UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS V - MINISTRO ALCIDES CARNEIRO
CENTRO DE CIÊNCIAS BIOLÓGICAS E SOCIAIS APLICADAS
PROGRAMA DE PÓS-GRADUAÇÃO EM RELAÇÕES INTERNACIONAIS

PEDRO HENRIQUE OLIVEIRA FRAZÃO

UM *BIG BROTHER* GLOBAL?
OS PROGRAMAS DE VIGILÂNCIA DA NSA À LUZ DA SECURITIZAÇÃO DOS ESPAÇOS SOCIOTECNOLÓGICOS

JOÃO PESSOA - PB
2016

PEDRO HENRIQUE OLIVEIRA FRAZÃO

UM *BIG BROTHER* GLOBAL?
OS PROGRAMAS DE VIGILÂNCIA DA NSA À LUZ DA SECURITIZAÇÃO DOS ESPAÇOS SOCIOTECNOLÓGICOS

Dissertação apresentada ao Programa de Pós-Graduação em Relações Internacionais da Universidade Estadual da Paraíba (PPGRI-UEPB) como requisito para a obtenção do título de Mestre em Relações Internacionais.

Orientadora: Prof.ª Dr.ª Silvia Garcia Nogueira

JOÃO PESSOA – PB
2016

F848b Frazão, Pedro Henrique Oliveira
Um big brother global? os programas de vigilância da NSA à luz da securitização dos espaços sociotecnológicos [manuscrito] / Pedro Henrique Oliveira Frazão. - 2016.
130 p. : il. color.

Digitado.
Dissertação (Programa de Pós-Graduação em Relações Internacionais) - Universidade Estadual da Paraíba, Centro de Ciências Biológicas e Sociais Aplicadas, 2016.
"Orientação: Profa. Dra. Silvia Garcia Nogueira, Departamento de Relações Internacionais".

1. Cibersegurança. 2. Securitização. 3. Vigilância cibernética. 4. Panóptico. 5. NSA. I. Título.

21. ed. CDD 327.12

PEDRO HENRIQUE OLIVEIRA FRAZÃO

UM *BIG BROTHER* GLOBAL?
OS PROGRAMAS DE VIGILÂNCIA DA NSA À LUZ DA SECURITIZAÇÃO DOS ESPAÇOS SOCIOTECNOLÓGICOS

Dissertação apresentada ao Programa de Pós-Graduação em Relações Internacionais da Universidade Estadual da Paraíba (PPGRI-UEPB) como requisito para a obtenção do título de Mestre em Relações Internacionais.

Aprovada em: 19/05/2016

Prof.ª Dr.ª Silvia Garcia Nogueira
Orientadora (UEPB)

Prof. Dr. Paulo Roberto Loyolla Kuhlmann
Examinador interno (UEPB)

Prof.ª Dr.ª Ana Paula Maielo Silva
Examinadora externa (UEPB)

DEDICATÓRIA

Dedico este trabalho aos meus pais, Edna e José, pelo amor incondicional e pelo apoio sem o qual nada disso seria possível.

AGRADECIMENTOS

À Universidade Estadual da Paraíba, pela estrutura de ensino que propiciou minha formação.

À professora Silvia Nogueira, pela confiança, pelos ensinamentos e pela orientação que possibilitaram a conclusão deste trabalho.

À banca examinadora, composta pelos professores Ana Paula Maielo e Paulo Kuhlmann, e à banca de qualificação, formada pelos professores Augusto Teixeira e Paulo Kuhlmann, pelas observações, sugestões e críticas.

Aos professores da graduação e da pós-graduação em Relações Internacionais da UEPB, pelo aprendizado, dedicação e paciência, em especial a Alexandre Leite, Anahi de Castro, Augusto Teixeira, Cristina Pacheco, Elias David, Eliete Gurjão, Gabriela Gonçalves, Henrique Altemani, Paulo Kuhlmann e Silvia Nogueira.

Aos funcionários da UEPB pelo trabalho exemplar e pelo carinho com que nos tratam.

À Coordenação de Aperfeiçoamento Pessoal de Nível Superior (CAPES) pelo auxílio financeiro à pesquisa.

Aos meus pais, Edna Oliveira Frazão e José Ailton Frazão, pelo carinho, dedicação e compreensão em todas as horas.

Ao meu irmão, George Oliveira Frazão, pela amizade fraterna.

Aos meus avós maternos, Jandira Melo de Oliveira e Francisco Chagas de Oliveira (*in memoriam*), e paternos, Neuza Fernandes Frazão (*in memoriam*) e Rosil Moraes Frazão (*in memoriam*), pelos ensinamentos advindos da experiência.

Aos meus familiares, em especial aos tios Edson Melo e Ingrid Saltão pelo incentivo e por cederem diversas vezes um espaço tranquilo para escrever este trabalho.

À família que a vida me proporcionou, meus amigos queridos Andrei de Ferrer, Anna Beatriz, Arthur Murta, Carina Rodrigues, Caroline Cevada, Daniel Colom, Elze Rodrigues, Inara Rosas, Luína Marinho, Luísa Nevett, Manoela Lemos, Marcela Dimenstein, Maria Olívia, Natália Nunes e Vitório Pimentel. Em especial, agradeço a Alan Manga por todo o companheirismo, força e ajuda diários.

Aos companheiros de biblioteca, Anna Beatriz e Diego Aranha. Essa trilha teria sido bem mais difícil sem vocês!

Aos meus colegas de sala. Conseguimos!!

A Edward Snowden, pela coragem que proporcionou ao mundo um grito de liberdade.

“Quanto mais a sociedade se distancia da verdade, mais ela odeia aqueles que a revelam”

(George Orwell)

RESUMO

O crescente uso do ciberespaço nas Relações Internacionais vem propiciando um novo cenário para a política mundial. A evolução dos meios digitais proporcionou um fluxo de dados nunca antes visto na história da humanidade, o que acabou ampliando o papel da informação enquanto moeda de troca nas relações de poder do cenário internacional atual. Uma das transformações observadas a partir deste processo foi o fortalecimento da vigilância – que ganha novas ferramentas no ambiente cibernético – enquanto mecanismo de monitoramento, manutenção da ordem, controle e aquisição de informações que tornem os atores internacionais relevantes nas novas relações de poder cibernéticas. Sendo assim, a presente dissertação analisa este fenômeno a partir de duas linhas principais que se complementam: a evolução da vigilância enquanto dimensão-chave da (ciber)segurança, através de uma abordagem panóptica e pós-panóptica e como estas perspectivas influenciam nos fenômenos atuais de vigilância cibernética. Para tanto, apresentam-se os estudos de Foucault acerca da sociedade disciplinar e os seus desdobramentos que deram lugar a uma sociedade de controle informacional, e as análises de Bauman sobre a modernidade líquida e como tais características podem influenciar a vigilância contemporânea. A segunda linha de análise, elaborada a partir dos dados levantados até então, aborda uma visão da vigilância cibernética enquanto ferramenta do processo de securitização do ciberespaço. Seguindo esta lógica, os estudos da Escola de Copenhague, baseados na teoria construtivista das Relações Internacionais, apontam um caminho propício para a compreensão do papel da vigilância cibernética dentro das questões de cibersegurança. Como exemplo de caso, examina-se como esse processo se deu dentro dos programas de vigilância global da NSA, revelados em meados de 2013 por Edward Snowden. A fim de alcançar tais objetivos, serão revisados autores clássicos dos estudos de vigilância e segurança, bem como novas abordagens; para a apresentação e análise do caso proposto, serão utilizados análises documentais, reportagens e discursos referentes às respostas internacionais em face das revelações dos programas da NSA.

PALAVRAS-CHAVE: Cibersegurança; Securitização; Vigilância cibernética; Panóptico; NSA

ABSTRACT

The increasing use of cyberspace in International Relations is providing a new scenario for world politics. The evolution of digital media has provided a data flow never before seen in human history, which eventually expanded the role of information as a bargaining chip in the power relations of the current international scenario. One of the changes observed from this process was the strengthening of surveillance – which gains new tools in the cyber environment – as a mechanism of monitoring, law enforcement, control and acquisition of information that makes international actors relevant in the new *cyberpower* relations. Thus, this dissertation analyzes this phenomenon from two main lines that complement each other: the evolution of surveillance as a key dimension of (cyber)security through a panoptic and post-panoptic approach and how these perspectives influence the current cyber surveillance phenomena. To do so, we present Foucault's studies of disciplinary society and its developments that have given rise to an information society of control, and Bauman's analysis on liquid modernity and how its characteristics can influence contemporary surveillance. The second line of analysis, drawn from the data collected so far, deals with a vision of cyber surveillance as a tool of cyberspace securitization process. Following this logic, studies of the Copenhagen School, based on the constructivist theory of International Relations, point out a favorable path to understanding the role of cyber surveillance within the cybersecurity issues. As an example case, we examine how this process took place within NSA programs of global surveillance revealed in mid-2013 by Edward Snowden. In order to achieve these objectives, classical authors of surveillance and security studies will be reviewed, as well as new approaches; for the presentation and analysis of the proposed case, documentary analysis, reports and speeches relating to international responses in the face of revelations of the NSA programs will be used.

KEYWORDS: Cybersecurity; Securitization; Cyber surveillance; Panopticon; NSA

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS

AOL	*America OnLine*
ASD	*Australia Signals Directorate*
AT&T	*American Telephone and Telegraph*
BND	*Bundesnachrichtendienst* (Alemanha)
CIA	*Central Intelligence Agency* (EUA)
CSEC	*Communications Security Establishment* (Canadá)
CSS	*Central Security Service* (EUA)
DDoS	*Distributed Denial-of-Service*
DGSE	*Direction Générale de la Sécurité Extérieure* (França)
DNI	*Digital Network Intelligence*
DNS	*Domain Name System*
EUA	Estados Unidos da América
GCHQ	*Government Communications Headquarters* (Reino Unido)
GCSB	*Government Communications Security Bureau* (Nova Zelândia)
GTE	*Global Telecoms Exploitation*
GVT	*Global Village Telecom*
IBM	*International Business Machines*
ICANN	*Internet Corporation for Assigned Names and Numbers*
IGF	*Internet Governance Forum*
ISP	*Internet Service Provider*
ITU	*International Telecommunications Union*
MTI	*Mastering The Internet*
NSA	*National Security Agency* (EUA)
ONU	Organização das Nações Unidas

SCS	*Special Collection Service* (EUA)
TIC	Tecnologia de Informação e Comunicação
VPN	*Virtual Private Network*
	World Wide Web

SUMÁRIO

INTRODUÇÃO

O crescente uso do ciberespaço nas relações entre os atores internacionais propicia um novo cenário para a política mundial, ao ter levado para esta nova arena diversos fenômenos políticos, econômicos e sociais, típicos do mundo tangível, tais como a vigilância. Este trabalho se propõe, portanto, a estudar seu impacto na segurança internacional, principalmente no que se refere à vigilância cibernética global. Como caso exemplar, utilizar-se-á os programas de ciberespionagem mundial da Agência de Segurança Nacional dos EUA (NSA, na sigla em inglês), trazidos à tona pelas denúncias apresentadas por Edward Snowden em meados de 2013.

Apesar de ser um caso típico da sociedade contemporânea, é histórico o caminho que esta vem tomando nas reconfigurações espaciais e temporais. Desde a formação das primeiras civilizações, passando pela criação dos grandes impérios, até a civilização moderna, as interações sociais partiram da convivência diária entre tribos à formação de uma aldeia global interconectada. Os últimos trinta anos, entretanto, foram cruciais para uma modificação profunda na forma como os seres humanos se relacionam devido principalmente ao surgimento de novas tecnologias que deixaram o tempo e o espaço cada vez mais relativos, impactando sobre diversas áreas da convivência humana.

Claro que muita coisa ocorreu entre uma pintura rupestre e a possibilidade de enviar mensagens instantâneas em redes capazes de organizar movimentos. Entretanto, vale salientar que não é intenção deste trabalho realizar um apanhado histórico da revolução tecnológica informacional, mas demonstrar, através da discussão acerca da vigilância cibernética global, a importância dessa nova ferramenta para as Relações Internacionais e para os estudos de Segurança Internacional.

A evolução da informática aliada ao surgimento da *internet* proporcionou uma crescente digitalização de documentos, imagens e materiais audiovisuais (MANOVICH, 2001) e uma aceleração na troca destes dados, propiciando, assim, um fluxo de informações nunca antes visto na história da humanidade. Isto tudo só é possível, claro, devido às características do ciberespaço, que fornecem as ferramentas necessárias para tal fenômeno.

O Estado, assim como a sociedade em geral, também sofreu profundas modificações com o advento destas tecnologias, criando novas possibilidades de ação e novos desafios. Como demonstra Leonardo Valente (2007), o ente estatal não perde sua finalidade nem seu poder na era da informação – não deixando de se basear no militar, no político e no econômico – antes,

ocorre um redimensionamento da busca pela influência no meio internacional, readaptando-se, assim, aos novos meios comunicacionais.

Tendo em vista as crescentes modificações que ampliaram o papel da informação enquanto moeda de poder em níveis nunca antes alcançados, torna-se cada vez mais nítida uma corrida cibernética entre os atores internacionais em busca não apenas de informações e conhecimentos que os tornem relevantes no meio internacional mas, também, de capacidades que proporcionem vantagens nas relações de poder, tais como o conhecimento técnico e a construção de uma geografia do fluxo de informações que seja favorável a este fim, o que traz consequências às relações entre os atores internacionais.

Isso ocorre devido à percepção de que não há como escapar dos novos espaços sociotecnológicos, uma vez que os processos sociais de globalização, apoiados por ideologias neoliberais, acabam guiando os atores nesse caminho. As consequências, entretanto, são distintas e, no que tange à vigilância cibernética global, as percepções são variadas. Nota-se, todavia, que os fenômenos ligados à ciberespionagem no nível internacional são cada vez mais frequentes dentro de uma lógica de militarização do ciberespaço. Eles envolvem, além da vigilância, outros tipos de conflitos cibernéticos, tais como os crimes comuns, a sabotagem, o terrorismo e a guerra cibernética, gerando o próprio conceito de cibersegurança, explorado neste trabalho.

A segurança sempre foi um tema de destaque no campo das Relações Internacionais, estando presente desde sua formação (RUDZIT, 2005). Inicialmente voltada para os estudos de guerra e paz, a evolução das análises de segurança, em conjunto com as mudanças sociais, vem propiciando o exame de novos objetos que fogem a esse padrão clássico. Logo, temas como a cibersegurança, e especificamente, nesse caso, a vigilância cibernética, acabam ganhando espaço dentro da área devido a novas abordagens que ampliam a visão da segurança internacional.

A perspectiva de securitização da Escola de Copenhague possibilita o entendimento do ciberespaço enquanto uma arena securitizada, ou seja, possuidora de ameaças socialmente aceitas por meio de um processo intersubjetivo. Sendo assim, enxerga-se nos espaços sociotecnológicos a existência de ameaças não apenas à sobrevivência dos atores estatais, em uma visão clássica das Relações Internacionais, mas a todos os agentes e indivíduos que ali estão presentes. Isso tudo através de atos de fala, ou discursos, de agentes securitizadores (Estados, grupos técnicos, indivíduos, entre outros) que estabelecem os sentimentos de ameaça.

A vigilância, como ferramenta das relações que envolvem um ciberespaço securitizado, entretanto, não é algo novo e típico da era da informação, como visto. Sua utilização para fins

de monitoramento, manutenção da ordem, espionagem e controle é antiga e autores como Foucault (2002), Deleuze (1992), Bauman e Lyon (2013) buscam compreender este fenômeno social. Todavia, o ciberespaço parece ter dotado a vigilância de força nunca antes observada, ampliando não apenas seu escopo de ação, mas também barateando os seus custos de aplicação. Portanto, torna-se fundamental um exame de como a vigilância vem sendo percebida ao longo do tempo e dos impactos que o mundo digital e as mudanças sociais advindas dele trouxeram a esta ferramenta.

É nesse ponto que os programas de vigilância da NSA se configuram, aqui, como caso exemplar dessas mudanças. Caracterizados pelo uso de ferramentas cibernéticas no monitoramento e na aquisição de informações de milhares de pessoas e instituições ao redor do mundo (incluindo desde cidadãos comuns a líderes mundiais e grandes empresas), este caso foi amplamente divulgado em meados de 2013, quando Edward Snowden, ex-funcionário da agência, revelou ao mundo sua existência através do vazamento de documentos internos, gerando uma percepção de ameaças à privacidade dos usuários.

Dentre os milhares de dados vazados pelo ex-agente, os programas *PRISM*, *Boundless Informant*, *X-Keyscore*, *Tempora*, *Muscular* e *Stateroom*, ganharam notoriedade por demonstrarem sistemas altamente desenvolvidos de captação de dados em diversos países e alianças internacionais na aplicação e manutenção dessa vigilância, através do grupo que ficou conhecido como *Five Eyes* (cinco olhos): EUA, Reino Unido, Canadá, Austrália e Nova Zelândia. A NSA e os EUA alegaram que tais programas seriam de extrema importância no combate ao terrorismo internacional.

As respostas internacionais aos vazamentos, entretanto, foram distintas, mas, em sua maioria, condenatórias. Na condição de agentes securitizadores, os principais alvos buscaram respostas do governo estadunidense, condenaram a vigilância cibernética global, demonstraram preocupação com a espionagem de nações aliadas e a descrença no uso dessas ferramentas para o único fim de combate ao terrorismo. Todavia, algumas contradições foram notadas nessas respostas, seja por receios de enfrentar um país do porte dos EUA ou pela possibilidade de alguns alvos possuírem programas semelhantes aos da NSA.

Tal perspectiva, de uma vigilância em nível global em que milhares (talvez milhões) de usuários estão sendo monitorados por agências de inteligência lideradas pela NSA, propiciou uma gama de análises acerca das consequências políticas, econômicas e sociais desse fenômeno. Dentre elas, destaca-se a analogia com o ficcional *Big Brother* de George Orwell, um governo totalitário em um futuro distópico apresentado na obra *1984*. Apesar das diferenças no que diz respeito principalmente ao regime político, a vigilância perpetrada pelo *Big Brother*

em pouco distingue-se do que se observa nos programas da NSA, nos quais a onipresença da vigilância e o controle do indivíduo saem das páginas do livro e encontram as manchetes de jornais e os artigos acadêmicos ao redor do mundo.

Senso assim, tais programas parecem apontar para um estudo atual acerca do impacto da vigilância cibernética global na sociedade e na segurança do meio internacional, em especial, na construção de ameaças intersubjetivas dentro dos espaços sociotecnológicos. Tal exame se faz necessário não apenas para uma melhor compreensão das suas consequências para as Relações Internacionais, mas também pela urgência que a ciência e a sociedade possuem em compreender os fatos do cotidiano.

Assistimos com mais frequência nos noticiários os casos em que informações foram roubadas, sistemas foram desativados, ataques a centros de dados foram realizados ou grandes manifestações foram organizadas rapidamente em redes sociais, seja por organizações de *hackers*, por Estados ou por indivíduos. Entretanto, as acusações da ciberespionagem estadunidense se mostram de grande relevância para o estudo por envolver diversos atores e por ampliar a vigilância a níveis nunca antes observados na humanidade.

As reconfigurações que os novos meios de comunicação e as suas consequências trazem para a área de estudo da segurança internacional – e também para outras áreas – não se encerram em si, mas são contínuas ao longo do tempo. Bruno Latour (2000) relembra que "estudamos a ciência em ação, e não a ciência ou a tecnologia pronta; para isso, ou chegamos antes que os fatos e máquinas se tenham transformado em caixas-pretas, ou acompanhamos as controvérsias que as reabrem". É nessa controvérsia recente, em que os agentes buscam se apoderar de dados e informações com a finalidade de manter sua relevância no meio internacional, que percebemos a relevância deste trabalho, tendo em vista que o fenômeno se encontra em um momento crucial de imersão, possibilitando uma compreensão mais complexa do tema.

