PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS
Programa de Pós Graduação em Relações Internacionais

Thiago Brandão Nogueira Germini

“THE SECURITY CHALLENGE OF OUR AGE”:
Uma análise dos discursos presidenciais e da NSA e DIA na gestão Obama sob a ótica de securitização

Belo Horizonte
2024

Thiago Brandão Nogueira Germini

“THE SECURITY CHALLENGE OF OUR AGE”:
Uma análise dos discursos presidenciais e da NSA e DIA na gestão Obama sob a ótica de securitização

Dissertação apresentada ao Programa de Pós-Graduação *Stricto Sensu* em Relações Internacionais da Pontifícia Universidade Católica de Minas Gerais, como requisito para obtenção do título de Mestre em Relações Internacionais.

Área de concentração: Segurança Internacional.

Linha de pesquisa: Segurança e Instituições Internacionais.

Orientador: Profª. Drª. Cristiano Garcia Mendes

Belo Horizonte
2024

FICHA CATALOGRÁFICA
Elaborada pela Biblioteca da Pontifícia Universidade Católica de Minas Gerais

Germini, Thiago Brandão Nogueira
G374s "The security challenge of our age" : uma análise dos discursos presidenciais e da NSA e DIA na gestão Obama sob a ótica de securitização / Thiago Brandão Nogueira Germini. Belo Horizonte, 2024.
100 f. : il.

Orientador: Cristiano Garcia Mendes
Dissertação (Mestrado) - Pontifícia Universidade Católica de Minas Gerais. Programa de Pós-Graduação em Relações Internacionais

1. Obama, Barack, 1961- - Discursos. 2. Snowden, Edward J., 1983-. 3. Cibernética. 4. Ciberespaço - Medidas de segurança. 5. Proteção de dados. 6. Segurança internacional. 7. Securitização. 8. Estados Unidos - Política e governo - Discursos, ensaios, conferencias. 9. Relações internacionais. I. Mendes, Cristiano Garcia. II. Pontifícia Universidade Católica de Minas Gerais. Programa de Pós-Graduação em Relações Internacionais. III. Título.

SIB PUC MINAS

CDU: 327.3

Ficha catalográfica elaborada por Pollyanna Iara Miranda Lima - CRB6/3320

Thiago Brandão Nogueira Germini

THE SECURITY CHALLENGE OF OUR AGE:
Uma análise dos discursos presidenciais e da NSA e DIA na gestão Obama sob a ótica de securitização

Dissertação apresentada ao Programa de Pós-Graduação *Stricto Sensu* em Relações Internacionais da Pontifícia Universidade Católica de Minas Gerais, como requisito para obtenção do título de Mestre em Relações Internacionais.

Orientador: Prof. Dr. Cristiano Mendes

Prof. Dr. Cristiano Garcia Mendes (Orientador) – PUC Minas

Prof. Dr. Jorge Mascarenhas Lasmar - PUC Minas

Prof. Dr. Áureo de Toledo Gomes - UFU

Prof. Dr. Leonardo César Souza Ramos - PUC Minas

Belo Horizonte, 02 de julho de 2024

AGRADECIMENTOS

A caminhada até aqui foi por momentos difícil e se cheguei até o final, é porque não andei sozinho. Meu maior agradecimento vai para a pessoa que tornou essa caminhada possível, minha mãe Fernanda. Seu apoio em todos os momentos (e correções ortográficas) permitiram que eu pudesse ter a dedicação que um mestrado demanda. Sem você eu certamente não estaria aqui. Aos meus familiares que me motivaram a sempre continuar: Vera Lúcia, Leonardo, Luciana, Maria Ilma e especialmente meu avô José Fernando e a meus irmãos Lara e Rafael.

À minha namorada Júlia, pelo companheirismo, compreensão e paciência de tentar entender todas as mudanças que ocorreram na pesquisa durante o percurso. Sua presença me ajudou a construir a disciplina necessária para a conclusão do estudo, além de me trazer confiança no trabalho que foi feito.

Aos meus amigos que me ouviram todas as minhas reclamações, dúvidas e andamentos do projeto entre sessões de Dungeons & Dragons e partidas de Magic: The Gathering durante os últimos anos: Ícaro, Daniel, Carolina e Fernando. E especialmente à Aguinner e Anderson, que além de serem meus colegas mais próximos auxiliaram na elaboração dos gráficos e formatação do trabalho.

Ao meu orientador desde a graduação, professor Cristiano, pela disponibilidade, compreensão e dedicação em me orientar nessa nova estrada. Agradeço também aos professores do PPG de Relações Internacionais da PUC Minas pelo compartilhamento de conhecimento e orientação no desenvolvimento do projeto e da pesquisa. Cabe também realçar que essa pesquisa foi possível devido ao apoio da Fundação de Amparo à Pesquisa do Estado de Minas Gerais (FAPEMIG). O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

RESUMO

A temática da cibersegurança se torna cada vez mais central dentro dos debates de segurança. O incidente com o malware Stuxnet e os vazamentos feitos por Chelsea Manning e Edward Snowden colocaram o governo estadunidense no centro das discussões sobre o tema. Dessa forma, o presente trabalho se propõe a fazer análise dos discursos presidenciais de Barack Obama, presidente em exercício durante esses incidentes, e dos diretores das agências relacionadas ao tema, a National Security Agency (NSA) e a Defense Intelligence Agency (DIA). Os discursos desses atores têm um peso considerável que pode moldar a opinião pública sobre a retirada das discussões sobre cibersegurança da esfera da política cotidiana e sua entrada na esfera de segurança. O objetivo geral foi a verificação ou não dessa tentativa. Nossa hipótese inicial foi de que houve essa tentativa de securitização devido à crescente importância da questão cibernética nas agenda de segurança dos EUA. O marco teórico utilizado para a análise foi Escola de Copenhague, devido ao seu foco na natureza discursiva do processo de securitização. A metodologia utilizada foi análise de discurso, que permite identificar termos e estratégias argumentativas para o convencimento da audiência alvo. Nossa conclusão ao final da pesquisa foi a de, baseado apenas numa análise discursiva, que não houve uma tentativa total de securitização da questão da cibersegurança.

Palavras-chave: Cibersegurança; Securitização; Estudos de Segurança Internacional; Barack Obama; Edward Snowden; Escola de Copenhague

ABSTRACT

The topic of cybersecurity is becoming increasingly central in debates about security. The incident with the Stuxnet malware and the leaks made by Chelsea Manning and Edward Snowden placed the US government at the center of discussions on the topic. Therefore, the present work proposes to analyze the presidential speeches of Barack Obama, president in office during these incidents, and the directors of the agencies related to the topic, the NSA and the DIA. The speeches of these actors have a considerable weight that can shape public opinion about the removal of discussions about cybersecurity from the sphere of everyday politics and its entry into the sphere of security. The general objective was to verify or not this attempt. Our initial hypothesis was that this securitization attempt occurred due to the growing importance of cyber issues on the US security agenda. The theoretical framework used for the analysis of the Copenhagen School, due to its focus on the discursive nature of the securitization process. A methodology used for discourse analysis, which allows identifying terms and argumentative strategies for the convention of the target audience. Our conclusion at the end of the research was, based only on a discursive analysis, that there was no total attempt to securitize the issue of cybersecurity.

Keywords: Cybersecurity; Securitization; International Security Studies; Barack Obama; Edward Snowden; Copenhagen School

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE QUADROS E TABELAS

Lista de siglas

CIA - Central Intelligence Agency
CS&C -Cybersecurity and Communications
DIA - Defense Intelligence Agency
DOD - Department of Defense
EC - Escola de Copenhague
EU - União Europeia
EUA - Estados Unidos da América
FBI - Federal Bureau Of Investigation
ISIS - Estado Islâmico do Iraque e Síria
NSA - National Security Agency
ONU - Organização das Nações Unidas
OTAN - Organização do Tratado do Atlântico Norte
PIB- Produto Interno Bruto
SIGINT - Inteligência de Sinais
URSS - União Das Repúblicas Socialistas Soviéticas
US-CERT - United States Computer Emergency Readiness Team

Sumário

INTRODUÇÃO

O avanço tecnológico que vem ocorrendo desde a segunda metade do século XX mudou radicalmente as formas como Estados e indivíduos se relacionam entre si. O aumento radical da velocidade de comunicação permitiu que a troca de informações que antes necessitavam ser fisicamente transportadas agora em instantes podem ser transmitidas para um número gigantesco de pessoas simultaneamente ao redor do globo.

Porém essas novas oportunidades para a troca de informações, comércio e integração também trazem consigo uma nova gama de riscos que antes não existiam. Apesar de hacks e roubos ocorrerem, o malware “Stuxnet” foi considerado a primeira arma digital, um software feito para causar danos e que inaugurou a era do *cyberwarfare* (Zetter, 2014). Os EUA são tidos como um dos principais envolvidos no desenvolvimento desse vírus, dada a capacidade tecnológica do país e sua posição de potência dentro do sistema internacional.

Porém os EUA também se viram envolvidos em seus próprios escândalos relacionados à cibersegurança. O caso de Chelsea Manning em 2009 e Edward Snowden mostraram como a internet pode ser utilizada para rapidamente publicizar erros cometidos pelo governo, de modo que ambos enfrentaram duras repercussões pelos seus atos. As revelações de Snowden de que o governo estadunidense espionava seus próprios cidadãos além de líderes globais foram especialmente danosas à imagem do governo para com seus cidadãos e internacionalmente.

Os incidentes citados ocorreram na gestão do 44º presidente dos EUA, Barack Obama. A gestão de Obama foi marcada pelo legado da presidência de George W. Bush na forma da Guerra ao Terror e dos conflitos em que os EUA haviam se envolvido (Iraque e Afeganistão). A crise econômica de 2008 ainda impactava a economia e a relação dos EUA com outros países, principalmente do mundo muçulmano, não se encontrava em boas condições.

Dessa forma, o presente trabalho visa analisar se houve um movimento securitizador vindo do presidente e dos diretores das agências ligadas ao Department of Defense (DOD), a National Security Agency (NSA) e a Defense Intelligence Agency (DIA) em relação à cibersegurança. Essas agências foram escolhidas devido ao fato de serem ligadas à questão da cibersegurança e também pelo fato da NSA ser a agência exposta por Snowden. Foram analisados apenas os

discursos proferidos pelo presidente e pelos diretores das agências, não contabilizando notas de imprensa, declarações oficiais por escrito ou outras formas de comunicação oficial. Os dados foram retirados diretamente dos sites da NSA, do DIA e do arquivo oficial da Casa Branca de Barack Obama .

A escolha pelos discursos se dá pelo fato que tendo como foco o processo de securitização como um movimento narrativo, atos de fala vindo de autoridades como o presidente e os diretores de agências governamentais têm considerável poder de convencimento para com a população. Dessa forma, a análise dos discursos do presente trabalho se torna especialmente relevante para compreender se houve um processo de securitização em relação à cibersegurança. Faz-se importante também lembrar que analisaremos apenas se houve uma tentativa de securitização, não o sucesso ou falha se a mesma for confirmada.

No Capítulo 1 se faz um retorno aos conceitos da teoria de securitização, os atores presentes nesse processo e as consequências do mesmo. A natureza discursiva do processo de securitização faz com que seja necessário que entendamos como um ato de fala pode convencer uma população alvo a legitimar a mudança de uma determinado tema para dentro da esfera da política de segurança. Se caracterizam também os três elementos necessários para que se identifique um processo de securitização: ameaça existencial, situação de emergência e possibilidade de quebrar regras.

No Capítulo 2 passamos para uma contextualização dos anos de presidência de Barack Obama, com um foco aprofundado nas questões de cibersegurança que se apresentaram durante esses anos. Inicialmente analisamos os antecedentes das eleições 2008, como a Guerra ao Terror e a crise financeira e seus impactos no ambiente político estadunidense da época. Após isso, passamos para um visão dos principais assuntos de geopolítica desse periódo, como a invasão da Crimeia pela Rússia e a ascensão do Estado Islâmico. Por fim passamos para uma análise focada na cibersegurança dentro do governo na gestão Obama,com uma atenção maior para o episódio relacionado ao ataque do malware Stuxnet e os escândalos sobre os vazamentos feitos por Chelsea Manning e Edward Snowden. O capítulo três irá apresentar o arcabouço metodológico do trabalho, demonstrando como a análise de discurso será utilizada para examinar os discursos selecionados.

Passando para os capítulos quatro, cinco e seis temos então uma análise dos discursos proferidos pelo presidente e pelos diretores das agências. Cada um

desses capítulos será focado em um dos elementos necessários para o processo de securitização: ameaça existencial, situação de emergência e possibilidade de quebra de regras. Foi feita uma seleção de termos relacionados ao processo de securitização e uma busca pela presença dos mesmos nos discursos selecionados. Após essa busca, analisamos o contexto em qual esses termos aparecem e se o emprego dos mesmos levava à um dos elementos necessários para um processo de securitização. Após essa análise passamos para as conclusões finais dos resultados da pesquisa.

1. A Escola de Copenhague e os processos de securitização

O campo de estudos de Segurança Internacional se encontra em uma posição central dentro do campo das Relações Internacionais. Devido à essa relevância diversas abordagens sobre o tema surgiram, cada uma com diferentes visões, postulados e formas de se pensar os dilemas de segurança presentes no sistema internacional. A Escola de Copenhague é uma das principais escolas de pensamento dentro do campo, de modo que se faz necessário um estudo da mesma para que possamos aplicá-la.

1.1 Estudos de segurança durante a Guerra Fria

O campo da Segurança Internacional tem sua gênese dentro das Relações Internacionais com a Guerra Fria. A polarização do sistema entre o bloco capitalista liderado pelos EUA e o bloco socialista liderado pela URSS levou a um estado de desconfiança entre os países, principalmente em relação àqueles que pertenciam ao bloco oposto ou mantinham posturas de neutralidade. (Kolodziej, 2005)

Nesse contexto, o foco principal do campo se mantém nas questões de natureza militar, visto que a insegurança dos países em relação às capacidades militares de outros países estava em alta. Segundo Muhammad e Riyanto (2021, p.230)

> A segurança era indissociável do aspecto militar, já que a maioria dos países se esforçavam para maximizar sua força militar, a fim de garantir a sua segurança e sobrevivência contra todos ameaças intencionais, incluindo tentativas de subjugar sua existência a outro Estado, organização terrorista ou outro grupo armado[1]

Fatores como avanços tecnológicos no desenvolvimento de armamentos, movimentações de tropas e pactos de defesa são alguns dos tópicos que se tornaram mais centrais e frequentes dentro dos estudos de segurança. Com essa

[1] Security was inextricably linked to the military aspect, as most countries strive to maximize their military strength in order to ensure their security and survival against all intended threats, including attempts to subjugate their existence to another state, terrorist organization, or other armed group. Tradução nossa.

priorização da esfera militar aliada ao contexto do sistema internacional da época, podemos facilmente compreender como as abordagens realistas das Relações Internacionais acabaram por serem as dominantes dentro dos estudos de segurança. A materialidade dos objetos de estudo era evidente, visto que essas ameaças eram tangíveis em sua natureza. Havia uma centralidade do Estado como o objeto ameaçado e também como o ameaçador, seguindo a lógica mais estatocêntrica observada na teoria Realista (Buzan, Waever, Wilde, 1998).

Podemos compreender o porquê da dimensão militar ser um dos pontos centrais nos estudos de segurança internacional. Conflitos militares, principalmente aqueles travados contra outros atores estatais, são situações onde as regras internas estabelecidas são temporariamente suspensas devido à ameaça existencial que uma guerra traz. Em situações de guerra total, onde toda a produção e toda a realidade social de um país se encontra direcionada para a guerra, garantias de direitos civis, liberdade de imprensa e liberdade econômica podem ser suprimidas pelo Estado em favor de uma coerência interna forçada necessária para que se possa lidar com a ameaça existencial de um situação de guerra total (Buzan, Waever, Wilde, 1998).

Um dos impactos das influências realistas e neorealistas dentro do campo da segurança é a pressão para um estreitamento do campo. Apenas assuntos de natureza militar eram considerados como ameaças ao Estado, de modo que visões mais amplas sobre o campo eram menos discutidas. De acordo com Buzan, Waever e Wilde APUD Lebow (1998, p.2)

> A defesa da posição tradicionalista começou com o desenrolar da Guerra Fria. Até tardiamente ainda se podiam encontrar argumentos para restringir o campo para “qualquer coisa que diga respeito à prevenção da guerra nuclear entre superpotências”[2]

Com o passar dos anos, desenvolveu-se dentro das Relações Internacionais uma literatura com vertentes mais liberais, com foco em fluxos de comércio e na cooperação entre os países. O chamado “debate neo-neo”[3], muito proeminente na

[2] The defense of the traditionalist position got underway as the Cold War unraveled. Until rather late one could still find arguments for restricting the field to “anything that concerns the prevention of superpower nuclear war”. Tradução nossa.

[3] O chamado “debate neo-neo” foi um embate de ideias entra teóricos neorrealistas e neoliberais na década de 1980 sobre a natureza do sistema anárquico e o papel da cooperação e do conflito entre

década de 80, no entanto, não foi tão impactante dentro dos estudos de segurança. Isso se deu devido ao fato de que os liberais tinham foco em questões de teor econômico, institucional e de cooperação. Os estudos de segurança então se mantiveram dentro da lógica realista de primazia da esfera militar. Um dos principais argumentos para essa visão mais "estreita" do campo, focada nas ameaças que outros Estados oferecem foi o de se manter uma coerência intelectual do campo, pois uma abertura maior para outros assuntos poderia acabar por expandir excessivamente a definição da área de estudos. Essa abertura, segundo Walt (1991) apud Buzan, Waever, Wilde (1998, p.3)

> Corre o risco de expandir excessivamente os "Estudos de Segurança"; por esta lógica, questões como poluição, doenças, abuso infantil ou recessões econômicas todos poderiam ser vistos como ameaças à "segurança". Definindo o campo dessa maneira destruiria sua coerência intelectual e tornaria mais difícil conceber soluções para qualquer um desses problemas importantes.[4]

Vemos então que o campo da segurança tem sua criação em um contexto geopolítico muito específico, que levou a disciplina a priorizar fatores e acontecimentos de natureza militar em primazia a outras discussões. A materialidade e o papel central do Estado dentro dos estudos foram marcas dos estudos de segurança dessa época. Porém com o passar do tempo, esse contexto geopolítico foi sendo alterado de modo que ocorreram mais aberturas para maiores mudanças e discussões dentro do campo.

1.2 O final da Guerra Fria e a ampliação dos estudos de segurança

Com a dissolução da União Soviética, um dos principais argumentos utilizado pelos defensores dessa definição mais militar e estadocêntrica foi perdido. Soma-se a isso o fato de que outros estudiosos já haviam mostrado um descontentamento

---

os Estados dentro do sistema, levando em conta a primazia do papel do Estado, a preferência sobre ganhos relativos *versus* ganhos absolutos entre outros temas.

[4] runs the risk of expanding "Security Studies" excessively; by this logic, issues such as pollution, disease, child abuse, or economic recessions could all be viewed as threats to "security." Defining the field in this way would destroy its intellectual coherence and make it more difficult to devise solutions to any of these important problems. Tradução nossa.

com essa abordagem clássica, tendo assim proposto novas abordagens dentro dos estudos de segurança que incluíssem temas fora do espectro militar, como questões de natureza econômica e ambiental. Segundo Baysal (2020, p.3)

> Devido à insatisfação com a estreita, estado-centrada e militar-orientada abordagem dos estudos de segurança tradicionais, novas abordagens de segurança começaram para emergir sob o tema geral de estudos críticos de segurança Essas novas abordagens ampliaram e aprofundou os estudos de segurança tanto agregando novos temas como meio ambiente e economia, quanto novos níveis como seres humanos individuais e segurança global[5]

Assim temos aqui dois fenômenos de expansão dentro dos estudos de segurança: um teórico e um de objeto. A expansão teórica significou que mais teorias das Relações Internacionais se debruçaram sobre a questão da segurança, tirando o monopólio que os realistas tinham sobre o campo. A expansão de objeto se refere ao fato de que agora se argumentava que mais tópicos e assuntos poderiam ser considerados questões de segurança para além apenas das questões militares. Essas expansões foram benéficas para o campo, visto que agora um maior número de pesquisadores estudava diferentes abordagens e objetos dentro dos estudos de segurança, o que permitiu uma visão mais abrangente e encompassadora sobre o campo como um todo.

A globalização dentro do sistema foi um fator importante na ampliação dos estudos de segurança, além da expansão de redes não-estatais de interação entre os países. Assuntos como a preservação ambiental, acordos comerciais e a cooperação internacional tiveram mais espaço dentro do debate geral do campo das relações internacionais, algo que foi refletido dentro do campo. Essa ampliação do debate sobre o campo levou à uma nova perspectiva sobre o que constituiria uma questão de segurança, de modo que Buzan, Waever e Wilde (1998) apontam quatro outros setores que podem se tornar questões de segurança devido à um mundo cada vez mais globalizado, interdependente e onde o papel da força militar vinha

[5] due to dissatisfaction with the narrow, state-centric, and military-oriented approach of traditional security studies, new approaches to security started to emerge under the general topic of critical security studies.1 These new approaches both widened and deepened security studies both by adding new issues like the environment and economics, and new levels like individual human beings and global security. Tradução nossa.

perdendo protagonismo. Esses setores são o político, econômico, social e ambiental.

No setor político, ameaças à segurança vem na forma de questionamentos em relação a elementos constituintes do Estado. Buzan, Waever e Wilde (1998) citam que ameaças à soberania, à legitimidade ou às instituições de Estado podem ser consideradas como ameaças existenciais, visto que se as mesmas são corroídas, a possibilidade de fragmentação nacional ou guerra civil se tornam maiores. Um caso que podemos utilizar para exemplificar essas ameaças no setor político é o dos movimentos que questionaram resultados eleitorais no Brasil e nos EUA, já que eles questionam a legitimidade das eleições de modo que podem criar crises de legitimidade dos governos eleitos.

No setor econômico, ameaças à segurança se caracterizariam como ameaças à economia nacional de determinados países. Essa ameaça provavelmente teria de afetar toda a cadeia produtiva e econômica de um país, não apenas grandes bancos ou empresas. De acordo com Buzan, Waever e Wilde (1998, p.22)

> Na economia de mercado, espera-se que as empresas, com poucas exceções, apareçam e desapareçam, e apenas raramente eles tentam securitizar sua própria sobrevivência. As economias nacionais têm uma maior reivindicação ao direito de sobrevivência[6]

Porém, no caso de economias onde uma empresa ou um conglomerado de empresas é responsável por uma parte considerável da economia, essas companhias podem ter uma chance maior de securitizar sua própria sobrevivência. Um país que se encontra nesse perfil é a Coreia do Sul, onde um pequeno número de companhias, os chaebols, concentra uma parcela enorme do PIB.[7]

O setor societal é aquele onde as ameaças são mais dificilmente definidas, pois ameaças à segurança no setor societal lidam com as identidades de grupo que não são necessariamente ligadas ao Estado . O dilema nas questões de segurança societal é que a mudança de identidades é algo que ocorre naturalmente, em ritmos

---

[6] In the market economy, firms are, with few exceptions, expected to come and go, and only rarely do they try to securitize their own survival. National economies have a greater claim to the right of survival. Tradução nossa.

[7] S. Korean chaebols comprise 84% of GDP but only 10% of jobs. Disponível em <https://english.hani.co.kr/arti/english_edition/e_business/949236.html>. Acesso em 19/04/2023

diferentes. Essa mudança seria securitizada em face de grandes mudanças em relação a essas identidades, muitas vezes devido a fatores exógenos à comunidade (Buzan, Waever, Wilde, 1998).

Já as ameaças no setor ambiental entram em voga quando temos um aumento da preocupação da sociedade global e dos atores internacionais com a preservação do meio ambiente e das diferentes espécies de seres vivos. A questão ambiental é o tema mais novo a ser contemplado dentro da agenda de segurança, principalmente devido ao crescente impacto das mudanças climáticas e com isso da conscientização de governos e de entidades da sociedade civil sobre o tema (Buzan, Waever, Wilde, 1998).

A incorporação desses temas antes excluídos dos debates sobre segurança traz consigo novas questões. Quando um tema é delimitado como uma questão de segurança, temos que ele sai da esfera da política cotidiana e entra na esfera da política de emergência.

Assim, a ampliação dos estudos de segurança veio com um olhar mais abrangente sobre o contexto no qual o sistema se encontrava após o fim da Guerra Fria e da bipolaridade dentro do sistema. Essa expansão possibilitou um aumento do escopo do campo, ainda que com essa expansão venham críticas em relação à uma suposta abertura exagerada na qual a definição de estudos de segurança seja perdida.

