais na internet.** Porto Alegre: Sulina, 2012.

REMINGTON, Thomas. SPIRITO, Chris. CHERNENKO, Elena. DEMIDOV, Oleg. KABERNIK, Vitaly. **Toward U.S.-Russia Bilateral Cooperation in the Sphere of Cybersecurity.** 2016. Disponível em: <https://futureofusrussiarelations.files.wordpress.com/2016/06/wg_working_paper7_cybersecurity_final.pdf> Acesso em: 16 mar. 2019

ROCHA, William M. **TECNOLOGIA ENQUANTO "NOVA" FONTE DE PODER NAS RELAÇÕES INTERNACIONAIS: a Vanguarda estratégica e os Gap's tecnológicos. 2016.** Disponível em: <http://www.seminario2016.abri.org.br/resources/anais/23/1474739168_ARQUIVO_ROCHA,W.TecnologiaePodernasRI.pdf>. Acesso em 01 fev. 2019

ROCHA, William M. **Tecnologia, poder e relações internacionais.** 2017. Disponível em: <https://www.mundorama.net/?article=tecnologia-poder-e-relacoes-internacionais-por-william-rocha>. Acesso em 01 fev. 2019

ROSA, Gabriel Artur Marra, SANTOS, Benedito Rodrigues dos. **Facebook e As Nossas Identidades Virtuais**. Brasilia: Thesaurus, 2013.

RÚSSIA. **Decreto do Presidente da Federação Russa nº 683**, de 31 de Dezembro de 2015, Стратегии национальной безопасности Российской Федерации до 2020 года. (Estratégia de Segurança Nacional da Federação Russa até o ano de 2020). Disponível;

<http://pravo.gov.ru/proxy/ips/?docbody=&prevDoc=102129631&%20backlink=1&&nd=102385609> Acesso em: 22 fev. 2019

RÚSSIA. **Lei Federal nº 149-FZ,** de 27 de julho de 2006. Federal Law on Information, Information Technologies and Protection of Information, traduzido pela Organização Mundial da Propriedade Intelectual. Disponível em: <https://wipolex.wipo.int/en/text/371388> Acesso em: 17 fev. 2019

SELEZNEVA, L. Post-Soviet russian foreign policy: between doctrine and pragmatism. **European Security**, v. 11, n. 4, p. 10-28, 2002.

SENHORAS, Eloi. (2014). **Movimentos pendulares nas relações bilaterais entre Rússia e Estados Unidos.** Conjuntura Global. 3. 10.5380/cg.v3i2.37590.

SHAKARIAN, Paulo; SHAKARIAN, Jana; RUEF, Andrew. **Introduction to CyberWarfare: A Multidisciplinary Approach**. Masachuttes: Elsevier, 2013.

SHARIKOV, Pasha. 2013. **Cybersecurity in Russian-U.S. Relations**. Disponível em: <https://www.cissm.umd.edu/publications/cybersecurity-russian-us-relations-0> Acesso: 19 mar. 2019

SHELDON, John B. "Deciphering Cyberpower Strategic Purpose in Peace and War". **Strategic Studies Quarterly.** v.5 no. 2, 2011. p.95-112.

SILVEIRA, Henrique Flávio Rodrigues da. **Um estudo do poder na sociedade da informação**. Ci. Inf. Brasília, v. 29, n. 3, p. 79-90, dezembro de 2000. Disponível em <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0100-19652000000300008&lng=en&nrm=iso>. Acesso em 12 fev. 2019.

SINGER, P. W.; FRIEDMAN, Allan. **Cybersecurity and Cyberwar: What everyone needs to know**. Oxford University Press: New York, 2014. Disponível em: <https://news.asis.io/sites/default/files/Cybersecurity_and_Cyberwar.pdf>. Acesso em 09 fev. 2019.

SOUZA JR, Alcyon F. de. **SEGURANÇA CIBERNÉTICA: Política Brasileira e a Experiência Internacional.** Dissertação apresentada em Gestão do Conhecimento e Tecnologia da Informação da Universidade Católica de Brasília. 2013. Disponível em: <https://bdtd.ucb.br:8443/jspui/bitstream/123456789/1417/1/Alcyon%20Ferreira%20de%20Souza%20Junior.pdf>. Acesso em 12 fev. 2019

THE INTERNACIONAL TELECOMMUNICATIONS UNION (ITU), (2008). **Overview of Cybersecurity**. Disponível em: <https://www.itu.int/rec/T-REC-X.1205-200804-I>. Acesso em 09 fev. 2019

THOMAS, Timothy, **"Nation-state Cyber Strategies: Examples from China and Russia,"** in Cyber powerand National Security, 2009, p.486.

TIRREEL, Wiliam K. **United States Cybersecurity Strategy, Policy, and Organization: poorly postured to cope with a post-9/11 security environment?** The George Washington University: Washington, 2012. Disponível em: <https://www.hsdl.org/?view&did=729810>.

Acesso em: 12 fev. 2019

UNITED NATIONS (2013). **General Assembly backs right to privacy in digital age**. UN News Centre. Disponível em: <http://www.un.org/apps/news/story.asp?NewsID=46780&Cr=privacy&Cr1=#.VL5wx0esVyW>. Acesso em 11 fev. 2019

UNITED NATIONS. **"Developments in the Field of Information and Telecommunications in the Context of International Security**," Blue Book Study Series, No. 33, 2001, p. 38.

UNITED STATES. **Department Of Defense's Strategy for Operating in Cyberspace**. Department of Defense: Washington, July, 2011. Disponível em: <http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf> Acesso em: 16 fev. 2019

_____. **Release of the 2018 National Cyber Strategy**. Disponível em: <https://www.state.gov/r/pa/prs/ps/2018/09/286093.htm> Acesso em: 25 fev. 2019

_____. **The DoD Cyber Strategy**. Department of Defense: Washington, april, 2015. Disponível em: <http://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf > Acesso em: 16 fev. 2019

_____. **The National Strategy to Secure Cyberspace**. The White House: Washington, February, 2003. Disponível em: <https://www.energy.gov/sites/prod/files/National%20Strategy%20to%20Secure%20Cyberspace.pdf > Acesso em: 20 fev. 2019

USECHE, Daniela A. Alba. **El espionaje y agencias de seguridad: los Estados Unidos y la Federación Rusa**. 2014. Disponível em: < https://www.publicacionesfac.com/index.php/cienciaypoderaereo/article/view/138/276> Acesso: 20 mar. 2019

WEBER, Max. 1999. Economia e sociedade: fundamentos da sociologia compreensiva. Brasília: UnB. 2 v.

WEISS, Charles. Science, technology and international relations. **Technology in Society**, v. 27, n. 3, p. 295-313, 2005.

WHITESIDE, Kelly. **Obama sends Message by Naming Sochi Olympics Delegation, USA TODAY** (Dec. 20, 2013), Disponível em: <http://www.usatoday.com/story/sports/olympics/sochi/2013/12/17/ white-house-sochi-olympics-delegation-to-include-gay-athlete/4051581/.> Acesso em: 15 mar. 2019

YANNAKOGEORGOS, Pano. Internet Governance and National Security. **Strategic Studies Quarterly**, v. 6, n. 3, 2012, p. 102-125.