Diante do explanado, cabe formular algumas questões centrais que dão estrutura ao trabalho proposto: 1) que modificações de fato o meio cibernético vem trazendo para o cenário internacional? 2) Quais as consequências disto para a segurança dos atores? 3) De que maneira a vigilância se apresenta como uma dimensão-chave desse processo e, com uma visão mais específica, como o caso da NSA auxilia na compreensão do fenômeno, ao formular discursos securitizadores que ampliam a sensação de ameaças tanto no ciberespaço quanto no meio internacional?

Para tanto, utilizar-se-á os estudos de Pierre Lévy e André Lemos (2010), que buscam compreender o funcionamento das novas mídias e do ciberespaço; Leonardo Valente (2007), David Rothkopf (1998), Nazli Choucri (2012) e Tim Jordan (2003), que analisam o impacto do

ciberespaço para as Relações Internacionais; Michel Foucault (2002), ao analisar os processos das relações de poder, da vigilância panóptica e da sociedade disciplinar; Deleuze (1992) e a sociedade de controle; Saco (2002) e Shapiro (1999), que ampliam estas abordagens para a sociedade informacional; Bauman e Lyon (2013), por levarem aspectos da sociedade contemporânea aos estudos da vigilância; Onuf (2002) e Wendt (1994), teóricos construtivistas das Relações Internacionais; Buzan, Waever e Wilde (1998), da Escola de Copenhague; Hansen e Nissenbaum (2009), que apresentam o ciberespaço como um setor analítico da securitização; Julian Assange (2013), criador do *WikiLeaks* (organização que divulga digitalmente documentos sigilosos de governos e outras instituições), que enfatiza em sua obra o processo de militarização e vigilância do ciberespaço através da apropriação desse novo mundo pelos agentes; e, por fim, Luke Harding (2014), autor que apresenta a história dos vazamentos dos programas de vigilância por Edward Snowden. Além desses autores, foram realizadas pesquisas em diversas redes de notícias, tais como *The Guardian*, *The Washington Post*, *New York Times*, *Globo*, *Le Monde*, *Der Spiegel*, entre outras, a fim de compreender a extensão atual do fenômeno analisado.

A coleta de dados ocorreu por meio de levantamento bibliográfico e documental, e de pesquisa na *internet* acerca da utilização do ciberespaço nas relações entre os atores internacionais e sua consequência para a segurança, e na vigilância cibernética, focando nos programas da NSA e nos discursos advindos do caso. Diante do levantamento de informações e das leituras realizadas, optou-se por um modelo de organização da dissertação composto por três capítulos, além da introdução e das considerações finais.

O primeiro capítulo do trabalho, intitulado "Ciberespaço: uma nova arena das Relações Internacionais", tem por intenção apresentar o que é o ciberespaço, seu funcionamento, seu uso e suas implicações para as Relações Internacionais para, em seguida tecer considerações sobre o que é a cibersegurança e suas variáveis, dentre elas a vigilância cibernética, foco de análise deste trabalho. Para tanto, serão levantados os principais conceitos que buscam conceber uma definição para este meio, sua evolução e seu impacto no mundo, como a sociedade vem fazendo uso desse espaço e como o Estado enxerga e se apropria dessa arena, culminando em diversas implicações para as Relações Internacionais e para a vigilância internacional.

O segundo capítulo, "O processo de securitização do ciberespaço: vigilância como dimensão-chave", busca apresentar a vigilância internacional enquanto um processo social histórico que possui efeitos importantes não apenas nas Relações Internacionais, mas em toda a sociedade e suas práticas, seja na área política, econômica, segurança ou nas relações pessoais cotidianas. Entretanto, a fim de delimitar o escopo destas visões que as ciências sociais nos

trazem e aprofundar os estudos nos efeitos que a vigilância promove na segurança internacional e seus fenômenos, a teoria de securitização da Escola de Copenhague é apresentada por fornecer meios para uma análise das ameaças que o ciberespaço pode proporcionar a esta área.

Já o terceiro capítulo, "O *Big Brother* global: os programas de vigilância da NSA e a securitização do ciberespaço", procura elaborar uma análise acerca dos programas de vigilância da NSA vazados pelo ex-funcionário desta agência, Edward Snowden, a partir das bases levantadas nos capítulos anteriores. Busca-se, dessa forma, compreender como uma vigilância a nível global vem sendo fomentada e securitizada no sistema internacional a partir de um ponto de vista distinto das análises de segurança do *mainstream* das Relações Internacionais, propiciando uma visão da sua construção social o que auxilia na ampliação do escopo de sua compreensão.

Por fim, serão apresentadas considerações finais da pesquisa, demonstrando como os resultados desse trabalho contribuem para os estudos no campo da vigilância e da segurança internacional que evoluem em conjunto com o desenvolvimento de novas tecnologias e, como consequência, dos usos sociais atribuídos a estas.

1. CIBERESPAÇO: UMA NOVA ARENA DAS RELAÇÕES INTERNACIONAIS

Este capítulo pretende apresentar o que é o ciberespaço, seu funcionamento, seus usos e suas implicações para as relações internacionais. Em seguida, tecerá considerações sobre o que é a cibersegurança e suas variáveis – dentre elas a vigilância cibernética, foco de análise deste trabalho. Com o intuito de alcançar tais objetivos, serão levantados os principais conceitos que buscam conceber uma definição para este meio, sua evolução e seu impacto no mundo, como a sociedade vem fazendo uso desse espaço e como o Estado enxerga e se apropria dessa arena[1], culminando em diversas implicações para as Relações Internacionais e para a vigilância internacional.

Vivemos hoje o que muitos autores chamam de revolução tecnológica informacional. O surgimento da informática e a criação da *internet* – em conjunto com o processo de globalização experimentado de forma intensa no final do último milênio – aparecem como alguns dos principais responsáveis por esta revolução. Tal mudança nas relações humanas possui implicações que vão além da rapidez do fluxo de informações, tendo um impacto direto no próprio funcionamento da sociedade e na forma como os atores se comportam em suas ações cotidianas, devido principalmente à formação de novos espaços de interação e, consequentemente, de organização social.

Nas Relações Internacionais não é diferente. As implicações do surgimento e da apropriação das ferramentas do ciberespaço pelos atores trazem consequências claras para a arena internacional. Além se auxiliar na geração de novas oportunidades provenientes do alto fluxo comunicacional que relativizou o tempo e o espaço, gerando possibilidades de um maior intercâmbio tecnológico, econômico e cultural, esse espaço também vem criando novos desafios ao tornar-se palco de disputas entre os agentes que materializam-se através de discursos e ações, tais como imposições por atores com maior relevância no jogo político, criação de sistemas de defesa de sua rede informacional, ataques digitais tendo alvos diversos e a vigilância cibernética, objeto deste trabalho que será aprofundado posteriormente.

Já é fato incontestável a presença constante desta virtualização das coisas, mesmo que o indivíduo não participe diretamente do processo, seja por vontade própria ou por exclusão. A troca de informações entre um avião e a torre de comando, o ato de sacar dinheiro em um banco, as teleconferências diplomáticas, as redes sociais, os *smartphones* cada vez mais conectados,

[1] Adota-se arena ou arena cibernética como termo análogo a ciberespaço no sentido em que este apresenta-se como um ambiente, um palco, no qual os atores inerentes executam suas ações.

entre outros diversos exemplos, são meios práticos de perceber como as relações sociais vêm se modificando pela presença maciça do ciberespaço, em especial após a criação da *internet*.

É importante ressaltar, entretanto, que não é só a tecnologia que vem moldando essas mudanças comportamentais na sociedade, nem os atores com maior relevância nas relações de poder que impõem de forma totalitária tais medidas. Também pesa nessa equação a forma como essas invenções estão sendo apropriadas pelos usuários e como a partir desse processo elas passam a evoluir. Bauman e Lyon (2013) buscam demonstrar que a discussão acerca da "culpabilidade" da tecnologia, no que tange as mudanças nas ações sociais, são impróprias para responder as questões urgentes que permeiam esta área na sociedade pós-moderna (ou modernidade líquida como chama Bauman):

> Os computadores não são os culpados, ao contrário do que sugerem alguns de seus críticos acostumados a "surfar", em vez de mergulhar e penetrar: a vertiginosa velocidade da brilhante carreira dos computadores deve-se ao fato de que eles oferecem a seus usuários uma oportunidade melhor de fazer o que sempre desejaram, mas não podiam, por fata de ferramentas adequadas. Mas também não são salvadores, como seus entusiastas, de joelhos, costumam afirmar com impaciência. Essa confusão tem raízes na forma como a condição existencial é manejada e empregada pelo tipo de sociedade que construímos enquanto éramos por ela construídos. E, para nos livrarmos dessa confusão (se é que isso é concebível), precisaríamos ir além da mudança de ferramentas – que, afinal, só nos ajudam a fazer o que de todo modo tentaríamos fazer, quer à maneira de uma fábrica caseira, quer utilizando a tecnologia de ponta que todos desejam. (BAUMAN & LYON, 2013, p. 52)

Levando tais considerações para as relações entre os atores internacionais, percebe-se que os atos perpetrados no mundo cibernético (estes aprofundados posteriormente) não são novidades absolutas, mas ganham força com a evolução na tecnologia comunicacional. A própria vigilância e outras técnicas de estratégia ofensiva/defensiva ganham uma nova roupagem na era da informação, mas não deixam de ter os velhos objetivos que podem ser úteis para a sobrevivência e o fortalecimento dos agentes, sejam eles angariar conhecimentos, proporcionar baixas, atacar um inimigo, defender-se, entre outros.

É necessário, entretanto, apresentar algumas das principais características deste meio para que se possa compreender como a revolução tecnológica vem proporcionando essas novas (e velhas) possibilidades de ações na sociedade e quais seus efeitos que acabam gerando um processo de securitização desse espaço devido a sentimentos de ameaças por parte dos atores que partem de discursos e ações perpetrados nessa nova arena social, política, militar e econômica.

1.1 Características do ciberespaço

Segundo André Lemos e Marcos Palácios (2001) um dos conceitos basilares para se compreender o que é o ciberespaço e como se dá seu funcionamento é o que os autores chamam de pervasividade:

> Algo é pervasivo quando se dissemina, difunde-se, infiltra-se por todas as dobras e frestas do tecido social. É assim a Tecnologia Informacional do final do milênio. A junção da Informática com as Telecomunicações, criando o que hoje denominamos Telemática, determina uma situação em que a influência tecnológica e seus impactos transformadores não ficam restritos a esta ou àquela sociedade. Tudo está sendo telematizado [...] (LEMOS; PALACIOS, 2001, p. 6)

A pervasividade acaba gerando novos espaços sociotecnológicos em que os indivíduos conectados à rede podem interagir uns com os outros, realizar transações bancárias, fazer compras, consumir produções artísticas, vigiar, cometer crimes, atacar algum alvo específico, entre outras possibilidades, sem que o espaço e o tempo sejam um empecilho. Dessa forma, cada vez mais a informação torna-se a base da sociedade globalizada, e a tecnologia é o meio pela qual essa informação é disseminada, construída e moldada atualmente. Apesar disso, utilizando novamente a ideia de Bauman e Lyon (2013) acerca da influência das TICs (Tecnologias de Informação e Comunicação), é importante ressaltar que a informação enquanto moeda de troca nas relações de poder sempre esteve presente na sociedade, mas tem sua relevância renovada e ampliada em um contexto de fluxos de informações nunca antes observados na história.

Os espaços sociotecnológicos avindos da pervasividade do meio cibernético também estão presentes nas relações internacionais. Philip Seib (2012) chama a atenção para alguns fenômenos ocorridos nessa área em sua obra *Real-time Diplomacy: Politics and Power in the Social Media Era* (Diplomacia em Tempo Real: Política e Poder na Era da Mídia Social), apresentando principalmente o caso da Primavera Árabe[2], as alterações e práticas na diplomacia advindas deste cenário e como as redes de mídia social afetam a estrutura política e o ativismo. Suas considerações finais demonstram como o mundo diplomático encontra-se em constante evolução a fim de lidar com as mudanças sócio-políticas advindas da apropriação e uso das mídias sociais pelos indivíduos.

[2] Caracterizada por uma onda de revoluções ocorrida no norte da África e no Oriente Médio, a Primavera Árabe é singular ao ponto em que proporcionou uma ação global de agentes não-estatais através das mídias digitais que proporcionaram não apenas a união de uma coletividade com objetivos comuns, mas foram a plataforma por excelência de suas ações.

A influência da pervasividade nas relações internacionais, entretanto, não fica apenas no plano diplomático e na política, adentrando em todos os seus campos (já que é algo pervasivo), incluindo a segurança. Julian Assange, criador do site de *hacktivismo*[3] *WikiLeaks*, afirma que a "próxima grande alavanca no jogo geopolítico serão os dados resultantes da vigilância" (ASSANGE, 2013, p. 23) e que o mundo deve estar em alerta para o perigo iminente de ter seus dados monitorados pelas potências hegemônicas. O que vem ocorrendo é o que o autor chama de "militarização do ciberespaço", uma vigilância constante da rede pelos serviços de inteligência.

Esses exemplos, que serão aprofundados posteriormente, demonstram como as relações sociais de cunho internacional, em toda a sua extensão, não fogem a essa face da modernidade que Castells (1999) chama de "Sociedade em Rede": uma sociedade que vê suas relações sociais, políticas e econômicas cada vez mais conectadas e interdependentes, através de tecnologias informacionais que acabam reformulando aspectos da sociedade e, ao mesmo tempo, sendo reformuladas por esta. Entretanto, este não é um processo que acontece de forma semelhante em todas as partes do globo, tendo muitas sociedades que ainda não fazem parte desse novo espaço ou que estão em processo de implementá-lo.

Mesmo com esta discrepância no acesso ao desenvolvimento e na adoção das TICs por parte de diferentes atores, percebe-se que o ciberespaço já não é uma arena fechada apenas aos que detém a tecnologia e o conhecimento necessário para acessá-lo. Martín-Barbero (2010) chama a atenção para o fato de hoje essas tecnologias não se voltarem mais apenas às questões financeiras típicas dos países desenvolvidos, mas servem como espaços de relações sociais cotidianas nas mais diversas áreas de sua diversidade. Claro que o baixo investimento em TICs nos Estados mais pobres afeta a diversidade de usuários conectados, mas o acesso ao ciberespaço também pode ser realizado através de *lan houses*[4] ou, mais recentemente, de celulares de baixo custo, não impedindo, assim, a expansão da cibercultura nestas regiões.

Por cibercultura, entende-se "um conjunto de técnicas (materiais intelectuais), de práticas, de atitudes, de modos de pensamento e de valores que se desenvolvem juntamente com o crescimento do ciberespaço" (LÉVY, 2007, p. 17) e tem, segundo André Lemos (2007), três princípios norteadores: a liberação dos polos de emissão, a conexão em larga escala e a reconfiguração da indústria cultural de massa e de instituições.

---

[3] *Hacktivismo* vem da junção do termo *hacker* e *ativismo*. O termo diz respeito à utilização da tecnologia para o alcance de fins políticos. No caso do *WikiLeaks*, a utilização da tecnologia se dá através da aquisição de documentos, principalmente por meio digital, e da divulgação desses na internet.

[4] Locais em que se pode acessar a internet por um preço baixo sem a necessidade de possuir um computador ou outro meio de acesso.

Esses três princípios norteadores que propiciam a formação de uma cibercultura, ou seja, um modo de agir, pensar e se comunicar típicos do espaço cibernético, são características fundamentais dessa arena que auxiliam na compreensão de porque o ciberespaço importa. A liberação dos polos emissores acaba retirando do processo comunicacional os intermediários, propiciando uma comunicação mais livre; a conexão em larga escala concebe a presença maciça de usuários que são os construtores dessa cibercultura, desse modo de agir e pensar online; e por fim, a reconfiguração da indústria de massa, ou seja, das mídias como a TV, o jornal e a revista, e de instituições, é possibilitada justamente pelas duas características anteriores que trazem novas formas de comunicação pós-massivas:

> Essa nova esfera pública digital não é recortada mais por territórios geográficos (os seus cortes relevantes correspondem antes às línguas, às culturas e aos centros de interesses), mas diretamente mundial. Os valores e os modos de ação trazidos pela nova esfera pública são a abertura, as relações entre pares e a colaboração. Enquanto as mídias de massa, desde a tipografia até a televisão, funcionavam a partir de um centro emissor para uma multiplicidade receptora na periferia, os novos meios de comunicação social interativos funcionam de *muitos para muitos* em um espaço descentralizado. Em vez de ser enquadrado pelas mídias (jornais, revistas, emissões de rádio ou de televisão), a nova comunicação pública é polarizada por pessoas que fornecem, ao mesmo tempo, os conteúdos, a crítica, a filtragem e se organizam, elas mesmas, em redes de troca e de colaboração. (LEMOS e LÉVY, 2010, p. 13)

Vale salientar, entretanto, que as funções massivas e pós-massivas coexistem e se alternam mesmo dentro de plataformas tipicamente pós-massivas. Como exemplo, é possível citar os jornais on-line, em que os usuários não possuem o poder de interação total, apenas consumindo as informações de forma massiva. No entanto tal jornal pode possuir uma extensão pós-massiva em um fórum de discussão ou um espaço que abra ao usuário comum a opção de enviar sua própria matéria.

Segundo Inês Amaral (2009), podemos apreender três pontos cruciais que caracterizam esse público pós-massivo e segmentado que consome e produz simultaneamente: participação, poder e mobilidade. A primeira e a segunda destas características fazem com que os usuários, dentro de seus grupos de interesse, ajam como filtro e como amplificadores das informações. Assim, a partir do momento em que se apropriam das plataformas digitais, fazem com que uma informação se destaque (ou não), ganhando importância (ou não), em detrimento de outra, através do uso das ferramentas do meio pelo qual está se comunicando. A mobilidade surge como a possibilidade de se comunicar instantaneamente, não sendo necessário um lugar fixo para tal ato.

Sendo assim, esses três pontos, somados às características da formação da cibercultura, acabam propiciando a formação de um pensamento coletivo global dentro deste espaço,

representando a diversidade humana mesmo com um processo de influência mútua (e por vezes não equilibrada) na identidade dos usuários. Essa ampla troca de informações entre os indivíduos conectados aos novos espaços sociotecnológicos, resulta no que Pierre Lévy (2007) denomina inteligência coletiva:

> É uma inteligência distribuída por toda a parte, incessantemente valorizada, coordenada em tempo real, que resulta em mobilização efetiva das competências. Acrescentemos à nossa definição este complemento indispensável: a base e o objetivo da inteligência coletiva são o reconhecimento e o enriquecimento mútuo das pessoas, senão o culto de comunidades fetichizadas ou hipostasiadas. (LÉVY, 2007, p. 28)

A inteligência coletiva de Lévy está intrinsecamente ligada à forma de utilização dos novos espaços sociotecnológicos pelos indivíduos, tais como os fóruns virtuais de discussão, as enciclopédias virtuais, os *blogs*, os *microblogs* e as redes sociais[5], onde os indivíduos podem interagir uns com os outros, opinando sobre diversos assuntos e compartilhando o que quiserem. Em verdade, a *internet* vai além disso, "ela é capaz de fazer emergir construções culturais e sociais inéditas, que se transformam praticamente em sujeito, ganham 'vida' própria, uma vida virtual equipada com inteligência artificial" (STOCKINGER, 2001, p. 111).

> A computação social da *Web* 2.0 aporta uma modificação essencial no uso da *web*. Enquanto em sua primeira fase a *web* é predominantemente para leitura de informações, esta segunda fase cria possibilidades de escrita coletiva, de aprendizagem e de colaboração na e em rede. Exemplos estão em expansão hoje, como comprovam a popularidade de redes sociais como *Facebook*, *Orkut*, *My Space*, *Multiply*, os *wikis*, *blogs* e *microblogs*, os instrumentos de publicação coletiva de fotos, vídeos e música (como *Flickr*, *YouTube*, *Bit Torrent*), e a emergência de redes de "etiquetagem" do espaço urbano com mapas digitais (*Google Earth*, *Maps*). (LEMOS & LÉVY, 2010, p. 52-53)

Sendo assim, a inteligência coletiva, proporcionada e abarcando novas formas de interação devido à *Web* 2.0, é onde se encontra o conhecimento das massas, a reunião da inteligência de diversos indivíduos que acaba gerando algo maior, coletivo, ampliado pelas TICs. É nesse ambiente abstrato que o fluxo de troca das informações ocorre e isso acarreta uma série de consequências, sendo, dessa maneira, o "lugar" em que tanto os usuários postam seus dados, quanto os agentes da vigilância encontram sua fonte.