1.3 A Escola de Copenhague e o processo de securitização

É nesse contexto de expansão do campo dos estudos de segurança que temos a obra de Barry Buzan, Ole Waever e Jaap de Wilde Security: A New Framework for Analysis” de 1998. Nesta obra os autores se aprofundam nas discussões referentes a uma gama maior de assuntos do que apenas aqueles de natureza militar, como os autores realistas e defensores de uma visão mais estreita do campo, defendem. A grande contribuição que podemos ver da Escola de Copenhague dentro dos estudos de segurança é a profundidade com a qual os autores se debruçam sobre o processo de securitização, sobre como determinados temas se tornam questões de segurança. De acordo com os autores (1998, p. 23)

> Segurança é o movimento que leva a política para além das regras estabelecidas no jogo e enquadra a questão como um tipo especial de política ou como acima da política. A securitização pode, portanto, ser vista como uma versão mais extrema de politização.[8]

Dessa forma vemos que o processo de securitização se dá para além da esfera da política cotidiana. A politização de um tema é o movimento em que um determinado assunto é levado para dentro das arenas de discussão política de forma que normas, leis e outros tipos de movimentação política ocorram em relação a esse tema. A securitização pode ser considerada como um passo para além de um processo de politização normal (Buzan, Waever, Wilde, 1998), de forma que os processos políticos que seriam observados em um processo de politização de um tema não são mais suficientes para que se possa lidar com um determinado tema. Essa insuficiência dos processos políticos padrões se dá devido à uma presença de ameaça existencial que exige dos tomadores de decisão ações em caráter emergencial para lidar com essa determinada ameaça, além da possibilidade da quebra de regras anteriormente estabelecidas. De acordo com Balzacq, Leonard e Ruzicka (2015, p.495)

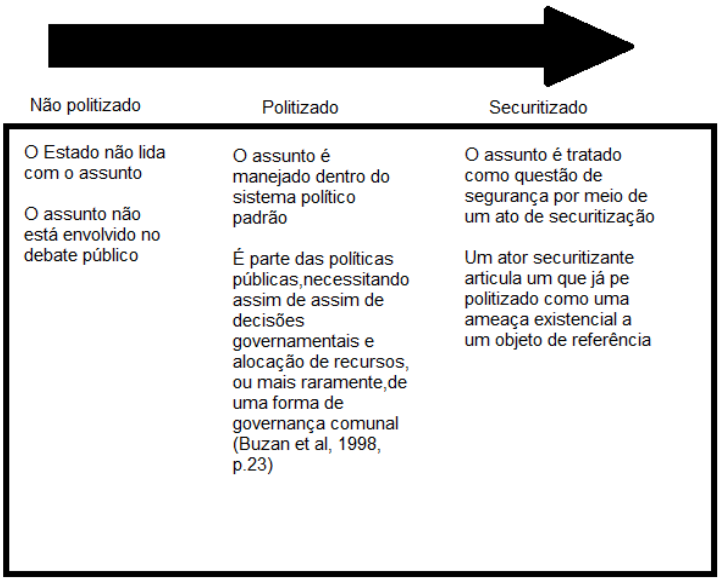
> A ideia-chave subjacente à securitização é que uma questão recebe relevância suficiente para ganhar o assentimento do público, o que permite que aqueles que estão autorizados a lidar com a questão para usar os meios que julgarem mais apropriados. Em outras palavras, a securitização combina a política de design de ameaças com a de gerenciamento de ameaças.[9]

---

[8] "Security" is the move that takes politics beyond the established rules of the game and frames the issue either as a special kind of politics or as above politics. Securitization can thus be seen as a more extreme version of politicization. Tradução nossa.

[9] The key idea underlying securitization is that an issue is given sufficient saliency to win the assent of the audience, which enables those who are authorized to handle the issue to use whatever means they deem most appropriate. In other words, securitization combines the politics of threat design with that of threat management. Tradução nossa.

Figura 1 - Processo de securitização



Fonte: (Contemporary Security Studies, 2013, p. 133)

Desse modo, vemos que nenhum assunto é por si só uma questão de segurança. Na verdade, o que se tem é um olhar lançado em determinados assuntos que os torna questões de segurança. A segurança é construída de forma a convencer o público que determinado assunto deve ser tratado como um tema de segurança, mas esse assunto não é assim por si próprio. Países que são aliados de longa data não tendem a construir percepções de ameaças em relação aos poderios militares uns dos outros. Ao mesmo tempo, um pequeno aumento de *capabilities* militares ou maior projeção internacional de um país tido como hostil pode ser rapidamente securitizado.

Vemos também que a Escola de Copenhague bebe de duas fontes teóricas distintas, o Construtivismo e o Realismo. A importância dada por Buzan, Waever e Wilde aos movimentos discursivos dentro do processo de securitização vai na direção oposta ao que se entendia nos estudos de segurança tradicionais, onde questões de natureza militar eram necessariamente consideradas questões de segurança. Mas eles ainda não abandonam totalmente as ideias realistas relacionadas às percepções de amigo/inimigo e de como o Estado acaba sendo o principal ator a ser ameaçado.

Além disso, temos dentro da teoria da escola de Copenhague a descrição do processo de desecuritização. Esse processo segue o caminho oposto do que foi

descrito, de modo que na dessecuritização um assunto antes alocado dentro da esfera da política de exceção acaba retornando ao debate político cotidiano. Principalmente em regimes democráticos, a manutenção de um estado de exceção pode levar à erosão de pontos centrais desse tipo de sistema político. Segundo Buzan, Waever e Wilde (1998, p. 29)

> A dessecuritização é a solução ideal de longo prazo, uma vez que significa não ter questões formuladas como “ameaças contra as quais temos contramedidas”, mas para tirá-los dessa sequência de ameaça-defesa e de volta a esfera pública

1.4 Elementos do processo de securitização

O processo de securitização como descrito por Buzan, Waever e Wilde é um processo discursivo que necessita que três fatores sejam observados para que ocorra. Segundo Taureck apud Buzan (2006, p.3) “um processo de securitização consiste em três etapas. São eles: (1) identificação de ameaça existencial; (2) ação de emergência; e (3) efeitos nas relações inter-unidades ao se libertar de regras”[10].

O elemento de ameaça existencial é necessário pois a ameaça à própria existência do elemento ameaçado alça à tomada de medidas não convencionais. De acordo com Buzan, Waever e Wilde (1998, p.24) “Se não lidarmos com este problema, todo o resto será irrelevante (porque não estaremos aqui ou não estaremos livres para lidar com isso à nossa maneira)[11]. Ou seja, com a própria existência do objeto de referência ameaçada, medidas extraordinárias se tornam aceitáveis e justificáveis. Essa ameaça existencial pode se caracterizar de diferentes maneiras dentro dos setores analisados por Buzan, Waever e Wilde. Ameaças existenciais no setor militar podem ser facilmente identificadas como movimentos de exércitos inimigos ou desenvolvimento de armas de destruição em massa, por exemplo. No setor econômico temos recessões ou quebras de grandes bancos, no setor político movimentos separatistas ou de questionamento do regime vigente. No setor ambiental, o aumento da temperatura global e o derretimento das

[10] A successful securitization consists of three steps. These are: (1) identification of existential threats; (2) emergency action; and (3) effects on inter-unit relations by breaking free of rules. Tradução nossa.
[11] If we do not tackle this problem, everything else will be irrelevant (because we will not be here or will not be free to deal with it in our own way. Tradução nossa.

calotas polares podem ser caracterizados como ameaças existenciais à espécie humana.

Do mesmo jeito temos a urgência na resolução de ameaças pois, se houvesse tempo hábil, soluções para essa ameaça poderiam ser discutidas e planejadas dentro da esfera política, com um amplo espaço para debate e participação de diversos setores da sociedade. O real espaço de tempo que configura urgência também é algo moldado de acordo com a natureza da ameaça em questão. Uma questão de urgência em relação ao derretimento das calotas polares pode representar anos, enquanto a resposta a um deslocamento de tropas inimigas para fronteiras deve ser dada em horas (Buzan, Waever, Wilde, 1998)

Esses dois fatores aliados levam a uma situação onde a quebra de regras estabelecidas se torna aceitável. Situações extraordinárias que exigem medidas drásticas em pouco tempo são casos onde o aumento do poder estatal para a resolução dessas ameaças se torna justificado visto o que está em jogo. De acordo com Hansen (2012, p.528) “há uma distinção entre o securitizado e o politizado, como "segurança' leva a política para além das regras estabelecidas do jogo e enquadra a questão como um tipo especial de política ou como acima da política”[12]. A quebra de regras e a suspensão de determinados processos delimitados dentro do jogo político tem como fim lidar com uma determinada ameaça existencial. Ou seja, inicialmente tem-se o entendimento que quando a situação for resolvida, as regras do jogo político voltam a imperar e os poderes expandidos do tomador de decisão são retornados ao seu estado anterior.

1.5 Atores do processo de securitização

Dada a natureza da segurança e dos processos de securitização como fenômenos sociais, devemos analisar os atores presentes nesses processos e quais papéis os mesmos desempenham. Buzan, Waever e Wilde (1998) elencam os principais atores presentes em um processo de securitização: os objetos de referência, os atores securitizadores e os atores funcionais.

[12] There is a distinction between the securitised and the politicized, as ‘security’ ‘takes politics beyond the established rules of the game and frames the issue either as a special kind of politics or as above politics. Tradução nossa.

O objeto de referência é aquele que estaria na posição de ameaçado, ou seja, que deve ser protegido. Na maior parte das vezes, esse objeto acaba por ser o Estado (Buzan, Waever, 1998), mas com a expansão dos estudos de segurança podemos ver como diferentes objetos de referência podem ser colocados. A segurança de indivíduos, pequenos grupos ou nações inteiras pode ser colocada como sendo ameaçada por outros atores e em necessidade de ser protegida. Uma diferença que cabe notar é o contraste quando nos referimos à segurança de Estados e das nações, já que segundo Buzan, Waever e Wilde (1998, p. 36) “Para um Estado, a sobrevivência é uma questão de soberania, e para uma nação é sobre identidade”. Assim, vemos que a sobrevivência de um Estado se encaixa dentro do setor político, e da nação no setor societal.[13]

Já o “ator securitizador", é aquele agente que deseja tornar um determinado assunto uma questão de segurança. Esse papel exige um capital social do ator de modo a convencer o maior número possível de pessoas com a retirada do tema em questão da esfera política para a esfera de segurança. Normalmente, vemos esses atores em posições dentro de órgãos estatais ou exercendo cargos públicos, de modo que a posição que esses cargos têm dentro da forma de organização social lhes dá uma maior influência para com o resto da sociedade. Buzan, Waever e Wilde (1998) argumentam que em Estados estáveis, principalmente democracias fortes, o Estado muitas vezes é visto como o único ator securitizador com legitimidade para fazer esse movimento. Devido a isso, vemos que a maior parte dos processos de securitização são caracterizados como top-down, ou seja, vem daqueles em posições que detém mais poder nas tomadas de decisão. Porém, isso não anula a existência de processos de securitização onde a iniciativa de mover um determinado tema para uma questão de segurança seja um clamor social e não vindo de uma figura com acesso à um maior capital político ou social.

Dentro desse processo temos também os atores funcionais, que não se encaixam em nenhuma das categorias citadas anteriormente, mas estão presentes e influenciam os processos de securitização. Ou seja, temos aqui atores que têm

[13] É nesse ponto sobre quais objetos estão sendo ameaçados que grande parte das críticas dos estudiosos tradicionais de segurança se concentram. Quando a possibilidade de diversos temas serem elevados para fora do âmbito da política e para dentro da esfera de segurança, há um risco real de que se haja um esvaziamento do termo e da esfera da segurança. Porém, a visão de que apenas o Estado pode ser considerado um objeto de referência para a segurança se mostra inadequada levando em consideração todo o debate e a expansão do campo que ocorreu nas últimas décadas.

suas próprias agendas e objetivos e que podem ser centrais dentro do processo de tomada de decisão sobre a securitização ou não de um tema. No exemplo de Buzan. Waever e Wilde (1998) citado anteriormente a companhia poluidora seria um ator funcional e atuaria contra um processo de securitização da questão ambiental na área onde a mesma polui, visto que isto chamaria mais atenção e aumentaria os poderes do Estado para lidar com as ações tomadas por essa empresa que danificam o meio ambiente. Esses atores funcionais podem atuar contra ou a favor da securitização do determinado tema.

O que temos em comum em todos esses atores é que eles operam na arena discursiva, demonstrando como a Escola de Copenhague tem um foco na segurança como uma construção social dada por meio do discurso. Essa abordagem mais próxima da vertente construtivista das relações internacionais insere uma outra categoria de análise dentro dos estudos de segurança para que assim possamos melhor compreender como o processo de securitização ocorre.

1.6 Securitização e discurso

O processo de securitização é, em sua essência, um processo discursivo. Ele é uma maneira pela qual um ator securitizador faz movimentos discursivos para tentar convencer a sua audiência alvo a aceitar a quebra de regras e a necessidade de se agir com urgência sobre um determinado tema. Segundo Balzacq (2005, p.171)

> Para a Escola de Copenhague (EC), a securitização tem como premissa um pressuposto principal: A própria enunciação da segurança cria uma nova ordem social em que o ‘política' está entre parênteses”

Desse modo, o ato de se declarar que algo é uma questão de segurança é uma tentativa de torná-lo. É necessário que estudemos como o discurso é utilizado para retirar temas da esfera da política cotidiana e levá-los para o campo da segurança. Segundo Buzan, Waever e Wilde (1998, p.25)

> A maneira de estudar a securitização é estudar o discurso e as constelações políticas: quando um argumento com esta estrutura retórica e

> semiótica particular alcançam efeito para fazer um público tolerar violações de regras que de outra forma tem que ser obedecido?[14]

Assim, o processo de securitização se inicia por meio de um movimento de securitização, onde o ator securitizador afirma que o objeto de referência está sob uma ameaça existencial. Ao fazê-lo, o ator securitizador busca convencer sua audiência-alvo de medidas que fogem ao escopo da discussão e do processo político padrão são necessários para se lidar com essa situação, visto que ela representa uma ameaça existencial ao objeto de referência e que há uma urgência temporal para a resolução (Balzacq, Leónard, Ruzicka, 2016)

Dessa forma, podemos observar que o modo de tentarmos identificar processos de securitização é por meio da análise das narrativas criadas em relação ao temas delimitados. Devido à sua presença na esfera narrativa, não encontraremos evidências de processos de securitização se focarmos em visões materiais do que seriam questões de segurança. A securitização é, primeiramente, um movimento discursivo perpetrado por atores que fazem uso de narrativas para elevar um tema ou ponto para fora da esfera política e para dentro da esfera de segurança. (Buzan Waever, Wilde, 1998)

Outro ponto importante a ser considerado é a audiência, ou seja, para quem se faz esse movimento de securitização. A audiência que se deseja convencer da necessidade de se levar um tópico para a agenda de segurança é a que irá dar a legitimidade para que isso seja feito. De acordo com Buzan, Waever e Wilde (1998, p.41) “há uma categoria separada de “audiência”, aqueles que o ator securitizador tenta convencer a aceitar procedimentos excepcionais devido à natureza de segurança específica de algum problema[15]”. Normalmente vemos a categoria de audiência se referir à população civil de um determinado país, mas também podemos observar essa categoria dentro do sistema, quando um ou mais países e/ou organizações internacionais tentam convencer outros Estados da importância de um determinado tema, como as mudanças climáticas ou um conflito regional.

Algo importante a se compreender em relação a esse processo é que a securitização não pode ser imposta unilateralmente, principalmente em sistemas

---

[14] The way to study securitization is to study discourse and political constellations: When does an argument with this particular rhetorical and semiotic structure achieve sufficient effect to make an audience tolerate violations of rules that would otherwise have to be obeyed? Tradução nossa.

[15] There is a separate category of “audience,” those the securitizing act attempts to convince to accept exceptional procedures because of the specific security nature of some issue. Tradução nossa.

democráticos fortes com presença de um debate político e sistemas de *accountability*. Por isso, mesmo que esse movimento de securitização ocorra, não há uma garantia que ele será bem sucedido. Pode-se não haver um convencimento da audiência em relação tanto à gravidade da ameaça quanto à necessidade de medidas de emergência urgentes. Os Estados democráticos normalmente tem diversas arenas nas quais os temas podem ser debatidos pelos representantes do povo e também possuem meios que a população pode fazer uso para se ser ouvida. Dessa maneira, pode-se ocorrer que um tomador de decisão faça um movimento de securitização sobre um determinado tema que não seja aceito pela sua audiência, mantendo assim o tema em questão na esfera política[16]. Segundo Buzan, Waever e Wilde (1998, p.25)

> Um discurso que toma a forma de apresentar algumas coisas como uma ameaça existencial a um objeto referente não cria por si só securitização - este é um movimento de securitização, mas a questão é securitizada apenas se e quando o público o aceitar como tal.[17]

Aqui também vale lembrarmos o papel dos atores funcionais que podem interferir no processo de securitização, tanto auxiliando ou prejudicando o convencimento da audiência. Atores favoráveis ao processo de securitização podem exagerar a ameaça que o sujeito de referência representa para assim tentar convencer a audiência da necessidade de medidas de exceção, enquanto atores contrários podem contestar a gravidade da ameaça e argumentar que já existem mecanismos dentro da política cotidiana para se lidar com esse determinado tema, que não há uma necessidade de urgência na resolução do mesmo.

A definição da segurança como um movimento discursivo, no qual se declarar um tema como uma questão de segurança é o que o faz ser em oposição à alguma característica natural do objeto é um dos pontos que nos ajudam a entender como a Escola de Copenhague se distancia dos estudos tradicionais de segurança. Ao colocar ênfase no campo discursivo dentro dos estudos de segurança, vemos que na verdade qualquer tema pode ser elevado para dentro da esfera da política de exceção se houver um movimento de securitização bem-sucedido, onde a

[16] Cabe-se aqui relembrar que este trabalho busca verificar se houve a tentativa de securitização por meio de discursos oficiais, não as ações concretas tomada pelo governo estadunidense no mesmo período.

[17] A discourse that takes the form of presenting something as an existential threat to a referent object does not by itself create securitization—this is a securitizing move, but the issue is securitized only if and when the audience accepts it as such. Tradução nossa.

audiência dê legitimidade para o tomador de decisão para a quebra de regras em relação ao tema delimitado.

1.7 Consequências do processo de securitização

Partindo do pressuposto de que o processo de securitização foi efetivo e um determinado tema foi elevado à esfera de segurança, quais serão as consequências desse processo? O que mudaria com a retirada do tema securitizado da esfera da política?

Inicialmente, temos a possibilidade da quebra de regras. Ao lidar com questões de segurança, o Estado tem poderes mais amplos que os normalmente aceitos. Regras institucionais que normalmente limitam o papel do Estado podem ser quebradas em nome da proteção contra uma ameaça existencial. Dessa forma, até mesmo governos de países com democracias fortes e bem-estabelecidas podem se tornar mais autoritários e repressivos quando enfrentados com uma situação tida como sendo de ameaça existencial. De acordo com Balzacq, Leonard e Ruzicka (2005, p.501)

> Securitizar uma questão, em última análise, permite que certas elites aumentem seu poder como consequência de receber privilégios especiais para lidar com uma questão de segurança ou, em outras palavras, se torna livre dos procedimentos e regras que os atores 'normalmente seriam mantidos em xeque' [18]

Além disso, a transparência governamental tende a diminuir, visto que o governo pode argumentar que um número cada vez maior de informações são consideradas sigilosas e que sua divulgação pode ser prejudicial para a capacidade do governo de lidar com o tema securitizado. Além disso, podemos ter um aumento dos gastos públicos relacionados ao tema securitizado visto que se ele é apresentado como uma ameaça existencial, as preocupações orçamentárias da máquina pública são de menor importância quando se discute a própria sobrevivência do objeto de referência (Buzan, Waever, Wilde, 1998).

---

[18] Securitizing an issue ultimately enables certain elites to increase their power as a consequence of being granted special privileges in dealing with a security issue or, in other words, breaking free from the procedures and rules that actors 'would otherwise be bound by'. Tradução nossa.

Uma das consequências negativas do processo de securitização é quando as prerrogativas dadas ao Estado para lidar com a questão de segurança se prorrogam. Quando isso acontece, ocorre uma normalização da quebra de regras e das outras prerrogativas dadas ao Estado para se lidar com a questão de segurança. Desse modo, essa normalização leva a um aumento geral do poder do Estado e também uma diminuição da transparência, fatores que são problemáticos quando pensados dentro do contexto de um sistema político democrático representativo. De acordo com Buzan, Waever e Wilde (1998, p.29)

> Mas a dessecuritização é a opção de longo prazo mais adequada, uma vez que significa não ter questões formuladas como “ameaças contra as quais temos contramedidas”, mas para tirá-los dessa sequência de defesa-ameaça e de volta à esfera pública normal.[19]

Além disso, assuntos que se tornam securitizados são passados para o topo da lista de prioridades, visto que são considerados ameaças existenciais que devem ser tratadas com urgência. Desse modo, assuntos que antes teriam um longo tempo até serem levados para as arenas públicas de discussão devido à uma longa lista de pautas que os antecedem podem ser rapidamente levados para o centro da discussão tanto dentro da esfera da política cotidiana quanto da política de segurança. Eles se tornam prioridades de governos e de instituições, de modo que mesmo que mais debates pudessem ser benéficos para a formulação de soluções mais adequadas, essa prioridade e urgência diminuem consideravelmente o espaço para essas discussões.

Dessa forma, vemos que as consequências de um processo de securitização bem sucedido é a expansão do poder estatal na prerrogativa de se lidar com a ameaça existencial. Essas prerrogativas, entretanto, são pensadas para serem temporárias. Teoricamente, após a ameaça existencial ser neutralizada ou reduzida para um ponto onde ela não é mais urgente ou existencial, deveria-se remover essas prerrogativas do Estado e voltar à normalidade. Porém, existem casos onde existem movimentos governamentais para uma perpetuação de uma percepção de um estado de medo e perigo com objetivo de manter essa expansão de poder

[19] But desecuritization is the optimal long-range option, since it means not to have issues phrased as “threats against which we have countermeasures” but to move them out of this threat-defense sequence and into the ordinary public sphere. Tradução nossa.

estatal por um tempo indeterminado. Essa normalização de prerrogativas que deveriam ser exceções à regra podem representar momentos em que o Estado visa expandir suas capacidades de controle e vigilância sobre a população, podendo passar por cima de direitos civis dos indivíduos.

Vemos assim como o processo de securitização traz consigo consequências que podem ter impactos negativos e positivos dentro das esferas da política interna e externa. Ele pode ser necessário, visto que determinado tópico pode representar concretamente uma ameaça existencial e levá-lo à esfera da segurança permite ao Estado ter maiores ferramentas e prerrogativas para lidar com o mesmo, preservando sua integridade e soberania.

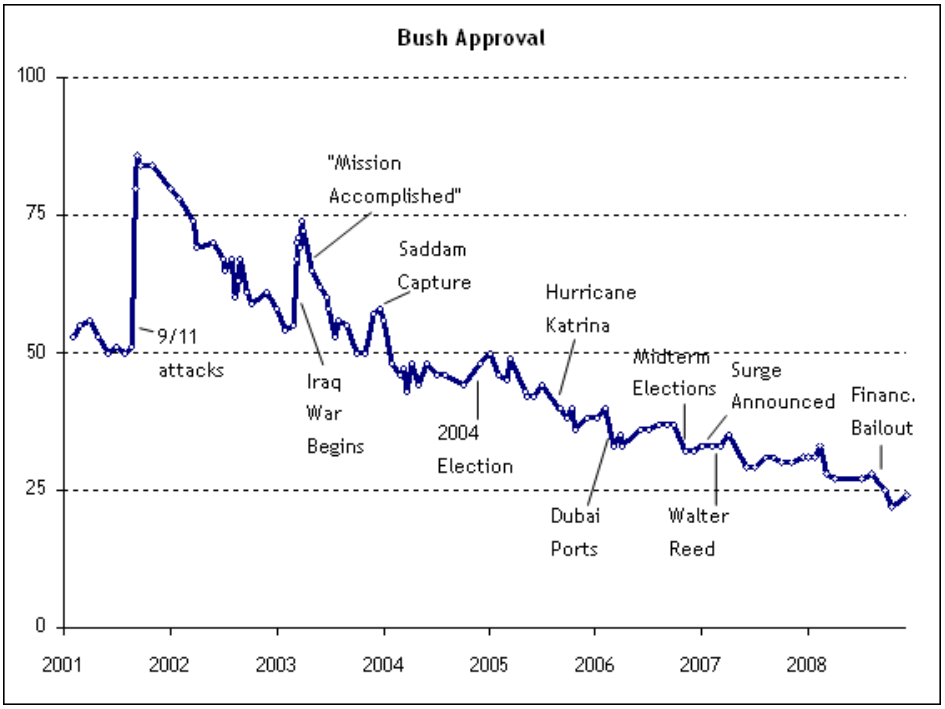
2. A GESTÃO DE BARACK OBAMA COMO PRESIDENTE DOS EUA

Neste capítulo, iremos analisar a gestão de Barack Obama e os principais acontecimentos políticos internos e externos desse período de 2009 à 2017. Essa releitura se faz necessária para entendermos melhor o contexto no qual os discursos que serão analisados foram proferidos. Inicialmente faremos uma observação mais abrangente do período e depois nos aprofundaremos nos incidentes relacionados à cibersegurança.