---

[5] Por *fóruns*, entende-se espaços na internet em que os usuários podem postar sua opinião acerca de um tema previamente estabelecido. *Blogs* são páginas na internet em que o usuário posta informações, fotos, música, videos, entre outros de forma cronológica sobre qualquer assunto e pode receber comentários sobre tais postagens. *Microblogs* são sites em que o usuário posta informações abertas ou privadas em poucos caracteres e segue as postagens dos usuários que desejar. *Redes Sociais* são a forma de interação social mais complexa na internet, onde os usuários podem compartilhar o que quiserem, conhecer novas pessoas, organizar eventos, entre diversos outros meios de interação.

As perguntas que surgem a partir da noção deste espaço abstrato são: onde ele estaria? Qual sua base tangível? Questões necessárias a fim de facilitar a compreensão e uso dos termos corretos. Confunde-se bastante nos jornais e artigos científicos este ambiente com a *internet* ou com a *web*, entretanto, elas são apenas parte de algo maior que representa o todo deste mundo sociotecnológico, o ciberespaço. Sendo assim, uma distinção entre *internet*, *web* e ciberespaço faz-se necessária para a compreensão do ambiente em que o objeto deste trabalho encontra-se em ação.

Segundo Canabarro e Borne (2013), o ciberespaço é tudo o que envolve o uso da eletroeletrônica e do espectro eletromagnético com o fim de trocas de informações através de redes, ou seja, a *internet* é apenas uma das tecnologias surgidas que fazem parte do ciberespaço. A questão que ronda a importância da *internet* está justamente no fato do seu crescimento exponencial, o que acabou transformando-a na "rede das redes". Sobre o funcionamento da *internet*, os autores afirmam que:

> Para entender o funcionamento da *Internet*, pensemos em um bolo. A Rede também é estruturada a partir de camadas (Zittrain, 2009). A camada inferior é composta pelos elementos físicos que dão suporte às conexões, ao fluxo e ao armazenamento de dados que circulam em formato digital. São componentes da camada inferior, por exemplo, as linhas telefônicas, os cabos de conexão, as antenas de transmissão, os satélites, os servidores, etc. A camada superior, por sua vez, é composta por informação. A informação é codificada e decodificada por padrões técnicos e lógicos que compõem a camada intermediária da *Internet*. Em outras palavras, a informação é traduzida na camada intermediária, de padrões compreensíveis por seres humanos para padrões computacionais, e vice-versa. (CANABARRO & BORNE, 2013, s/p)

É a partir desta explicação que se distingue a *internet* da *web*, sendo esta última uma das ferramentas da camada intermediária da *internet*. Foi a *web* (que parte da sigla , ou *World Wide Web*) que proporcionou uma grande expansão da *internet* por criar protocolos que permitiram a interação homem-máquina de forma universal e inteligível ao homem. Sendo assim, entende-se que a *internet* vai além da *web*, existindo outros tipos de padrão, mesmo que este seja o mais difundido.

Tendo o explicitado acima como base e para fins de análise, a opção pelo uso do termo ciberespaço no trabalho parte da amplitude com que este consegue abarcar as diversas formas de tecnologias utilizadas no seu processo de militarização e no consequente uso destas para fins de vigilância, como será demonstrado posteriormente. A compreensão do funcionamento da tecnologia, entretanto, não é suficiente para entender as modificações ocorridas a nível internacional. Como visto anteriormente, a influência dos novos meios faz parte de uma co-construção em que tanto a sociedade quanto a tecnologia em si são moldadas através de um

processo de apropriação do ciberespaço, ou seja, as formas com que os usuários finais fazem uso deste e como são influenciados a partir desse uso.

Para tanto, entender a influência do ciberespaço nas relações internacionais, seus efeitos e suas implicações e apresentar alguns conceitos como *cyberpolitik*, *cyberpower* e cibersegurança que auxiliam nesse sentido, são etapas necessárias para compreender causas e consequências dos casos de vigilância cibernética da sociedade em rede e como esta questão alcança debates de proporções internacionais, sendo alçada ao nível de ameaça à segurança internacional.

1.2 O Ciberespaço e as Relações Internacionais

Tendo em vista a maior importância relegada à informação atualmente, e esta perpassar pelos cabos e satélites do ciberespaço, não há como negar a importância desta instância na busca pelo poder no tabuleiro das relações internacionais.

Antes de qualquer afirmação, entretanto, é necessário frisar que este trabalho compartilha dos pressupostos apontados por Leonardo Valente (2007) de que as esferas do poder tradicional continuam as mesmas dentro dos Estados: a militar, a política e a econômica. Não é possível afirmar que o ciberespaço por si só, mesmo após a revolução comunicacional advinda do surgimento dos meios que criaram uma cultura de massa (como o rádio e a TV) e da *internet*, é uma esfera de poder paralela às supracitadas. Dessa forma, a mídia é vista e analisada como um *pilar fluido de poder*:

> Em nosso caso, quando nos referimos a um pilar fluido, estamos nos referindo a uma estrutura fundamental à manutenção do poder de um Estado, mas que não opera sozinha, que age em outras estruturas e que precisa que elas funcionem, e bem, para poder atuar. (VALENTE, 2007, p. 35)

Dessa forma, a ideia de *fluido*, para Valente, está ligada ao termo criado por Zygmunt Bauman (2001, p. 8), em que demonstra como os fluidos "se movem facilmente", diferentemente dos sólidos que "têm dimensões espaciais claras". Sendo assim, os fluidos "não fixam o espaço nem prendem o tempo", sendo difícil contorná-los ou controlá-los. O ciberespaço, dessa forma, invade os *pilares sólidos* do poder criando novos desafios e novas oportunidades, mas sendo extremamente difícil mensurá-lo no tempo e no espaço.

Apesar da apropriação deste conceito para a compreensão do papel do ciberespaço e da mídia como um todo nas relações de poder internacionais neste trabalho, Charaudeau (2009) ressalta uma outra perspectiva que o aponta como um quarto poder – aqui, entretanto, a "quarta posição" aparece após os poderes Executivo, Legislativo e Judiciário. Para o autor, a comunicação manipula e é manipulada, principalmente por fazer parte da concorrência capitalista das indústrias midiáticas, transformando-se, assim, em uma "máquina midiática" que produz informação para as massas em larga escala e de forma imediata. Entretanto, Charaudeau afirma que para ser um poder *de facto*, as mídias deveriam ditar normas comportamentais, ter a capacidade de impor sanções e possuir indivíduos passíveis dessa "manipulação" diante de regras declaradas assim como o poder militar, político e econômico possuem.

O que o ciberespaço realizou no campo do poder foi uma modificação na forma como os agentes internacionais põem em prática suas ações na busca pela sua sobrevivência no meio internacional e pelos seus interesses. Valente (2007) afirma que as inovações tecnológicas na mídia possuem tanto a capacidade de ampliar as três esferas do poder como de colocá-las em inoperância. Consequentemente, assistimos hoje a uma tentativa desenfreada dos agentes de se adequarem à nova realidade da era da informação, uma corrida tecnológica virtual e física, seja através do controle e da supremacia dos meios técnicos, da presença marcante, dos discursos proferidos, entre outras formas, o que acaba gerando um processo de securitização do ciberespaço como será apontado no próximo capítulo.

Não é à toa que os atores internacionais, principalmente os Estados, vêm realizando altos investimentos na área de segurança cibernética, não apenas como forma de defesa contra ataques externos, mas também com intenções ofensivas. O quadro da União Internacional de Telecomunicações (ITU, na sigla em inglês) a seguir demonstra quais os principais países que vêm desenvolvendo sua segurança cibernética. O índice utilizado pela ITU varia de zero a um e leva em consideração cinco áreas de comprometimento dos países: medidas legais, medidas técnicas, medidas organizacionais, capacidade de construção e cooperação internacional.

Quadro 1
Ranking global das 5 primeiras posições de países comprometidos com a segurança cibernética

País	Índice	Ranking	País	Índice	Ranking
EUA	0.824	1	Brasil	0.706	5
Canada	0.794	2	Estônia	0.706	5

Austrália	0.765	3	Alemanha	0.706	5
Malásia	0.765	3	Índia	0.706	5
Omã	0.765	3	Japão	0.706	5
Nova Zelândia	0.735	4	Coreia do Sul	0.706	5
Noruega	0.735	4	Reino Unido	0.706	5

Fonte: Disponível em: <https://.itu.int/pub/D-STR-SECU-2015> Acesso em: 12 dez 2015.

O quadro auxilia na demonstração do quão pronto estaria um país a nível nacional para as questões que envolvem segurança no mundo cibernético. Logo, percebe-se que os investimentos na área de segurança são cruciais atualmente tendo em vista a importância que o ciberespaço tem ganhado nos últimos anos e as suas possibilidades de ataque, contra-ataque e enquanto ferramenta essencial de vigilância.

Tendo isso em vista, é notável que a diminuição das distâncias, a circulação de informação em tempo real, as possibilidades quase infinitas de comunicação, o surgimento das agências de notícias internacionais com informações 24 horas, entre outras características desta nova era, constroem tanto novos meios de ação quanto novos empecilhos para os agentes internacionais. Ao mesmo tempo em que negociações políticas e econômicas no meio internacional tornam-se menos custosas e de fácil acesso, a possibilidade do uso ofensivo desse espaço e a dificuldade no controle com que a informação percorre o globo cria novos agentes e fatores que dificultam a ação estatal tais como a opinião pública, a própria imprensa, organizações ciberativistas, *hackers*, entre outros.

Logo, analisar os principais efeitos que a pervasividade do ciberespaço traz às relações internacionais e como ela gera a uma forma genérica da *realpolitik* de Kissinger, a chamada *cyberpolitik*, é fundamental para a compreensão de como esta nova arena proporciona a formação de novos atores que possuem um papel crucial na vigilância cibernética, uma das grandes ameaças do novo século.

1.2.1 Os efeitos do ciberespaço nas Relações Internacionais

Os efeitos que o desenvolvimento das TICs vem gerando no cenário internacional datam do final da década de 1960, entretanto, ganharam força com a intensificação da comercialização e disseminação na sociedade civil, tendo como pano de fundo o marco histórico do fim da Guerra Fria e as suas consequências para as relações internacionais (CASTELLS, 1999). A vitória do bloco capitalista, o processo de globalização e as inovações tecnológicas proporcionaram maior interação entre os atores, ampliando o papel da informação enquanto ferramenta fundamental para as relações de poder no cenário internacional. Afinal, quem detém informação, possui supremacia nas relações de poder. Segundo David Rothkopf (1998), os efeitos do ciberespaço proporcionado pela evolução das TICs no meio internacional podem ser expressos a partir de sete fenômenos que dialogam entre si:

- a *capacidade de interconexão*, passando a ser desnecessário encontros físicos;
- a *descentralização e a desagregação*, tendo em vista que a facilidade de comunicação dificulta a centralização das negociações no governo central;
- a *desintermediação*, que anula a necessidade de um meio para a comunicação (tais como o correio, a TV, o rádio, etc.), consequência da comunicação face-a-face;
- o *deslocamento do real para o virtual*, aumentando, assim, a presença de um ator em outro , sem a necessidade de encontros físicos;
- a *aceleração*, devido ao pressuposto do instantâneo;
- a *amplificação*, em que temas ganham grande repercussão (imprensa e opinião pública);
- e o *aumento da assimetria de poder*, já que as potências possuem maior capacidade de se adequar às novas mídias, demonstrando, assim, que as relações entre os Estados não estão caminhando para uma democratização deste meio.

Interligando-se os principais efeitos levantados por Rothkopf (1988), é possível gerar uma base analítica para os fenômenos que vêm ocorrendo no ciberespaço dentro do escopo das relações internacionais. Essas características podem ser expressas como o modo pelo qual os atores apropriaram-se das TICs, de como se desenvolveu uma cibercultura das relações de poder, ou melhor, como delimitaram as consequências desse processo. A diminuição dos encontros físicos e a aceleração das comunicações, relativizando o espaço e o tempo, a presença maciça de atores e as modificações nas instituições permitiram que esses usuários agissem de forma mais autônoma e enfática, sem precisar de intermediários para tal; ao mesmo tempo em

que possibilitou o surgimento de novos agentes que utilizaram a pervasividade do ciberespaço para agir de forma descentralizada.

Isto acaba gerando consequências para o jogo político cibernético, como uma maior participação popular (ou pelo menos o desejo de participação) devido à amplificação dos debates; ao mesmo tempo em que cria uma arena de debates distante de ser igualitária, tendo em vista a discrepância na relação de poder entre os atores, mas que também possibilita ações "vindas de baixo", ou seja, atos realizados por agentes que, fora do meio cibernético, pouco poderiam fazer frente ao poder estatal. Um exemplo disso é a existência de organizações civis não-estatais, muitas vezes percebidas como ilegais, tais como o *WikiLeaks* e o *Annonymous*[6], que geram sérios problemas a alguns atores mais preponderantes, como os Estados e as empresas de tecnologia, através de ações como a divulgação de informações confidenciais ou ataques a sistemas de dados.

Dessa forma, esse processo de apropriação, ou seja, os efeitos apresentados por Rothkopf (1998), acaba trazendo mudanças tão profundas na forma como o jogo político internacional molda-se que o autor cunhou o termo *cyberpolitik* para conceitualizar tais novidades. Juntamente com esse conceito, apresenta-se a seguir também a ideia de poder dentro das relações cibernéticas, denominado de *cyberpower*.

1.2.2 Cyberpolitik e *Cyberpower*

Os efeitos do ciberespaço nas relações internacionais são tão impactantes que Rothkopf criou um novo termo para a *realpolitik*[7] da era da informação, a *cyberpolitik*:

> A *Realpolitik* da nova era é a *Cyberpolitik*, na qual os atores nas Relações Internacionais, principalmente os estados, terão seu poder dimensionado e fortalecido pelo poder da informação. Os fins continuarão os mesmos, mas os meios para se alcançarem esses fins serão modificados de forma drástica. (ROTHKOPF, 1998, p. 3 *apud* VALENTE, 2007, p. 38)

[6] O *Annonymous* é uma comunidade descentralizada no ciberespaço formada por usuários que agem de forma coordenada anonimamente contra alvos que consideram lesivos aos seus interesses ou ao interesse coletivo. Funciona através de debates em fóruns online nos quais chega-se a um consenso quanto ao objetivo das ações programadas, geralmente contra instituições governamentais ou grandes corporações. Estão associados ao ativismo cibernético internacional, ou seja, ações ativistas que ocorrem dentro da internet a fim de alcançar uma meta comum, mas também organizam atos reais, o que dificulta a definição de líderes dos movimentos.

[7] Segundo Henry Kissinger (2001), *Realpolitik* é "a política externa baseada em cálculos de poder e nos interesses nacionais".

Os recursos fornecidos pela revolução comunicacional aos agentes internacionais passam, então, a ser estratégicos para o alcance dos seus interesses e da sobrevivência neste meio. Segundo Valente (2007), os outros recursos tanto de *hard* quanto de *soft power* já estariam bastante disseminados, não proporcionando mais seus fins de barganha e/ou sanção. A informação, nesse caso, passa a ser central para os atores, que agiriam através do meio virtual (*internet*, TV, rádio, etc.), disseminando seus interesses na forma de discursos.

Aqui, os discursos são vistos como "toda prática expressiva de linguagem que vise à produção e à circulação social do sentido" (RABAÇA & BARBOSA, 1995), sendo assim, os discursos disseminados no meio internacional acabam construindo a forma como o ciberespaço é visto e utilizado pelos atores internacionais, tanto suas possibilidades de agir neste meio quanto as ameaças advindas deste, dando um sentido a esta arena. É essa construção que gera o processo de securitização do espaço cibernético (essa debate será ampliado no segundo capítulo deste trabalho).

Para Valente, o que diferencia os discursos atuais é que o meio virtual amplifica e fortifica seus objetivos devido às suas características de pervasividade e de convergência. Utilizando-se das ideias de Michel Foucault, Valente (2007, p. 40) ressalta que "não haveria recurso melhor para essa busca [pelo poder], pois para ele [Foucault] as ligações entre o discurso e o poder são extremamente íntimas".

> Ou seja, para conquistar o poder é preciso ter o poder da informação e ter o poder significa também ter em mãos o sistema de informação e de discursos dominantes no cenário internacional. Se o grande espaço para o discurso contemporâneo é o virtual, Foucault reforça a tese de Rothkopf, de que a *Cyberpolitik* será o grande cenário das ações dos Estados. (VALENTE, 2007, p. 41)

Sendo a *ciberpolitik* o cenário por excelência das relações internacionais do século XXI, o que se entende como poder dentro deste espaço, ou seja, como se dão as relações de poder[8] neste meio, também passa por algumas modificações em sua definição, devido às características únicas das TICs anteriormente citadas. Tim Jordan (2003) afirma que:

> *Cyberpower* é a forma de poder que estrutura a cultura e a política no ciberespaço e na *Internet*. É composto de três regiões inter-relacionadas: o indivíduo, o social e o imaginário. *Cyberpower* do indivíduo consiste em avatares, hierarquias virtuais e espaço informacional e resulta em ciberpolítica. Poder aqui aparece como a posse de

[8] Aqui, o conceito de poder é entendido do mesmo modo que Foucault (1988): "Trata-se [...] de captar o poder em suas extremidades, lá onde ele se torna capilar; captar o poder nas suas formas e instituições mais regionais e locais, principalmente no ponto em que, ultrapassando as regras de direito que o organizam e delimitam, ele se prolonga, penetra em instituições, corporifica-se em técnicas e se mune de instrumentos de intervenção material, eventualmente violentos." (FOUCAULT, 1988, p. 182)

> indivíduos. *Cyberpower* do social é estruturado pela espiral de technopower e pelo espaço informacional dos fluxos e resultada na elite virtual. Poder aqui aparece como formas de dominação. *Cyberpower* do imaginário consiste na utopia e distopia que compõem o imaginário virtual. Poder aqui aparece como constituinte da ordem social. Todas as três regiões são necessárias para mapear o *cyberpower* no total e nenhuma região é dominante sobre qualquer outra. (JORDAN, 2003, p. 208, tradução nossa)

O poder em si não está ligado ao ato de tomar uma decisão política, mas a tudo que estrutura e limita o ciberespaço culturalmente e politicamente, e define as relações de autoridade. A fim de constituir uma ampla gama de análise das relações de poder dentro do ciberespaço, o autor buscou subdividir as esferas pelas quais esta relação circula e se interrelaciona. Essa forma complexa de analisar o poder auxilia na explicação do porquê certos conflitos e cooperações nesse meio tendem a ocorrer em determinadas áreas.

Ao definir o *cyberpower* dos indivíduos, ou seja, dos atores que utilizam este espaço, Jordan (2003) busca delimitar o ato de "viver" no espaço cibernético, as experiências dos usuários a partir da criação de seus avatares[9]. Este nível de análise auxilia na compreensão de alguns aspectos como: "fluidez de identidade, anti-hierarquismo, espaços de informação e a forma como estes sustentam uma política amarrada através dos dois eixos de acesso ao ciberespaço e os direitos neste ambiente" (JORDAN, 2003, p. 209, tradução nossa). Sendo assim, analisa-se neste nível aspectos ligados ao ator quanto ao seu uso, comprometimento, normas aplicadas e demanda nos espaços sociotecnológicos.

O *cyberpower* dos indivíduos conecta-se ao do social a partir do momento em que estes avatares interagem e formam grupos que se especializam em certas áreas da arena virtual, criando, assim, uma elite virtual e uma hierarquia de dominação. A espiral de *technopower* à qual o autor se refere está ligada ao processo de especialização desses grupos sociais que ocorre da seguinte forma: ao criar-se uma TIC ela gera uma série de informações e formas de apropriação que acabam demandando o surgimento de novas tecnologias para suprir as defasagens anteriores. Este processo é constante e gera novos grupos que dominam essas tecnologias formando novas elites. Um exemplo claro dessa espiral são as frequentes mudanças nos meios pelo qual construímos nossas "redes sociais" no ciberespaço; em menos de 15 anos diversos sistemas foram criados e se extinguindo de acordo com a demanda, tais como: *ICQ*, *Mirc*, *MSN*, *Orkut*, *Twitter*, *Facebook*, *Instagram*, *Whatsapp*, entre muitos outros. Em todos esses exemplos, o ator utiliza o serviço mas não domina o meio.

O mesmo ocorre se levarmos estes dois primeiros níveis de análise para as relações internacionais. Os principais atores que utilizam o ciberespaço e que estão dentro do escopo

[9] Personificação virtual do usuário real; perfil.

das RI (discutidos de forma aprofundada na próxima seção deste tópico) podem ser analisados no nível do *cyberpower* dos indivíduos: são suas experiências, sua apropriação desse espaço, que irão gerar suas demandas e a criação das elites virtuais nesse meio. Se há uma securitização desse espaço, uma demanda pela formação de sistemas de defesa, ataque e vigilância global, um grupo especializado surge desse espiral de *technopower*, cria as tecnologias necessárias e torna-se dominante neste aspecto das relações de poder, delimitando as possibilidades de escolhas que os atores possuem no ciberespaço.

Tratando-se do *cyberpower* do imaginário, Jordan (2003) afirma que este é o que constitui a ordem social dentro do ciberespaço. Este nível está ligado ao imaginário coletivo e à percepção de que há uma comunidade virtual muito além dos usuários que um indivíduo tem contato:

> As esperanças e medos que constituem este imaginário coletivo são expressos como um paraíso de imortalidade e onipotência contraposto a um inferno de vigilância total e armas totalitárias perfeitas. Mesmo que a tecnologia para criar qualquer um destes sempre parece estar quase pronta, e assim exige urgência e empenho dos membros da comunidade virtual, o propósito essencial da imaginação coletiva ou imaginário não é criar o céu e/ou o inferno, mas através do reconhecimento mútuo dessas esperanças e medos criar a comunidade virtual. (JORDAN, 2003, p. 210, tradução nossa)

Sendo assim, a ordem existente no ciberespaço parte desse imaginário gerado a partir de um pensamento coletivo dos atores. Esse reconhecimento mútuo de que o espaço virtual pode gerar tanto possibilidades de cooperação, assemelhando-se a uma visão de mundo da teoria liberal das relações internacionais, quanto uma arena anárquica semelhante ao sistema internacional da teoria realista, perpassa a ideia de que na verdade esse espaço é construído de acordo com que os agentes fazem dele, parafraseando o autor construtivista Alexander Wendt (1994). Dessa forma, compreende-se que os discursos que geram a *cyberpolitik* estão em constante mutação e são as ferramentas por excelência dessa construção do imaginário coletivo que gera uma ordem em frequente mutação.

Vale salientar ainda uma distinção entre a política e o poder apresentada por Bauman e Lyon (2013): enquanto este último encontra-se cada vez mais em um espaço global, não mais preso às fronteiras dos Estados, a política continua localizada no ente estatal, não tendo capacidade de ação em nível mundial. Segundo os autores, “sem o controle político, o poder torna-se fonte de grande incerteza, enquanto a política parece irrelevante para os problemas e temores da vida das pessoas” (BAUMAN & LYON, 2013, p. 13). Essa relação ambígua é importante para compreendermos o poder de vigilância atualmente tendo em vista que as fronteiras estão cada vez mais relativizadas como será demonstrado posteriormente.

Tendo estes conceitos-chave para a análise do ciberespaço enquanto nova arena de ação dos atores internacionais, faz-se necessário uma breve apresentação de quem são esses indivíduos, esses agentes, e como eles fazem uso do *cyberpower* dentro da lógica da *cyberpolitik*, afinal, para uma análise aprofundada de como a vigilância cibernética toma forma, seus objetivos e consequências, é importante reconhecer quem são os atores que fazem parte desta relação de poder.

1.2.3 O ciberespaço e seus atores

Segundo Valente (2007), uma das formas de ação dos discursos dos agentes internacionais – nesse caso, especificamente o Estado – através do *cyberpower* teria como alvo inicial a opinião pública de um outro país. A opinião pública serviria como um meio para o verdadeiro objetivo de atingir o Estado-alvo. Dessa forma, a imposição de novas ideias na opinião pública pressionaria o governo a tomar novas posições ou até mesmo poderia levar a derrubada de um governo por parte da população.

Neste ponto, Valente absorve os pressupostos realistas das relações internacionais de que os Estados são os atores mais importantes do cenário internacional, logo a ação de influência da opinião pública partiria sempre de um Estado visando atingir outro país e não a própria população. Mesmo criticando a ideia realista de Morgenthau que afirma ser desnecessária para os estudos neste campo a presença de elementos que não a política racional dos Estados tais como a opinião pública e o direito internacional, Valente reafirma a presença do Estado como único ator *de facto* no meio internacional.

Ora, afirmar que o Estado é o único *global player* capaz de influenciar a opinião pública de um país e tendo como único fim o próprio Estado, é negar todas as características das novas mídias com funções pós-massivas que expandem o poder de ação dos indivíduos. A ubiquidade, a convergência e a alta mobilidade (propiciada pelo advento dos *smartphones*) dos novos meios, somados à *Web* 2.0 que "cria possibilidades de escrita coletiva, de aprendizagem e de colaboração na rede" (LEMOS & LÉVY, 2010, p. 52), geram, assim, um espaço de "todos" que libera os polos emissores, não mais dependentes do controle dos produtores das grandes mídias com funções massivas (TV, rádio, etc.) nem dos Estados e seu controle midiático.

Pensar que os efeitos das novas mídias nas relações internacionais restringem-se apenas ao nível estatal é negar a existência de diversos atores e fatores que influenciam no jogo de

poder neste meio, assim como visto no caso da espionagem brasileira pelo governo estadunidense e nos vazamentos de informações por organizações de ciberativistas como o *WikiLeaks*. Segundo Joseph Nye (2002):

> Há quatro séculos, o estadista e filósofo inglês Francis Bacon escreveu que informação é poder. No começo do século XXI, uma parcela muito maior da população tem acesso a esse poder, tanto dentro de cada país como entre eles. Os governos sempre se preocupam com o fluxo e o controle da informação, e o período atual não é o primeiro a se ver seriamente afetado pelas mudanças na tecnologia da informação. Atribui-se à invenção dos tipos móveis de Gutemberg, que permitiram a impressão da Bíblia, tornando-a acessível a grandes segmentos da população europeia, papel de grande importância no advento da Reforma. Os panfletos e os comitês de correspondência pavimentaram a independência dos Estados Unidos. No mundo rigorosamente censurado da França do século XVIII, as notícias que circulavam pelos mais diversos meios – oral, manuscrito, impresso – ajudaram a divulgar os fundamentos da Revolução Francesa. Como argumenta o historiador Robert Darnton, de Princeton, "toda era foi uma era da informação, cada qual à sua maneira". Mas nem mesmo Bacon teria sido capaz de imaginar a revolução da informação do presente. (NYE, 2002, p. 84)

Sendo assim, apesar de Nye reforçar o argumento da importância da informação para a política e para as relações entre os Estados, também afirma que a população passa a ter um maior acesso ao poder devido às novas tecnologias informacionais e comunicacionais. Dessa forma, o autor demonstra uma disseminação de poder para fora da esfera dos Estados, gerando, assim, indivíduos e grupos sociais não-estatais aptos a influenciar a política global.

Para Onuf (2002), um dos principais autores da corrente teórica construtivista das Relações Internacionais, os agentes não são os Estados, nem os Órgãos Internacionais, nem qualquer outra organização política, mas sim os próprios seres humanos enquanto seres sociais que constroem mundos[10] que façam sentido para si. Segundo o autor, existem os indivíduos agentes, que constroem os mundos, e os observadores, que os analisam e influenciam a partir do momento em que se aproximam mais e mais destes mundos.

> Para qualquer um de nós enquanto agentes, o mundo é toda a experiência. Assim que nos afastamos e nos tornamos observadores, vemos muitos mundos, mundos dentro de mundos, alguns dos quais nós pertencemos, outros não. Por definição, todo o mundo em que vivemos é ilimitado. Os limites de quase todos os mundos são mais fáceis de discernir quando nos afastamos deles. Por outro lado, somos obrigados a nos aproximar para ver muito do que acontece dentro desse mundo. Quanto mais perto estamos, mais provável é que tenhamos um efeito sobre o que vemos. Agentes, observadores: talvez a distinção seja analítica, mas indispensável na prática. (ONUF, 2002, p. 119, tradução nossa)

[10] Para Onuf (2002), não existe apenas um mundo (estrutura), mas diversos mundos como o dos eventos (onde os Estados agem), o da política, o das relações formais (fetas pelos agentes), o das atividades técnicas e dos serviços públicos, e o dos acadêmicos (que observam e influenciam outros mundos).

Já para outro construtivista, Wendt (1994), o principal ator a ser estudado na construção das relações internacionais é o Estado, que ainda concentra grande parte das decisões tomadas em nível internacional e pode manipular a opinião pública e o nacionalismo: grandes influenciadores das tomadas de decisões internas. Contudo, com o crescimento de alguns grupos não-estatais (WENDT, 1994, p. 9), o autor atenta para o aumento de importância que eles adquiriram. São atores que estão fora do modelo Westfaliano e que podem ajudar a formar identidades coletivas não-nacionais – o que mudaria a estrutura internacional.

Como visto anteriormente, o ciberespaço parece proporcionar a formação de uma identidade coletiva entre os grupos de indivíduos que agem nesta nova arena. A nível dos atores, o *cyberpower* proporciona a qualquer usuário essa fluidez identitária e uma não hierarquização de suas relações; socialmente, a relação de dominação existe, mas não impede que novos indivíduos e grupos alcancem outros patamares nas relações de poder; por fim, a ordem é estabelecida justamente por essa coletividade e pelos discursos e ações que podem modificar a estrutura. Sendo assim, o sistema formado em Westfalia é afetado pela ação desses novos atores, mas não desmembrado, tendo em vista que os Estados ainda concentram grande parte do poder – militar, político e econômico – mas cada vez mais o *cyberpower* é disseminado entre novos agentes.

Como exemplo disso, é possível observar que cada vez mais as empresas multinacionais têm autonomia econômica para agir unilateralmente, possuindo, assim, cada vez mais poder de influência, tanto na população quanto no próprio Estado. Na esfera política, o próprio vazamento das informações pelo Snowden com a ajuda da mídia é um exemplo, tendo em vista que tais ações tiveram um alcance internacional e colocaram em xeque as relações entre os Estados envolvidos. Militarmente, o processo de securitização do ciberespaço parece apontar para o surgimento de um novo *front* de conflitos virtuais, incluindo não apenas Estados, mas diversos atores que conseguem alcançar um certo nível de ação como será apontado posteriormente.

Dessa forma, a *cyberpolitik* não é, e nunca foi, restrita à ação única dos Estados, tendo em vista a presença maciça de diversos atores não-estatais que alteram e são alterados dentro dessa nova arena. Claro que o Estado, devido aos recursos que possui, tem certa preponderância nos novos meios, principalmente no que tange questões de segurança; são eles os detentores da estrutura física dos cabos de fibra óptica e das tecnologias mais modernas, entretanto, como visto, a própria constituição do ciberespaço como uma arena aberta permite distintas formas de apropriação.

A partir das definições acerca da relação entre o ciberespaço e as relações internacionais, seus efeitos que geram a *cyberpolitik* e o *cyberpower* e como atores não-estatais mostram-se cada vez mais presentes nesse espaço, têm-se a base necessária para se adentrar nos preceitos que conceituam a cibersegurança e, por fim, iniciar a apresentação e análise da vigilância enquanto dimensão-chave das relações de poder no ciberespaço e nas relações internacionais.

1.3 Cibersegurança

A segurança sempre foi um dos principais objetos de estudo das Relações Internacionais, se não o principal. O nascimento deste campo de estudo enquanto ciência tem na sua concepção a preocupação com a segurança, seja no campo normativo ao tentar evitar a ocorrência de novas guerras no pós-Primeira Guerra, quanto nos estudos realistas focando na sua inevitabilidade. Durante a Guerra Fria, foi o tópico mais estudado na área e com o advento dos ataques terroristas de 11 de setembro voltou à voga (RUDZIT, 2005).

Saindo do campo científico, o tema também tem grande repercussão entre os atores internacionais. Não é à toa que os gastos com segurança, por parte principalmente dos Estados, ainda são uma prioridade (SILVA FILHO & MORAES, 2012). Apesar do senso comum apontar questões de segurança apenas como gastos ligados ao uso da força por um Estado, as constantes mudanças no sistema internacional também repercutiram no que se entende enquanto segurança internacional.

Como demonstra Rudzit (2005), os debates iniciais de fato prenderam-se à questão do poder e da paz: enquanto o realismo e seus principais expoentes, Carr, Morgenthau, Waltz e Mearsheimer, enxergam a segurança como uma relação de poder, ou seja, o ator que alcança um maior nível de "poder" possui mais segurança no meio internacional; os liberais (ou idealistas), baseados em Kant, acreditavam que a segurança era uma consequência da paz que deveria ser almejada enquanto norma internacional. A partir da década de 1970, o termo começa a ganhar novos ares, entrando no debate as questões econômicas e ambientais que também possuíam consequências para a segurança dos Estados, principalmente a partir da teoria da interdependência complexa de Keohane e Nye (1977), que, de forma resumida, demonstrou o quanto os Estados estão atualmente interligados e dependentes uns dos outros, e um fenômeno ocorrido em um local pode ter consequências sérias em um país a quilômetros de distância.

Com o fim da Guerra Fria no final da década de 80 e o consequente esfriamento do uso da força pelas grandes potências, pelo menos no que tange as disputas entre elas, uma série de novos estudos que ampliaram ainda mais o conceito de segurança surgiram como resposta aos fenômenos que emergiram nesse período e que antes eram sufocados pela disputa ideológica. Foi neste momento que o Construtivismo e a Escola de Copenhague e seus estudos acerca da securitização, que serão explorados de forma aprofundada no segundo capítulo e servirão de base para a análise de casos que envolvem cibersegurança e vigilância no terceiro, ganharam relevância na área das Relações Internacionais.

A perspectiva de Copenhague permitiu que diversos novos temas ganhassem relevância dentro do escopo da segurança. Ao delimitar suas bases a partir da epistemologia construtivista das Relações Internacionais, a securitização permite analisar as questões de segurança como fenômenos socialmente construídos nas quais os discursos, ou atos de fala, como denominam Buzan, Waever e Wilde (1998), constituem ou não se um objeto é securitizado no meio internacional, dependendo da aceitação dos outros atores.

Sem adentrar de forma aprofundada na teoria, objeto do próximo capítulo, percebe-se que é a partir dessa noção que a cibersegurança ganha espaço nos debates atuais que envolvem a segurança no cenário internacional. A partir do momento em que se expoem as fragilidades e ameaças desse espaço anteriormente apresentado neste trabalho, os debates ganham proporções globais acerca de diversos tópicos, como hackativismo, cibercrimes, espionagem cibernética, sabotagem cibernética, terrorismo cibernético, ciberguerras, entre outros. Cepik, Canabarro e Borne (2014, p. 237), elaboraram um quadro de categorização da tipologia de conflitos cibernéticos, a partir do desenvolvimento de Möckly (2012):

Quadro 2
Tipologia de conflitos cibernéticos

Tipo de conflito	Caracterização
Hackativismo	Mistura de ações *hacker* com ativismo político. Geralmente tem como objetivo a inviabilização de sítios eletrônicos e servidores.
Crime cibernético	Desenvolvimento de ações ilícitas com o emprego de computadores e da *Internet*.
Espionagem cibernética	Acesso não autorizado a computadores e servidores com a finalidade de se testar a configuração e os sistemas de defesa de um determinado computador, ou ganhar acesso a informações sigilosas.
Sabotagem	Criação de empecilhos ao desenvolvimento de processos e rotinas de

cibernética	trabalho nos setores público e privado a partir de meios eletrônicos.
Terrorismo cibernético	Ataques ilícitos *contra* computadores – e a informação neles armazenada – e redes computacionais com o objetivo de intimidar ou coagir governos e/ou suas populações para o alcance de objetivos políticos. Dos ataques, *deve* decorrer a violência contra bens e pessoas, tanto quanto for necessária para se gerar o nível de medo adequado ao rótulo de 'terrorismo cibernético' (grifos dos autores). Nas palavras de Möckly (2012, p. 116, tradução dos autores): "O termo é também usado de forma imprecisa e vaga para incidentes cibernéticos de natureza política variada".
Guerra cibernética	Emprego de meios eletrônicos para atrapalhar as atividades de um inimigo, bem como atacar sistemas de comunicação. Nas palavras de Möcly (2012, p. 116, tradução dos autores): "[o] termo é também usado de forma imprecisa e vaga para incidentes cibernéticos de natureza política variada".

Fonte: MÖCKLY, 2012, p. 116. Elaboração: CEPIK; CANABARRO; BORNE, 2014, p. 237

Apesar da categorização auxiliar na compreensão dos diferentes tipos de conflitos cibernéticos, questiona-se, todavia, quais seriam essas fragilidades do ciberespaço. Que ameaças essa arena pode apresentar aos atores internacionais que justifiquem tais preocupações? Afinal, o que é cibersegurança? Se tomarmos como base o explicitado anteriormente acerca das características do ciberespaço, é possível apreender que os novos espaços sociotecnológicos representam uma faceta importante das relações sociais atuais e começam a abarcar uma série de fenômenos que já ocorrem no meio físico, levando-os para o mundo virtual.

Como visto a partir da conceitualização de *cyberpower* por Jordan (2003), a ordem no meio cibernético por vezes assemelha-se bastante ao que se encontra nas teorias das Relações Internacionais acerca da ordem internacional. Sendo assim, dimensões-chave no que diz respeito à segurança internacional também estão presentes no mundo cibernético devido à sua amplitude que questiona as mais diversas tentativas de limitá-lo a fronteiras construídas por atores como os Estados.

De forma técnica, a fim de uma definição de compreensão prática, a ITU define cibersegurança como:

> Cibersegurança é o conjunto de ferramentas, políticas, conceitos de segurança, salvaguardas de segurança, orientações, abordagens de gestão de riscos, ações, treinamento, melhores práticas, garantia e tecnologias que podem ser usadas para proteger o ambiente cibernético e os ativos de organizações e usuários. Os ativos de organizações e usuários incluem dispositivos de computação, pessoal, infraestrutura, aplicativos, serviços, sistemas de telecomunicações, bem como a totalidade das informações transmitidas e/ou armazenadas no ambiente cibernético conectado. A

> cibersegurança se esforça para garantir a realização e manutenção das propriedades de segurança dos ativos de organizações e usuários contra riscos de segurança relevantes no ambiente cibernético. Os objetivos gerais de segurança incluem o seguinte: disponibilidade; integridade, que pode incluir autenticidade e não-repúdio; confidencialidade. (ITU, 2008, p. 2-3, tradução nossa)

Como visto, a definição técnica de cibersegurança está ligada principalmente à salvaguarda de informações e infraestrutura e estipula alguns objetivos básicos como a disponibilidade, a integridade e a confidencialidade. Os meios pelos quais estes objetivos devem ser alcançados são listados de forma clara a fim de abarcá-los em uma definição ampla. Entretanto, este conceito não contempla o porquê da necessidade da cibersegurança nem o que isso significa do ponto de vista político e social. Sendo assim, faz-se necessário delinear quais são os principais discursos e ações nesse meio que promovem a necessidade dos atores se defenderem no ciberespaço.