2.1 Antecedentes da gestão Obama

Quando Barack Obama assumiu a presidência dos EUA em 20 de janeiro de 2009, o país vivia um período ainda instável. O sentimento de insegurança criado pelos atentados no World Trade Center e no Pentágono em 2001, que somados tomaram 2977 vidas inocentes, ainda pairava sobre mentalidade dos estadunidenses. A resposta do então presidente George W. Bush, do Partido Republicano, foi uma caça aos culpados e a criação da chamada “Guerra ao terror”. O terrorismo se solidificava como o inimigo público dos EUA, de modo que a administração Bush deu respostas duras em relação aos percebidos como culpados. A administração Bush fez uso de diferentes interpretações de conceitos como *jus ad bellum* e *jus in bellum* para justificar dentro da esfera do direito internacional seu direito de fazer ataques em solo estrangeiro contra o ator não-estatal (a Al-Qaeda) que havia lhes atacado (Deeks, 2016). Dessa forma, os EUA justificaram, dentro do sistema internacional, ações que já gozavam de amplo apoio em seu ambiente doméstico. A aprovação popular de Bush subiu vertiginosamente após sua resposta aos ataques, dando a ele uma aprovação raramente alcançada por outros presidentes ou chefes de Estado.

Gráfico 1 - Aprovação popular de George W. Bush



Fonte; Pew Research Center, 2008

Essa aprovação de Bush deu a ele o capital político para iniciar as invasões no Afeganistão em 2001 e no Iraque em 2003, além de aprovar diversos dispositivos legais para o combate ao terrorismo, o mais importante e conhecido deles sendo o “Patriot Act” de 2001. Esse ato permitia ao governo americano, em nome do combate ao terrorismo, ampliar sua rede de vigilância tanto dentro quanto fora dos EUA, obtendo dados sem autorização judicial. Além disso, o Patriot Act também previa a detenção por tempo indeterminado sem julgamento de imigrantes suspeitos de planejar ou participar de atentados terroristas. Essas detenções ocorriam na prisão da Baía de Guantánamo em Cuba, que ao operar fora do território americano dava aos oficiais ali estacionados a oportunidade de fazer uso de técnicas de tortura e interrogatório que não seriam permitidas em solo americano. Segundo Deeks (2016, p.649)

> O governo Bush afirmou com firmeza seus pontos de vista sobre a aplicação da lei de direitos humanos às atividades militares. Em particular, deixou claro que não interpretava o Pacto Internacional sobre Direitos Civis e Direitos Políticos aplicáveis a indivíduos detidos em Guantánamo[20]

[20] The Bush administration firmly asserted its views on the application of human rights law to military activities. In particular, it made clear that it did not interpret the International Covenant on Civil and Political Rights as applying to individuals held at Guantanamo. Tradução nossa.

Além da Guerra ao Terror, o fim da presidência Bush foi marcado pela crise econômica mundial de 2008, que teve um forte impacto na economia americana. A classe média americana foi especialmente afetada, visto que a bolha imobiliária estadunidense finalmente estourou. Dessa forma, que a classe média que havia adquirido imóveis e utilizado de hipotecas nos anos anteriores foi duramente impactada (Reinhart, 2011). Essa crise teve repercussões negativas por todo o globo, de modo que governos de todo o mundo se viram obrigados a intervir para salvar bancos de falência e impedir que a crise se aprofundasse ainda mais.

Os EUA na gestão de Bush mantiveram um papel de liderança, principalmente dentro da luta global contra o terrorismo. Esse protagonismo americano era observado desde a década de 90 quando o colapso da URSS deixou os EUA numa posição estabelecida como superpotência global, numa ausência de atores que tivessem capacidades de desafiar sua hegemonia dentro do sistema internacional. Essa posição lhes permitiu ir contra as resoluções da ONU e do direito internacional nas duas invasões feitas durante esse período. Vemos aqui a posição privilegiada que os EUA gozavam neste período, de forma que os mesmos tinham uma enorme capacidade de atuar em favor de seus interesses dentro do sistema internacional, com poucas represálias efetivas feitas contra eles.

2.2 Eleição de 2008 e mandatos subsequentes

A eleição presidencial de 2008 foi contenciosa dentro dos EUA. George W. Bush já havia concorrido a seus dois mandatos, e seu vice-presidente Dick Cheney decidiu não concorrer pelo partido republicano. A disputa então foi entre Barack Obama, senador de Illinois pelo Partido Democrata e John McCain, senador do Arizona pelo Partido Republicano. De acordo com Hillygus (2009, p.841)

> Em muitos aspectos, o resultado da eleição presidencial de 2008 deveria ser bastante fácil de prever. Com o índice de aprovação do presidente George Bush pairando em torno de 30 por cento, uma guerra impopular se arrastando para seu sexto ano e uma economia nacional fraca e piorando,

> a maioria das previsões previu que seria um ano marcante para os Democratas[21].

A guerra do Iraque iniciada em 20 de março de 2003 , quando Bush gozava de alta aprovação popular e capital político, se estendeu por mais tempo do que o inicialmente planejado. O apoio da população à guerra ao terror foi se reduzindo, assim como o apoio popular de Bush. Além disso, a crise de 2008 que afetou profundamente a classe média americana também diminuiu a confiança da população no governo, visto que vários cidadãos iam à falência e o governo ofereceu os resgates fiscais apenas aos bancos.

Com esse contexto social, político e econômico, poderíamos prever que o campo estaria preparado para uma vitória democrata. Barack Obama, senador pelo Estado de Illinois, venceu as prévias do partido democrata contra uma figura já conhecida e com passagem pela Casa Branca, a senadora Hillary Clinton. Obama teve um enorme sucesso no marketing de campanha, com seus slogans “Change” e “Yes we can” representando um desejo de mudança na política americana. Obama vinha com um discurso conciliador desde antes de sua candidatura, como exemplificado em seu discurso na convenção do partido democrata em 2004, onde afirmou:

> Agora mesmo enquanto falamos, há aqueles que estão se preparando para nos dividir, os mestres da propaganda, os vendedores de anúncios negativos que adotam a política do 'vale tudo'. Bem, eu digo a eles esta noite, não há uma América liberal e uma América conservadora; há os Estados Unidos da América. Não existe uma América Negra e uma América Branca e América Latina e América Asiática; há os Estados Unidos da América.[22]

Projetava-se em Obama uma imagem de conciliador, um candidato que pudesse trazer de volta uma ideia de união para dentro dos EUA. Além disso, a figura do primeiro presidente negro carregava um signficado simbólico muito forte para as as comunidades negras dentro dos EUA, visto que o cargo de presidente

---

[21] In many respects, the outcome of the 2008 presidential election should have been quite easy to predict. With President George Bush's approval rating hovering around 30 percent, an unpopular war dragging into its sixth year and a weak and worsening national economy, most forecasts predicted it to be a banner year for the Democrats. Tradução nossa.

[22] Keynote speech at the Democrat National Conference 2004. Disponível em: <http://americanradioworks.publicradio.org/features/blackspeech/bobama.html>. Acesso em 21 de agosto de 2023.

estadunidense havia sempre sido ocupado por homens brancos. Obama, filho de um imigrante queniano e de uma estudante americana, foi ligado à comunidade negra em seu Estado de Illinois, angariando grande apoio dos afro americanos quando anunciou sua candidatura (Ford, Johnson, Maxwell, 2010).

Obama venceu a corrida eleitoral contra John McCain com 53% dos votos populares e 68% dos votos no colégio eleitoral[23]. Teve um desempenho positivo mesmo em Estados considerados redutos republicanos como a Carolina do Norte. Esse bom desempenho nessas áreas indicam que a mensagem passada de mudança dentro da política americana conseguiu ressoar mesmo entre aqueles que tradicionalmente não votariam no partido democrata.

Após tomar posse, as primeiras ordens executivas (13491 e 13492)[24] de Obama visaram assegurar tratamento humano aos detidos em operações de combate ao terrorismo, proibindo assim a tortura durante interrogatórios, e o fechamento da prisão na Baía de Guantánamo. A prisão foi uma questão contenciosa, devido aos episódios de tortura que ali ocorreram e pelo fato dos detentos serem mantidos ali sem julgamento. O fechamento da prisão recebeu forte oposição dentro do Congresso estadunidense, de maneira que a prisão permanece em operação até os dias atuais.

Em relação à política externa, houve uma mudança considerável em relação àquela feita por Bush. Segundo Corvaja (2015, p.21)

> Quando assumiu o cargo em 2008, Obama tentou realinhar os EUA política externa e de segurança, com enfoque na diplomacia, reconciliação e contenção. Pontos proeminentes em sua agenda incluíam um “reset” com a Rússia após a crise da Geórgia – incluindo uma redução de armas nucleares e o projeto “Global Zero” – assim como a reconciliação com o mundo muçulmano – recorde-se seu discurso em Cairo neste contexto – e uma conclusão para os conflitos no Oriente Médio, particularmente no Iraque e no Afeganistão. No mesmo tempo, os EUA queriam restabelecer seu papel como um país confiável e sólido parceiro em relação aos seus aliados tradicionais, recuando das tendências unilateralistas do governo anterior. Isso seria, porém, exigem que os parceiros desempenhem o seu

[23]Disponível em <https://www.presidency.ucsb.edu/statistics/elections/20>. Acesso em 21 de agosto de 2023.
[24]Disponível em <https://www.presidency.ucsb.edu/documents/barack-obama-event-timeline>. Acesso em 21 de agosto de 2023.

> papel e assumam maior responsabilidade, especialmente no que diz respeito às questões regionais.

Vemos assim que Obama visava uma mudança na direção da política externa americana. Antigas relações de rivalidade como a com a Rússia seriam reavaliadas, de modo a reduzir a inimizade entre os países e tentar abrir mais caminhos para a cooperação. Houve movimentos desse tipo também em relação ao mundo árabe, cuja relação com os EUA havia rapidamente se deteriorado após as ações militares no Iraque e no Afeganistão. Além disso, houve uma tentativa de se "liderar por trás", onde os EUA providenciaram apoio aos seus aliados sem tomar o protagonismo em determinadas questões. Dessa maneira, haveria uma maior carga sobre esses países aliados, que agora teriam que arcar com maiores custos de negociações e em questões de cunho mais regional (Corvaja, 2015).

Esse passo para trás em relação aos seus aliados foi interpretado de diferentes formas. Aqueles mais alinhados com essa visão de política externa argumentam que os EUA não deveriam arcar com um custo tão elevado em relação aos seus aliados, e que eles deveriam arcar com uma parte maior dos custos, mas ainda contando com o apoio estadunidense. Os críticos viam como os EUA recuando de sua posição de liderança dentro do sistema internacional e deixando um vácuo que poderia ser preenchido por outros atores com aspirações de potências, como Rússia e China. A imagem americana havia sofrido com o impacto dos conflitos que haviam sido iniciados na gestão Bush e que ainda não haviam sido concluídos. De acordo com Haar (2016, p.3) "Quando Obama tomou posse em 2009, ele herdou duas guerras em terras distantes lutando contra terroristas, uma altamente impopular (Iraque) e a outra indo mal (Afeganistão)"[25]. Porém essa estratégia teve resultados negativos, principalmente no Oriente Médio. De acordo com Corvaja, (2015, p. 22)

> Muitos especialistas consideram o resultado destes projetos desastroso. Isto não é à toa que Patrick Keller descreve os resultados do período de mandato de Obama como o "desastre de Obama": A Síria e o Iraque cairam em um pesadelo sob os ataques do chamado Estado Islâmico e ameaça atrair os EUA de volta ao conflito mais intensamente. As relações com a

[25] When Obama was sworn in 2009 he inherited two wars in distant lands fighting terrorists, one highly unpopular (Iraq) and the other going badly (Afghanistan). Tradução nossa.

> Rússia voltaram a um estado semelhante ao da Guerra Fria, e a Ucrânia é outro Estado falido agora precisando de ajuda. A China está agindo com crescente crueldade e agressão na Ásia, e as conquistas feitas através do envolvimento dos EUA no Afeganistão permanecem extremamente pequenas.[26]

Essa mudança acabou por render diversas críticas a Obama pela forma como a política externa americana estava sendo conduzida durante seu mandato. Obama também restringiu o escopo no qual os EUA atuam dentro do sistema internacional, por vezes aquém do que lhe seria permitido dentro das delimitações do direito internacional. Segundo Deeks (2016, p.646)

> A administração Obama adotou repetidamente uma abordagem notavelmente diferente, empregando uma abordagem que poderíamos caracterizar como "minimalismo executivo". Ou seja, a administração Obama sinalizou a outros Estados o seu interesse na auto-restrição, fazendo menos afirmações substantivas e retóricas ousadas relacionadas com o jus ad bellum e o jus in bello. Tem perseguido isso objetivo, em parte através do estabelecimento de várias políticas que autorizam um âmbito de ação mais restrito do que o que alguns acreditam que o direito internacional permite[27]

Entretanto, isso não quer dizer que a administração Obama não teve sua quota de ações extraterritoriais e contra outros Estados e indivíduos tidos como ameaças. Apesar do uso extensivo de drones pelos EUA como uma estratégia de combate ao terrorismo ter começado em 2004 (Plaw, Flicker e Willians, 2011), na gestão Obama o número de ataques de drones cresceu vertiginosamente. Os

---

[26] Many experts view the outcome of these projects as disastrous. It is not for nothing that Patrick Keller describes the results of Obama's period in office as the "Obama debacle": Syria and Iraq have descended into a nightmare under the attacks from the so-called Islamic State and threaten to draw the USA back into the conflict more intensely. Relations with Russia have reverted to a state similar to that during the Cold War, and Ukraine is another failing state now in need of assistance. China is acting with increasing ruthlessness and aggression in Asia, and the achievements made through the USA's engagement in Afghanistan remain vanishingly small. Tradução nossa.

[27] The Obama administration has repeatedly taken a notably different tack, employing an approach that we might characterize as "executive minimalism." That is, the Obama administration has signaled to other states its interest in self-constraint by making fewer bold substantive and rhetorical claims related to the jus ad bellum and jus in bello. It has pursued this objective partly by establishing various policies that authorize a narrower scope of action than what some believe international law permits

números são incertos, mas se sabe que mais de 500[28] desses ataques foram realizados durante seus oito anos de governo. O custo político desse tipo de operação é vertiginosamente menor do que ações militares convencionais, visto que não há a presença de soldados em solo estrangeiro, de modo que o custo logístico e a fatalidade para tropas americanas também é muito menor. Porém, abre-se um debate relacionado à legalidade desses ataques, visto que são execuções extrajudiciais ocorridas em territórios estrangeiros.

Uma das operações mais convencionais feitas por Obama foi a que encontrou e matou Osama Bin Laden, o arquiteto dos ataques às Torres Gêmeas e líder do grupo terrorista Al Qaeda. Ele foi encontrado em um complexo em Abbottabad no Paquistão, para onde os EUA despacharam uma equipe de elite com ordens para capturá-lo ou matá-lo. Após entrar em confronto com os fuzileiros navais, Bin Laden foi morto e seu corpo retirado do local e supostamente sepultado no mar de acordo com a tradição islâmica. Cabe aqui analisarmos uma divergência em relação ao discurso relacionado à essa operação. Em seu discurso após a confirmação da morte de Bin Laden, Obama disse: “Ao longo dos anos, deixei repetidamente claro que tomaríamos medidas no Paquistão se soubéssemos onde estava Bin Laden. Isso é o que fizemos.”[29]. Porém, segundo Deeks (2016, p.652)

> As únicas operações militares dos EUA desde 2009 que parecem ter ocorrido sem o consentimento do governo anfitrião ou autorização do Conselho de Segurança são as incursões no Paquistão para capturar ou matar Osama bin Laden e matar os Taliban líder Mullah Mansour[30]

Aqui vemos diferenças na interpretação do discurso de Obama. Ao dizer que tomaria medidas no Paquistão caso Bin Laden estivesse lá, vemos que isso se aproxima mais de uma comunicação de que determinada ação será realizada do que um pedido de permissão para fazê-la. No mesmo discurso, Obama enfatiza a

---

[28] Disponível em <https://www.thebureauinvestigates.com/stories/2017-01-17/obamas-covert-drone-war-in-numbers-ten-times-more-strikes-than-bush>. Acesso em 22 de agosto de 2023.

[29] Over the years, I’ve repeatedly made clear that we would take action within Pakistan if we knew where bin Laden was. That is what we’ve done. Tradução nossa. Disponível em <https://obamawhitehouse.archives.gov/blog/2011/05/02/osama-bin-laden-dead>. Acesso em 22 de agosto de 2023

[30] The only U.S. military operations since 2009 that seem to have occurred without consent by the host government or Security Council authorization are the incursions into Pakistan to capture or kill Osama bin Laden and kill Taliban leader Mullah Mansour. Tradução nossa.

cooperação entre os EUA e o Paquistão em relação ao combate contra o terrorismo. Porém a comunicação de eventuais ações não necessariamente significa o consentimento ou a cooperação do país no qual tais ações serão realizadas. Dessa forma, apesar de Obama ter uma postura mais diplomática em relação ao uso da força em territórios estrangeiros, ele ainda fez uso do poderio militar estadunidense quando os interesses americanos convergem para essa ação.

O que podemos observar nesse primeiro governo Obama é que houve uma tentativa de se distanciar da política externa de Bush, que tinha uma postura mais intervencionista e com uso maior de força militar devido aos ataques do 11 de setembro. Essa reorientação da política externa, apesar de bem planejada, sofreu sérias críticas devido à perda do protagonismo dos EUA dentro do sistema, que deixou vácuos de poder que foram ocupados por outros atores ou que levaram a situações de instabilidade política. Obama buscou outras maneiras de proteger os interesses dos EUA na esfera global, mas o fez evitando o uso de forças militares *in loco*, de maneira a evitar o alto custo político de ações como essas.

Em 2012, Obama disputou a eleição contra Mitt Romney, candidato pelo partido republicano. Obama não enfrentou séria oposição dentro de seu próprio partido, sendo naturalmente indicado para concorrer à uma reeleição. Apesar de ter vencido no colégio eleitoral e no voto popular, o partido democrata teve um queda no percentual no voto popular, com um resultado de 51,1% contra 47,2% dos republicanos[31]. Em relação ao seu segundo mandato, Obama manteve as suas diretrizes de política interna e externa. Internamente, o foco em questões de bem estar social e inclusão se manteve, mesmo sobre duras críticas de seus opositores.

O mesmo ocorreu na política externa, onde promessas de se retirar as tropas do Afeganistão e do Iraque não foram cumpridas devido à complexidade da situação ali encontrada, com uma piora devido ao crescimento do Estado Islâmico do Iraque e da Síria (ISIS). Apesar de ter discursado no Cairo tentando uma reaproximação, essa melhora nas relações não foi alcançada nas partes onde os EUA ainda se envolviam em conflitos no Oriente Médio. Segundo Haar (2012, p.10)

> Obama assumiu o cargo há quatro anos com um plano ambicioso para reduzir os antagonismos entre os EUA e os muçulmanos do mundo. Ele

[31] Disponível em <https://www.presidency.ucsb.edu/statistics/elections/2012>. Acesso em 28 de agosto de 2023.

> pretendia alcançar os inimigos da América com uma mão aberta em vez de punho cerrado. No entanto, a política de Obama não teve sucesso e no final do seu primeiro mandato ele mudou estratégia para sanções ao Irã e um alvo preventivo de abordagem assassina contra militantes islâmicos, autorizando até agora mais ataques de drones contra terroristas do que seu antecessor, George W. Bush havia endossado[32]

Dois acontecimentos internacionais marcaram o segundo governo Obama e impactaram fortemente a política externa americana nesse segundo mandato. Primeiramente em fevereiro de 2014 tivemos a invasão da Crimeia, região sudeste da Ucrânia que foi invadida por forças russas após um período de instabilidade política relacionada ao então presidente ucraniano Viktor Yanukovich. A postura pró-Rússia de Yanukovich não foi aceita por parte da população, que iniciou uma onda de protestos contra o ex-presidente após o mesmo se negar a assinar um acordo de cooperação com a União Europeia (EU) (Bebler, 2015). O presidente russo Vladimir Putin acusou os EUA e a UE de tentar expandir sua esfera de influência até às fronteiras russas, de modo que no início do ano de 2014 se tem a invasão da península de Crimeia e sua posterior anexação ao território russo, essa ocorrido após um referendo onde a maioria da população se mostrou favorável à integração ao território russo[33].

Ainda em 2014, voltamos nossa atenção agora para o Oriente Médio, onde após a instabilidade e os vácuos de poder deixados após a Primavera Árabe em 2011 abriram espaço para a ascensão do Estado Islâmico do Iraque e da Síria (ISIS). Esse grupo terrorista de cunho fundamentalista islâmico vinha crescendo na região, tomando territórios de diversos países e construindo uma poderosa máquina midiática de recrutamento, recebendo membros vindo da Europa Ocidental e de países ainda mais distantes. Em janeiro de 2014 o grupo tomou a cidade de Raqqa na Síria, declarando-a capital de seu califado. A expansão territorial continua e o grupo captura a cidade de Mosul, a segunda maior do Iraque antes de se renomear como Estado Islâmico (EI)(Tønnessen, 2019).

---

[32] Obama took office four years ago with an ambitious plan to reduce the antagonisms between the U.S. and the Muslim world. He intended to reach out to America's enemies with an open hand rather than a clenched fist. However, Obama's policy did not succeed and by the end of his first term he shifted strategy toward sanctions for Iran and a preemptive targeted killing approach against militant Islamists, authorizing far more drone strikes on terrorists than his predecessor George W. Bush had endorsed. Tradução nossa.

[33] Cabe-se notar que a realização e o resultado desse referendo são contestadas pelas autoridades ucranianas (Grant, 2015)

Esses dois acontecimentos reverberaram fortemente dentro dos EUA, visto que impactam duas regiões contenciosas dentro da geopolítica global. Sendo assim, os EUA lidaram com esses desenvolvimentos de uma forma menos interventora do que outras administrações. Segundo Corvaja (2015, p.20) “Empregando uma retórica inspirada na do presidente liberal Wilson e centrando-se na diplomacia, na inclusão e, não menos importante, na cautela, Obama parecia ser a tão esperada contrapartida do seu antecessor George W. Bush”. Dessa forma, vemos que mesmo que inicialmente a gestão Obama tentasse exercer uma medida de cautela em sua política externa, ela foi muito criticada pois se entendeu que uma falta de proatividade e engajamento estadunidense levou essas situações a se deteriorar a pontos que poderiam ter sido evitados. No caso da Ucrânia, não ocorreu uma corrida para que o país ingressasse na Organização do Tratado do Atlântico Norte (OTAN) como uma forma de protegê-la da agressão russa. De acordo com Glaser e Thrall (2017, p.11)

> Após a expulsão do presidente ucraniano, Viktor Yanukovych, em fevereiro de 2014 e a subsequente anexação russa da Crimeia e ações militares contínuas na parte oriental do país, o Presidente Obama de fato, resistiu aos apelos para apressar a entrada da Ucrânia na aliança da OTAN, de fornecer armas aos ucranianos locais para lutar contra os separatistas apoiados pela Rússia, ou mesmo responder com intervenção militar direta dos EUA.[34]

Dessa forma, críticos fazem o argumento de que a cautela americana em intervir no conflito deu abertura para que a Rússia continuasse sua agressão e anexasse a região da Crimeia. Essa invasão colocou a Europa em alerta visto que anos mais tarde a Rússia lançou uma invasão em larga escala do território ucraniano, deixando a Europa e os EUA em situação de alerta sobre os próximos movimentos russos.

Esse mesmo argumento de que uma falta de intervenção americana leva a um escalonamento da violência e da instabilidade foi feito em relação ao crescimento do EI. Ainda em Glaser e Thrall (2017, p.15)

---

[34] Following the ouster of Ukrainian President Viktor Yanukovych in February 2014 and subsequent Russian annexation of Crimea and extended military actions in the eastern part of the country, President Obama did indeed resist calls to rush Ukraine into the NATO alliance, provide arms to local Ukrainians to fight off Russian-backed secessionists, or even respond with direct U.S. military intervention.Tradução nossa.

> Obama assumiu o cargo soando como um presidente comprometido com a moderação. Ele estava determinado a acabar com a guerra no Iraque e pôr fim à guerra contra o terrorismo, mas em vez disso Obama viu-se perseguindo uma estratégia muito semelhante à lançada pela administração Bush. Apesar de ter aposentado oficialmente a frase "guerra global ao terror", a administração Obama, no entanto, comprometeu-se com os mesmos objetivos centrais: destruir a Al Qaeda e grupos terroristas de alcance global alcançar e trabalhar para diminuir as condições profundas que levam ao terrorismo. Esta escolha estratégica, por sua vez, garantiu que Obama prosseguiria uma campanha expansiva e fortemente militarizada contra primeiro a Al Qaeda e depois o Estado Islâmico.[35]

Portanto as questões no Oriente Médio continuaram a ser de grande importância para a política externa americana nos anos da gestão de Barack Obama. Apesar de não ter iniciado nenhuma invasão ou intervenção militar direta na região, como Bush havia feito no caso do Iraque e do Afeganistão, a presença militar americana era sentida na região por meio de inúmeros ataques de drones e por operações especiais dos EUA que lidavam com alvos e situações específicas (Glaser, Thrall, 2017).

Vemos então que essas duas situações colocam no centro da discussão dois dos inimigos percebidos dos EUA, que por vezes anteriores foram tidos como ameaças existenciais para o país: a Rússia, que durante o período da Guerra Fria era a maior ameaça aos EUA devido à sua rivalidade, aliada ao fato de possuir um arsenal nuclear; e o terrorismo de cunho islâmico fundamentalista, que foi o principal inimigo dos estadunidenses durante a primeira década do século XXI devido ao trauma sofrido pelo ataque de 11 de setembro de 2001.