Os discursos que alertam para a presença de ameaças no espaço cibernético existem desde o seu surgimento e expansão. Segundo Schjolberg (2008), já na década de 1970 os debates acerca dos cibercrimes estavam postos nas agendas jurídicas dos Estados Unidos, alertando para as ameaças que os computadores e as redes poderiam trazer à sociedade. Atualmente, diversos Estados já possuem legislações que buscam regulamentar essas atividades, mesmo que alguns de forma tardia, e há uma tentativa de harmonização internacional das definições, principalmente através de organismos internacionais, apesar das dificuldades como demonstram Lopes e Teixeira Jr. (2010, s/p):

> Com pouca (ou quase nenhuma regulamentação), o ciberespaço dá vida a uma série de ilicitudes conhecidas como cibercrimes ou cybercrimes. Após tentativa de tipificação e punição dos tais cibercrimes, no âmbito do Direito Internacional, em 2001, com a Convenção de Budapeste – Convenção sobre o Cibercrime –, ficou latente a dificuldade que os Estados têm em conduzir acordos multilaterais que envolvam um ambiente cujos poderes sobre o mesmo não estão bem delimitados. Questões como territorialidade, governança, direitos humanos e soberania são ainda deveras discutidas em vários âmbitos: acadêmico, jurídico, militar, diplomático – a própria ONU possui um fórum sobre a questão da Governança Global da *Internet*, o IGF/UN – e civil.

Dentre os cibercrimes mais comuns, é possível citar as fraudes financeiras, a extorsão, a pornografia infantil, a pedofilia, a divulgação de conteúdo privado, o tráfico de órgãos e de drogas, a invasão de computadores, redes e sistemas, o ciberterrorismo, a espionagem, entre diversos outros. Uma das características marcantes, entretanto, principalmente para as Relações Internacionais e os estudos de cibersegurança internacional, é a ciberguerra que pode, ou não, ser categorizada como ou fazer uso do cibercrime, como visto no quadro 2. Esta aparente

contradição revela muito mais questões internas ao Estado e suas regulamentações e a falta de um direito internacional que defina crimes cibernéticos de guerra, como demonstram os autores, que um problema de conceituação. Ainda segundo Lopes e Teixeira Jr. (2010, s/p):

> Cyberwars ou ciberguerras, basicamente, são modalidades estratégicas que se caracterizam por objetivos como o de obter informações privilegiadas e/ou desestabilizar determinado sistema gerenciador de informações baseadas em redes de computadores de um ou mais ente estatal, utilizando, para tal, o ambiente cibernético. Logo, tanto pode ser a obtenção ilegal de informações sigilosas de um Estado (ciberespionagem) quanto pode ser uma pane gerada numa infraestrutura informacional tendo como pano de fundo a impossibilidade de um (ou mais) Estado manter contato entre si e os seus.

Existem diversos fenômenos em que os elementos de uma ciberguerra podem ser encontrados e alguns deles serão apresentados e analisados no terceiro capítulo deste trabalho com base no exposto até então e na teoria de Securitização apresentada no próximo capítulo. A partir desta definição, entretanto, é possível destacar, para fins de análise deste trabalho, a presença da ciberespionagem, ou vigilância cibernética[11], como dimensão-chave dos meios pelos quais se constituem um conflito cibernético.

Tais conceitualizações, entretanto, necessitam de um aprofundamento importante para o entendimento da vigilância a partir do momento em que se percebe que as principais análises sobre o tema ficam restritas a estudos técnicos e estratégicos, deixando de lado a evolução histórica da vigilância e seus impactos sociais. David Lyon, na introdução escrita em sua obra conjunta com Bauman, alerta que:

> Se partirmos simplesmente de novas tecnologias ou de regimes regulatórios, poderemos formar uma ideia da amplitude desse fenômeno. Mas será que conseguiremos compreendê-lo? Decerto, ter uma noção da magnitude e da rápida difusão do processamento de dados é fundamental para que a onda de vigilância seja avaliada pelo que ela é; e descobrir exatamente quais chances e oportunidades de vida são afetadas por esse fenômeno irá galvanizar os esforços no sentido de controlá-lo. Mas este diálogo [o livro] tem uma pretensão maior: a de cavar mais fundo – investigar as origens históricas e ocidentais da vigilância atual e sugerir questões éticas, assim como políticas, sobre sua expansão. (BAUMAN & LYON, 2013, p. 9-10)

Sendo assim, nota-se até aqui que de fato há um impacto das TICs atualmente no que tange a segurança dos atores e, especificamente, a vigilância nas mais diversas variáveis, seja na área militar, política, econômica, social, individual, entre outras. Percebe-se, entretanto, que

[11] Enquanto a vigilância está ligada ao ato de vigiar para fins geralmente voltados ao controle da ordem e à segurança, a espionagem é caracterizada pela obtenção de informações sigilosas, geralmente de um inimigo, para fins de vantagens estratégicas. Apesar de possuírem definições distintas, a espionagem não deixa de ser um ato de vigilância e vice-versa, tendo em vista que ao vigiar, não se deixa de obter informações; e ao espionar, utiliza-se dos meios da vigilância.

o ambiente sociotecnológico, onde a vigilância se desenvolve atualmente, não deixa de ser um espaço socialmente construído, que ganha sentido a partir de sua apropriação. Logo, como alertou Lyon, é necessário aprofundar mais na questão da vigilância para se compreender seus efeitos sociais e políticos.

* * *

Como introdução aos estudos da cibersegurança e da vigilância cibernética, este capítulo buscou apresentar brevemente o que é o ciberespaço enquanto uma nova arena das relações sociais e, consequentemente, internacionais. Para tanto, foi necessário percorrer um caminho que partiu desde a compreensão do que é este meio, como funciona, suas características e implicações para as relações entre os atores internacionais, como ele possibilita a construção e reconstrução de novos e velhos conceitos, para, por fim, adentrarmos no que é cibersegurança.

Dessa maneira, tentou-se construir uma base para análise com o fim de entendermos como a vigilância cibernética opera tanto no meio local, controlando as massas e adquirindo dados pessoais importantes, como global, que, de forma quase semelhante, também busca informações que permitam um conhecimento acerca do que os atores internacionais pretendem, quais seus interesses e como irão alcançá-los. Esta diferenciação entre nível local e global, cara às relações internacionais, perde força, entretanto, quando observamos que o ciberespaço propicia uma mundialização de quase todas as relações sociais, seja pela formação de uma cibercultura, de uma inteligência coletiva, ou pelas características globais e sem fronteiras deste espaço.

Como demonstraram Lemos e Levy, essa "nova esfera pública digital não é recortada mais por territórios geográficos (os seus cortes relevantes correspondem antes às línguas, às culturas e aos centros de interesses), mas diretamente mundial" (LEMOS & LEVY, 2010, p. 13), logo, a quebra na rigidez das análises acompanha os próprios fenômenos que cada vez mais fogem aos referenciais tradicionais de que apenas os Estados são atores fundamentais ao sistema internacional.

Antes de adentrarmos nos fenômenos propriamente ditos, é necessário compreendermos o que é essa vigilância globalizada: quais são suas características? Ela realmente só é possibilitada pelo advento do ciberespaço? O que os estudos tradicionais de vigilância podem nos ensinar acerca da sua versão 2.0? Além disso, faz-se necessário ampliar o aporte teórico que nos permita conceber essa vigilância como objeto de preocupação dentre os seus principais

atores. Sendo assim, a teoria da securitização, já citada anteriormente, parece apontar um caminho para esta análise.

2. O PROCESSO DE SECURITIZAÇÃO DO CIBERESPAÇO: VIGILÂNCIA COMO DIMENSÃO-CHAVE

Este capítulo tem como objetivo apresentar a vigilância internacional como um processo social histórico que possui efeitos importantes não apenas nas relações internacionais mas em toda a sociedade e suas práticas, seja na área política, econômica, segurança ou nas relações pessoais cotidianas. Entretanto, a fim de delimitar o escopo destas visões que as ciências sociais nos trazem e aprofundar os estudos nos efeitos que a vigilância promove na segurança internacional e seus fenômenos, a teoria de securitização da Escola de Copenhague é apresentada por fornecer meios para uma análise das ameaças que o ciberespaço pode proporcionar a esta área.

Tendo em vista as características do ciberespaço apresentadas no capítulo anterior, que servirão de base para a apresentação da vigilância e do seu processo de securitização, percebe-se que não apenas a tecnologia influencia nas mudanças sociais que vêm surgindo no ciberespaço, somando-se a esta questão as relações de poder, a apropriação pelos atores e a sua diversidade, seus efeitos que geram uma *cyberpolitik* e um *cyberpower* e, por fim, a própria concepção da necessidade de uma cibersegurança, cara aos novos espaços sociotecnológicos.

São diversos os casos em que este processo é perceptível na arena internacional, tais como as denúncias da existência dos programas de vigilância da NSA[12], responsáveis por uma vigilância a nível mundial de diversos usuários; a aquisição de informações sigilosas do governo brasileiro por essa agência, divulgada por Edward Snowden[13]; a aquisição de dados secretos de governos por organizações não-governamentais como o *WikiLeaks*[14]; e a cessão de dados pessoais para terceiros (incluindo Estados) por parte de empresas como *Google* e *Microsoft*[15] – alguns destes aprofundados no terceiro capítulo.

Sendo assim, inicia-se este estudo com uma breve apresentação da vigilância enquanto dimensão-chave da modernidade e como sua evolução histórica proporcionou um alargamento de suas ações dentro do ciberespaço. Por fim, apresenta-se a teoria de securitização do

[12] Disponível em: <https://.washingtonpost.com/news/wonk/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/> Acesso em: 06 sep 2015

[13] Disponível em: <http://g1.globo.com/tudo-sobre/edward-snowden/Acesso em: 06 sep 2015

[14] Disponível em: <http://noticias.terra.com.br/mundo/estados-unidos/wikileaks-publica-17-milhao-de-documentos-diplomaticos-dos-eua,88137a21e96ed310VgnCLD2000000ec6eb0aRCRD.html> Acesso em: 06 sep 2015

[15] Disponível em: <http://.cartacapital.com.br/internacional/eua-tem-acesso-direto-aos-servidores-de-google-facebook-e-apple-diz-jornal-5976.html> Acesso em: 06 sep 2015

ciberespaço dentro do contexto da vigilância para apreender quais as ameaças latentes para os atores, para, no próximo capítulo, delinearmos algumas considerações acerca dos programas de vigilância perpetrados pela NSA.

2.1 Vigilância: uma dimensão-chave da (ciber)segurança

A vigilância não é um fenômeno novo, tendo sido utilizada pela sociedade muito antes de se imaginar a concepção de um ciberespaço. É caracterizada pelo monitoramento de pessoas, lugares, atividades ou o que quer que se queira vigiar e pode ter diversas finalidades. Sua utilidade nas relações de poder perpassa diversas facetas sociais, partindo da simples função de manter a ordem e a segurança, passando pelo ato de conseguir informações particulares para uso de terceiros, até a persecução de um controle social mais amplo.

Enquanto ferramenta de controle, ganhou notoriedade acadêmica na modernidade, sendo uma das dimensões que explica a disciplina e a punição. Como demonstra Foucault (1988), a vigilância e a disciplina têm papel fundamental ao "controlar a 'alma' para manter o comportamento e a motivação" (BAUMAN & LYON, 2013, p. 55-56). Ao utilizar o panóptico de Bentham para explicar as relações de vigilância e controle na sociedade moderna, o filósofo francês consegue delinear um panorama de análise de extrema relevância até os dias atuais.

O surgimento do ciberespaço, entretanto, impactou o poder de vigilância ao ampliá-lo a níveis globais, saindo da esfera local. Como visto anteriormente, o poder aqui ganha proporções mundiais enquanto a política e seus atos ainda ficam presos ao espaço estatal. Isso causa uma série de incertezas sociais já que a rigidez das estruturas de poder e controle já não é a mesma em algumas situações, principalmente as que envolvem esse novo fluxo da relativização do espaço e do tempo. O panóptico começa então a ser questionado por alguns autores por não conseguir responder às novas demandas, enquanto outros enxergam na verdade a existência de um superpanóptico cibernético que a todos tenta controlar.

Sendo assim, a contemporaneidade e suas características fluidas, que por vezes mantêm aspectos da modernidade e em outras situações dissolve-os, exigem uma explicação das duas visões: uma análise do panóptico de Bentham e da sociedade de controle a fim de compreender a ideia do superpanóptico cibernético; e outra com a visão de um mundo pós-panóptico, que mantém algumas instituições fixas no modelo moderno, mas em certas áreas enxerga a vigilância como um fenômeno mais voluntário que imposto.

2.1.1 O Panóptico de Bentham e a Sociedade de Controle

A fim de compreendermos essa vigilância em escala global, apresentada a partir das novas interações que ocorrem no ciberespaço, é importante tomarmos como referência alguns pressupostos acerca do Estado, do poder e da vigilância para Foucault (1988). Segundo o autor, o Estado não é o único detentor do poder, sendo apenas um dos instrumentos pertencentes ao sistema de poderes, o que dialoga com a análise dos atores do ciberespaço elaborada no capítulo anterior. Logo, é possível inferir que a vigilância do ciberespaço não ocorre apenas pela força do Estado, mas também de outros agentes.

Da mesma forma, o poder não se encontra em nenhum lugar específico da estrutura social, mas está presente em toda essa estrutura através das relações de forças entre os atores. É uma ação constituída por práticas. Estando o poder em todas as camadas sociais, não é percebido por Foucault como algo apenas negativo, mas possui também uma eficácia produtiva, um papel disciplinar. Esse poder que disciplina está em toda parte e age de forma discreta, como demonstra Foucault:

> [...] na oficina, na escola, no exército funciona como repressora toda uma micropenalidade do tempo (atrasos, ausências, interrupções das tarefas), da atividade, (desatenção, negligência, falta de zelo), dos discursos (tagarelice, insolência), do corpo (atitudes "incorretas", gestos não conformes, sujeira), da sexualidade (imodéstia, indecência). Ao mesmo tempo é utilizada, a título de punição, toda uma série de processos sutis, que vão do castigo leve a privações ligeiras e a pequenas humilhações. Trata-se ao mesmo tempo de tornar penalizáveis as frações mais tênues da conduta, e de dar uma função punitiva aos aparelhos aparentemente indiferentes do aparelho disciplinar: levando ao extremo, que tudo possa servir para punir a mínima coisa; que cada indivíduo se encontre preso numa universalidade punível-punidora. (FOUCAULT, 2002, p. 149)

É esse poder disciplinador, através da percepção de um olhar sempre presente e, ao mesmo tempo, oculto, que gera o que o autor chama de autovigilância. O panóptico de Bentham, apresentado por ele, exemplifica essa ideia do olhar constante e anônimo. Segundo o jurista do século XVIII, o panóptico seria uma estrutura arquitetônica circular com vigilantes situados em uma torre no centro. Foi pensado com o intuito de racionalizar a vigilância através de um poder que seria visível (a torre), mas inverificável (o observado nunca saberia se estaria ou não sendo vigiado). Seria, então, o ciberespaço um grande panóptico global, no qual os

atores ali presentes estariam submetidos a este olhar oculto e as relações de força gerariam o poder disciplinador?

Deleuze (1992) vai apontar que a sociedade atual, a sociedade do controle, é, na verdade, a evolução da sociedade disciplinar apresentada por Foucault, tendo em vista que o avanço tecnológico desde meados do século XX proporcionou o surgimento de novas técnicas de vigilância. As tecnologias agora passam a ser móveis, estando em todos os lugares, ubíquas, não sendo mais necessário o confinamento. Segundo Valéria Marcondes (2005), a sociedade de controle teria como base um código (ou senha) individual que dá acesso ou não à informação, havendo uma contraposição dos indivíduos e não mais uma junção em um único corpo. "Não se está mais diante do par massa-indivíduo [estes] tornam-se 'dividuais', divisíveis, e as massas tornam-se amostras, dados, mercados ou 'bancos'" (DELEUZE, 1992, p. 221-222).

Marcondes (2005) ainda aponta três estudos importantes acerca do poder e da vigilância no ciberespaço: um com uma visão *tecnófoba*, ou seja, que vê na evolução da tecnologia a decadência humana; e dois *tecnorealistas*, que tentam analisar o ciberespaço de forma neutra, apontando tanto o lado positivo quanto o negativo. Willian Bogard (1996) enxerga a vigilância no ciberespaço como uma crescente ausência de privacidade gerada justamente pela evolução das tecnologias digitais; é uma hipervigilância em que nada escapa; ela não é apenas uma observação, mas uma interferência direta na vida das pessoas observadas, sendo um instrumento do poder utilizado por atores como as autoridades (o Estado), as empresas (o mercado capitalista) e os *hackers*.

As duas outras visões apresentam os estudos de Diana Saco (2002) e Shapiro (1999) que não negam a visão de Bogard, mas percebem outras possibilidades dentro do ciberespaço. Para Saco, a tecnologia não é neutra e suas consequências não podem ser analisadas como dadas. Enxerga o ciberespaço como um espaço social, em que se criam condições tanto para o surgimento de ativismos democráticos quanto para uma maior vigilância governamental, "não é apenas físico, mas também mental e vivido; é um conjunto de componentes combinados; é um outro espaço, um contra-espaço de relações, interações, ações ou contra-ações; relações também entre espaços, palavras e coisas" (MARCONDES, 2005, p. 76). Sendo esse espaço heterotópico, ambíguo, as novas tecnologias também são vistas como dispositivos de vigilância, sendo o ciberespaço um *superpanóptico* que foge aos limites das instituições disciplinares e abandona a subjetividade por agir através de categorizações humanas "lidas" por uma máquina que constrói um banco de dados sobre cada pessoa.

Quanto à privacidade, há uma grande discussão acerca de até onde vale a pena exigir uma vigilância zero no ciberespaço. Claro que estamos expostos a diversos tipos de invasões

de privacidade como o uso dos dados pessoais (muitas vezes concedidos "inocentemente" pelo próprio usuário) por terceiros, o acesso à situação financeira de um indivíduo e o roubo de dados como o do cartão de crédito. Entretanto, por outro lado, uma exacerbação da privacidade pode abrir caminhos para a corrupção, além de ser uma preocupação do próprio governo que pode deixar de arrecadar certos impostos (MARCONDES, 2005, p. 76).

Assim como Saco, Shapiro (1999) percebe tanto a vigilância quanto as possibilidades de liberdade no ciberespaço, sendo a tecnologia co-moldada pela interação entre as técnicas e as relações sociais, como visto anteriormente. Segundo o autor, o ciberespaço propicia a passagem de certas relações de poder do setor público para o privado, dessa forma, tanto os governos quanto as empresas e o próprio usuário podem definir o que será acessado, o que Shapiro chama de personalização das experiências. Esta característica pode ser uma desvantagem do ciberespaço pois afasta o usuário da realidade social, em um processo de auto alienação, o que, de acordo com o autor, deve ser combatido através da maior interação com a criação de fóruns de debates online sem um *gatekeeper*[16].

Quanto à vigilância, Shapiro (1999) ressalta a existência de um mercado da privacidade, ou seja, diversas empresas oferecem serviços online "gratuitos" em troca de suas informações e, para que ela não faça uso destas, o usuário deve pagar um certo valor. Entretanto, o autor ressalta que não se deve deixar todas essas questões na mão do indivíduo, a "real liberdade requer moderação e um saudável senso de limites: uma mistura entre poder individual e autoridade do Estado" (SHAPIRO, 1999, p. 231), ou seja, há uma necessidade mínima de vigilância a fim de suplantar os males da personalização da experiência online.

Como visto anteriormente, esses pensadores acrescentam novas abordagens ao pensamento de Foucault acerca da vigilância na sociedade cibernética. Enquanto ferramentas do poder, essas tecnologias de fato apresentam força suficiente para suprimir liberdades e impor limites. Apesar disso, a possibilidade de emancipação dentro do ciberespaço é possível e novas oportunidades podem ser criadas para os usuários, ao mesmo tempo em que o superpanóptico parece criar uma vigilância excessiva e propiciar uma aceleração no processo de personalização.

> Somos seres cada vez mais individualizados em meio à multidão. Porém uma individualidade vigiada. Estar sozinho não significa, há muito, ter privacidade, apenas seu um [sic] simulacro.[17] (MARCONDES, 2005, p. 78)

[16] A característica de filtrar e amplificar as informações é o que os estudiosos da área de comunicação denominam de *gatekeepeing*. Tradicionalmente, os *gatekeepers* são os editores das mídias com funções massivas que definem quais dados irão ser repassados ao público. Nas funções pós-massivas, o *gatekeeper* sofre uma mudança radical, passando a ser o próprio usuário, que consome/produz os dados que lhe interessarem.

[17] Imitação, representação; criação de algo que possa parecer real; ilusão.

Nesse sentido, tendo em vista que as relações internacionais são, antes de tudo, relações humanas, o processo de vigilância global no ciberespaço não foge ao seu escopo de estudo. Como visto, as ferramentas de vigilância surgem a partir das relações de poder e no âmbito internacional não é diferente, propiciando ações de atores como os Estados, as grandes corporações, *hackers* e ciberativistas. Entretanto, as relações de força entre esses atores nem sempre são equilibradas. Apesar de as propriedades do ciberespaço propiciarem uma emancipação virtual ao indivíduo que assim o queira, os dispositivos de vigilância aparentam ser mais fortes entre os Estados e as corporações que dominam as técnicas, os fluxos e os meios coercitivos. Mesmo assim, alguns indivíduos, principalmente os *hackers*, parecem cada vez mais romper essa barreira como veremos em exemplos posteriores.

É neste momento que se percebe com certa nitidez uma corrida cibernética entre os atores internacionais na busca por relevância no meio internacional. Sendo a informação uma moeda de grande valor no jogo político, o uso de técnicas de vigilância a fim de obter dados sigilosos parece mesmo ser a próxima grande questão como afirma Assange (2013), e os programas da NSA vêm para comprovar isto. Dessa forma, essa espionagem constante e ininterrupta através de um superpanóptico, possibilitada pelo desenvolvimento de novas tecnologias, seria o meio pelo qual a vigilância agiria no ciberespaço. Entretanto, como visto no início desta seção, a contemporaneidade parece proporcionar uma certa fluidez a esta visão rígida de controle social e as características panópticas da vigilância ganham novas variáveis.

2.1.2 Implicações da contemporaneidade à vigilância: um mundo pós-panóptico?

A modernidade líquida, como denomina Bauman (2001), é o tempo atual em que vivemos, incluindo suas instituições e relações que dão base à contemporaneidade. Segundo o autor, vivemos em uma época de liquidez em que todo o referencial sólido da modernidade é questionado, caracterizando uma lógica do agora, do consumo, do gozo e da artificialidade. Esse processo, claro, gera uma série de inseguranças e incertezas, características marcantes da atualidade. Entretanto, não é uma ruptura com os referenciais modernos, trata-se na verdade de um processo de mudança no qual estamos presentes.

Seja nas relações pessoais e de trabalho, no consumo, no sexo, etc., todas essas questões passam por um processo de desfragmentação e desregulação, perdem seu sentido original e

passam a ser vistas não como algo permanente, sólido, mas como algo momentâneo, que pode durar ou não. Bauman (2001) observa que as relações sociais tornam-se cada vez mais conexões, ou seja, não possuem mais laços rígidos, são frágeis e fáceis de "desconectar". O consumo, o agora, o prazer são a base dessa mentalidade contemporânea e acabam validando as normas e instituições atuais.

O mesmo vale para a vigilância enquanto dimensão-chave da modernidade. O panóptico de Betham apresentado anteriormente representa a tentativa de controle da "alma" a partir de uma imposição, da vigilância contante: é neste ponto que Foucault chama atenção para a visibilidade enquanto perigosa para os indivíduos e como nós mesmos somos corresponsáveis por esta armadilha. Afinal de contas, como afirmam Bauman e Lyon (2013), somente uma análise do porquê nos expomos em redes sociais, usamos cartões de crédito, mostramos nossos documentos, já seria uma análise panóptica de grande relevância.

Apesar disso, percebe-se hoje alguns fenômenos um tanto paradoxais dessa análise panóptica na sociedade líquida, pois, ao mesmo tempo em que há exemplos em que há um panoptismo claro e duro como nas cadeias, nas clínicas psiquiátricas e em programas de vigilância mundial como os da NSA, há uma vigilância aparentemente mais suave como no caso do consumo, em que "se há um poder pan-óptico, ele está a serviço dos marqueteiros, desejosos de induzir e seduzir os incautos" (BAUMAN & LYON, 2013, p. 57). Isto claramente não quer dizer que a ideia panóptica de dominação deixou de existir na sociedade contemporânea, pelo contrário, as TICs deram ferramentas às instituições panópticas que nenhum carcereiro do início do século XX poderia sequer imaginar.

Enquanto o panoptismo continua presente em certas áreas da sociedade como as instituições de confinamento, as técnicas de vigilância em outros campos sociais não mais estão presas a este padrão sólido da modernidade, estando no que poderia se chamar de um estágio pós-panóptico, caracterizado por:

> Tudo – padrões de dominação, filosofia e preceitos pragmáticos de gerenciamento, veículos de controle social, o próprio conceito de poder (ou seja, o modo de manipular probabilidades para aumentar a possibilidade de uma conduta desejável e reduzir a um mínimo as chances do oposto) – parece caminhar na mesma direção. Tudo se move, da imposição à tentação e à sedução, da regulação normativa às relações públicas, do policiamento à incitação do desejo; e tudo assume, a seu turno, o papel principal no que se refere a atingir os resultados desejados e bem-vindos, dos chefes aos subordinados, dos supervisores aos supervisionados, dos pesquisadores aos pesquisados, em suma, dos gerentes aos gerenciados. (BAUMAN & LYON, 2013, p. 59)

Sendo assim, o processo de vigilância e dominação parece estar hoje muito mais vinculado à sedução e à tentação, tendo como referenciais morais e éticos a lógica do agora, do consumo e do prazer, do que à velha imposição coercitiva e manipuladora. Os comportamentos esperados pelos que possuem o poder de vigilância são conseguidos voluntariamente, bem ao estilo "faça você mesmo"; afinal quem hoje em dia vai se negar a ter um celular de última geração que permite trabalhar em qualquer lugar 24h por dia, além de tornar mais fácil a sua localização? Quem não irá ceder dados e informações a empresas que oferecem serviços "essenciais" no meio cibernético como *Google*, *Facebook*, *Microsoft* e *Apple*? Quem não irá postar fotos daquelas férias maravilhosas em suas redes sociais a fim de ganhar muitos "likes" (ou pelo menos grande parte dos usuários irá)?

> Em suma, tal como os caramujos transportam suas casas, os empregados do admirável novo mundo líquido moderno precisam crescer e transportar sobre os próprios corpos seus pan-ópticos pessoais. [...] Tentados pelo encanto dos mercados de consumo e assustados com a possibilidade de que a nova liberdade em relação aos chefes se desvaneça, juntamente com as ofertas de emprego, os subordinados estão preparados para o papel de autovigilantes que se tornam redundantes em relação às torres de vigilância do esquema Bentham e Foucault. (BAUMAN & LYON, 2013, p. 61)

O exemplo pode estar ligado principalmente às relações de trabalho, mas o mesmo se aplica a diversas áreas das relações sociais, como o consumo, as conexões pessoais, o sexo, o próprio uso do ciberespaço enquanto arena sociotecnológica onde parte dessas relações ocorrem. Sendo assim, a cessão de dados, a autovigilância, a permissão concedida aos vigilantes e a vigilância das pessoas ao seu redor (principalmente através das redes sociais atualmente) são encaradas pelos indivíduos quase como naturais e típicas dos tempos atuais, seja pelos "ganhos" que estes obtêm a partir destes consentimentos, pela sensação de segurança que estes atos podem proporcionar e/ou pelo prazer que podem gerar.

É nesse ponto que os autores chamam a atenção para o fato de Foucault ter distinguido disciplina e segurança, sendo, para ele, duas instâncias que não se conectavam. Entretanto, as conexões eletrônicas demonstram que há sim uma ligação:

> A segurança transformou-se num empreendimento orientado para o futuro – agora nitidamente descrito no filme e no romance intitulados Minority Report (2002) – e funciona por meio da vigilância, tentando monitorar o que *vai* acontecer pelo emprego de técnicas digitais e raciocínio estatístico. Como assinala Didier Bigo, essa segurança opera acompanhando "*qualquer coisa que se mova* (produtos, informações, seres humanos)". Assim, a segurança funciona a distância tanto no espaço quanto no tempo, circulando de maneira fluida, juntamente com os Estados-nação, mas para além deles, num domínio globalizado. Tranquilidade e recompensas acompanham esses grupos móveis para os quais essas técnicas são feitas como se fossem "naturais". Processos de estereotipia e medidas de exclusão estão à espera dos grupos desafortunados o

> bastante para serem rotulados de “indesejados”. (BAUMAN & LYON, 2013, p. 12-13)

Este processo de classificação social descrito pelos autores é o que Didier Bigo (2006) chama de ban-óptico, ou seja, parte da ideia de banir, separar, e aqui se aplica muito mais em um contexto de segurança e categorização social. O ban-óptico é caracterizado pelo uso das tecnologias a fim de separar as pessoas “desejadas” das “indesejadas”, ou seja, a partir de perfis sociais distingue-se quem estará sob vigilância mais dura. Isto torna-se claro quando tratamos, por exemplo, do terrorismo: pessoas com traços árabes serão postas sob forte esquema de vigilância se comparadas a pessoas brancas. Como demonstram Bauman e Lyon, as características do ban-óptico são:

> [...] o poder excepcional em sociedades liberais (estados de emergência que se tornam rotineiros), traçar perfis (excluir certos grupos, categorias de pessoas excluídas de forma proativa em função de seu potencial comportamento futuro) e normalizar grupos não excluídos (segundo a crença no livre movimento de bens, capital, informações e pessoas). (BAUMAN & LYON, 2013, p. 63)

O que diferencia o ban-óptico do panóptico de Bentham é que o primeiro está geralmente em espaços transnacionais, de transição, como aeroportos, portos e fronteiras, e a ideia por trás deste dispositivo é manter afastados os indesejados, quanto que no panóptico a lógica é manter dentro e controlado. O que Bauman chama atenção é que geralmente os ban-ópticos guardam os lugares onde a vigilância é do tipo “faça você mesmo”, ou seja, regiões tidas como desenvolvidas ou até mesmo em algumas áreas em desenvolvimento. Dessa forma, se você não tem um cartão de crédito ou um *smartphone*, você não está apto a entrar nas sociedades do tipo “faça você mesmo”; em suma:

> O principal propósito do ban-óptico é garantir que o lixo seja separado do produto decente e identificado a fim de ser transferido para um depósito adequado. Uma vez lá, o pan-óptico garante que o lixo ali permaneça – de preferência, até que a biodegradação complete seu curso. (BAUMAN & LYON, 2013, p. 67)

O mesmo ocorre nas relações entre entes estatais e outros atores internacionais. Enquanto alguns são banidos (principalmente os Estados falidos), outros fazem parte do seleto grupo “faça você mesmo”. Entretanto, ainda há um outro conceito importante para se compreender esse mundo pós-panóptico, o sinóptico de Thomas Mathiesen (1998). Enquanto o panóptico é um sistema de poucos vigiando muitos, o sinóptico apropria-se dos meios de comunicação de massa para cunhar a lógica de muitos que controlam poucos, sendo desnecessário a existência física de uma instituição panóptica para fins de vigilância. Para

Bauman, entretanto, o sinóptico não deixa de ser uma vigilância do tipo "faça você mesmo", mesmo que o termo tenha sido cunhado muito antes do desenvolvimento do ciberespaço e das mídias digitais. Se a ideia é manter uma autovigilância e um autogerenciamento que propicie a entrega voluntária de dados e trabalho, manter essa lógica é papel do sinóptico.

> Evidentemente, o mecanismo para a montagem de minipan-ópticos do tipo "faça você mesmo", móveis portáteis e pessoais, é fornecido comercialmente. Os potenciais internos é que têm a responsabilidade de escolher e adquirir o mecanismo, montá-lo e colocá-lo para funcionar. Embora o monitoramento, a verificação e o processamento da volátil distribuição de iniciativas sinópticas individuais mais uma vez exijam profissionais, são os "usuários" dos serviços do *Google* ou do *Facebook* que produzem a "base de dados" – a matéria-prima que os profissionais transformam nas "categorias-alvo" de compradores potenciais, na terminologia de Gandy – mediante suas ações difusas, em aparência autônomas, embora sinopticamente pré-coordenadas. (BAUMAN & LYON, 2013, p. 73)

Esses profissionais, claro, estão longe de serem comparados aos vigilates do panóptico tradicional, mas são eles que rastreiam os desejos e as tentações dos indivíduos, altamente mutantes, a fim de mantê-los dentro dos comportamentos desejáveis a partir de uma lógica sinóptica. São os marqueteiros que vendem as nossas próprias vontades e um marketing eficiente, deve possuir características tanto sinópticas quanto ban-ópticas, categorizando quem de fato pode consumir ou não.

Sendo assim, a vigilância contemporânea recebe novos meios de ação caracterizados justamente por essa modernidade líquida que questiona valores e instituições de uma modernidade anterior, sólida. Como visto, o mundo pós-panóptico traz uma série de novas categorias de análise para a vigilância no ciberespaço que leva em consideração não apenas a vigilância cercada em um grande superpanóptico digital, mas também a sinóptica e ban-óptica que nos auxiliam a compreender esse tipo de comportamento "faça você mesmo" muito presente entre os atores que fazem uso dos espaços sociotecnológicos.

Dessa maneira, os autores fornecem categorias que conectam características sociais contemporâneas às novas tecnologias e que impactam no estudo da vigilância internacional em algumas de suas vertentes. São essas categorias que nos permitem compreender não apenas o porquê de alguns usuários fornecerem seus dados de forma tão disciplinada e não questionadora, mas também como estes atores adentram e participam do processo de vigilância, sendo eles próprios alvo e vigilante, seja dentro da lógica da vigilância "faça você mesmo", do ban-óptico ou do sinóptico. Isto fica claro quando observamos a cessão de dados a empresas ou quando categorizamos socialmente certos grupos e os banimos (tais como os árabes serem os principais terroristas para alguns grupos sociais).

Apesar das preocupações latentes com a segurança cibernética, com a privacidade dos usuários e com a governança do ciberespaço, muitos dos discursos também prezam pela existência de uma vigilância menos dura, e muitos dos atores corroboram e perpetuam tal condição. É por isso que hoje diversas ameaças recebem respostas distintas: ao mesmo tempo em que os programas da NSA e sua vigilância global são vistos como ameaçadores à segurança e aos direitos dos Estados e do próprio indivíduo, há uma interpretação de que o vazamento de documentos sigilosos por organizações como o *WikiLeaks* seria na verdade um ritual democrático e necessário[18]; ora, não seriam esses dois fenômenos formas da mesma vigilância? Estas contradições, características da modernidade líquida, tornam-se relevantes, assim, para os estudos acerca da vigilância.

* * *

Seja através de um superpanóptico ou dos novos meios de controle advindos da modernidade líquida apresentada por Bauman e Lyon (2013), a vigilância cibernética mostra-se presente como uma das grandes ameaças da contemporaneidade. Como visto, há muito as relações internacionais já foram afetadas pelas características do ciberespaço e de sua apropriação, e a vigilância, que ganha novos músculos com o advento das TICs, não foge a esse campo.

Exemplos de conflitos, caracterizados como ciberguerras (mesmo que uma guerra virtual de grandes proporções de fato ainda não tenha tomado forma), temos aos montes. Enquanto ataques diretos a sistemas que colocaram a segurança da sociedade em risco, temos exemplos ainda incipientes como os ataques *DDoS*[19] e os *worms*[20] como o *Stuxnet*, tido como o ataque cibernético mais bem sucedido até então ao colocar em inoperância usinas de enriquecimento de urânio do Irã (LOBATO & KENKEL, 2015). Já como método de espionagem e vigilância, os exemplos já citados até aqui demonstram um desenvolvimento tecnológico avançado e uma apropriação da vigilância que não vê mais apenas os Estados e

[18] Para mais informações sobre o tema: PAIT, Heloisa & PINHEIRO, Ruan. Vazamento de informações: um ritual democrático na era da comunicação em rede. In: **Cadernos Adenauer: Cibersegurança**, Rio de Janeiro, n. 4, p. 09-32, 2014.

[19] Um *DDoS* (ataque de negação de serviço) é caracterizado por tornar os recursos de um sistema indisponíveis para seus usuários.

[20] *Worm* é um programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o *worm* não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar.

outros setores burocráticos como os únicos (ou mais importantes) agentes securitizadores (*WikiLeaks*, *hackers*, os próprios usuários, entre outros).

Sendo assim, uma análise a partir da securitização da Escola de Copenhague parece nos permitir uma perspectiva de como essas ameaças surgem e do porquê de o ciberespaço ter se tornado uma arena securitizada, tendo em vista a percepção crescente da existência de ameaças permanente nesse novo tabuleiro, no qual, em pleno século XXI, os agentes já não podem se recusar a estar. Dessa forma, a securitização do ciberespaço, tornando-o um novo *front* de conflitos no qual a vigilância torna-se uma arma de extrema importância, apresenta-se como consequência desse processo. Logo, apresenta-se a seguir uma breve explanação da perspectiva de securitização a fim de contemplar este processo pelo qual o ciberespaço vem passando.

2.2 O Processo de Securitização do Ciberespaço e da Vigilância Cibernética

Como visto no primeiro capítulo deste trabalho, a ideia do que é segurança nas Relações Internacionais é vasta e altamente debatida. Existem diversas teorias que buscam compreender este conceito-chave para a área, que estão imbuídas por questões filosóficas, epistemológicas, ontológicas e até mesmo históricas e geográficas. Para este trabalho, entretanto, a visão de segurança da Escola de Copenhague parece auxiliar na compreensão de como os atores internacionais passaram a visualizar o ciberespaço como uma arena de ameaças mútuas.

O crescimento do construtivismo e o debate epistemológico no pós-Guerra Fria foram essenciais para o surgimento da perspectiva de securitização de áreas antes não observadas como foco dos estudos de segurança pelas teorias do *mainstream*, já que o conceito estava sempre ligado à agenda de *hard power*. Sendo assim, a Escola trouxe novas perspectivas para tais estudos, contribuindo principalmente em três áreas: conceito de securitização; unidades de análise; segurança multissetorial (DUQUE, 2008).

Assim como na teoria construtivista, o conceito de securitização na Escola de Copenhague parte da premissa que o mundo é socialmente construído. Sendo assim, Buzan, Waever e Wilde (1998), principais autores da Escola, demonstram que as ameaças e os receios também são moldados através de discursos e percepções construídos no seio das relações sociais, ou seja, é um processo que parte da intersubjetividade e não da objetividade racionalista.

O processo de securitização de um tema parte de atos de fala[21], ou discursos de securitização. Esses atos, por si só, são um meio de ação pois acarretam um grau de intersubjetividade tanto dos que proferem quanto dos que interpretam tais discursos. Dessa forma, algo só é securitizado quando o público (geralmente a opinião pública) aceita o discurso enquanto ameaça ou receio e demanda uma reação de seu agente, tirando o tema securitizado da esfera normal das relações políticas, tratando-o de forma emergencial e tomando as devidas ações que podem, ou não, incluir o uso da força (BUZAN *et al*, 1998).

Entretanto, é importante ressaltar que o uso inapropriado da perspectiva de securitização pode contribuir também de forma negativa, aumentando a sensação de insegurança e levando a formação de políticas devastadoras levando em conta a segurança dentro de um tema relacionado (BIGO, 2006). Isto ocorre justamente por esta perspectiva permitir que diversos temas sejam alçados aos debates internacionais de segurança a partir de atos de fala que seduzem a opinião pública e permitem que os agentes interessados ajam de forma inapropriada. Um bom exemplo desta situação foi a Guerra do Iraque de 2003[22].

Em relação às unidades de análise, Buzan, Waever e Wilde (1998) ressaltam três: 1) os objetos referentes, ou seja, aquilo que está sendo ameaçado e que possui legitimidade para clamar por sobrevivência (tradicionalmente o Estado, mas não o único, especialmente no caso do ciberespaço); 2) os atores securitizadores, que iniciam o processo de securitização utilizando principalmente o discurso para delimitar a ameaça ao objeto referente; 3) os atores funcionais, cujo papel é ter influência suficiente no tema securitizado, mas não ser o objeto nem o agente iniciador.