Na política interna, os democratas sofreram uma derrota nas eleições de meio de mandato de 2014, onde os democratas perderam 13 assentos no

---

[35] Obama came into office sounding like a president committed to restraint. He was determined to end the war in Iraq and bring the war on terror to a close, but instead Obama found himself pursuing a very similar strategy to the one launched by the Bush administration.40 Despite officially retiring the phrase "global war on terror," the Obama administration nonetheless committed itself to the same core objectives: destroying Al Qaeda and terrorist groups of global reach and working to diminish the root conditions that lead to terrorism. This strategic choice, in turn, ensured that Obama would pursue an expansive and heavily militarized campaign against first Al Qaeda and then the Islamic State. Tradução nossa.

Congresso e 9 no Senado[36]. Essa perda de maioria nas casas prejudicou a capacidade dos democratas de passarem legislações, dificultando a governabilidade do segundo mandato de Obama. A insatisfação com a política externa se aliou à insatisfação da população com as medidas internas, como o Obamacare, que apesar de tentar trazer uma forma de cobertura de saúde para a população, foi duramente criticado, enfrentando oposição nas esferas estaduais.

Em relação às agências, tanto a NSA quanto o DIA são órgãos subordinados ao Departamento de Defesa (DOD) que respondem diretamente ao presidente dos EUA. O DOD lida primariamente com as ameaças fora dos EUA, enquanto o Departamento de Segurança Nacional (DHS) tem um foco maior para dentro do território nacional. Ambas as agências lidam com informações confidenciais visto seu papel central na comunidade de inteligência estadunidense.

A NSA teve uma enorme liberdade de atuação dentro dos EUA no período pós 11 de setembro devido ao Patriot Act, como citado no capítulo dois. Comunicações onde um dos envolvidos se encontrava fora do território estadunidense foram consideradas passíveis de serem coletadas pela agência, com a ressalva que não fossem direcionadas aos cidadãos estadunidenses (Landau, 2013). Quando a extensão da coleta foi revelada, houve uma comoção interna e externa contra a espionagem feita pelos EUA contra seus próprios cidadãos e líderes de outras nações, inclusive as aliadas. Já o DIA, por ser uma agência ligada à inteligência para suporte de ações militares em territórios estrangeiros, não foi tão impactada quanto a NSA.

O que vemos na segunda gestão de Obama é uma tentativa geral de continuação das diretrizes de política externa do primeiro mandato, mesmo havendo casos se necessitasse do uso de medidas mais incisivas. Porém a insatisfação da população aliada à uma crescente popularização de um discursos de extrema direita e à rejeição de Hillary Clinton como candidata à presidência levaram à uma vitória republicana em 2016, com a eleição de Donald Trump para o cargo de presidente.

[36] Disponível em <https://www.presidency.ucsb.edu/documents/barack-obama-event-timeline> . Acesso em 28 de agosto de 2023.

2.3 A questão da cibersegurança no governo Obama

A cibersegurança foi em determinados momentos um ponto central dentro da discussão política na gestão de Barack Obama. Devido aos escândalos relacionados ao tema e como eles pautaram o debate, se faz necessário que analisemos esses temas com maior profundidade.

2.3.1 Stuxnet

Em relação ao campo da cibersegurança, o primeiro governo Obama enfrenta duas situações que colocaram essa discussão no centro do debate público e político estadunidense, com repercussões de escala global. Os incidentes dos vazamentos feitos por Chelsea Manning e o ataque feito como vírus Stuxnet, ambos em 2010, colocaram as operações cibernéticas conduzidas pelos EUA em cheque. O Stuxnet é um malware do tipo worm[37] que foi utilizado em uma operação cibernética contra o programa nuclear iraniano. Ele foi inicialmente descoberto em uma companhia de software em Belarus que estava analisando computadores iranianos quando os engenheiros de software Sergey Ulasen e Oleg Kupreev notaram que o que parecia ser um vírus comum na verdade tinha uma programação muito mais desenvolvida do que a antes pensada. De acordo com Zetter (2014, p.8)

> Ele não estava apenas usando um rootkit habilidoso para se ocultar e torná-lo invisível aos mecanismos antivírus, mas também estava usando uma exploit[38] de zero-day[39] para se propagar de máquina para máquina – um exploit que atacava uma função tão fundamental para o sistema operacional Windows, que colocar milhões de computadores em risco de infecção[40]

[37] Um worm é um tipo de software clandestino que, uma vez colocado em um computador, permite que haja um controle remoto dessa máquina por alguém que não seja o dono da mesma. (McKay, Porche, Sollinger, 2011)

[38] Exploits são falhas ou bug dentros de softwares que podem ser usados para causar comportamentos não previstos.

[39] Zero-day é o termo utilizado para se referir à um bug ou falha de um sistema onde seu desenvolvedor acabou de descobri-la, tendo então “0 dias” para consertá-la.

[40] Not only was it using a skillful rootkit to cloak itself and make it invisible to antivirus engines, it was using a shrewd zero-day exploit to propagate from machine to machine—an exploit that attacked a

O software malicioso havia colocado as máquinas iranianas em um *reboot loop*, onde elas iniciavam o sistema e logo o mesmo desligava. Os técnicos iranianos haviam inclusive reinstalado o sistema operacional dessas máquinas, mas o erro persistia. A suspeita foi então de que o vírus havia se espalhado pela rede iraniana, de modo que ao se reconectar a máquina a essa rede, a mesma era reinfectada. Além disso, um rootkit de nível kernel[41] impedia que programas de antivírus conseguissem detectar esse novo malware (Zetter, 2014).

Após os engenheiros divulgarem seus achados em fóruns de língua inglesa, vários outros membros da comunidade de cibersegurança observaram que outras máquinas haviam sido infectadas. Porém um fato se destacava: esse malware, agora já denominado Stuxnet, não havia tentado roubar informações bancárias ou financeiras. Na verdade, ele parecia ter sido desenvolvido para afetar programas de controle industrial, o que causou um estranhamento visto que não há um ganho monetário nesse tipo de hacking. Um usuário do fórum onde Ulasen e Kupreev primeiramente haviam publicado sobre o malware levantou a possibilidade de que o verdadeiro uso desse software seria para espionagem (Zetter, 2014).

Ao se infiltrar nos computadores das instalações, o Stuxnet alterou as configurações das centrífugas de resfriamento, causando dano às mesmas e assim comprometendo a pesquisa nuclear iraniana. Apesar de não ter sido o primeiro uso de *cibercapabilities* para se causar dano a um país inimigo, o caso Stuxnet demonstrou o maior potencial de ataques feitos por meios cibernéticos. De acordo com McKay, Porche, Sollinger, (2011, p.1)

> Embora o Stuxnet possa não ter sido o primeiro desse tipo, ele ultrapassou limites significativos em termos de capacidade e, mais importante, de emprego. A capacidade que demonstrou é impressionante. Seus criadores muito provavelmente penetraram em redes fechadas e sem ar, o que permitiu Stuxnet invadir um sistema de controle nuclear. Contudo, de maior significado é o fato de que o Stuxnet representa agora o exemplo mais

function so fundamental to the Windows operating system, it put millions of computers at risk of infection. Tradução nossa

[41] O nível kernel é o nível mais alto de autorização de um computador, de modo que malwares rodando nesse nível dificilmente são detectados por programas antivírus..

> conhecido de um ataque cibernético patrocinado pelo Estado. ataque contra outro governo que supostamente resultou em danos físicos[42]

As suspeitas iniciais caíram sobre Israel, inimigo de longa data do Irã e que vê uma arma nuclear iraniana como uma ameaça direta à sua sobrevivência. Além disso, Israel se destaca na região do Oriente Médio como um dos países que mais investem em tecnologia, já possuindo uma desenvolvida doutrina de ciberdefesa e cyber warfare[43]. Porém, mesmo com essas vantagens, Israel sozinho dificilmente teria conseguido criar um vírus tão eficiente e complexo como o Stuxnet. Apontou-se então uma coprodução do vírus com os EUA, uma potência no campo cibernético e da computação. O apoio dos EUA à Israel já é um relacionamento de longa data, de modo que havia um interesse em comum em impedir ou pelo menos adiar o acesso iraniano à tecnologia de armamentos nucleares. Além disso, o uso de ataques cibernéticos se alinha com a tendência da administração Obama de utilizar soluções, mesmo que violentas, que não envolvam a presença de tropas americanas em solo estrangeiro, como no caso dos ataques de drones.

O Stuxnet representou um avanço preocupante dentro da esfera da cibersegurança, devido à sua capacidade de se infiltrar em todas as versões do sistema operacional Windows desde a versão 2000. Sendo esse o sistema operacional mais utilizado no mundo, suas aplicações para uso ofensivo, espionagem e roubo de dados são amplas. Dessa forma, outros países já preparam contramedidas para ataques desse tipo além de tentarem desenvolver suas próprias versões do malware.

2.3.2 Chelsea Manning

Já o caso de Chelsea Manning foi um vazamento de informações sigilosas que danificou a reputação dos EUA em relação às suas relações diplomáticas. Chelsea Manning (anteriormente Bradley Manning), foi uma militar americana que

---

[42] While Stuxnet may not have been the first of its kind, it did cross significant thresholds in terms of capability and, more importantly, employment. The capability it demonstrated is impressive. Its creators very likely penetrated air-gapped, closed networks, which enabled Stuxnet to worm its way into a nuclear control system. However, of more significance is the fact that Stuxnet now represents the most well-known instance of a state-sponsored cyber attack against another government that reportedly resulted in physical damage. Tradução nossa.

[43] Disponível em <https://www.gov.il/en/departments/general/cyber_security_methodology_2> Acesso em 17 de outubro de 2023.

usando de seu acesso privilegiado à informação dentro da estrutura do exército americano, vazou uma enorme quantidade de documentos relacionados à invasão do Iraque, num caso que ficou conhecido como “Diários de Guerra do Iraque”.

Manning, analista de inteligência na Guerra do Iraque, copiou mais de 400.000 documentos confidenciais em um CD da cantora Lady Gaga, antes de transferir esses documentos para um cartão SD para levá-los de volta para os EUA durante sua saída autorizada para descanso (Manning, 2022). Manning então tentou em vão contactar diversos jornais e veículos de mídia estadunidenses para que o material pudesse ser publicado, expondo assim as violações de direitos humanos que os EUA haviam cometido durante a campanha do Iraque. Após não receber respostas, Manning enviou os documentos para o site Wikileaks, de Julian Assange, já conhecido por divulgar documentos sigilosos anteriormente. De acordo com Colvin (2018, p.28)

> Outras publicações do WikiLeaks nesta categoria incluem uma coleção de telegramas diplomáticos sauditas e e-mails do governo de Bashar al-Assad na Síria, bem como cadeias de e-mail de dentro da Convenção Nacional Democrata e da campanha presidencial de 2016. Estas coleções são um recurso valioso para análises de tendências políticas e compromissos, bem como para o contexto de incidentes individuais[44]

Esses vazamentos trouxeram à tona casos de mortes de civis, casos de tortura e da morte de dois jornalistas da agência de notícias Reuters, que foram alvejados por um helicóptero norte-americano após seus equipamentos serem confundidos com armas[45]. Tais acontecimentos levaram à uma repercussão negativa da maneira como os EUA conduziram a invasão. Além disso, também ocorreram os chamados “Cableleaks”, incidente onde comunicações diplomáticas dos EUA também foram vazadas por meio do Wikileaks.

Chelsea foi acusada por diversos crimes e detida em uma prisão militar enquanto aguardava julgamento. Segundo ela (2022, p.185)

---

[44] Other WikiLeaks publications in this category include a collection of Saudi diplomatic cables and emails from the Bashar al-Assad government in Syria as well as email chains from within the Democratic National Convention and 2016 Presidential campaign. These collections are a valuable resource for analyses of policy trends and trade-offs as well as the background to individual incidents. Tradução nossa.

[45] Disponível em <https://www.theguardian.com/world/2010/oct/22/iraq-war-logs-military-leaks>. Acesso em 27 de agosto de 2023.

> Depois de toda a negociação pré-julgamento, eu enfrentava vinte e duas acusações, principalmente por contornar medidas de segurança e armazenar indevidamente material classificado, bem como roubo e divulgação não autorizada sob a Lei de Espionagem[46]

Aqui vemos que as repercussões judiciais sobre os *whistleblowers* como Manning acabam vindo dentro de atos relacionados à violações de cibersegurança e à acusações de espionagem, a última podendo chegar à pena capital de acordo com o Espionage Act de 1917[47]. Apesar de ter sido enquadrada nas acusações de espionagem, Manning não compartilhou esses arquivos com potenciais inimigos dos EUA, mas sim disponibilizou o material amplamente na internet. De acordo com Colvin (2018, p.38)

> Esta confusão proposital de denúncia de irregularidades com espionagem ou traição também existe ao nível da lei. Muitos notaram quão inapropriado é que Os *whistleblowers* americanos são processados sob uma lei que os classifica como espiões. Entre as acusações criminais que Chelsea Manning enfrentou na corte marcial estava o de “ajudar o inimigo”[48]

No fim do julgamento, Manning declarou-se culpada de 10 das 22 acusações feitas contra ela, sendo assim sentenciada a 35 anos de prisão em uma instituição militar prisional. Devido às questões relacionadas à sua disforia de gênero e o tratamento recebido durante sua detenção anterior e após ao julgamento, houve um movimento que denunciava o tratamento recebido por ela como tortura e e desproporcional ao dano real causado por seus atos. Ainda em Colvin (2018, p,39)

> Se a retórica nos casos de denúncia é muitas vezes altamente exagerada, o tratamento dos contadores da verdade no sistema de justiça criminal às vezes ascendeu ao nível de crimes de Estado em si. Em 2012, o Relator

---

[46] After all the pretrial negotiation, I was facing twenty-two charges, mostly for circumventing security measures and improperly storing classified material, as well as theft and unauthorized disclosure under the Espionage Act.

[47] Disponível em <https://d1lexza0zk46za.cloudfront.net/history/am-docs/espionage-act-1917.pdf>. Acesso em 22 de outubro de 2023.

[48] This purposeful confusion of whistle-blowing with espionage or treason also exists at the level of the law. Many have noted how inappropriate it is that American whistle-blowers are prosecuted under a statute that brands them as spies. Among the criminal charges Chelsea Manning faced at court martial was that of “aiding the enemy”. Tradução nossa.

> Especial da ONU, Juan Mendez, concluiu que o tratamento dispensado a Chelsea Manning em prisão preventiva, incluindo substanciais o tempo em confinamento solitário para "vigilância de prevenção de lesões" constituiu um tratamento cruel, desumano e degradante. Depois de cumprir 7 anos de prisão, uma duração sem precedentes para um *whistleblower* nos EUA, os restantes 28 anos da sua sentença "claramente desproporcional" foram comutados por Barack Obama num dos seus últimos atos no cargo.[49]

Após a comutação de sua sentença por Barack Obama, Chelsea se manteve como uma ativista pela transparência governamental. Ela concorreu ao Senado americano e recebeu diversos prêmios de entidades ligadas ao livre acesso de informação.

2.3.3 Edward Snowden

Um escândalo ocorrido em 2013 teve um impacto severo na política americana foi outro episódio de vazamento de dados. Dessa vez, Edward Snowden, funcionário da Agência de Segurança Nacional (NSA) vazou documentos que demonstravam que o governo americano tinha em operação uma rede de espionagem de seus próprios cidadãos sem autorização judicial (Jordan, 2015). Aqui vemos uma diferença em relação ao conteúdo e à percepção que os casos Snowden e Manning receberam do governo americano e da população. Manning expôs documentos que mostravam violações dos direitos humanos cometidos pelos EUA fora de seu território e contra estrangeiros, não implicando o governo americano em atos contra seus próprios cidadãos. Já Snowden demonstrou o oposto, comprovando que o Estado americano havia, continuamente, violado o direito à privacidade de seus cidadãos ao espioná-los sem autorização judicial. Nesse caso houve uma divisão ainda maior na opinião pública, pois apesar de ter vazado documentos que poderiam prejudicar operações e interesses

[49] If the rhetoric in whistle-blower cases is often highly exaggerated, the treatment of truthtellers in the criminal justice system has on occasion risen to the level of state crimes in and of itself. In 2012, UN Special Rapporteur Juan Mendez found that the treatment meted out to Chelsea Manning in pre-trial detention, including substantial time in solitary confinement on "prevention of injury watch" constituted cruel, inhuman and degrading treatment. After serving 7 years in prison, itself an unprecedented term for a whistle-blower in the US, the remaining 28 years of her "clearly disproportionate" sentence were commuted by Barack Obama in one of his last acts in office. Tradução nossa.

estadunidenses mundo afora, ele também expôs excessos do governo em relação aos seus próprios sujeitos. De acordo com Colvin (2018, p.26)

> A divulgação de questões levantadas pelos documentos de Snowden produziu uma maior consciência popular sobre a vigilância estatal, e as questões levantadas através de estruturas formais de responsabilização em diferentes países. A opinião pública se provou mais receptiva em algumas regiões do que em outras, mas é justo dizer que os documentos de Snowden capacitaram os críticos existentes da vigilância e dos ativistas da privacidade a apresentar o seu caso em vários fóruns diferentes[50]

As relações dos EUA com outros países foram mais impactadas no caso Snowden, visto que a espionagem de telefones de chefes de Estado ,ainda que aliados, como o da então chanceler alemã Angela Merkel (Colvin APUD Bamford 2014,2016). O caso ganhou notoriedade dentro das discussões sobre proteção e privacidade de dados, de modo que vários países passaram novas leis relacionadas a esse tema ou atualizaram as já existentes (Colvin, 2018). Dilma Rousseff, presidente brasileira na época, fez menção ao ocorrido em sua fala na Assembleia Geral das Nações Unidas de 2013, condenando as ações de espionagem do governo estadunidense[51].

Ao contrário de Manning, Snowden não chegou a ser preso por seus atos de vazamento. Em 2013 ele fugiu para Hong Kong e de lá para a Rússia, onde iniciou um processo de pedidos de asilo a quaisquer países que pudesse lhe conceder asilo político. Segundo o próprio Snowden (2019, p,236)

> Ficamos presos no aeroporto por quarenta dias bíblicos e quarenta noites. Ao longo daqueles dias, candidatei-me a um total de vinte e sete países em busca de asilo político. Nenhum deles estava disposto a se levantar à pressão americana, com alguns países recusando abertamente, e outros

[50] Reporting on issues raised by the Snowden documents produced greatly heightened popular awareness of state surveillance, and those issues being raised through formal accountability structures within different countries. Public opinion proved more receptive in some regions than others, but it is fair to say that the Snowden documents empowered existing critics of surveillance and privacy activists to push their case in a number of different fora. Tradução nossa.

[51] Disponível em <https://g1.globo.com/mundo/noticia/2013/09/dilma-diz-na-onu-que-espionagem-fere-soberania-e-direito-internacional.html>. Acesso em 22 de outubro de 2023.

> declarando que não puderam sequer considerar meu pedido até que eu chegasse em seu território - um feito que era impossível[52]

Os EUA exerceram uma forte pressão para que Snowden fosse entregue à eles para ser julgado nos EUA. Uma das alternativas mais prováveis era a de se buscar asilo no Equador, país que já havia oferecido asilo a Julian Assange em sua embaixada em Londres. Ainda em Snowden (2019, p.228)

> O Equador, pelo menos em 2013, tinha uma crença arduamente conquistada na instituição do asilo político. Mais notoriamente, a embaixada do Equador em Londres tinha se tornado, sob Corrêa, o porto seguro e reduto de Julian Assange do WikiLeaks. Eu não tinha vontade de morar numa embaixada, talvez porque já tivesse trabalhado em uma. Ainda assim, os meus advogados de Hong Kong concordaram que, dada a circunstâncias, o Equador parecia ser o país com maior probabilidade de defender meu direito ao asilo político e os menos propensos a serem intimidados pela ira do hegemona que governou seu hemisfério[53]

A jornada até o Equador se provou inviável visto que não havia voos diretos entre os países e quaisquer aviões que Snowden embarcasse para ir até lá poderiam ser obrigados a pousar, de forma que ele seria levado para as autoridades locais e provavelmente extraditado. A possibilidade da presença dele no avião presidencial boliviano levou a um incidente diplomático onde o avião foi forçado a aterrissar quando voltava de uma viagem diplomática na Rússia e revistado em busca do *whistleblower*. Devido à impossibilidade de se sair do território russo sem a ameaça de extradição, Snowden acabou por requisitar extensões de sua residência temporária na Rússia até que em 2022, o presidente russo Vladimir Putin concedeu à ele cidadania russa, impedindo assim sua extradição (Snowden, 2019).

---

[52] we were trapped in the airport for a biblical forty days and forty nights. Over the course of those days, I applied to a total of twenty-seven countries for political asylum. Not a single one of them was willing to stand up to American pressure, with some countries refusing outright, and others declaring that they were unable to even consider my request until I arrived in their territory—a feat that was impossible. Tradução nossa.

[53] Ecuador, at least in 2013, had a hard-earned belief in the institution of political asylum. Most famously, the Ecuadorean embassy in London had become, under Correa, the safe haven and redoubt of WikiLeaks' Julian Assange. I had no desire to live in an embassy, perhaps because I'd already worked in one. Still, my Hong Kong lawyers agreed that, given the circumstances, Ecuador seemed to be the most likely country to defend my right to political asylum and the least likely to be cowed by the ire of the hegemon that ruled its hemisphere. Tradução nossa.

Assim como Manning, Snowden se tornou um ativista pela liberdade de informação e contra o sistema de vigilância em massa estabelecido pelos EUA tanto dentro quanto fora de seu território. Além disso, esses casos mostram como a gestão Obama lidou de forma rigorosa com os *whistleblowers*, já que segundo Colvin (2018, p.40) “a administração Obama processou mais *whistleblowers* sob a Lei de Espionagem do que todas as administrações anteriores juntas”. Nisso vemos que a gestão Obama mantém uma política dura em relação à proteção de informações tidas como sigilosas, colocando esses *whistleblowers* como ameaças à segurança nacional e fazendo uso das legislações referentes à espionagem e a cibersegurança para julgá-los como traidores que ativamente prejudicam a segurança e os interesses dos EUA dentro do sistema global.

3. ANÁLISE DOS DISCURSOS PRESIDENCIAIS E DOS DIRETORES DA NSA E DO DIA

Neste capítulo serão analisados tanto os discursos selecionados do Presidente Barack Obama quanto das agências NSA e DIA durante os anos de 2008 à 2016. Serão procurados nesses discursos palavras, comparações, metáforas e outros movimentos discursivos que indiquem tentativas de mover a questão da cibersegurança para a política de segurança. Faremos uso de uma metodologia de análise de discurso para buscarmos se houve uma construção temática sobre a cibersegurança como uma questão a ser elevada para dentro de uma esfera da política de exceção.

Os elementos buscados serão aqueles descritos por Buzan, Waever e Wilde (1998) em relação aos movimentos de securitização: ameaça existencial, senso de urgência e possibilidade da quebra de regras. Além disso, iremos mostrar quais estratégias foram utilizadas pelos emissores dos discursos analisados

3.1 Esquema metodológico

Como vimos anteriormente no capítulo 2, movimentos de securitização são essencialmente movimentos discursivos. Com isso, podemos agora fazer uma análise mais prática do modelo de securitização desenvolvido por Buzan, Wilde e Waever (1998) Essa análise será feita por meio de diversos documentos oficiais, além de declarações oficiais de membros das agências de segurança estadunidenses e documentos disponibilizados ao público que fazem referência a esse tema. Foram analisados 3455 discursos publicamente disponibilizados nos sites oficiais da Casa Branca de Obama e das agências. Desses discursos temos que 3425 foram presidenciais, 17 foram da NSA e 13 do DIA. Essa discrepância se dá pois o presidente é uma figura mais pública que os diretores das agências, que não dão declarações e discursos públicos na mesma frequência que o presidente. Ademais, visto que o discurso é nosso objeto de pesquisa decidimos por manter os trechos em seu idioma original durante o andamento do projeto,visto que traduções podem alterar elementos que se fazem presente no texto original.

Esses discursos foram escolhidos pois os movimentos de securitização visam convencer uma audiência-alvo (normalmente a população do país) de que o tema

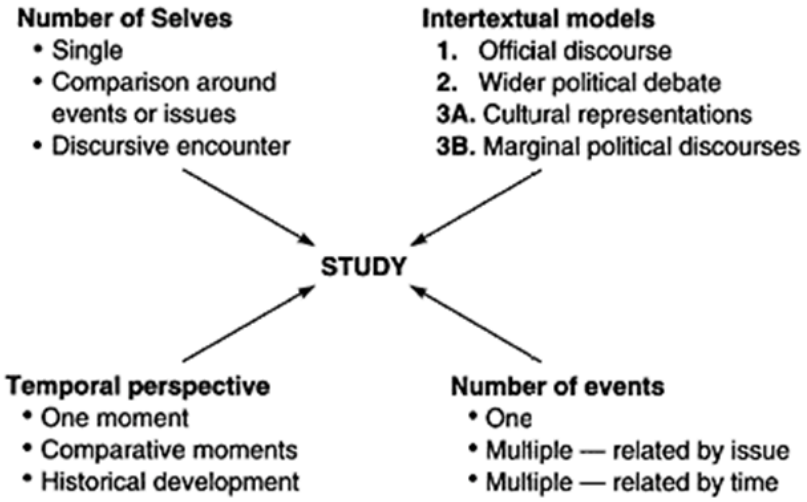
em questão deve ser levado para a esfera da segurança. Logo, discursos, declarações oficiais e documentos disponíveis para o público podem pautar essa discussão. As agências escolhidas para análise foram a Agência de Segurança Nacional (NSA) e a Agência de Defesa de Inteligência (DIA), ambas subordinadas ao Departamento de Defesa (DOD). Os discursos das agências foram levantados de seus sites oficiais, assim como os de Obama do arquivo da administração do mesmo.

Cabe aqui ressaltar que essas não são as únicas agências governamentais estadunidenses que se ocupam sobre a temática da cibersegurança. Existem outras que também lidam com esse tema como a Equipe de Preparação para Emergências Informáticas dos Estados Unidos (US-CERT) e o Escritório de Cibersegurança e Comunicações (CS&C), ambas subordinadas ao Departamento de Segurança Nacional. O recorte desta pesquisa foi feito em relação às duas agências escolhidas que se ocupam de questões além da proteção territorial dos EUA contra ataques terroristas e ameaças internas. Além disso, a NSA foi o pivô de um dos escândalos de vazamento de dados e espionagem.

Ao analisar se esses movimentos discursivos tentaram levar a questão da cibersegurança para fora da política cotidiana e para dentro da política de segurança, iremos buscar os três elementos essenciais descritos por Buzan, Waever e WIlde (1998) em um movimento de securitização: a ameaça existencial à um determinado objeto de referência, a urgência ao se lidar com o tema e a possibilidade da quebra de regras. A hipótese apresentada é que houve uma tentativa de securitização do tema.

Para prosseguirmos com essa análise de conteúdo dos discursos, documentos oficiais e declarações públicas, faremos uso do “modelo de pesquisa de análise de discurso” proposto por Lene Hansen em sua obra “Security as Practice: Discourse Analysis and the Bosnian War” de 2006. Nela, a autora se debruça sobre como a análise de discurso como ferramenta metodológica e como o discurso pode ser utilizado para entendermos a construção de políticas. Hansen também criou um modelo de estudo que faz uso de quatro elementos para analisar os discursos, sendo eles: o número de atores, o modelo intertextual, a perspectiva temporal e o número de eventos.

Figura 2: Modelo de análise de discurso



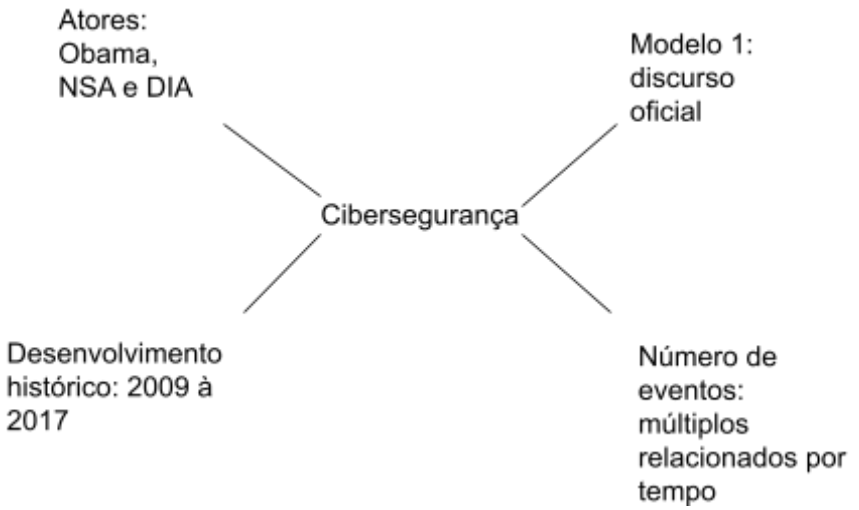
Fonte: (Hansen, 2006, p.72)

Nesse esquema elaborado por Hansen, temos a divisão dos elementos a serem analisados juntamente com as características dos mesmos. Inicialmente, é necessário a delimitação do número de selves a serem analisados: se será apenas um, se haverá uma comparação entre diferentes eventos ou temas ou encontros discursivos. Esses selves são os atores que serão analisados dentro das dinâmicas discursivas escolhidas. Em relação aos modelos intertextuais, se será analisado apenas o discurso oficial, o debate político sobre determinado tema, as representações culturais mais abrangentes sobre o tema ou ainda discursos políticos marginais. Neste ponto temos uma expansão gradual do escopo da pesquisa, que pode se ocupar apenas do discurso oficial, do discurso apresentado pelas autoridades quanto se expandir para outras áreas dentro do discurso político e cultural. No escopo temporal da análise, a escolha deve ser feita sobre uma análise de apenas um momento temporal, sobre vários momentos em uma análise comparada ou sobre uma análise sobre como os discursos se apresentam em um desenvolvimento histórico. A análise de um momento temporal único é focada em um momento singular, enquanto as análises comparadas e de desenvolvimento histórico nos permitem observar como o discurso sobre um determinado tema se apresenta tanto numa comparação quanto numa evolução temporal. Por último, os eventos a serem analisados também devem ser escolhidos, se será apenas um evento ou múltiplos eventos relacionados por tema ou pelo recorte temporal. A

escolha dos eventos segue a mesma lógica do recorte temporal, de modo que a análise pode ser tanto focada em um único evento que será analisada ou em múltiplos eventos, de modo a nos proporcionar uma análise comparativa baseada tanto por tempo quanto por temas relacionados.

Com base nesse modelo elaborado por Hansen, podemos adaptá-lo à pesquisa ao delimitarmos as variáveis dentro de cada ponto do esquema apresentado. Em relação ao número de atores, iremos analisar tanto os discursos de Obama durante sua presidência quanto o que foi declarado pela NSA e pelo DIA, totalizando três selves. Os discursos de Obama que foram analisados foram aqueles em que termos relacionados à cibersegurança (*Cybersecurity, cyber attack, hacker, cyber space, cyber threat* e *malware*). Apesar dos diretores das agências escolhidas terem sido trocados durante os oito anos do governo Obama, eles serão tratados como um único ator pois seus discursos representam as agências que os mesmos chefiavam. Nos modelos intertextuais, visto que frequentemente o processo de securitização tem uma abordagem top-down e que iremos analisar os discursos, documentos e declarações oficiais, iremos nos ater ao ponto (1), o discurso oficial. Nossa perspectiva temporal foi delimitada como os anos da presidência de Barack Obama, ou seja, do dia 20 de janeiro de 2009 até o dia 20 de janeiro de 2017. Já nos números de eventos, trabalhamos com múltiplos eventos relacionados por tempo, de modo a entender como a questão da cibersegurança foi evoluindo nos discursos oficiais durante os anos da gestão Obama. Com essas informações, podemos aplicar o modelo feito por Hansen à pesquisa da seguinte maneira.

Figura 3: Modelo de análise de discurso para pesquisa



Fonte: elaborado pelo autor

Tendo em vista o modelo de análise apresentado e o recorte de pesquisa, iremos averiguar se durante a gestão de Barack Obama houve tentativas vindas do presidente e dos diretores da NSA e do DIA de securitizar a questão da cibersegurança. Para selecionar os discursos a serem analisados, recorremos aos sites oficiais dessas agências que disponibilizam esses discursos, declarações e documentos para o público. Foram analisados um total de 33 discursos, declarações oficiais e audiências no Senado, sendo 17 delas vindas da NSA, e 13 do DIA.

Os termos apresentados são relacionados à área da cibersegurança pois se referem a diversos conceitos presentes dentro do campo. Cibersegurança se referindo ao campo como um todo e também à segurança de um país ou de empresas em relação aos seus dados, suas redes e seus computadores. Cyberattack seriam ações ofensivas feitas por meio de computadores contra alvos selecionados. Cyberspace caracteriza as redes de conexão entre diversos computadores e sistemas. Cyberthreat é o termo utilizado para se designar possíveis ameaças relacionadas a ataques cibernéticos ou outras vulnerabilidades ligadas às redes. Hackers é o termo utilizado para designar indivíduos que usam de seu conhecimento para obter dados sigilosos. Tanto vírus quanto malware são utilizados para se referir a programas maliciosos que infectam computadores, geralmente para tomar o controle dos mesmos ou roubar os dados ali armazenados.

Vírus é o termo mais coloquial, sendo que malware é o utilizado mais formalmente dentro da área.

Tabela 1 - Ocorrência de palavras relacionadas à cibersegurança

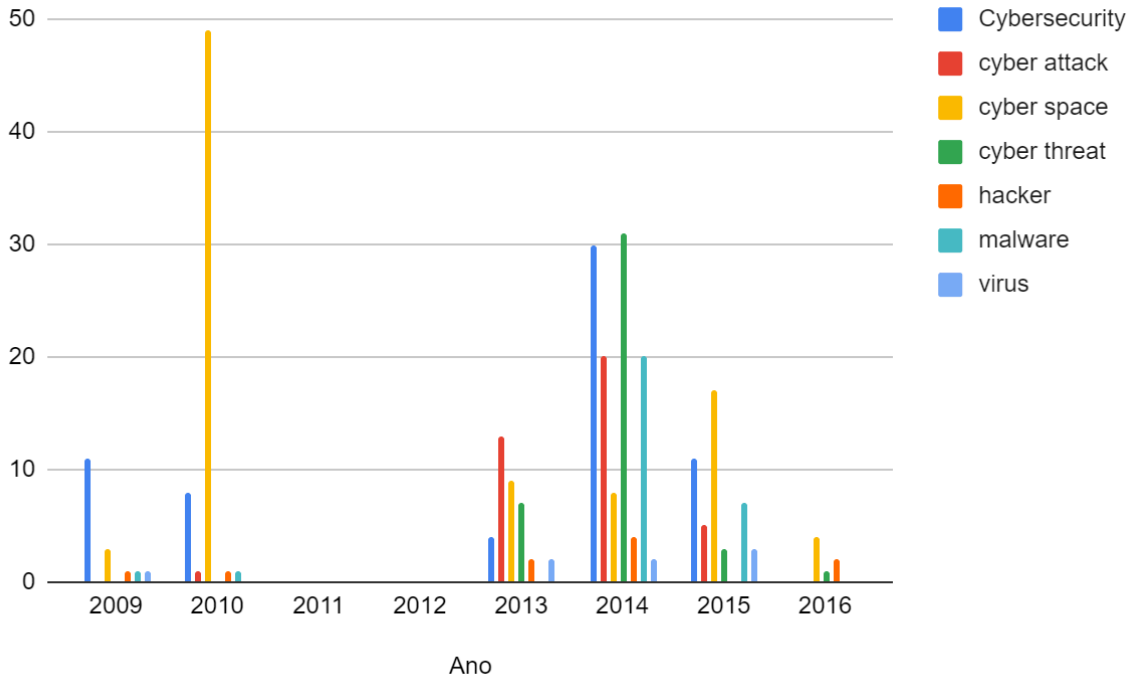
Termos	NSA	DIA	Total
Cybersecurity	63	2	**65**
Cyberattack	28	18	**46**
Cyberspace	71	15	**86**
Cyberthreat	30	12	**42**
Hackers	7	12	**19**
Virus	8	0	**8**
Malware	29	0	**29**

Fonte: elaborado pelo autor com base em dados primários

Vemos aqui que esses termos relacionados se fazem mais presentes nos discurso e declarações vindas da NSA, visto que a mesma é a agência mais relacionada à inteligência de sinais (SIGINT), ou seja, informações coletadas por meio de interceptações de chamadas telefônicas, pela internet e por outros meios de comunicação eletrônica[54]. O DIA é uma agência que trabalha com a análise de inteligência, sendo alimentada por informações vindas de diversas outras agências focadas em coleta, como a NSA e a Central Intelligence Agency (CIA). Ademais, se adicionarmos um elemento temporal na frequência com que esses termos aparecem, teremos mais uma variável de análise.

[54]Disponível em < https://www.nsa.gov/Signals-Intelligence/Overview/>. Acesso em 6 de novembro de 2023.

Gráfico 2 - Ocorrência de termos relacionados à cibersegurança pelas agências NSA e DIA por ano 2009-2016



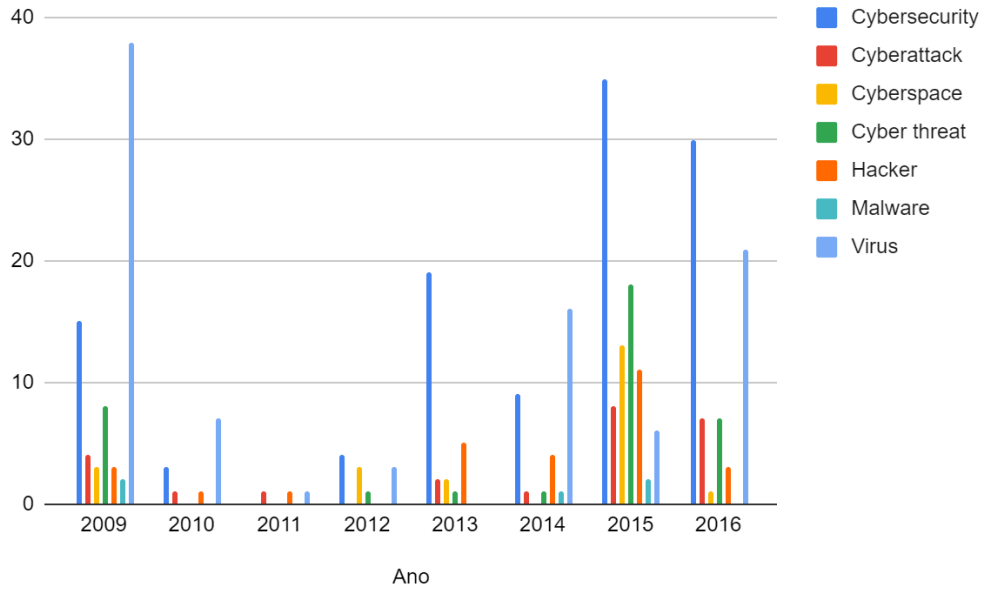
Fonte: Elaborado pelo autor

Aqui vemos uma maior presença desses termos nos anos de 2009 e 2010, seguidos de dois anos sem que os mesmos apareçam em discursos oficiais dessas agências, para então terem um ressurgimento vertiginoso. Se retornarmos aos incidentes de cibersegurança citados no capítulo anterior, veremos que esses aumentos ocorreram nos anos de 2010 e 2013, os anos em que ocorreram os incidentes dos malware Stuxnet e dos vazamentos feitos por Chelsea Manning (2010) e os vazamentos de Edward Snowden (2013). Assim, podemos conjecturar que esses incidentes projetaram o tema da cibersegurança para uma posição mais central dentro do discurso oficial do governo estadunidense. A NSA se viu especialmente no centro da discussão pois foi a agência que Snowden expôs como o centro de um esquema de coleta de informações de diversos indivíduos, tanto cidadãos estadunidenses quanto de outros países, incluindo chefes de Estado (Jordan, 2015).

Vemos que principalmente em 2014, ano seguinte ao incidente Snowden, o uso dos termos “cibersegurança” e “ciber ameaça” nos discursos oficiais da NSA tem um aumento vertiginoso, juntamente com um aumento de menor quantidade do resto dos termos. Com esses dados em mente, podemos começar a analisar se juntamente com esse aumento do uso dos termos sobre cibersegurança após os três grandes incidentes houve uma tentativa governamental de securitizar essa área temática.

Em relação aos discursos presidenciais, foram analisados 73 discursos proferidos por Barack Obama nos anos em que o mesmo ocupou o cargo de presidente dos EUA. Os discursos escolhidos foram aqueles em que termos relacionados à temática da cibersegurança foram encontrados.

Gráfico 3 - Uso de termos relacionados à cibersegurança nos discursos oficiais de Barack Obama



Fonte: elaborado pelo autor

Vemos aqui que as falas de Obama seguem em parte a tendência observada nas falas da NSA e do DIA,embora com certas divergências. Nos primeiros anos não temos uma presença tão expressiva desses termos nos discursos oficiais, com exceção do termo cibersegurança aparecendo significativamente em 2009/2010. Porém em 2013/2014 vemos uma incongruência maior se desenhando. Nesses

anos, os termos pesquisados começam a aparecer mais em 2013 e aumentam para a maior frequência em 2014.Isso se dá devido ao impacto que o caso Snowden teve dentro da comunidade de cibersegurança e dos desenvolvimentos geopolíticos ocorridos naquele ano, como citado no capítulo anterior. O caso Snowden colocou a rede de coletas de dados ilícita dos EUA no centro das discussões, de modo que faz sentido que Obama não se refira muito ao tema, visto sua posição como presidente da nação que conduziu essa rede de espionagem.

O que vemos nos discursos de Obama em 2015/2016 é um aumento considerável da presença dos termos relacionados à cibersegurança, na contramão das agências. Porém, ao analisarmos o cenário político americano, vemos que esse aumento tem uma razão interna. A corrida eleitoral americana já se preparava para as eleições de novembro de 2016, com Donald J. Trump concorrendo pelo Partido Republicano e Hillary Clinton pelo Partido Democrata. Essa corrida eleitoral mostrou o desgaste da figura de Hillary dentro dos EUA e acabou com a eleição de Trump, até então um outsider da política. O fato importante relacionado à cibersegurança nesse período foi a suspeita de interferência nas eleições por agentes russos infiltrados. De acordo com um relatório temático publicado pelo *think tank* The Third Way (2019, p.3)

> A interferência da Rússia nas eleições presidenciais de 2016 – nas quais usou ferramentas cibernéticas maliciosas para espalhar desinformação e invadir infraestrutura eleitoral e Contas do Partido Democrata a favor do então candidato Donald Trump – demonstra o grave perigo que as ameaças cibernéticas podem representar para a segurança nacional dos EUA e a confiança na democracia americana.[55]

Em 2018, o FBI chegou a indiciar 11 russos por cibercrimes, crimes de identidade, além de outros crimes focados em pessoas empresas ligados ao processo eleitoral estadunidense[56]. Esse aumento de interferência externa no processo eleitoral demonstra que o ciberespaço e ciber operações podem ser uma

[55] Russia's interference in the 2016 presidential election—in which they used malicious cyber tools to spread disinformation and hack into election infrastructure and Democratic Party accounts in favor of then-candidate Donald Trump—demonstrates the grave danger cyber threats can pose to US national security and confidence in American democracy. Tradução nossa.
[56] RUSSIAN INTERFERENCE IN 2016 U.S. ELECTIONS. Disponível em <https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections>. Acesso em 06/03/2024.

maneira de desestabilizar ou influenciar em processos políticos de outros países de maneira menos evidente e invasiva que ações como ameaças militares.

3.2. Ameaça existencial

Neste capítulo, exploraremos a presença de elementos relacionados à percepção de ameaça existencial. Além disso, discutiremos como os documentos lidam com os vários tipos distintos de referências. Abordaremos ainda o papel desempenhado pelos inimigos nos documentos, a maneira como os autores recorrem a exemplos históricos e a influência da audiência nessas obras.

3.2.1 A presença de termos relacionados à ameaça existencial

Voltando aos elementos presentes no processo de securitização descritos por Buzan, Waever e Wilde (1998), uma aparente ameaça existencial se faz necessária dentro de um movimento securitizador, pois coloca a própria sobrevivência do objeto de referência. Dessa forma, foi feita uma busca dos termos *attack, security, threat, risk, danger, critical, enemy* e *war.* Esses termos estão relacionados às percepções de ameaças a um determinado objeto, de modo que podem ser indícios de uma tentativa de securitização.

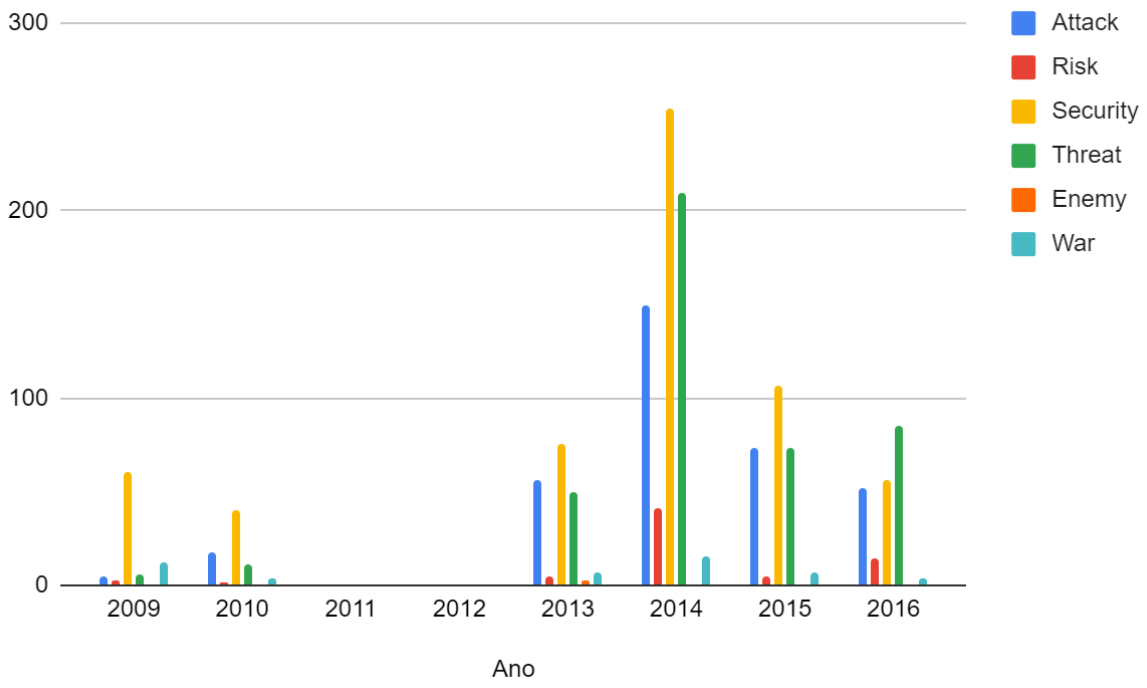
Quadro 1 - Ocorrência de palavras relacionadas à ameaça existencial nos discursos oficiais das agências

Termos	**NSA**	**DIA**	**Total**
Attack	142	134	**276**
Risk	30	37	**67**
Security	180	196	**376**
Threat	122	235	**357**
Danger	14	16	**31**
Critical	95	28	**123**

Fonte: elaborado pelo autor com base em dados primários

Devido ao papel designado pelas agências, vemos que esse termos relacionados à ameaças são recorrentes, com os termos “security” e “threat” sendo os mais recorrentes nos discursos. Vemos que ambas ocorrem em maior número quando analisamos os discursos do DIA, visto que seu papel como uma agência de inteligência ligada à defesa dos EUA. O uso de palavras que evocam esse sentimento são utilizadas para o poder de convencimento do ator securitizador. Para identificar esse aspecto, buscamos a frequência com que palavras relacionadas à ameaça existencial ocorreram nos discursos analisados.

Gráfico 4 - ocorrência de termos relacionados à ameaça existencial 2009-2016 nos discursos das agências



Fonte: elaborado pelo autor

No gráfico vemos que em relação aos termos relacionados apenas à segurança, o ano de 2010 foi bem menos expressivo do que quando comparado à quantidade de termos relacionados à cibersegurança, como evidenciado no gráfico dois apresentado anteriormente. Porém, uma outra tendência há de ser observada, visto que temos um pequeno aumento da recorrência desses termos no ano de 2013 seguido de um aumento vertiginoso no ano de 2014. As questões da invasão da Ucrânia e da expansão do Estado Islâmico, já citados no capítulo anterior,

explicam esse aumento devido ao fato de serem desenvolvimento importantes na geopolítica global no ano.

A frequência desses termos se manteve em correlação com os números apresentados anteriormente em relação à cibersegurança, com exceção em 2009-2010, onde não vemos um uso tão expressivo desses termos. Em 2014 Rajesh De, chefe do departamento legal da NSA, discursou em na Faculdade de Direito de Georgetown sobre os perigos que as ciberameaças representam para os EUA:

> We also have seen a disturbing trend in the evolution of the cyber threat around the world. **As General Keith Alexander, the Director of NSA, describes it, the trend is one from "exploitation" to "disruption" to "destruction."** In fundamental terms, the cyber threat has evolved far beyond simply stealing-the stealing of personal or proprietary information, for example-to include more disruptive activity, such as distributed denial of service attacks that may temporarily degrade websites; **and more alarmingly, we now see an evolution toward truly destructive activity.**[57]

Neste trecho, Rajesh coloca que as ciber ameaças não são mais apenas sobre roubo de dados ou disrupção de serviços, mas podem sim ter capacidades destrutivas. Essa progressão faz com que uma maior atenção do governo à área se torne lógica, visto que se o escopo da ameaça aumenta a preocupação com a mesma deve aumentar concomitantemente.

No seu discurso em Stanford em 2015, Obama traz a ideia de que a cibersegurança não deve ser uma questão de política, mas de segurança.

> **And so defending against cyber threats, just like terrorism or other threats, is one more reason that we are calling on Congress, not to engage in politics -- this is not a Republican or Democratic issue -- but work to make sure that our security is safeguarded** and that we fully fund the Department of Homeland Security.[58]

---

[57] Também temos observado uma tendência perturbadora na evolução da ameaça cibernética em todo o mundo. Como descreve o general Keith Alexander, diretor da NSA, a tendência é de "exploração" para "perturbação" e "destruição". Em termos fundamentais, a ameaça cibernética evoluiu muito além do simples roubo - o roubo de informações pessoais ou proprietárias, por exemplo - para incluir atividades mais perturbadoras, como ataques distribuídos de negação de serviço que podem degradar temporariamente websites; e o mais alarmante é que vemos agora uma evolução em direção a atividades verdadeiramente destrutivas. Tradução e grifo nossos.