A abordagem multissetorial trazida pelos autores da Escola de Copenhague faz uma separação analítica entre os setores militar, político, econômico, societal e ambiental. Enquanto as áreas política e militar sempre foram priorizadas durante o período da Guerra Fria, concebia-se a ideia de que a segurança estaria necessariamente ligada a esses dois setores; a expansão apresentada por Buzan, Waever e Wilde (1998), demonstra que outros nichos também são fonte de processos de securitização, como o econômico, o societal e o ambiental.

Para fins de análise do trabalho, os setores militar, político, econômico e societal mostram-se de grande relevância no processo de securitização do ciberespaço.

[21] Entende-se aqui por atos de fala os discursos em que as sentenças ditas são percebidas enquanto ações. Estes atos podem ser locutórios, ou seja, a fala de uma sentença, ilocutórios, a intenção desse discurso, e perlocutórios, o efeito do ato de fala (BUZAN *et al*, 1998).

[22] A Guerra do Iraque de 2003 foi um dos braços do combate ao terrorismo perpetrado pelos EUA após os ataques de 11 de setembro. Os discursos ameaçadores de que o Iraque de Saddam Hussein estaria construindo armas de destruição em massa realizado por representantes do governo estadunidense acabou exacerbando a realidade iraquiana e construindo uma ameaça irreal (DUQUE, 2008).

Tradicionalmente, o setor militar sempre esteve envolvido com o Estado e com as Forças Armadas; o político, com questões de soberania e ideologia; o econômico ligado a objetos referentes supranacionais, como regimes e mercado, ou a atores não-estatais como corporações trans/multinacionais, consumidores, entre outros; já o societal, percebido mais recentemente, está ligado ao surgimento de identidades coletivas que possuem um funcionamento independentemente do Estado, tais como nações, religiões, ou uma inteligência coletiva global e conectada como visto anteriormente.

Sendo assim, e tendo como base os conceitos apresentados pela Escola de Copenhague, é possível perceber um processo de securitização do ciberespaço e da vigilância cibernética através da retórica dos principais atores que geram ameaças dentro do mundo virtual. Como visto, entretanto, os atores presentes no ciberespaço, enquanto uma arena global e interconectada, não se restringem apenas aos Estados, sendo percebidos diversos outros agentes tais como organizações estatais e não-estatais, corporações, forças militares, sociedade civil e até mesmo indivíduos agindo sozinhos. Como demonstram Lobato e Kenkel (2015):

> Discursos sobre segurança do ciberespaço exigem um alargamento do conceito tradicional de segurança que foca apenas no poder militar e na habilidade do Estado de enfrentar ameaças (Walt 1991). A incorporação das tecnologias de informação nos conflitos de guerra contemporâneos, operações de hackers, ameaças aos dados e à privacidade dos usuários, e o interesse civil e militar na área, tudo justifica o espaço crescente que a cibersegurança tem ocupado no campo da segurança internacional. (LOBATO & KENKEL, 2015, p. 30, tradução nossa)

Dessa forma, nos quatro setores supracitados, é possível demonstrar diversos exemplos da construção desse processo de securitização. Na área militar, o uso de armas como a espionagem, a derrubada de sistemas de informação, entre outras é algo já existente ocasionando o que muitos autores chamam de ciberguerra, como visto no capítulo anterior. Já no setor político, os discursos de soberania estatal ainda estão presentes, principalmente no que tange as regras de uso do ciberespaço em território nacional, além das ameaças geradas por atos de fala contrários ou a favor do uso militar no ciberespaço.

No meio econômico, a presença de grandes corporações que oferecem serviços em troca de dados de usuários em uma lógica de mercado, que vigiam as ações destes dentro do ciberespaço e que muitas vezes repassam esses dados a outros atores como os Estados, mostram-se como importantes agentes desse processo. Por fim, o setor societal aparece como a base da securitização, tendo em vista ser o grande agente construtor desta arena virtual, sendo alvo e/ou agressor, nesse processo constante de criação de uma identidade, de uma inteligência

coletiva, por vezes não consciente, que acaba gerando novas oportunidades, mas também ameaças.

Estes quatro setores, entretanto, são acrescidos de um setor específico das questões que analisam a securitização do ciberespaço. Segundo Hansen e Nissenbaum (2009), um ciber-setor já teria alcançado as condições necessárias para tornar-se um campo específico das análises dentro da lógica da Escola de Copenhague. Suas características, que auxiliam na compreensão da vigilância cibernética enquanto um tema securitizado, serão apresentadas em conjunto com os outros setores no decorrer deste capítulo.

2.2.1 Setor militar

A questão que vem redefinindo o cenário internacional não é a revolução comunicacional em si, mas o massivo fluxo de dados decorrente das formas de apropriação do ciberespaço e a tentativa de controle dos meios de transmissão destas informações: "para conquistar o poder é preciso ter o poder da informação e ter o poder significa também ter em mãos o sistema de informação e de discursos dominantes no cenário internacional" (VALENTE, 2007, p. 41). Logo, a dominação da informação por parte dos atores, principalmente daqueles politica e economicamente mais poderosos, não se delimita apenas ao mundo virtual, mas também está diretamente ligada ao mundo físico.

Segundo Assange (2013), as redes de fibra óptica – os cabos por onde os dados da *internet* trafegam – estariam sendo arquitetadas de forma que o fluxo de informações perpasse as fronteiras dos países hegemônicos, fazendo com que a captação dos dados enviados pela rede mundial de computadores seja um trabalho mais fácil para os serviços de inteligência e para as corporações que ali estão. É possível citar dois exemplos importantes desse fenômeno: o primeiro seria o *backbone*[23] da América Latina que passa diretamente pelas fronteiras dos EUA; e um segundo exemplo seria a construção do *backbone* africano pela China que possui fortes interesses econômicos no continente.

Uma ressalva importante, entretanto, é a existência da criptografia como forma de resguardar a segurança das informações enviadas pela rede. A criptografia tem o poder de codificar as informações que só poderão ser decodificadas pelo receptor caso este possua uma

[23] "Espinha dorsal" da internet, por onde todos os dados enviados em um determinado país trafegam.

"chave" para tal fim. O que o criador do *WikiLeaks* ressalta, todavia, é que muitos países em desenvolvimento, incluindo o Brasil, acabam adquirindo hardwares (a parte física usada em computadores) e softwares (o programa instalado) de corporações que possuem ligação direta com os atores interessados em adquirir tais informações criptografadas, causando sérias dúvidas quanto à segurança internacional: como garantir que dados secretos não sejam espionados através de uma vigilância global do ciberespaço, ou que o sistema informacional não seja destruído em uma ciberguerra?

Como consequência dessa dominação física dos meios de transmissão de dados pela *internet*, os Estados e as corporações (que muitas vezes detêm o mesmo interesse no caso da *internet*, o de adquirir informações e vigiar os usuários) começam então a especializar-se nas capacidades de ação dentro do mundo cibernético, dessa forma, "o ciberespaço se torna um novo *front* para atividades de inteligência, contrainteligência, sabotagem e terrorismo" (LOPES & TEIXEIRA JR., 2011). É justamente a finalização do processo que Assange (2013) chamou de "militarização do ciberespaço". Entretanto, é importante salientar que não são apenas estes atores que fazem parte do processo de vigilância do ciberespaço, como visto anteriormente. Organizações não-estatais e até mesmo indivíduos agindo por conta própria também estão presentes nessa rede de vigilância, seja com intuito de adquirir informações, de emancipar-se ou de atacar um alvo por questões meramente pessoais, mas que afetam de alguma maneira a segurança internacional.

O Estado e as corporações não são os únicos atores capazes de agir na vigilância cibernética do meio internacional, justamente pelas características do ciberespaço já apontadas até então. Como visto, a ubiquidade e a convergência acabaram gerando um espaço de todos que libera os polos emissores, mesmo que ainda haja uma vigilância social constante, mas não necessariamente em estilo panóptico. É, de certa forma, a ideia que Shapiro (1999) chamou de personalização, juntamente com a possibilidade de emancipação e de adquirir controle sobre as emissões e recepções.

Tornam-se cada vez mais perceptíveis casos em que a vigilância é exposta através do roubo de informações, da desativação de sistemas, de ataques a centros de dados ou da organização rápida de grandes manifestações; sejam estes casos perpetrados por organizações de *hackers*, por Estados, por grandes corporações ou por usuários comuns.

Casos recentes como o vazamento de mais de 1,7 milhão de documentos diplomáticos estadunidenses pelo *WikiLeaks* que abalaram as relações com diversos países[24]; a acusação de que grandes corporações da *internet* como *Facebook*, *Google* e *Microsoft* estariam compartilhando informações de seus usuários com o governo dos EUA[25]; a organização de grandes manifestações em todo o mundo (como a Primavera Árabe e o movimento brasileiro de julho de 2013) coordenadas rapidamente em redes sociais[26]; a revelação de Edward Snowden em meados de 2013 acerca da grande máquina de vigilância global dos EUA, os programas da NSA que utilizam-se do ciberespaço a fim de adquirir informações acerca de alvos estatais, empresariais e individuais; e o roubo e divulgação na *internet* no final de 2014 de informações sigilosas da *Sony Pictures*, o que gerou um jogo de forças nas relações de poder, tendo os EUA acusado a Coreia do Norte de realizar o ataque, mesmo que um grupo de *hackers* tenha assumido a responsabilidade e o país asiático se eximido da culpa[27].

Questões como essa trazem à tona o debate sobre as intenções de países como EUA, China, Rússia, de corporações como *Facebook*, *Google* e *Microsoft*, e de outros atores como o *WikiLeaks*, ao adquirir informações sigilosas através da vigilância cibernética. Os EUA, por exemplo, continuam a utilizar o discurso contra o terrorismo como forma de embasar suas ações, desrespeitando muitas vezes normas internacionais, mas a obtenção da informação vai muito além do combate ao terror, podendo ter adquirido dados que dizem respeito a projetos de indústria nacional ou intenções políticas e econômicas que podem vir a favorecer o governo americano.

Sendo assim, fica claro que os ataques ocorridos dentro do ciberespaço, como os citados acima, acabam por trazer consequências para a segurança internacional. Como visto anteriormente, Shapiro (1999) demonstra que um pouco de vigilância é necessário para uma relação saudável entre os atores no ciberespaço, mas o crescimento do medo de ter informações roubadas através desta vigilância constante e inverificável, e o receio de perder grandes parcelas de privacidade faz com que estes atores busquem munir-se com as armas existentes a fim de evitar possíveis ataques externos.

---

[24] Disponível em: <http://noticias.terra.com.br/mundo/estados-unidos/wikileaks-publica-17-milhao-de-documentos-diplomaticos-dos-eua,88137a21e96ed310VgnCLD2000000ec6eb0aRCRD.html> Acesso em: 06 sep 2013

[25] Disponível em: <http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html> Acesso em: 06 sep 2013

[26] Disponível em: <http://exame.abril.com.br/rede-de-blogs/o-que-te-motiva/2013/06/19/primavera-arabe-e-outono-brasileiro/> Acesso em: 06 sep 2013

[27] Disponível em: <http://g1.globo.com/tecnologia/noticia/2014/12/eua-indicam-coreia-do-norte-como-responsavel-pelo-ataque-sony.html> Acesso em: 20 dez 2014

2.2.2 Setor político

O processo de militarização está intimamente ligado à politização das relações no ciberespaço. Tendo em vista as consequências do ciberespaço para as Relações Internacionais e o surgimento da concepção da *cyberpolitik*, já apontados anteriormente, as relações de poder e os discursos provenientes dos atos de fala demonstram com certa nitidez a existência de um *cyberpower* que perpassa as relações dos agentes tanto dentro do espaço virtual quanto externamente, no ambiente físico, quando assuntos referentes ao ciberespaço.

A própria discussão tradicional de defesa do Estado e da soberania também permeia a retórica do *cyberpower*. A busca pela normatização do uso do ciberespaço (e aqui principalmente da *internet*) pelos órgãos estatais dentro das fronteiras nacionais, a criação de um regime internacional da *internet* que resguarde os direitos humanos e a proeminência estatal, o uso legítimo da força (virtual ou não) como resposta a acusações de espionagem ou a ataques cibernéticos, entre outros exemplos, demonstram como alguns dos discursos que acabam gerando a securitização dessa arena ainda estão ligados à defesa do Estado enquanto ator mais relevante.

Apesar disso, é cada vez mais frequente a influência política de outros atores não estatais. As corporações são peças-chave nas relações de poder no ciberespaço, tendo em vista sua própria evolução e o seu funcionamento baseado no papel de diversas empresas. Como demonstra Lucero (2011), o complexo sistema de funcionamento da *internet* é mantido atualmente pelo setor privado em sua grande maioria, através de uma concessão dos EUA. Essa proeminência privada acaba sendo a base de muitos dos discursos de defesa do papel do Estado tanto na manutenção da *internet* como na criação de um regime internacional aos moldes tradicionais (Estados e Organizações Internacionais). A vigência atual, entretanto, também possui seus interesses e seu poder de barganha e não está disposta a ceder sua participação aos Estados sem a devida compensação de suas perdas.

Da mesma forma que as corporações, outras organizações não-estatais e indivíduos como ONGs, grupos ciberativistas, *hackers* e delatores (como o Edward Snowden) também ganham espaço na retórica do meio virtual, auxiliando no processo de securitização desse espaço. O grupo *WikiLeaks* é um dos exemplos desse fenômeno; ao adquirir informações secretas dos EUA e divulgá-las, causou uma série de constrangimentos internacionais que levaram à condenação nos EUA de alguns de seus membros, incluindo Julian Assange, um dos

líderes do movimento que se encontra refugiado na embaixada do Equador em Londres desde o ano de 2012.

De forma semelhante, o caso Snowden, também envolveu a divulgação de informações secretas estadunidenses, no caso, provas da espionagem em diversos países e empresas, incluindo o Brasil, a presidente Dilma Rousseff e a empresa Petrobrás. A diferença, entretanto, está no método de apreensão das informações: enquanto Assange utilizou formas de *hackear*[28] o governo estadunidense, Snowden trabalhava na Agência Nacional de Segurança e tinha acesso às informações, delatando o ocorrido.

Nos dois casos, o que se apreende no que diz respeito à securitização da arena virtual são os discursos proferidos por grupos civis de *hackers* ou por cidadãos com acesso a informações confidenciais (experts) que atingem o patamar de discussões da agenda internacional. As consequências do caso Snowden, por exemplo, para os debates acerca da segurança virtual alcançaram a Assembleia Geral da ONU e o maior empenho de alguns países (Brasil dentre estes) em formular um regime internacional com princípios e normas claras de funcionamento e manutenção.

Sendo assim, a retórica acerca da espionagem cibernética ganha força política e legitimidade de alcance global. Os discursos presentes acabam construindo uma nova ameaça perceptível no ciberespaço e que deve ser condenada e combatida internacionalmente, mesmo que muitos dos atores façam uso de tal ferramenta militarizada.

O setor político, dessa forma, apresenta-se como um dos pilares que auxiliam na compreensão da securitização do ciberespaço, tendo em vista os discursos apresentados no cenário internacional acerca das ameaças e vantagens que esta arena apresenta. Está conectado ao setor militar por propiciar ao mesmo tempo base legítima (socialmente legitimada) para a defesa e para a agressão.

2.2.3 Setor Econômico

[28] *Hackear* é o ato de modificar um sistema de informática, seja o dispositivo (hardware), os programas (software) ou uma rede de computadores, através dos conhecimentos técnicos necessários. O termo vem do verbo em inglês *to hack* que significa cortar de forma grosseira e de seu substantivo, *hack*, ou solução improvisada (gambiarra) em português.

O setor econômico possui grande importância na securitização do ciberespaço, afinal, como visto anteriormente, a base de funcionamento da rede está nas mãos do setor privado, mesmo que como forma de concessão pelos EUA. Segundo Lucero (2011), há uma grande discussão tanto no meio acadêmico quanto nas organizações internacionais que tratam sobre o tema acerca da existência de um possível regime de governança da *internet* baseado principalmente no setor privado.

A própria evolução da *internet* possui fortes conexões com este setor. Durante a expansão da rede na década de 1990, criada inicialmente com fins militares e acadêmicos em meados da década de 1960, as empresas de tecnologia foram as grandes interessadas nesse processo, tendo em vista que dependiam da padronização para a exploração comercial. Sendo assim, os anos 90 foram marcados pela construção de um "regime" técnico liderado pelo setor privado.

Mesmo com o aumento de debates a nível internacional em que os Estados vêm demandando maior participação nesse processo, até hoje observa-se a proeminência do setor econômico no que tange às normas e princípios de conexão à rede: estabilidade, competição, coordenação privada e representação. A solução apresentada para a questão da coordenação, o grande debate dos anos 90, foi a criação da ICANN (Corporação da *Internet* para Atribuição de Nomes e Números) em 1998, uma organização privada sem fins lucrativos que pôs fim à "Guerra do DNS"[29] e deu início a uma nova fase da padronização mundial de protocolos de comunicação, vigente atualmente.

Dessa forma, todos os debates internacionais, o que acaba envolvendo uma série de discursos securitizadores, possuem entre seus atores uma forte presença do setor econômico que busca defender seus interesses na área. Não é à toa que parte das preocupações ligadas à securitização do ciberespaço e da vigilância cibernética estão relacionadas ao poder que as grandes corporações possuem no que tange à utilização da *internet* pelos usuários, tais como a própria ICANN (alvo de grandes críticas por parte de alguns Estados que não concordam com a proeminência do setor privado e dos EUA), o *Google*, o *Yahoo*, o *Facebook* a *Microsoft* e a *Apple*.

Quando se trata exclusivamente de vigilância cibernética, a influência do setor econômico é fundamental para se compreender o processo de securitização. Excluindo a ICANN (que possui uma responsabilidade técnica, de padronização), as outras empresas

[29] Do inglês *Domain Name System*, é o sistema que permite que nós humanos consigamos compreender os números dos protocolos de comunicação correspondentes aos dados que acessamos na internet. A "Guerra do DNS" refere-se aos debates acerca de sua padronização.

supracitadas são apontadas como as grandes responsáveis pelo armazenamento de dados de usuários que acabam utilizando seus serviços de forma voluntária por uma série de necessidades externas como demonstraram Bauman e Lyon (2013) anteriormente.

Acusações[30] apontam que essas empresas são responsáveis pelo repasse desses dados a terceiros, incluindo Estados interessados e outras corporações, o que amplia o escopo de vigilância e controle desses atores. A questão que muitos internautas desatentos não percebem é que grande parte desses dados repassados possuem autorização do próprio usuário do serviço ao aceitar as políticas da empresa sem ao menos ler quais são. Um exemplo claro disso foi a recente alteração nos termos de uso do Instagram, rede social de fotos pertencente ao *Facebook*, na qual todas as fotos publicadas ali passam a pertencer à empresa e não mais ao fotógrafo[31].

Dessa forma, percebe-se que o setor econômico, representado principalmente pelo "regime" técnico de governança da *internet* e pelas grandes corporações da área de tecnologia que agem no ciberespaço, pode ter seu papel dentro do processo de securitização tanto como um objeto referente, quanto como um ator securitizador ou funcional, tendo em vista sua importância neste meio, tornando-o tanto alvo quanto fomentador de ameaças. Logo, a análise da retórica neste campo mostra-se necessária tendo como fim uma maior abrangência na compreensão do processo de securitização do ciberespaço.

2.2.4 Setor Societal

Apesar de todo o conhecimento proporcionado pela revolução tecnológica informacional, não é possível afirmar que este é um processo universal e uniforme, principalmente no que tange à formação de uma identidade coletiva cibernética. Muitas sociedades ainda não fazem parte deste mundo digital, outras estão em processo de implementá-lo e poucas podem se denominar completamente informatizadas, ou ainda digitalmente letradas, como explica Henry Jenkins (2008) ao se referir à capacidade de discernimento e maturidade com relação a todas as opções de escrita que o ciberespaço possibilita ao usuário.