[58] E, portanto, a defesa contra ameaças cibernéticas, tal como o terrorismo ou outras ameaças, é mais uma razão pela qual apelamos ao Congresso, não para se envolver em política - esta não é uma questão republicana ou democrata - mas para trabalhar para garantir que a nossa segurança

Aqui o presidente equaliza ciber ameaças com outros tipos de ameaças que os EUA enfrentam, em especial o terrorismo. Ao clamar para que não se politize a questão entre Republicanos e Democratas, ele coloca a necessidade de que a segurança dos EUA esteja resguardada contra essas ciberameaças, visto que elas podem representar ameaças existenciais contra os EUA. Essa chamada por suporte bipartidário se repetiu em um discurso de Obama na National Governors Association em 2016: “So, fighting terrorism and gun violence, **combating cyber attacks and cyber threats, guarding against the outbreak of disease -- these are some areas where there shouldn’t be any dispute**”[59].

Em 2013, no Avaliação Anual de Ameaças apresentada ao Comitê de Forças Armadas do Senado, o diretor do DIA afirmou: “

> **I believe the most pressing threat facing our country is the threat from CYBER attacks**. The daily occurrences of attacks are damaging on a variety of levels and they are not only persistent and dangerous, the likelihood of serious damage to our national security is very real.[60]

Em sua fala almirante coloca abertamente que a ameaça de ciberataques é, na sua visão, a maior ameaça enfrentada pelos EUA no momento. Ele afirma que existe uma constância nesses ataques, demonstrando que é uma preocupação constante e não casos esporádicos. Além disso, se coloca que ,além de constantes, a capacidade de danos sérios à segurança nacional do país é real, trazendo assim um grau maior de legitimidade para a construção da cibersegurança como uma questão de segurança.

O que podemos analisar com o uso dos termos relacionados à ameaça é que a questão da cibersegurança é colocada como uma preocupação de segurança nacional e com um crescente potencial destrutivo. O que se vê presente é que a

---

esteja salvaguardado e que financiemos integralmente o Departamento de Segurança Interna. Tradução e grifo nossos.

[59] Assim, combater o terrorismo e a violência armada, combater ataques cibernéticos e ameaças cibernéticas, proteger-se contra surtos de doenças – estas são algumas áreas onde não deveria haver qualquer disputa. Tradução e grifo nossos.

[60] Eu acredito que a ameaça mais premente que o nosso país enfrenta é a ameaça dos ataques cibernéticos. As ocorrências diárias de ataques são prejudiciais a vários níveis e não são apenas persistentes e perigosas, a probabilidade de danos graves à nossa segurança nacional é muito real. Tradução e grifo nossos.

temática da cibersegurança é de preocupação em relação a objetos específicos dentro do governo e do sistema financeiro estadunidense.

3.2.2 Objetos de referência apontados nos discursos

Outro ponto a ser delimitado dentro dos discursos é quais objetos de referência são referenciados nos mesmos. Voltando aos conceitos de Buzan, Waever e Wilde (1998), o objeto de referência é aquele cuja sobrevivência está sendo ameaçada. Esse objeto se encontra numa posição de necessidade de proteção contra uma determinada ameaça, de modo que se a situação não for tratada.

Em 2014, o então presidente da NSA, almirante Michael Rogers, foi chamado a depor em um audiência ao senado estadunidense sobre o tema da cibersegurança, onde ele declarou fortes preocupações com os impactos de grandes ciberataques nos EUA:

> It's not hard to understand how difficult it would be if the power or the water was shut off, but imagine if one of our adversaries was able to shut down key American financial transactions. **Economy would grind to a halt. Even worse, imagine if a foreign cyberattacker altered or deleted key financial transaction data so that we couldn't verify account balances or what companies owe each other from today. It certainly would be chaos**. (Rogers, Michael, 2014)[61]

. Nesse discurso,temos a presença de dois objetos de referência: as redes de infraestrutura críticas citadas em “power” e “water” e a economia. O almirante Rogers faz aqui uma previsão dos impactos que os ataques cibernéticos teriam na vida do cidadão estadunidense. Quando ele se refere às dificuldades que a falta de abastecimento de energia ou água trariam, esses problemas têm um teor temporário, visto o uso do termo “shut off”, de modo que elas eventualmente

[61] Não é difícil compreender quão difícil seria se a energia ou a água fossem cortadas, mas imagine se um dos nossos adversários conseguisse encerrar transações financeiras americanas importantes. A economia iria parar. Pior ainda, imagine se um ciberataque estrangeiro alterasse ou apagasse dados importantes de transações financeiras para que não pudéssemos verificar os saldos das contas ou o que as empresas devem umas às outras a partir de hoje. Certamente seria um caos. Tradução e grifo nossos.

poderiam ser religadas ou restabelecidas. Porém, quando ele coloca que se a partir de hoje não se pudesse saber quem devia quem, aqui tem-se a criação de uma hipótese de dano permanente para o futuro do sistema financeiro americano. O termo “critical” aparece muitas vezes se referindo à “critical infrastructure”, de modo a trazer uma ideia de que a infraestrutura crítica dos EUA pode ser alvo de ataques, comprometendo sistemas essenciais ao funcionamento da vida dos estadunidenses.

Ao retornarmos ao discurso de Barack Obama em Stanford em 2015, o então presidente colocou como brechas de cibersegurança podem levar a ataques que trariam danos físicos às infraestruturas centrais dos EUA.

> Much of our critical infrastructure -- our financial systems, our power grid, health systems -- run on networks connected to the Internet, which is hugely empowering but also dangerous, and creates new points of vulnerability that we didn’t have before. Foreign governments and criminals are probing these systems every single day. **We only have to think of real-life examples -- an air traffic control system going down and disrupting flights, or blackouts that plunge cities into darkness -- to imagine what a set of systematic cyber attacks might do. So this is also a matter of public safety**. (Obama, Barack, 2015)

Nesse discurso Obama dá mais exemplos sobre como a interconectividade dos sistemas de infraestrutura crítica pode ser utilizada por criminosos ou governos estrangeiros como aberturas para ataques dentro do território americano. Ao dar exemplos concretos de que forma esses ataques podem afetar a população, Obama demonstra que esses danos vão além de questões mais relacionadas ao universo ciber como o roubo de dados. Vemos que a infraestrutura crítica dos EUA é novamente tida como estando sob ameaça.

Em 2010, no Center for Strategic and International Studies, o general Keith Alexander, então diretor da NSA, fez a seguinte ponderação: “America 's very wealth and strength make it a target in cyberspace. And one of the pillars of that strength, **our military, is at risk, perhaps to an even greater degree**”[62]. Nesse ponto ele coloca as forças armadas americanas como vulneráveis a esse tipo de ataque. Ao dizer que um dos pilares da força estadunidense está em risco, ele ao mesmo tempo exalta o papel das

[62] A própria riqueza e força da América fazem dela um alvo no ciberespaço. E um dos pilares dessa força, os nossos militares, está em risco, talvez num grau ainda maior. Tradução e grifo nossos.

forças armadas e aumenta a legitimidade de uma ameaça cibernética, visto que ameaça diretamente a esfera militar.

Voltando à fala de Obama em 2016 na National Governor Association, ele coloca a ação de hackers e Estados rivais como ameaças à valores, instituições e ao próprio público americano:

> Hackers and nations have **targeted our military, our corporations, the federal government, and state governments. They're a threat to our national security, they're also a threat to our economic leadership. They're a threat to our critical infrastructure. They're a threat to the privacy and public safety of the American people.** [63]

Ao analisarmos essa fala, em um único movimento discursivo, Obama colocou que ciber operações feitas por hackers e nações rivais são ameaças a nove objetos de referência diferentes. Esses objetos citados vão desde instituições governamentais até direitos individuais dos cidadãos americanos.

Em 2014 na conferência Cyber Maryland, Keith Alexander cita os setores determinados como críticos dentro pelo governo estadunidense:

> And then a third mission is, when directed by the president or the secretary of defense, to provide our capabilities to support and defend critical U.S. infrastructure.T**he U.S. government has designated approximately 16 sectors in the private industry as being critical to the nation's security. So think of water, think of power,think of aviation, fuel, financial, et cetera**.[64]

Aqui vemos uma expansão ainda maior do que seriam os objetos necessários de proteção, ou seja, ameaçados. O general cita os sistemas de distribuição de água e energia, já anteriormente citados e os mais frequentes quando se fala dos impactos de ciberataques. A esses ele soma o sistema financeiro, também comumente citado, e partes da indústria como aviação e combustível.

---

[63] Os hackers e as nações têm como alvo os nossos militares, as nossas empresas, o governo federal e os governos estaduais. São uma ameaça à nossa segurança nacional e também uma ameaça à nossa liderança económica. Eles são uma ameaça à nossa infraestrutura crítica. São uma ameaça à privacidade e à segurança pública do povo americano. Tradução e grifo nossos.

[64] E depois, uma terceira missão é, quando dirigida pelo presidente ou pelo secretário da defesa, fornecer as nossas capacidades para apoiar e defender infra-estruturas críticas dos EUA. O governo dos EUA designou aproximadamente 16 setores da indústria privada como sendo críticos para a segurança da nação. Então pense em água, pense em energia, pense em aviação, combustível, finanças, etc. Tradução e grifo nossos.

Observando os discursos analisados, o que podemos inferir é que um número grande de objetos de referência estão presentes nos discursos relacionados à cibersegurança. Os mais comuns são a infraestrutura crítica (principalmente água e energia) e o sistema financeiro. Isso se dá devido à interconectividade do mundo e dos sistemas atuais, de modo que praticamente todo sistema considerado vital tem alguma conexão com a internet e o ciberespaço, sendo assim vulnerável de alguma forma a operações cibernéticas ofensivas. Ao colocar esse grande números de objetos de referência, reforça-se a ideia de que não existe nenhum sistema totalmente seguro, de modo que a legitimidade da construção discursiva da cibersegurança como questão de segurança é aumentada.

3.2.3 Inimigos indicados nos discursos analisados

Outro ponto necessário de ser observado com criteriosidade é a construção dos autores dessas ameaças aos diversos objetos de referência. Na audiência citada anteriormente, Rogers afirma que os EUA se encontram em uma posição vulnerável a operações cibernéticas hostis, listando inclusive possíveis autores

> I believe our advanced nation state adversaries have the ability to cause such damage. These nations lack a strong motive at this moment to conduct such an attack and are deterred only by the fear of U.S. retaliation. **Our critical infrastructure networks are extremely vulnerable to such a damaging attack, and we can't count on a deterrence if we're already in an adversarial position with a nation like China or Russia**. And we can't count on the fact that less rational actors might also gain access to those critical systems. (Rogers, Michael, 2014)[65]

Aqui vemos que Rogers não só afirma que existem adversários dos EUA com capacidade e motivo para perpetrar esses ataques, ele coloca a China e a Rússia como os principais adversários. Ambos os países têm relações tensas com os EUA, e ao trazer os dois maiores adversários dos EUA como possíveis responsáveis por um eventual ciberataque, Rogers aumenta a credibilidade da ameaça que esses

[65] Acredito que os nossos adversários avançados, os Estados-nação, têm a capacidade de causar tais danos. Estas nações não têm neste momento um motivo forte para conduzir tal ataque e são dissuadidas apenas pelo medo de retaliação dos EUA. As nossas redes de infra-estruturas críticas são extremamente vulneráveis a um ataque tão prejudicial, e não podemos contar com uma dissuasão se já estivermos numa posição adversária com uma nação como a China ou a Rússia. E não podemos contar com o fato de intervenientes menos racionais também poderem ter acesso a esses sistemas críticos. Tradução e grifo nossos.

ataques teriam e também quem o estaria ameaçando (China e Rússia). Na última frase ele também não descarta que atores menos racionais poderiam ter acesso a esses sistemas. Podemos aqui teorizar que ele se refere a inimigos não-estatais que não seriam dissuadidos pelo medo de uma retaliação norte-americana. Um tipo de grupo que se enquadra nessa definição são grupos terroristas, que dentro do discursos político estadunidense são retratados como “loucos” ou “não-racionais” (Jackson, 2005). Aqui vemos que Rogers traz em um único movimento discursivo os principais antagonistas no discurso político norte-americano, de modo que temos aqui a identificação de inimigos e introduzindo uma nova esfera na qual os mesmos poderiam agir contra o Estado norte-americano e contra seus cidadãos.

Se analisarmos a Avaliação Anual de Ameaça elaborada pelo DIA e apresentada pelo general Michael Flynn em 2015, vemos que ele cita mais dois Estados como possíveis autores ou patrocinadores de ciber operações contra os EUA:

> **Iran and North Korea now consider disruptive and destructive cyberspace operations a valid instrument of statecraft**, including during what the U.S.considers peacetime. These states likely view cyberspace operations as an effective means of imposing costs on their adversaries while limiting the likelihood of damaging reprisals.[66]

Vemos então a indicação de outros dois Estados com visões hostis aos estadunidenses como usuários de ciber operações ofensivas. Esses dois atores estatais, no entanto, não têm a mesma posição de rivalidade com os EUA que potências como China e Rússia têm. Essa assimetria de poder favorece a narrativa de que esses países podem fazer uso do ciberespaço para tentar contornar a diferença colossal de poderio militar entre elas e os EUA, visto que a barreira para se operar no ciberespaço é baixa se comparada à outras formas de projeção de poder.

Esses países foram citados também na audiência no Senado em 2014 na fala almirante Rogers: “Thousands of companies trying tos hare **malicious source**

[66] O Irã e a Coreia do Norte consideram agora as operações disruptoras e destrutivas no ciberespaço um instrumento válido de política, inclusive durante o que os EUA consideram tempos de paz. Esses Estados provavelmente veem as operações no ciberespaço como meios eficazes de impor custos aos seus adversários, limitando ao mesmo tempo a probabilidade de represálias prejudiciais. Tradução e grifo nossos.

code that may have originated in Russia or China or Iran or North Korea or some international organized crime element"[67]. Aqui vemos que o almirante além de citar os Estados adversários dos EUA ele resgata novamente a ideia de que atores não-estatais possam também serem os responsáveis por ataques às empresas estadunidenses.

Na Avaliação de Ameaças de 2014 o general Flynn também destaca a crescente preocupação com a ameaça que atores não estatais representam:

> I think that what is a **serious threat that we are paying very close attention to are these non-nation state groups and actors, al-Qaeda being among them as one organization among many**. Others are what I would just describe as the transnational organized criminal elements that are also operating in the cyber domain and they have no rules that they have to adhere to and they are increasingly adapting to an environment that is actually benefiting them[68]

Aqui Flynn coloca uma especial atenção do DIA em relação às ameaças que atores não-estatais representam no ciberespaço, citando a al-Qaeda como exemplo. Ele também afirma que esses atores não estão sujeitos às mesmas regras que atores estatais, de modo que o uso do ciberespaço se torna especialmente propício para essas organizações. Em outro debate envolvendo vários membros da comunidade de inteligência David Shedd, vice diretor do DIA também elencou a possibilidade de ameaças internas sobre a cibersegurança estadunidense: "there's a significant DOD component to it, including from DIA, **one that wakes me up at night in terms of the insider threat**, because of the dynamics that you have"[69]. A menção de ameaças internas como agentes duplos ou traidores se faz relevante visto que o caso Snowden ocorreu quando um funcionário com autorização de acesso a essas informações decidiu publicá-las para o mundo. Desse modo, se

---

[67] Milhares de empresas que tentam compartilhar códigos-fonte maliciosos que podem ter origem na Rússia, na China, no Irã, na Coreia do Norte ou em algum elemento do crime organizado internacional.Tradução e grifo nossos.

[68] Penso que uma ameaça séria à qual estamos a prestar muita atenção são estes grupos e intervenientes não estatais, entre os quais a Al-Qaeda é uma organização entre muitas. Outros são o que eu descreveria apenas como elementos do crime organizado transnacional que também operam no domínio cibernético e não têm regras a cumprir e estão cada vez mais a adaptar-se a um ambiente que realmente os beneficia. Tradução e grifo nossos.

[69] Há um componente significativo do DOD nisso, inclusive do DIA, que me acorda à noite em termos de ameaça interna, por causa da dinâmica que você tem. Tradução e grifo nossos.

implica que os EUA não enfrentam apenas ameaças externas, mas também internas dentro da sua estratégia de cibersegurança.

Voltando ao discurso de Obama em Stanford, ele também menciona os possíveis autores de ataques contra os sistemas norte-americanos: “**Foreign governments and criminals** are probing these systems every single day”[70].Aqui, Obama menciona “governos estrangeiros e criminosos” como tentando explorar a vulnerabilidade desses sistemas todos os dias, novamente trazendo a identificação de possíveis inimigos. Visto que a palavra do presidente dos EUA tem um peso discursivo maior do que a do presidente da NSA, aqui Obama não cita países específicos como possíveis autores devido à possibilidade de causar atritos diplomáticos. Ao colocar ameaças físicas que podem ocorrer devido a ciberataques, Obama traz a percepção de que esses ataques podem representar ameaças existenciais para os EUA.

Os inimigos indicados nos discursos sobre cibersegurança são compostos de dois grupos: nações com quem os EUA já tem um histórico de rivalidade ou hostilidade e atores não-estatais como organizações criminosas e grupos terroristas. Ao trazer inimigos já estabelecidos dentro do discurso político estadunidense, esses discursos ganham maior legitimidade quando colocam a cibersegurança como uma questão de segurança nacional.

3.2.4 A presença de comparações históricas nos discursos

Ao analisarmos os discursos selecionados, uma comparação histórica se faz presente em algumas dessas falas. Observamos que a figura de Pearl Harbor foi invocada como uma estratégia de comparação em relação ao dano que possíveis ciberataques poderiam causar dentro dos EUA. Esse sentimento foi exposto na audiência no Congresso estadunidense onde o almirante Michael Rogers levantou a possibilidade de um ciberataque que causasse danos catastróficos na infraestrutura crítica norte-americana. “There has been a lot of talk over the years about

[70] Governos estrangeiros e criminosos investigam esses sistemas todos os dias. Tradução e grifo nossos.

hypothetical dangers of a cyber Pearl Harbor, and it's certainly become a bit of a cliché in cybersecurity circles.(Rodger, Michael, 2014)[71]"

Aqui Rodger faz um discurso com um apelo poderoso para o imaginário político estadunidense. O ataque à Pearl Harbor em 7 de dezembro de 1941 foi um episódio marcante dentro da história dos EUA, sendo o maior ataque sofrido em seu território até então. A morte de 2403 cidadãos norte-americanos em seu solo natal foi o evento que confirmou a entrada dos EUA no conflito, antes mais focado no teatro de guerra da Europa. Esse ataque foi resgatado durante o 11 de setembro por George W. Bush, comparando os ataques às torres gêmeas ao ataque surpresa japonês em 1941 (Jackson apud Bush, 2005). Quando Rogers faz essa declaração sobre "os perigos de um Pearl Harbor digital" ele reaviva a memória não só das vidas perdidas durante o ataque, mas do impacto que o mesmo tem no imaginário coletivo do país. Além disso, Pearl Harbor foi um claro ato de guerra, de modo que conceber a ideia de um Pearl Harbor cibernético leva a ideia de que um ataque cibernético poderia ser considerado uma declaração bélica da mesma maneira que um ataque físico à uma base militar. Além disso, devemos notar que a associação à Pearl Harbor também classifica os ataques como traiçoeiros e não-provocados, colocando os EUA numa posição não apenas de vítimas de um ataque injustificado, mas de um ataque realizado por meios covardes e criminosos (Jackson, 2005).

Em 2013, o diretor do DIA, Tenente General Michael Flynn discursou na International & National Security Summit onde também colocou a cibersegurança como a maior possível aos EUA no momento.

> Now we are all aware of the cyber threat – you spent a significant part of this afternoon talking about its various forms, **from rogue hackers to insider threats to state-sponsored actors – and in May, appropriately at Pearl Harbor, Secretary Hagel said in no uncertain terms that the devastatingly destructive potential of cyber attacks has become the security challenge of our age.** (Flynn, Michael, 2013)[72]

[71] Tem-se falado muito ao longo dos anos sobre os perigos hipotéticos de um Pearl Harbor cibernético, e isso certamente se tornou um clichê nos círculos de segurança cibernética.. Tradução e grifo nossos.

[72]Agora estamos todos conscientes da ameaça cibernética – vocês gastaram uma parte significativa desse tarde falando sobre suas diversas formas, desde hackers desonestos até ameaças internas até atores patrocinados pelo Estado – e em maio, apropriadamente em Pearl Harbor, o Secretário Hagel disse em termos inequívocos que o potencial devastadoramente destrutivo dos ataques cibernéticos tornaram-se o desafio de segurança da nossa época. Tradução e grifo nossos..

Aqui vemos novamente a figura de Pearl Harbor sendo utilizada para dar maior legitimidade para a afirmação de que o potencial destrutivo dos ciberataques se tornou o maior desafio da era atual. O termo “appropriately at Pearl Harbor” seguido de “devastatingly destructive potential” serve como uma maneira de se lembrar da destruição do ataque japonês, mas trazendo essa memória e conectando-a à uma ameaça atual. Ao se referir aos ciberataques como o “grande desafio de segurança de nossa era”, Flynn coloca que nos encontramos em uma nova era, uma onde o potencial destrutivo não é mais visto apenas em ações militares diretas, mas em ataques cibernéticos que podem ter o mesmo tipo de impacto.

Em 2010 John C. Inglis, vice-diretor da NSA, também trouxe a memória de Pearl Harbor e dos ataques de 11 de setembro de 2001 como uma lembrança da missão das agências de inteligência: “Because our fundamental charge is to not have a crisis; it's actually to avert the crisis. **We're not here to prepare for the next 9/11 or prepare for the next Pearl Harbor; we're here to actually avert that”**[73]. Aqui Inglis conjura a memória dos dois maiores ataques ocorridos em território estadunidense e que deixaram cicatrizes profundas dentro do imaginário coletivo do país. Ao colocar fortemente que a missão das agências é prevenir ataques dessa magnitude e que tomaram a vida de muitos norte-americanos, ele coloca que as crises que essas agências existem para prevenir estão no mesmo patamar desses dois episódios.

Voltando ao discurso de Rajesh De em Georgetown, ele também traz de volta o fantasma dos ataques do 11 de setembro para dar legitimidade à fala de que ciberataques podem ter níveis elevados de destruição e perda de vidas: “A cyber attack perpetrated by nation states or violent extremist groups **could be as destructive as the terrorist attack on 9/11**”[74].

O que vemos é que os dois exemplos históricos presentes nesses discursos são os mais traumáticos dentro da história estadunidense, de modo que trazê-los para uma comparação com possíveis ciberataques aumenta a legitimidade da

---

[73] Porque a nossa missão fundamental é não ter crise; na verdade, é para evitar a crise. Não estamos aqui para nos prepararmos para o próximo 11 de Setembro ou para nos prepararmos para o próximo Pearl Harbor; estamos aqui para realmente evitar isso. Tradução e grifo nossos.

[74] Um ataque cibernético perpetrado por Estados-nação ou grupos extremistas violentos pode ser tão destrutivo como o ataque terrorista de 11 de Setembro. Tradução e grifo nossos.

ameaça. Isso se dá pois esses ciberataques estão sendo colocados no mesmo patamar de eventos como o 11 de setembro de 2001 e o ataque japonês à Pearl Harbor.

3.2.5 O papel da audiência na dinâmica dos discursos.

Dentro dos discursos analisados, outro ponto que deve ser observado é que o tom do discurso muda consideravelmente quando os chefes dessas agências falam com o público em geral e quando falam em conferências ou painéis voltados à membros da comunidade de inteligência e tecnologia. Um exemplo disso é como o almirante Rogers define as potenciais ciberameaças em frente ao senado estadunidense:

> This is something real that is impacting our nation and those of our allies and friends every day. And it is doing it in a meaningful way that is **literally costing us hundreds of billions of dollars**, that is leading to a reduced sense of security and **that has the potential to lead to truly significant, almost catastrophic failures** if we don't take action.[75]

Aqui vemos que o uso de expressões como “literalmente nos custando bilhões de dólares” e “falhas catastróficas” são movimentos discursivos impactantes. O tom mais alarmista apresentado nessa audiência é possível pois o público alvo desse discurso (o Senado estadunidense) não tem, em sua maioria, profundo conhecimento sobre o tema. Desse modo, é menos provável que os interlocutores tenham questionamentos técnicos ou mais profundos sobre as informações ali apresentadas. O tom é bem diferente daquele presente quando Rogers fala na conferência International Conference on Cyber Security na universidade de Fordham em 2015, voltada para militares membros da comunidade de inteligência e cibersegurança:

---

[75] Isto é algo real que está impactando nossa nação e a de nossos aliados e amigos todos os dias. E está a fazê-lo de uma forma significativa que nos custa literalmente centenas de bilhões de dólares, que está a levar a uma sensação de segurança reduzida e que tem o potencial de levar a falhas verdadeiramente significativas, quase catastróficas, se não tomarmos medidas. Tradução e grifo nossos,

> So, in the next five years, let me look at it from a challenge perspective.The challenge that concerns -- the challenges that concern me in the next five years is does **the line between actions by nation-states, groups and individuals start to blur**, and do you start to see, for example, nation-states turning to criminal actors, turning to surrogates, turning to others as a vehicle to, try to complicate our ability to do attribution, identify who conducted the act.[76]

Nesta fala vemos que apesar da ideia de séria ameaça ser mantida, o tom utilizado é menos alarmista visto que a audiência tem um maior conhecimento e familiaridade sobre o tema. Ao se dirigir à uma audiência já familiar com o tema, não se faz necessário o convencimento da mesma da importância do tema ou dos perigos que ciberameaças como hackers ou ciber operações ofensivas de outros Estados. Nesse caso, a discussão se torna mais focada em conceitos comuns entre o emissor e a audiência.

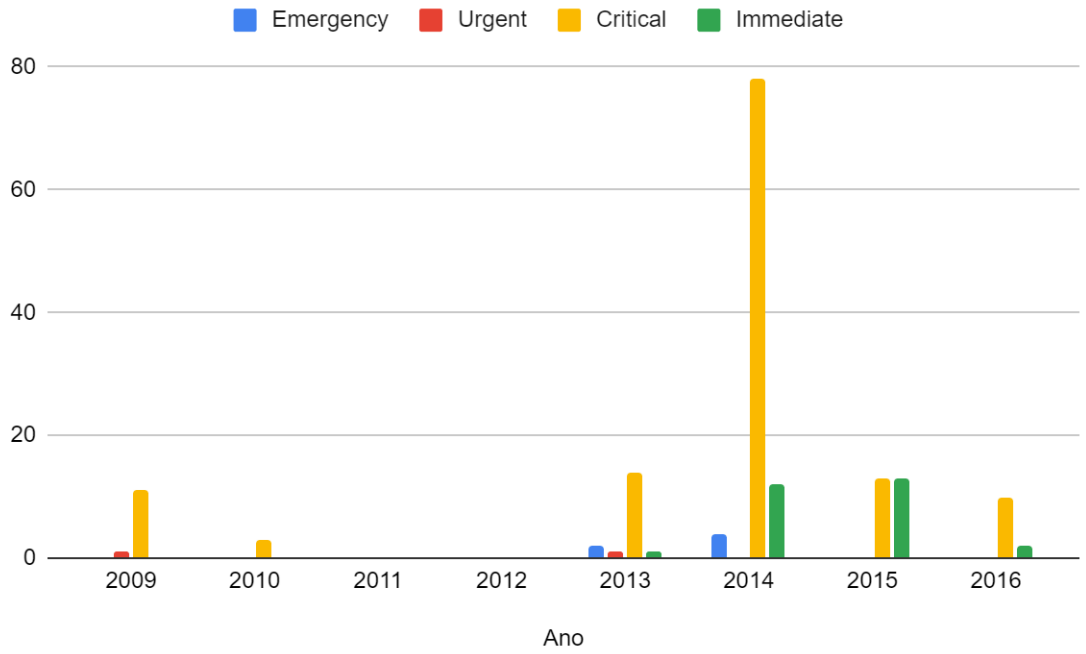
3.3.Situação de emergência

Outro fator igualmente necessário para que possamos caracterizar algo como um movimento de securitização é a colocação da questão como uma emergência. Isso ocorre pois se um determinado assunto não é enquadrado como operando numa limitação de tempo ele pode ser discutido dentro das arenas de debate político estabelecidas, de modo que medidas de exceção não necessitam de ser tomadas devido ao tempo hábil para se lidar com o assunto. Essa urgência temporal dá às autoridades maiores prerrogativas de lidar com o tema sem que ocorram maiores debates sobre o mesmo. A dimensão temporal de emergência torna ações que antes seriam debatidas com mais tempo e por um número maior de atores sejam tomadas sem essa deliberação, diminuindo assim o tempo de resposta dos atores (Buzan, Waever, Wilde, 1998). As palavras analisadas para essa parte da análise foram “*emergency”*, “*urgent”*, “*critical”* e “*immediate”*.

---

[76] Assim, nos próximos cinco anos, deixem-me olhar para isto numa perspectiva de desafio. O desafio que me preocupa - os desafios que me preocupam nos próximos cinco anos é se a linha entre as ações dos Estados-nação, dos grupos e dos indivíduos começa a diminuir. Você começa a ver, por exemplo, Estados-nação recorrendo a atores criminosos, recorrendo a substitutos, recorrendo a outros como um veículo para, tentar complicar a nossa capacidade de fazer atribuição, identificar quem conduziu o ato. Tradução nossa e grifo nossos.

Gráfico 5 - ocorrência de termos relacionados à ameaça existencial 2009-2016 nos discursos das agências



Fonte: elaborado pelo autor

O que podemos observar no gráfico apresentado é a baixa ocorrência desses termos nos discursos oficiais dos representantes dessas agências, com os termos "*emergency*" aparecendo um total de 6 vezes, "*urgent*" um total de 2 vezes e "*immediate"* um total de 18 vezes. O outlier na análise sendo o termo "*critical"*, aparece um total de 129 vezes sendo dessas 38 relacionado ao termo "*critical infrastrucuture"*, já analisado como um dos objetos de referências dos discursos. Além disso, o termo é empregado muitas vezes como um adjetivo, de forma a caracterizar a importância de um determinado objeto. Um exemplo desse uso pode ser visto quando general Flynn discursa sobre a importância de recursos naturais na 4ª cerimônia de entrega de prêmios da Intelligence and National Security Alliance: "international outreach will need our help dealing with regional disputes over **critical natural resources** that are quickly dwindling in supply"[77].

O que podemos inferir aqui é que o termo relacionado à importância da questão da cibersegurança aparece em uma frequência muito acima dos termos

[77] O alcance internacional precisará da nossa ajuda para lidar com disputas regionais sobre recursos naturais críticos cuja oferta está diminuindo rapidamente. Tradução e grifo nossos.

relacionados à temporalidade ou urgência. Ou seja, apesar de a temática da cibersegurança ser colocada como de grande relevância, isso não se traduz em um senso de urgência no tratamento da questão. Dessa forma, apesar de ser um tema central dentro da área de segurança e inteligência, não se tem uma necessidade ou oportunidade para se elevar à uma matéria de urgência para a população como um todo.

Na Audiência da Câmara de 2014 sobre Ameaças de Cibersegurança temos um dos momentos onde mais se identificam movimentos para criar um senso de urgência em relação aos ciberataques e à cibersegurança estadunidense. O almirante Michael Rogers, diretor da NSA no momento, faz por mais de uma vez declarações que trazem a necessidade de celeridade nas resoluções relacionadas à cibersegurança.

> We must be ready for a damaging cyberattack against our critical infrastructure. If the Senate does not **act swiftly**, both houses of Congress will have to start from scratch next year, moving new bills. **Given the cyberthreats we face, this could be an unnecessary and dangerous delay** when we are so close to an agreement that protects privacy and our economy and our national security (Rogers, Michael, 2014). [78]

Aqui o diretor da NSA urge para que os membros do Congresso americano cheguem a conclusões, pois a reiniciação do processo levaria um tempo que poderia deixar os EUA vulneráveis a ciberataques. Vemos aqui que essa urgência para que não haja um atraso tido como desnecessário para a discussão dessas leis se coloca como uma tentativa de enquadramento de uma situação de emergência. Nessa mesma audiência ele também argumenta que as ameaças não esperam por ações do Congresso para que ocorram.

> This committee has been **sounding the alarm on the cyberthreat for years and has twice led the House passage of critical cyber legislation**.

[78] Devemos estar preparados para um ataque cibernético prejudicial contra a nossa infraestrutura crítica. Se o Senado não agir rapidamente, ambas as casas do Congresso terão que partir do zero no próximo ano, movendo novas leis. Dadas as ameaças cibernéticas que enfrentamos, isso poderia ser um atraso desnecessário e perigoso quando estamos tão perto de um acordo que protege a privacidade, nossa economia e nossa segurança nacional. Tradução nossa.

> But the threat has not waited on the full Congress to act (Rogers, Michael, 2014). [79]

Na mesma audiência, as preocupações de Rogers foram reiteradas pelo congressista Dutch Ruppersberger, que também clamou por maior celeridade nas decisões relacionadas à proteção dos EUA contra ciberataques. “We're watching the threat grow and spread. Attacks have hit the State Department and the White House. **The danger is not waiting. So what's the full Congress waiting for**?”[80]. Dessa forma vemos que esse sentimento de urgência não vinha apenas dos diretores das agências, mas também por políticos estadunidenses. Porém essa audiência se demonstrou como um ponto fora da curva, visto que ao analisarmos os demais discursos selecionados não encontramos uma repetida tentativa de posicionar a questão da cibersegurança como uma questão de urgência. Nessa audiência temos um movimento discursivo voltado para uma percepção de um atraso estadunidense em relação aos possíveis autores de ataques cibernéticos contra o governo e a população norte-americana. Aqui a emergência é caracterizada quando se coloca que os EUA estariam defasados ou mal-preparados no caso de um ataque, de modo que a necessidade de se prepararem para um se torna uma questão de urgência.

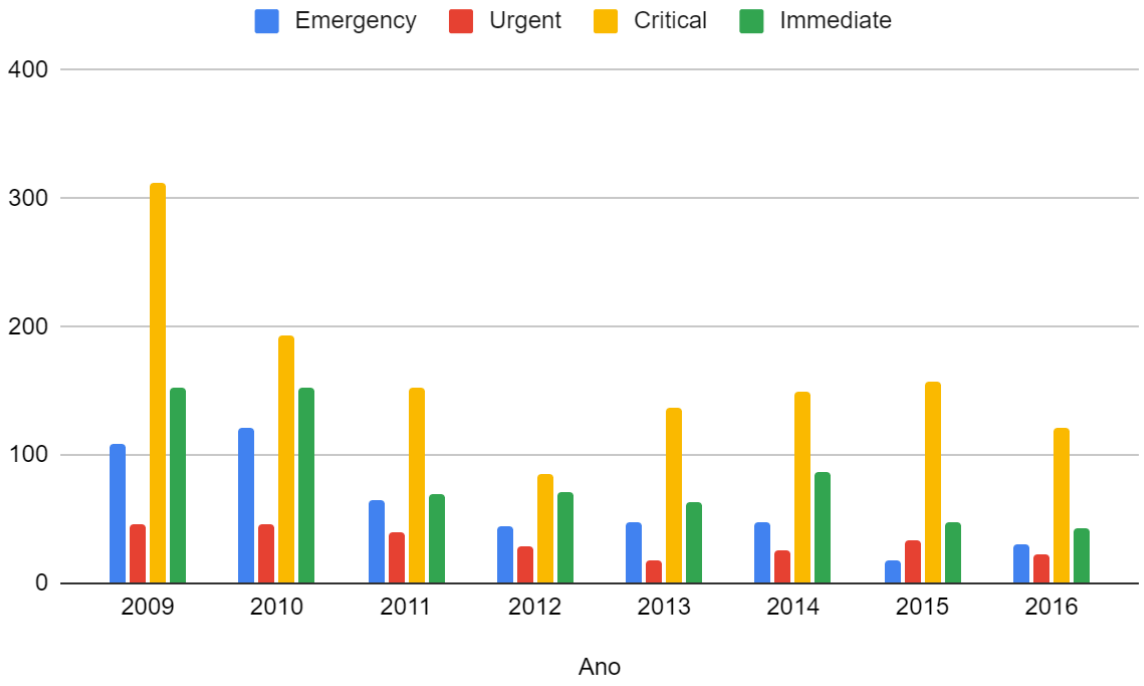
Porém ao analisarmos os demais discursos selecionados não encontramos uma repetida tentativa de posicionar a questão da cibersegurança como uma questão de urgência. Uma possibilidade do porque esse processo é mais presente nessa audiência no Congresso em 2014 é que ela ocorre no ano seguinte ao incidente de Edward Snowden, que como já analisamos foi um estopim para que a temática da cibersegurança tomasse uma posição central dentro do debate político principalmente nos EUA. Tanto que apesar de ser introduzida em 2013, foi apenas em 2015 que o USA Freedom Act foi promulgado, uma lei que buscava frear a coleta em massa dos dados de cidadãos americanos pela NSA, mas ainda assim estendia prerrogativas do Patriot Act para as agências.

---

[79] Este comitê tem soado o alarme sobre a ameaça cibernética há anos e tem liderado por duas vezes a aprovação de legislação cibernética crítica na Câmara. Mas a ameaça não esperou que todo o Congresso agisse. Tradução e grifo nossos.

[80] Estamos observando a ameaça crescer e se espalhar. Os ataques atingiram o Departamento de Estado e a Casa Branca. O perigo não está esperando. Então, o que todo o Congresso está esperando. Tradução nossa.

Gráfico 6 - Ocorrência de termos relacionados à situação de emergência 2009-2016 nos discursos presidenciais



Fonte: elaborado pelo autor

Passando agora para a análise dos discursos presidenciais em relação aos termos escolhidos para situação de emergência, aqui vemos uma presença bem mais significativa desses termos. Porém não se aparenta haver uma correlação entre o uso dos termos pelas agências e pelo presidente. "*Critical*" aparece novamente como o termo mais utilizado, aparecendo 1345 vezes durante os anos de mandato de Barack Obama, se referindo à "*critical infrastructure*" em apenas 59 ocasiões. Desse modo, um dos principais objetos de referência nos discursos sobre cibersegurança não teve uma presença expressiva nos discursos presidenciais. Além disso, vemos que o ano com maior uso do termo "*critical*" nos discursos presidenciais não foi o de maior uso das agências, demonstrando não haver uma correlação entre o discurso oficial do presidente e das agências.

"*Emergency*" aparece em 129 vezes ligado ao termo "*emergency room*", demonstrando uma preocupação do presidente em relação ao sistema de saúde estadunidense, como visto em uma entrevista dada ao canal de notícias PBS em 2016: "is if they're not getting health insurance through you, then that means that

they're relying on the **emergency room** and they're relying on taxpayers"[81]. O termo "*urgent*" é em todos os anos o menos presente, e quando usado se refere a diferentes termos, mas principalmente vemos seu uso principalmente no termo "*urgent challenges*". Esse termo em si aparece relacionado à mudanças climáticas: "especially when it comes to solving **urgent challenges** like climate change*?*"[82], como dito no State of The Union Address de 2016; e à potenciais ameaças aos EUA "on the North Korean nuclear issue, which represents a shared challenges confronting all three countries -- **an urgent challenge**"[83], em um pronunciamento com o presidente sul-coreano e o primeiro-ministro japonês em 2016. Por último, "*immediate*" aparece relacionado a diversos outros termos como "*needs*","*action*" e "*consequences*", como no caso da fala do presidente sobre a situação do Japão em 2011: "The Red Cross is providing assistance to help meet the **immediate needs** of those who've been displaced"[84]. Além disso, também não encontramos nenhuma ocorrência dos termos buscados relacionados diretamente ao termo "*cyber*" nos discursos presidenciais.

Uma hipótese que pode ser levantada com base nesses dados é a de que os atores analisados (Obama e os diretores das agências) viam que a população no geral não aceitaria facilmente um sentimento de urgência em relação à cibersegurança. Isso se daria pois não houve nenhum evento de grandes proporções que alçasse a temática da cibersegurança para o centro do debate e que gerasse um clima de medo e insegurança levando a um movimento discursivo para a transposição do tema para a esfera da política de emergência. Um exemplo do oposto disso foram os ataques do 11 de setembro, onde após os ataques o discurso oficial de uma situação de emergência foi facilmente aceito pela população.

Além disso, se compararmos os dados apresentados no gráfico 5 com os dados sobre o uso de termos de cibersegurança nos discursos presidenciais apresentados no gráfico 2, vemos que os anos em que Obama mais se referiu à cibersegurança não tiveram um aumento expressivo do uso dos termos relacionados à situação de emergência. O que podemos inferir com os dados

[81]é que se eles não estão recebendo seguro saúde através de você, isso significa que eles estão contando com o pronto-socorro e com os contribuintes. Tradução e grifo nossos.
[82]especialmente quando se trata de resolver desafios urgentes como as alterações climáticas?. Tradução e grifo nossos.
[83] sobre a questão nuclear norte-coreana, que representa um desafio comum que os três países enfrentam - um desafio urgente. Tradução e grifo nossos.
[84] A Cruz Vermelha está prestando assistência para ajudar a atender às necessidades imediatas daqueles que foram deslocados. Tradução e grifo nossos.

apresentados é que apesar de haver um reconhecimento pelas agências e pelo presidente da importância da temática da cibersegurança para os EUA, não se configura ainda uma situação de emergência, onde o tempo para se lidar com a questão é limitado. Dessa maneira, o que observamos é que os atores analisados, apesar de colocarem a questão da cibersegurança como de alta relevância, não fazem o movimento de tentar criar uma percepção de urgência sobre o tema.

3.4. Possibilidade de quebra de regras

Outro elemento que se faz necessário para que possamos identificar um movimento de securitização é a possibilidade da quebra de regras. Essa possibilidade deve ser legitimada pela audiência alvo do discurso securitizador, sendo assim convencida da necessidade da mesma. É necessário lembrar que aqui nos referimos à *possibilidade* da quebra de regras, não à necessidade de quebra. É inteiramente plausível que questões de segurança sejam resolvidas sem a quebra de regras pré-estabelecidas (Buzan, Waever, Wilde, 1998).

Porém, quando vamos analisar esse caso na questão da cibersegurança, principalmente em relação ao caso Snowden, podemos observar que existe uma inversão da ordem do processo descrito por Buzan, Waever e Wilde (1998). Aqui temos que já havia uma quebra de regras anterior aos movimentos de securitização, porém a mesma era mantida em sigilo de Estado. Para que se obtenha autorização judicial para a gravação de informações e ligações de um cidadão estadunidense, as agências de segurança e inteligência necessitam de argumentar a necessidade da mesma para um juiz. De acordo com Landau (2013, p.55)

> Para cumprir a Quarta Emenda, os dois principais estatutos de escuta telefônica dos EUA, Título III do Omnibus de 1968 Lei de Controle do Crime e Ruas Seguras e a Inteligência Estrangeira de 1978 Lei de Vigilância (FISA), exigem uma razão específica e articulável para escuta telefônica. Os toques do Título III exigem causa provável de que o suspeito seja cometeu ou está prestes a cometer um crime grave, enquanto os grampos da FISA exigem que haja causa provável de que o alvo seja uma potência estrangeira ou um agente de uma potência estrangeira, e que o objetivo do grampo é a inteligência estrangeira. O uso de uma escuta telefônica é

> normalmente um último recurso – isto é, quando a informação procurada não pode ser razoavelmente obtida por outros meios.[85]

O vazamento de Snowden demonstrou que o governo fazia esses grampos, além da coleta de informações e metadados, sem autorização judicial. Essa vigilância mais ostensiva se viu legitimada na esteira dos ataques de 11 de setembro de 2001 e com a subsequente aprovação do Ato Patriota. O medo que a sociedade americana sentia após os ataques legitimou para a população uma expansão do sistema de vigilância ostensiva com a esperança de que assim ataques terroristas da magnitude do 11 de setembro não se aconteceriam novamente (Ünver, 2018).

Com o passar dos anos, essa vigilância começou a ser questionada, mas o processo não diminuiu, pelo contrário. Quando Snowden disponibilizou as provas da espionagem americana, tanto de seus cidadãos quanto de residentes e chefes de Estado estrangeiros, houve tentativas de autoridades governamentais para legitimar esses atos em nome da segurança nacional. Michelle Van Cleave, que trabalhou nos gabinetes de inteligência de Bush e Obama, faz o seguinte argumento

> Por exemplo, em 1998, houve um vazamento de que a NSA tinha a capacidade de ouvir as conversas de telefone por satélite de Osama bin Laden. E então Bin Laden parou de usar aquele telefone. Quem sabe se poderia ter havido uma oportunidade de evitar o ataque terrorista de 11 de Setembro, quatro anos mais tarde, se essa linha não tivesse desaparecido? (Van Cleave, Michelle, 2013, p.2)[86].

Ou seja, vemos que nessa ocasião as regras já haviam sido quebradas, mas com a divulgação pública desta quebra o governo se viu na necessidade de legitimar a mesma. Além disso, existe também um movimento para se deslegitimar os responsáveis pelos vazamentos, citando perdas de vidas e perdas estratégicas

---

[85] To comply with the Fourth Amendment, the two primary US wiretap statutes, Title III of the 1968 Omnibus Crime Control and Safe Streets Act and the 1978 Foreign Intelligence Surveillance Act (FISA), require a specific, articulable reason for wiretapping. Title III taps require probable cause that the suspect is committing, has committed, or is about to commit a serious crime, whereas FISA taps require that there be probable cause that the target is a foreign power or an agent of a foreign power, and that the purpose of the tap is foreign intelligence. Use of a wiretap is typically a last resort—that is, when the information sought can't reasonably be obtained by other means. Tradução nossa.

[86] For example, in 1998 there was a leak that NSA had the ability to listen to Osama bin Laden's satellite phone conversations. And then Bin Laden stopped using that phone. Who knows whether there might have been a chance to prevent the terrorist attack on September 11 four years later had that line not gone dark?. Tradução nossa.

para os EUA. Em 2014 o diretor da DIA Michael Flynn foi questionado por uma senadora sobre os danos que Snowden teria causado aos militares, dando a seguinte resposta.

> On the report that you're indicating or highlighting, we do have I believe a session in about a week for this committee to go through the entire report. The strongest word that I can use to describe you know, how bad this is, this has caused grave damage to our national security. I think another way to address your question, **what are the costs that we are going to incur because of the scale and the scope of what has been taken by Snowden**. And I won't put a dollar figure but I know that the scale or the cost to our nation obviously in treasure, in capabilities that are going to have to be examined, reexamined, and potentially adjusted, but I think that the greatest cost that is unknown today, but we will likely face is the cost in human lives on tomorrow's battlefield or in some, someplace where we will put our military forces – you know, when we ask them to go in to harm's way. **That's' the greatest cost that we face with the disclosures that have been presented so far. And like I said, the strongest word that I can use is this has caused grave damage to our national security** (Flynn, Michael, 2014)[87]

Além disso, no World Threat Assessment de 2014, se afirma que o DIA vem trabalhando numa força tarefa para que se pudesse mensurar a extensão dos danos que foram causados pelos vazamentos de informações da NSA, além de corroborar a ideia de que esses atos causaram ameaças graves à segurança dos EUA.

> **DIA is leading an Information Review Task Force to examine grave damage caused to Department of Defense equities and US national security as a result of the unauthorized NSA disclosures.** An emerging threat that concerns the department involves the potential for **foreign**

[87] No relatório que você está indicando ou destacando, acredito que temos uma sessão em cerca de uma semana para esta comissão analisar todo o relatório. A palavra mais forte que posso usar para descrever, você sabe, o quão ruim isso é, isso causou graves danos à nossa segurança nacional. Penso que outra forma de responder à sua pergunta: quais são os custos que iremos incorrer devido à escala e ao alcance do que foi feito por Snowden. E não vou colocar um valor em dólares, mas sei que a escala ou o custo para a nossa nação, obviamente, em tesouros, em capacidades que terão de ser examinado, reexaminado e potencialmente ajustado, mas acho que o maior custo que é desconhecido hoje, mas que provavelmente enfrentaremos é o custo em vidas humanas no campo de batalha de amanhã ou em algum lugar onde colocaremos nossos forças militares – você sabe, quando lhes pedimos que entrem em perigo. Isso é o maior custo que enfrentamos com as divulgações que foram apresentadas até aqui. E como eu disse, a palavra mais forte que posso usar é que isso causou graves danos à nossa segurança nacional. Tradução nossa e grades nossos.

> **intelligence entities to compromise critical supply chains or corrupt key components bound for vital war-fighting systems.** Additionally, a few transnational terrorist groups have developed effective intelligence and counterintelligence capabilities—we have seen this manifest in Iraq and Afghanistan, and terrorist groups are now using and sharing the knowledge and experience they gained in those conflicts. (Flynn, Michael, 2014)[88].

Vemos aqui a legitimação de que esses atos de espionagem e vigilância ostensiva, apesar de irem contra regras estabelecidas dentro dos EUA, eram tidos como necessários para que o país mantivesse seus cidadãos seguros e suas operações em solo estrangeiros em funcionamento. Desse modo, o discurso oficial vinha tentar legitimar essa quebra de regras *à priori* fazendo uso da argumentação de que ela era necessária para que eles tivessem a capacidade de lidar com ameaças aos EUA antes que elas ocorressem. Porém a eficácia dessa vigilância foi questionada após os vazamentos. Segundo Landau (2013, p.59)

> Nas audiências de 18 de junho, o Diretor Geral da NSA, Alexander disse que a vigilância americana ajudou a prevenir “potenciais eventos terroristas mais de 50 vezes desde 11/09.” (Isto foi posteriormente alterado para 54, dos quais 42 eram conspirações terroristas, e 12 eram “apoio material” aos terroristas; 13 deles envolviam os EUA[89]

Inicialmente esses números podem parecer elevados, porém uma análise mais detalhada mostra que muitos desses incidentes não representavam real risco ou foram descartados com base na falta de evidências (Landau, 2013). Assim, os esforços de legitimação dessa quebra de regras não foram bem recebidos, de modo

---

[88] A DIA está liderando uma Força-Tarefa de Revisão de Informações para examinar danos graves causado às ações do Departamento de Defesa e à segurança nacional dos EUA como resultado de as divulgações não autorizadas da NSA. Uma ameaça emergente que diz respeito ao departamento envolve o potencial de entidades de inteligência estrangeiras comprometerem cadeias de abastecimento críticas ou componentes-chave corrompidos destinados a combates vitais sistemas. Além disso, alguns grupos terroristas transnacionais desenvolveram capacidades eficazes de inteligência e contra-inteligência - vimos isso se manifestar no Iraque e no Afeganistão, e grupos terroristas estão agora a utilizar e a partilhar o conhecimento e a experiência que adquiriram nesses conflitos. Tradução nossa e grifo nossos.

[89] At hearings on 18 June, NSA Director General Alexander said that American surveillance had helped prevent “potential terrorist events over 50 times since 9/11.”33 (This was later amended to 54, of which 42 were terrorist plots, and 12 were “material support” to terrorists; 13 of these involved the US. Tradução nossa.

que a vigilância da NSA exposta por Snowden foi considerada ilegal pela suprema corte americana em 2020[90].

Obama também citou esses acontecimentos em discursos oficiais visto a centralidade que os incidentes tomaram dentro da política estadunidense quando foram revelados. Em 2016, numa entrevista no festival South by Southwest, o presidente foi perguntado sobre o debate entre privacidade e segurança presente na área de tecnologia e em sua resposta comentou sobre o caso Snowden:

> I will say, by the way, that -- and I don't want to go too far afield -- but the Snowden issue **vastly overstated the dangers to U.S. citizens in terms of spying**, because the fact of the matter is, is that actually **our intelligence agencies are pretty scrupulous about U.S. persons**, people on U.S.soil.[91]

O que vemos na fala de Obama são duas estratégias para se minimizar a revelação de que os EUA estavam espionando seus próprios cidadãos sem ordens judiciais. Primeiramente, ele afirma que o perigo que os cidadãos correm por espionagem foi exagerado, de modo que o cidadão comum não precisaria se preocupar com a espionagem feita pelo governo. Após minimizar esses perigos, Obama reafirma um comprometimento das agências com os dados de cidadãos americanos e pessoas em solo americano.

Em janeiro de 2015, Obama voltou a tratar do tema quando em uma coletiva de imprensa ao lado do então primeiro ministro britânico David Cameron:

> And the biggest damage that was done as a consequence of the Snowden disclosures was, I think, in some cases, a complete undermining of trust. Some would say that was justified. **I would argue that although there are some legitimate concerns there, overall,the United States government and, from what I've seen, the British government, have operated in a scrupulous and lawful way to try to balance these security and privacy concerns.** And we can do better, and that's what we're doing.

---

[90]Disponível em <https://www.theguardian.com/us-news/2020/sep/03/edward-snowden-nsa-surveillance-guardian-court-rules>. Acesso em 16 de novembro de 2023.

[91] A propósito, direi que - e não quero ir muito longe - mas a questão de Snowden exagerou enormemente os perigos para os cidadãos dos EUA em termos de espionagem, porque a verdade é que, na verdade, a nossa inteligência as agências são bastante escrupulosas em relação às pessoas dos EUA, às pessoas em solo americano. Tradução e grifo nossos.

Aqui vemos que Obama adota outra estratégia para lidar com o escândalo. Primeiramente ele se refere à quebra de confiança entre o governo e a população e demonstra que entende aqueles que se sentiram traídos. Imediatamente após isso, ele põe que apesar dessas preocupações serem legítimas, o governo estadunidense age dentro da lei e com cuidado para tentar balancear o debate entre privacidade e segurança. Além disso, ele também coloca o governo britânico em conjunto com o norte-americano, de modo a se fazer entender que ambos os governos têm atuado de maneira correta, mesmo com as ressalvas que possam ser levantadas sobre essa atuação.

Já em 2014 na Análise sobre Inteligência de Sinais, Obama traz o motivo pelo qual é necessário que os EUA tenham as ferramentas que levaram à essa violação de privacidade:

> First, everyone who has looked at these problems, including skeptics of existing programs,recognizes **that we have real enemies and threats, and that intelligence serves a vital role in confronting them**. We cannot prevent terrorist attacks or cyber threats without some capability to penetrate digital communications -- **whether it's to unravel a terrorist plot; to intercept malware that targets a stock exchange; to make sure air traffic control systems are not compromised; or to ensure that hackers do not empty your bank accounts.** We are expected to protect the American people; that requires us to have capabilities in this field.[92]

O argumento utilizado aqui é o de que mesmo os mais céticos em relação aos programas de vigilância concordam que eles são uma necessidade visto os inimigos que o país enfrenta. Depois, ele dá exemplos de ameaças que tornam necessário que o governo tenha a capacidade de forçar o acesso à comunicações digitais. Entre as ameaças citadas temos ataques terroristas, que como citado anteriormente, tem uma forte presença dentro do imaginário estadunidense. Além disso, vemos que aqui ele resgata novamente os objetos de referência delimitados

[92] Em primeiro lugar, todos os que analisaram estes problemas, incluindo os cépticos em relação aos programas existentes, reconhecem que temos inimigos e ameaças reais e que a inteligência desempenha um papel vital no confronto com eles. Não podemos prevenir ataques terroristas ou ameaças cibernéticas sem alguma capacidade de penetrar nas comunicações digitais – seja para desvendar uma conspiração terrorista; interceptar malware direcionado a uma bolsa de valores; garantir que os sistemas de controle de tráfego aéreo não sejam comprometidos; ou para garantir que os hackers não esvaziem suas contas bancárias. Espera-se que protejamos o povo americano; isso exige que tenhamos capacidades neste campo. Tradução e grifo nossos.

previamente: a economia (“the stock exchange” e “your bank accounts”) e os sistemas de infraestrutura crítica (“air traffic control systems”).

Vemos então que ocorreu sim uma tentativa de legitimação da possibilidade da quebra de regras relacionadas à cibersegurança, com foco nos sistema de vigilância massiva promovidos pela NSA. Outras estratégias discursivas utilizadas foram a minimização da questão, a reafirmação do compromisso dos agentes com a segurança dos dados dos estadunidenses e a exemplificação das ameaças que fazem essa vigilância necessária. Porém essa legitimação foi feita *à posteriori*, quando o governo americano se viu na necessidade justificar o porquê do avançado sistema de coleta de dados feito sem autorização judicial.

Considerações finais

O presente trabalho visou buscar se dentro dos discursos de Barack Obama como 44º presidente dos EUA e dos chefes das agências de inteligência NSA e DIA houveram movimentos para a securitização da cibersegurança. Inicialmente,se faz necessário um retorno à teoria de securitização desenvolvida por Buzan, Waever e Wilde (1998). Os conceitos elaborados pela Escola de Copenhague foram expandidos nos anos seguintes, trazendo maior robustez de argumentos e proporcionando um novo olhar sobre como a segurança acaba por ser não uma característica inerente a certos temas ou setores. O que podemos observar através dessa perspectiva é que a construção de ameaças e a recolocação de temas dentro do espectro da política de segurança são movimentos da esfera discursiva. Sendo assim, atos de fala relacionados a um determinado tema podem colocá-lo dentro da esfera da política de exceção quando os mesmos forem aceitos e legitimados pela audiência. Desse modo, a análise de discurso se mostrou o método mais adequado para o presente trabalho. Especialmente o método proposto por Lene Hansen (2006), onde temos uma atenção considerável dada ao papel social do enunciador, além de sua formação ideológica,entre outros aspectos.

Após esse retorno aos conceitos de securitização, voltamos ao ano de 2008, quando Barack Hussein Obama foi eleito para o cargo máximo do executivo estadunidense, o primeiro negro a ocupar o cargo. Foi um período conturbado dentro do país que ainda se via no centro da Guerra ao Terror declarada por George W Bush após o atentado contra as Torres Gêmeas em 11 de setembro de 2001. As invasões do Afeganistão e do Iraque colocaram os americanos em situações complexas no Oriente Médio e com o mundo árabe. A crise imobiliária de 2008 abalou as estruturas do sistema bancário e financeiro dos EUA, afetando os mercados globais e afundando o país em uma grave recessão. Nesse cenário de profundas mudanças e insegurança, Obama foi eleito pelo Partido Democrata sob o slogan de “Yes, we can”, tentando trazer uma mudança sentida como necessária pela maioria da população.

Durante os 8 anos da gestão Obama, apesar de um redirecionamento na política externa, muito do legado de Bush e da Guerra ao terror foi continuado, como as guerras no Oriente Médio e a prisão de Guantánamo. Porém, casos relacionados

à cibersegurança tomaram momentaneamente o centro das discussões durante a gestão. Analisamos como os casos do malware Stuxnet e dos vazamentos de informações feitos por Chelsea Manning e Edward Snowden se tornaram pontos de discussão dentro da política estadunidense. O caso Snowden em particular teve um impacto internacional visto que demonstrou como os EUA espionaram não só em seus próprios cidadãos mas também em líderes e chefes de Estado.

Após entendermos o contexto em que esses eventos e discursos estavam inseridos, analisamos os discursos para verificar a presença dos elementos identificados por Buzan, Waever e Wilde (1998) como necessários para uma tentativa de securitização: ameaça existencial, situação de emergência e possibilidade da quebra de regras. Inicialmente vemos fortes elementos relacionando a questão da cibersegurança como uma ameaça existencial. Além da presença dos termos selecionados, temos a identificação de inimigos já presentes dentro do imaginário político estadunidense, comparações com ataques de Pearl Harbor e do World Trade Center, além da identificação de que os alvos seriam sistemas que colocariam em risco a vida da população. Tanto os discursos do presidente quanto dos diretores das agências não hesitaram em afirmar que a cibersegurança representava uma ameaça real aos EUA.

Porém, ao buscarmos os elementos de situação de emergência e possibilidade da quebra de regras, não foram encontradas evidências de uma recorrente tentativa de convencimento da população, como havia ocorrido em relação à ameaça existencial. A presença dos termos relacionados à situação de emergência nos discursos das agências não foi expressiva e nos discursos presidenciais ela não se mostrou relacionada à questões de cibersegurança. Um *outlier* foi o caso da Audiência da Câmara de 2014 sobre Ameaças de Cibersegurança. Nessa audiência encontramos tanto nas falas do Almirante Michael Rodgers quanto de congressistas falas que traziam uma maior sensação de urgência relacionada à temática da cibersegurança. Porém fora dessa audiência esse padrão não se repetiu. Em relação à possibilidade de quebra de regras, o que observamos são atos de fala das agências e de Obama *a posteriori* tentando justificar a necessidade de uma quebra de regra já ocorrida ou diminuir sua gravidade. Os argumentos utilizados foram a prevenção de ataques terroristas, ou no caso de Obama, a minimização do impacto dessas violações de direitos na

população e a reafirmação da cautela dos funcionários das agências com os dados dos cidadãos.

Feita a análise dos discursos selecionados e das estratégias utilizadas nos mesmos, vimos que houve um foco consideravelmente maior na caracterização da cibersegurança como ameaça existencial. Houve não só uma maior frequência de discursos retratando como os EUA estariam sob o perigo de serem atacados por meios cibernéticos, mas também o uso de diferentes estratégias argumentativas que reforçam essa ideia para a população. Essa frequência e argumentação não se repetiu quando analisamos os mesmos discursos em busca de referências aos outros dois elementos do processo de securitização. Dessa forma, podemos concluir que nos discursos analisados não houve por completo uma tentativa de Obama e dos diretores das agências de se realocar a discussão sobre cibersegurança para dentro da esfera da política de segurança.

Porém aqui se cabe citar uma das críticas feitas à Escola de Copenhague por membros da Escola Galesa de Estudos de Segurança. Ao analisarmos apenas os discursos como objeto de estudo para delimitar se houve ou não a securitização de um determinado tema, podemos não dar a devida atenção aos desenvolvimentos concretos que ocorrem sobre o tema fora do campo comunicativo, dificultando sua aplicação em problemas práticos (Rafeeq APUD Doe, 2018). Temos também que a Escola de Copenhague mantém um foco estadocêntrico forte, colocando o mesmo como o ator principal dentro do debate sobre segurança, deixando de lado questões não ligadas à ele. Dessa forma, uma análise das políticas concretas tomadas pela administração Obama referentes à cibersegurança pode levar a outra conclusão, visto que o intuito deste trabalho foi analisar apenas os discursos oficiais.

Referências

ALEXANDER. Keith. **Center for Strategic and International Studies (CSIS) CSIS Cybersecurity Policy Debate Series: U.S.Cybersecurity Policy and the Role ofU.S. CYBERCOM.** 2010. Disponível em <https://www.nsa.gov/DesktopModules/ArticleCS/Print.aspx?PortalId=75&ModuleId=13096&Article=1620145>. Acesso em 10 de junho de 2024.

BALZACQ, Thierry. **The Three Faces of Securitization: Political Agency, Audience and Context.** European Journal of International Relations Vol. 11(2): 171–201. 2005. [DOI: 10.1177/1354066105052960]

BALZACQ, Thierry; LÉONARD, Sarah; RUZICKA, Jan. **Securitization' revisited: theory and cases.** International Relations 2016, Vol. 30(4) 494–531. DOI: 10.1177/0047117815596590

BAYSAL, Basar. **20 Years of Securitization: Strengths, Limitations and A New Dual Framework.** Uluslararası İlişkiler Dergisi 17, no. 67 (September 2020): 3-20. https://doi.org/10.33458/uidergisi.777338.

BEBLER, Anton. **Crimea and the Russian-Ukrainian Conflict.** Romanian Journal of European Affairs 15(1):35-54. 2015

BEBLER, Anton. **Crimea and the Ukrainian-Russian conflict.** In: BEBLER, Anton. **"Frozen conflicts" in Europe**. Verlag Barbara Budrich. 2015

BRENNAN, John *et al*. **Transcript: National Security Summit INSA/AFCEA Intelligence Community Panel.** 2014. Disponível em <https://www.dia.mil/DesktopModules/ArticleCS/Print.aspx?PortalId=110&ModuleId=29499&Article=567086>. Acesso em 10 de junho de 2024.

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

COLLINS, Alan (org.). **Contemporary Security Studies.** Oxford: Oxford University Press, 2013.

COLVIN, Naomi. **Whistle-Blowing as a Form of Digital Resistance: State Crimes and Crimes Against the State.** State Crime Journal , Vol. 7, No. 1, State Crime and Digital Resistance (Primavera 2018), pp. 24-45. Pluto Journals.

CORVAJA, Alessandro. **OBAMA'S FOREIGN POLICY LEGACY RETREAT OR REPOSITIONING?**. Security Policy and Crisis Management. Konrad Adenauer Stiftung, 2015

DE, Rajesh. **Remarks of Rajesh De, General Counsel, National Security Agency Georgetown Law School.** 2013. Disponível em <https://www.nsa.gov/DesktopModules/ArticleCS/Print.aspx?PortalId=75&ModuleId=13096&Article=1620139>. Acesso em 10 de junho de 2024.

DEEKS, Ashley. **The Obama Administration, International Law, and Executive Minimalism.** The American Journal of International Law Vol. 110, No. 4 (October 2016) ,pp. 646-662. Cambridge University Press.

FLYNN, Michael T. **2013 Annual Threat Assessment.** 2013. Disponível em <https://www.dia.mil/DesktopModules/ArticleCS/Print.aspx?PortalId=110&ModuleId=29499&Article=567076>. Acesso em 10 de junho de 2024.

FLYNN, Michael T. **2014 Annual Threat Assessment.** 2013. Disponível em <https://www.dia.mil/DesktopModules/ArticleCS/Print.aspx?PortalId=110&ModuleId=29499&Article=567085>. Acesso em 10 de junho de 2024.

FLYNN, Michael T. **2015 Annual Threat Assessment.** 2013. Disponível em <https://www.dia.mil/DesktopModules/ArticleCS/Print.aspx?PortalId=110&ModuleId=29499&Article=567087>. Acesso em 10 de junho de 2024.

FLYNN, Michael. **DIA Director Flynn: Unauthorized Disclosures Have "Caused Grave Damage to Our National Security".** 2014. Disponível em <https://www.dia.mil/DesktopModules/ArticleCS/Print.aspx?PortalId=110&ModuleId=29499&Article=567078>. Acesso em 10 de junho de 2024.

FLYNN, Michael. **Lt. Gen. Flynn 4th Annual INSA Achievement Awards -- As Prepared for Delivery.** 2013. Disponível em <https://www.dia.mil/DesktopModules/ArticleCS/Print.aspx?PortalId=110&ModuleId=29499&Article=567073>. Acesso em 10 de junho de 2024.

FLYNN. Michael T. **Lt. Gen. Flynn INSA IC Summit Remarks.** 2013. Disponível em <https://www.dia.mil/DesktopModules/ArticleCS/Print.aspx?PortalId=110&ModuleId=29499&Article=567074>. Acesso em 10 de junho de 2024.

FORD, Pearl K; JOHNSON, Tekla A; MAXWELL, Angie. **"Yes We Can" or " Yes We Did"?: Prospective and Retrospective Change in the Obama Presidency.** Journal of Black Studies , Janeiro 2010, Vol. 40, No. 3, SPECIAL ISSUE: Barack Obama's Improbable Election and the Question of Race and Racism in Contemporary America (JANUARY 2010), pp. 462-483

GLASER, John; THRALL, Trevor. **Obama's Foreign Policy Legacy and the Myth of Retrenchment.** Cato Institute. 2017.

GRANT, Thomas D. **Annexation of Crimea.** The American Journal of International Law , Vol. 109, No. 1 (Janeiro 2015), pp. 68-95. Cambridge University Press.

HAAR, Roberta. **Great expectations or great disappointments?: Reflections on Obama’s foreign policy.** Atlantisch Perspectief, Vol. 40, No. 2 (2016), pp. 3-8 (6 pages).

HANSEN, Lene. **Reconstructing desecuritisation: the normative-political in the Copenhagen School and directions for how to apply it.** Londres. Review of International Studies (2012), 38, 525–546. doi:10.1017/S0260210511000581

HANSEN, Lene. **Security as practice: discourse analysis and the Bosnian war.** Londres: Routledge, 2006.

HILLYGUS, D.Sunshine. **Understanding the 2008 Presidential Election: Introduction.** The Public Opinion Quarterly, vol. 73, no. 5, 2009, pp. 841–44. Oxford University Press. Oxford.

INGLIS. John C. **Remarks by Mr. John C. Inglis, DeputyDirector, National Security Agency, atthe GEOINT Symposium 2010.** 2010. Disponível em <https://www.nsa.gov/DesktopModules/ArticleCS/Print.aspx?PortalId=75&ModuleId=13096&Article=1620141>. Acesso em 10 de junho de 2024.

JORDAN, Tim. **Information Politics: Liberation and Exploitation in the Digital Society.** Pluto Press. 2015

KOLODZIEJ, Edward. **Security and International Relations.** Londres, Cambridge University Press, 2005.

LANDAU, Susan. **Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations.** IEEE Security Privacy 11, no. 4 (Julho 2013): 54–63.
MANNING, Chelsea. **README.txt: a memoir.** 1 edição. Nova Iorque. Farrar, Straus and Giroux. 2022.

MCKAY, Shawn; PORCHE, Isaac R; Sollinger, Jerry M. **A Cyberworm that Knows No Boundaries. 1 edição** Rand Corporation. 2011.

MUHAMMAD, Ali; RIYANTO. Sugent. **International Security Studies: Origins, Development and Contending Approaches.** Austral: Brazilian Journal of Strategy & International Relations e-ISSN 2238-6912 | v.10, n.20, Jul./Dec. 2021 | p.230-249

OBAMA, Barack. **Keynote speech at the Democrat National Conference 2004**. Disponível em: <http://americanradioworks.publicradio.org/features/blackspeech/bobama.html>. Acesso em 21 de agosto de 2023.

OBAMA, Barack. **Osama Bin Laden Dead.** Disponível em <https://obamawhitehouse.archives.gov/blog/2011/05/02/osama-bin-laden-dead>. Acesso em 22 de agosto de 2023

OBAMA, Barack. **Remarks by the President at National Governors Association Reception.** 2016. Disponível em <https://obamawhitehouse.archives.gov/the-press-office/2016/02/21/remarks-president-national-governors-association-dinner>. Acesso em 10 de junho de 2024.

OBAMA, Barack. **Remarks by the President at PBS NewsHour Town Hall Discussion with Gwen Ifill for Elkhart, IN Residents.** 2016. Disponível em <https://obamawhitehouse.archives.gov/the-press-office/2016/06/02/remarks-president-pbs-newshour-town-hall-discussion-gwen-ifill-elkhart>. Acesso em 10 de junho de 2024.

OBAMA, Barack. **Remarks by the President at South By Southwest Interactive.** 2016. Disponível em <https://obamawhitehouse.archives.gov/the-press-office/2016/03/14/remarks-president-south-southwest-interactive>. Acesso em 10 de junho de 2024.

OBAMA, Barack. **Remarks by the President at the Cybersecurity and Consumer Protection Summit.** 2015. Disponível em <https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit>. Acesso em 10 de junho de 2024.

OBAMA, Barack. **Remarks by the President on Review ofSignals Intelligence.** 2014. Disponível em <https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence>. Acesso em 10 de junho de 2024.

OBAMA, Barack. **Remarks by the President on the Situation in Japan.** 2011. Disponível em <https://obamawhitehouse.archives.gov/the-press-office/2011/03/17/remarks-president-situation-japan>. Acesso em 10 de junho de 2011.

OBAMA, Barack; CAMERON, David. **Remarks by President Obama and Prime Minister Cameron of the United Kingdom in Joint Press Conference.** 2015. Disponível em <https://obamawhitehouse.archives.gov/the-press-office/2015/01/16/remarks-president-obama-and-prime-minister-cameron-united-kingdom-joint->. Acesso em 10 de junho de 2024.

OBAMA, Barack; GEUN-HYE, Park; ABE, Shinzo. **Remarks by President Obama, President Park Geun-Hye of the Republic of Korea, and Prime Minister Shinzo Abe of Japan After Trilateral Meeting.** 2016. Disponível em <https://obamawhitehouse.archives.gov/the-press-office/2016/03/31/remarks-president-obama-president-park-geun-hye-republic-korea-and-prime>. Acesso em 10 de junho de 2024.

OBAMA,Barack. **Remarks of President Barack Obama – State of the Union Address As Delivered.** 2016. Disponível em <https://obamawhitehouse.archives.gov/the-press-office/2016/01/12/remarks-president-barack-obama-%E2%80%93-prepared-delivery-state-union-address>. Acesso em 10 de junho de 2016.

PLAW, Avery; FLICKER, Matthew; WILLIAMS, Brian. **Practice Makes Perfect?: The Changing Civilian Toll of CIA Drone Strikes in Pakistan.** Perspectives on Terrorism, Vol. 5, No. 5/6 (December 2011), pp. 51-69

RAFEEQ, Harem. **Copenhagen school versus Welsh School of security studies.** 2018

REINHART, Vincent. **A Year of Living Dangerously: The Management of the Financial Crisis in 2008.** Journal of Economic Perspectives**,** 25 (1): 71-90. DOI: 10.1257/jep.25.1.71

ROGERS, Michael. **CyberMaryland 2014 Conference.** 2014. Disponível em <https://www.nsa.gov/DesktopModules/ArticleCS/Print.aspx?PortalId=75&ModuleId=13096&Article=1619405>. Acesso em 10 de junho de 2024.

ROGERS, Michael. **Fordham University's Fifth International Conference on CyberSecurity (ICCS 2015).** 2015. Disponível em <https://www.nsa.gov/DesktopModules/ArticleCS/Print.aspx?PortalId=75&ModuleId=13096&Article=1619308>.Acesso em 10 de junho de 2024.

ROGERS, Michael. **Hearing of the House (Select)Intelligence Committee Subject:"Cybersecurity Threats: The WayForward".** 2014. Disponível em <https://www.nsa.gov/DesktopModules/ArticleCS/Print.aspx?PortalId=75&ModuleId=13096&Article=1620360>. Acesso em 10 de junho de 2024.

S. Korean chaebols comprise 84% of GDP but only 10% of jobs. Disponível em <https://english.hani.co.kr/arti/english_edition/e_business/949236.html>. Acesso em 19/04/2023

SNOWDEN, Edward. **Permanent Record.** Macmillan. 2019

TAURECK, Rita. **Securitization theory and securitization studies.** 2006. http://dx.doi.org/10.1057/palgrave.jird.1800072

Thematic Brief: US Cybersecurity Efforts. The Third Way. 2019. Disponível em <https://www.thirdway.org/primer/thematic-brief-us-cybersecurity-efforts>. Acesso em 10 de junho de 2024.
theory and cases. International Relations 2016, Vol. 30(4) 494–531. DOI: 10.1177/0047117815596590

TONNESSEN, Truls. **The Islamic State after the Caliphate.** Perspectives on Terrorism , Fevereiro 2019, Vol. 13, No. 1 (February 2019), pp. 2-11. Terrorism Research Initiative

ÜNVER, H. Akin. **Politics of Digital Surveillance, National Security and Privacy.** 2018. Centre for Economics and Foreign Policy Studies

VAN CLEAVE, Michelle. **MYTH, PARADOX & THE OBLIGATIONS OF LEADERSHIP: Edward Snowden, Bradley Manning and the Next Leak.** 2013. Center for Security Policy.

ZETTER, Kim. **Countdown to Day Zero: Stuxnete and the launch of the world's first digital weapon.** 1 edição. Nova Iorque. Crown Publishing Group. 2014.