Autores como Hall (1992), Bauman (1999), Castells (1999), Wallerstein (2000), Cruz (2004), entre outros, já discutiram acerca do processo de globalização e da sua face excludente,

[30] Disponível em: <http://.cartacapital.com.br/internacional/eua-tem-acesso-direto-aos-servidores-de-google-facebook-e-apple-diz-jornal-5976.html> Acesso em: 06 sep 2015
[31] Disponível em: <https://tecnoblog.net/120608/instagram-termos-servico/> Acesso em: 06 sep 2015

em que sociedades economicamente pobres acabam ficando à margem deste processo. Entretanto, vale salientar que mesmo as sociedades excluídas acabam tendo contato com os novos processos, devido principalmente ao seu caráter expansivo, pervasivo, de difícil controle e muito mais social que tecnológico, o que acaba levando a tais sociedades ideias e pensamentos de diversos locais distintos, transformando-se, assim, em um processo de *glocalização*. Segundo Ulrich Beck (1999), este é um processo no qual o global e o local não se excluem, mas intercalam-se, fazendo com que as ideias trazidas pela globalização sejam traduzidas em um contexto local. Jesús Martín-Barbero (2010) afirma que:

> [...] o novo sentido que o local começa a ter nada tem de incompatível com o uso das tecnologias comunicacionais e das redes informáticas. Hoje essas redes não são unicamente o espaço no qual circulam capital, as finanças, mas também um lugar de encontro de multidões, de minorias e comunidades marginalizadas ou de coletividades de pesquisa e trabalho educativo ou artístico. (MARTÍN-BARBERO, 2010, p. 59)

Apesar de o mundo estar cada vez mais conectado ao ciberespaço, principalmente através da *internet*, ainda é possível perceber um grande abismo entre os Estados desenvolvidos e os em desenvolvimento[32]. Existem diversos fatores que explicam esta discrepância, mas o baixo investimento em tecnologias informacionais e comunicacionais nos países mais pobres faz com que o preço final para a população destes Estados seja elevado. Dessa forma, observa-se nos países em desenvolvimento o grande uso de *lan houses* e de celulares com *internet* importados da China – mais acessíveis à população de baixa renda – tornando difícil mensurar as reconfigurações sociais oriundas do processo de penetração na cibercultura.

Sendo assim, apesar de o processo de globalização deixar de lado parte da população mundial, a expansão do ciberespaço parece alcançar diferentes públicos, surgindo, assim, uma cibercultura e uma inteligência coletiva a nível quase global. Tais questões implicam em uma série de impactos para o processo de securitização, tendo em vista que tudo parte de uma construção social, das realidades intersubjetivas que são co-construídas ao longo do tempo. Logo, a formação de identidades fora do âmbito estatal pode gerar ameaças à segurança internacional.

Exemplos desse processo não faltam. A Primavera Árabe e a revolta de milhares de pessoas que agiram coletivamente em âmbito internacional também através do ciberespaço é um destes. O surgimento de grupos de *hackers* que, independente da nacionalidade, unem-se

[32] Não existe uma definição oficial do conceito de países desenvolvidos e em desenvolvimento, entretanto, refere-se a Estados desenvolvidos como aqueles com altas taxas de crescimento econômico, de industrialização, de segurança e de desenvolvimento humano, enquanto que os em desenvolvimento são caracterizados por possuírem taxas inferiores se comparadas às dos desenvolvidos.

por possuírem objetivos e interesses comuns, tais como os *Annonymous*. Logo, é perceptível uma participação cada vez maior da sociedade civil e de alguns indivíduos enquanto agentes influentes no processo de securitização do ciberespaço e na construção dos discursos internacionais sobre o tema.

2.2.5 O Ciberespaço como setor autônomo

Apesar de uma análise a partir destes 4 campos já se mostrar importante no que tange a securitização do ciberespaço, Hansen e Nissenbaum (2009) ainda ressaltam que a segurança cibernética por si só já teria alcançado o patamar de um novo setor na abordagem multissetorial da Escola de Copenhague que dialoga diretamente com os demais:

> Muito no entanto mudou desde que a Escola de Copenhague fez esta avaliação [os cinco setores]: a segurança cibernética encontra-se securitizada com sucesso como evidenciado por desenvolvimentos institucionais tais como o estabelecimento da Comissão de Proteção de Infraestrutura Crítica pelo presidente Clinton em 1996, o posicionamento proeminente da segurança cibernética dentro do Departmento de Segurança Interna [dos EUA], a formulação pelo presidente Bush da Estratégia Nacional para a Segurança do Ciberespaço em 2003, e a criação de um centro de defesa cibernética apoiado pela OTAN na Estónia em 2008. Mas também não é possível manter a visão da segurança cibernética como isolada de outros setores da segurança. De fato, nas palavras de Rachel E. Yould (2003: 78) "parece que ele pode ser o fator subjacente comum sobre a qual todos os setores de segurança estão destinados a convergir". (HANSEN & NISSENBAUM, 2009, p. 1157, tradução nossa)

A teorização que Hansen e Nissenbaum (2009) trazem reforça a ideia de que o ciberespaço *de facto* já é um espaço totalmente securitizado e que traz características próprias às questões que envolvem a segurança internacional. Para os autores, há três padrões de segurança dentro deste setor: a hipersecuritização (*hypersecuritization*), está ligada a lógica do efeito em cadeia, ou seja, fenômenos que ocorram dentro do ciberespaço podem ter consequências em outros setores importantes como o militar, o político, o societal e o financeiro, elevando, assim, a securitização a níveis de risco e ameaça além do padrão.

Outro padrão seriam as práticas de segurança do dia-a-dia que podem dar base a sensação de uma hipersecuritização, tendo em vista que são as pequenas ameaças diárias que podem gerar preocupações maiores, tais como o receio de ser infectado por um vírus de computador. Segundo Lobato e Kenkel (2015), este padrão está diretamente ligado à

responsabilidade dos usuários (alvos das práticas diárias) enquanto audiência desses discursos ameaçadores, por possibilitarem tanto o aumento quanto a redução da sensação de insegurança no ciberespaço.

O terceiro padrão, da tecnificação (*technification*), é o espaço relegado aos discursos dos técnicos na área, das pessoas com reconhecido grau de conhecimento técnico sobre o ciberespaço. Como demonstram Lobato e Kenkel (2015), eles acabam legitimando a cibersegurança quando apoiam discursos de hipersecuritização e influenciam a opinião pública: "a mobilização da tecnificação dentro da lógica da securitização é, dessa forma, o que permite a constituição particular de autoridade epistêmica e legitimidade política" (HANSEN & NISSENBAUM, 2009, p. 1167, tradução nossa). É esta autoridade que legitima o "bom conhecimento" dos técnicos *vs.* o "mau conhecimento" dos *hackers*.

Acerca dos objetos referentes desse processo, Lobato e Kenkel (2015) afirmam que:

> Enquanto Hansen e Nissenbaum (2009) consideram interconectividade uma idiossincrasia que une uma constelação inteira de objetos referentes, pode-se inferir que as redes que determinam sistemas e serviços constituem um objeto referente comum aos cenários de hipersecuritização, de práticas do dia-a-dia e de tecnificação. Isto não é dizer que não há objetos referentes interligados na rede, mas que a securitização frequentemente ocorre para promover sua integridade. Até mesmo possíveis objetos referentes distintos são geralmente pensados em relação à própria rede: Estados e coletividades interconectados, redes de negócios e computadores, redes governamentais (informações confidenciais), militares e de infraestrutura crítica (dependentes de sistemas de hardware). Além do mais, mesmo que os autores enfatizem a ligação entre cibersegurança e segurança militar (Hansen e Nissenbaum 2009:1162-1164), eles não elaboram nas suas diferenças. Essa distinção é de extrema importância tendo em vista que ela permite a diferenciação entre a lógica de segurança e a lógica militar [...]. (LOBATO & KENKEL, 2015, p. 31, tradução nossa)

Sendo assim, pode-se inferir ao menos duas colocações de grande importância na compreensão do ciberespaço enquanto um setor próprio da securitização e que auxilia nas análises da formação de uma vigilância global digital: primeiro, temos que mesmo com a existência de diversos objetos referentes nos espaços sociotecnológicos, típico de uma arena em que quase tudo encontra-se interligado, infere-se que as redes são um objeto comum a todos os casos, sendo ela parte inalienável do processo ao qual este trabalho se propõe estudar, esteja ele em qualquer dos padrões supracitados; a segunda colocação está na distinção entre a lógica militar e a lógica da segurança (cibernética ou não), o que a escolha por uma análise baseada em uma visão social e securitizada da vigilância cibernética pode vir a desembaraçar vários nós.

Apesar disso, é importante ressaltar que ao conceber o ciberespaço e seus fenômenos como um setor autônomo, não se está retirando do estudo proposto as influências dos outros

setores da securitização. Afinal, uma análise multissetorial está no centro da busca por um entendimento ampliado e socialmente baseado do que se entende como ameaça e objeto securitizado. Logo, a vigilância cibernética, mesmo estando dentro das redes que conectam distintas fronteiras, possui características de diversos setores como apresentado anteriormente e como será aprofundado no próximo capítulo.

* * *

A securitização do ciberespaço, perpassando também pelos processos de militarização, politização e de participação do setor econômico e da sociedade, além de sua teorização enquanto um setor autônomo, parecem, assim, ser um elemento chave para a compreensão das questões que envolvem a vigilância desse ambiente a nível internacional e com a participação dos mais diversos atores. Os discursos da sociedade de controle ganham espaço e amplificam-se a medida em que a apropriação do espaço cibernético torna-se uma realidade cada vez mais incontestável, gerando um sentimento de ameaça à segurança dos usuários, dos Estados, das organizações e das corporações.

A visão de um superpanóptico global na sociedade contemporânea propicia um espaço de vigilância nunca antes visto, enquanto a vertente da modernidade líquida não nega a força que esta arena concebe à vigilância, mas aponta outros caminhos interessantes que devem ser levados em consideração. Os atores veem-se, então, em um ambiente onde as relações de poder espelham vigiados e vigilantes, em uma dinâmica que põe em risco a estabilidade do meio internacional. Diversos fenômenos de proporções globais ocorrem em decorrência desse fenômeno que, aparentemente, tende a aumentar de acordo com o avanço da tecnologia e das diversas formas de controle social.

Sendo assim, é papel da academia realizar estudos acerca dos casos ocorridos e dos novos acontecimentos que estão por vir, analisando-os a fim de construir experiências que possam auxiliar na construção de um ciberespaço mais equilibrado, em que a vigilância não impeça uma emancipação positiva de seus usuários, e que o dilema de segurança cibernética possa ser amenizado.

Nesse sentido, o próximo capítulo se propõe a analisar os programas de vigilância da NSA vazados em junho de 2013 por Edward Snowden a fim de auxiliar na construção desse conhecimento acerca do fenômeno da vigilância cibernética, tendo em vista a singularidade que o caso apresenta, principalmente no que tange à multiplicidade de atores envolvidos, o alcance dos programas nunca antes visto na história, suas características panópticas rígidas que somam-

se a características mais “maleáveis”, entre outros pontos, como demonstrado no capítulo a seguir.

3. O *BIG BROTHER* GLOBAL: OS PROGRAMAS DE VIGILÂNCIA DA NSA E A SECURITIZAÇÃO DO CIBERESPAÇO

Este capítulo procura elaborar uma análise acerca dos programas de vigilância da NSA (Agência de Segurança Nacional dos Estados Unidos) vazados por seu ex-agente, Edward Snowden, a partir dos conceitos e teorias levantados nos capítulos anteriores. Busca-se, dessa forma, compreender como a vigilância em nível global vem sendo fomentada e securitizada no sistema internacional a partir de um ponto de vista distinto das análises de segurança do *mainstream* das Relações Internacionais, propiciando, dessa maneira, uma visão da sua construção social, auxiliando na ampliação do escopo de sua compreensão.

Com tal intuito, faz-se necessário apresentar a NSA e seus programas de vigilância através dos *slides* de apresentações vazados por Snowden; demonstrar qual a conexão desse fenômeno com as características do ciberespaço, ou melhor, como tais aspectos propiciam a ocorrência de uma vigilância a nível global; investigar a sua natureza panóptica, assim como seus traços do tipo "faça você mesmo", banópticos e sinópticos; averiguar o processo de construção das ameaças que geram uma securitização do fenômeno apresentado a partir dos discursos, documentos, posicionamentos e atos dos Estados Unidos e seus aliados, fomentadores da vigilância, de Estados e organizações alvo, e de outros atores funcionais que tiveram influência nesse percurso, além de uma busca em meios especializados, tais como a mídia e as redes sociais, acerca da percepção dessas ameaças pelo público.

3.1 A NSA e seus programas de vigilância global

A Agência de Segurança Nacional dos Estados Unidos é, segundo seu próprio site, o "lar dos fabricantes e decifradores de códigos da América" (NSA, 2011, s/p, tradução nossa). Ela foi fundada em 1952 e desde então é um dos maiores órgãos provedores de informações para os tomadores de decisões e líderes militares estadunidenses. Funciona em conjunto com o Serviço Central de Segurança (CSS, na sigla em inglês) desde 1972 (ano de sua fundação), tornando-se, assim, o maior órgão de dados de criptologia do mundo.

A NSA e o CSS, são parte integrante do Departamento de Defesa dos EUA, estando vinculados, dessa forma, ao governo estadunidense. Sua capacidade de adquirir informações

(dentre estas, dados criptografados e sigilosos) é única no mundo, sendo capaz de interceptar dados de todo o planeta. Essa agência provê seus serviços a "Comunidade de Inteligência, agências governamentais, parceiros industriais, e aliados selecionados e coalizões parceiras", além de "entregar informação crítica, estratégica e tática para os planejadores e combatentes de guerra" (NSA, 2011, s/p, tradução nossa).

Claro que tudo isso só é possível devido a existência do próprio ciberespaço, do modo como se deu a sua construção e da influência que esse vem exercendo no mundo político como visto no primeiro capítulo deste trabalho. São nos espaços sociotecnológicos que a NSA e o CSS vasculham os mais diversos dados a fim de encontrar algo que seja de interesse de suas operações. Não é à toa que os EUA aparecem em primeiro lugar na tabela apresentada no mesmo capítulo como o Estado que mais investe em segurança cibernética e o resultado disso são órgãos e agências como a própria NSA.

Com o objetivo de manter a segurança nacional dos EUA e de seus aliados, a agência trabalha principalmente através do recolhimento de dados e da quebra de criptografia. Como visto, a criptografia é um meio pelo qual os dados podem circular pelo ciberespaço de forma mais segura, pois apenas remetente e destinatário possuem a "chave" para "abrir" os dados e ter acesso às informações transmitidas. É deste ponto que parte a crítica do criador do *WikiLeaks*, Julian Assange, ao alertar que muitas das empresas que criam programas de criptografia estão ligadas a governos como o dos EUA, o que facilita a quebra desses códigos. Outro fator facilitador também já citado anteriormente, é a constituição física dos cabos que transportam os dados, os *backbones*, que passam pelas fronteiras estadunidenses e ficam armazenados em servidores que possuem sua localização física ou em solo americano ou em países aliados, como demonstrado em um dos documentos vazados por Snowden no Anexo A.

Além dos meios pelo qual a NSA age a fim de quebrar códigos e recolher informações, ela também exige um alto nível de confidencialidade em suas operações, característica marcante dos trabalhos de inteligência, e possui como principais missões as descritas abaixo:

> Nossa missão *Information Assurance* [Garantia de Informação] confronta o formidável desafio de evitar que adversários estrangeiros tenham acesso a informação de segurança nacional sensível ou confidencial. Nossa missão *Signals Intelligence* [Sinais de Inteligência] coleta, processa e divulga informações de inteligência de sinais estrangeiros para fins de inteligência e contra-inteligência e para apoiar as operações militares. Esta Agência também permite que operações *Network Warfare* [Guerra em Rede] derrotem terroristas e suas organizações em casa e no exterior, de acordo com as leis norte-americanas e com a proteção da privacidade e das liberdades civis. (NSA, 2011, s/p, tradução nossa)

Apesar da agência preservar em sua descrição a manutenção de direitos e liberdades, além de apresentar como meta única a segurança nacional em suas missões, o que se têm apreendido acerca do funcionamento da NSA é justamente o oposto do que o governo estadunidense quer que a população acredite através da construção de uma definição própria. Os vazamentos de apresentações internas demonstram que, na prática, seus programas de vigilância ultrapassam qualquer fronteira de direito, moral ou ética que se possa apregoar.

O debate valorativo acerca das capacidades vigilantes da NSA e do CSS, entretanto, não é o foco destinado a esta dissertação (mesmo adentrando de maneira tangencial nesta questão), apesar de ser um trabalho de extrema importância que pode apontar os rumos para os quais a sociedade de controle e a vigilância líquida caminham. Para esta análise, interessa compreender até que ponto os programas de vigilância global da NSA estão ligados aos conceitos de panóptico, banópticos, sinópticos e de vigilância do tipo "faça você mesmo", além de delinear a construção das ameaças decorrentes de sua existência que colocam o sistema internacional em alerta.

Dessa maneira, a NSA, enquanto o maior centro de dados de criptologia do mundo, somado aos programas de vigilância vazados por Edward Snowden através de apresentações internas demonstradas a seguir, apresentam uma série de questões que são colocadas em debate entre os atores do meio internacional: até que ponto a agência pode ser entendida apenas como uma ferramenta da inteligência estadunidense e dos seus aliados? Que aliados são esses, tendo em vista que muitos deles aparecem na lista de espionados? Qual a abrangência dessa vigilância? Quais são os dados analisados por este órgão? Os indivíduos comuns estão livres desse tipo de espionagem? Até que ponto isso interfere no dia-a-dia das pessoas? Entre outras diversas dúvidas que geram um mal-estar entre os agentes e acabam levando a construção de ameaças e a formação de um processo de securitização.

Entre afirmações da necessidade de sua existência por parte dos EUA e de alguns aliados de um lado, e críticas acerca do *modus operandi* da NSA de outro, como será apresentado posteriormente, percebe-se a necessidade de uma análise das informações vazadas por Snowden a fim de primeiramente compreender o funcionamento desses programas de vigilância de alcance global para depois delinear suas principais características como uma nova face da vigilância contemporânea que se dá principalmente em âmbito digital, o que gera percepções de ameaças que, apesar de semelhantes, se distinguem de ameaças clássicas devido a este "novo" espaço de ações e reações em que o *know how* dos diversos agentes pode consagrar à sua sobrevivência.

* * *

O que ficou conhecido como "caso Snowden", no Brasil e "Snowden files" (arquivos de Snowden), nos EUA, denota os eventos que tiveram início em junho de 2013, quando foram vazadas informações de que a NSA (Agência de Segurança Nacional dos EUA) teria uma série de programas de vigilância global que estaria recolhendo dados sigilosos de pessoas, governos e empresas, tanto em âmbito doméstico quanto internacional. O responsável pelos vazamentos foi Edward Snowden, um analista de sistemas que trabalhava na NSA no setor de criptografia.

Luke Harding (2014), jornalista do *The Guardian*, detalhou em sua obra "*The Snowden Files: the inside story of the world's most wanted man*" (Os Arquivos de Snowden: a história interna do homem mais procurado do mundo) como se deu o processo de vazamento das informações, porém, os primeiros jornais a noticiarem o ocorrido foram o próprio *The Guardian* e o *The Washington Post*, os quais receberam as informações diretamente de Snowden. A reação estadunidense foi rápida, apresentando acusações formais de traição contra o ex-agente e exigindo sua prisão imediata.

Após a exigência, Snowden conseguiu fugir dos EUA para Hong Kong, onde encontrou-se com Glenn Greenwald e Laura Poitras, também jornalistas do *The Guardian*, entregando uma série de documentos internos que comprovavam suas acusações. Os jornalistas foram responsáveis por analisar os documentos e formular as diversas matérias que saíram neste período, revelando com detalhes os programas estadunidenses de vigilância global e alguns casos isolados que envolveram empresas, governos e cidadãos comuns. Em junho de 2013, Snowden embarcou para a Rússia, onde encontra-se asilado atualmente.

Em entrevista à *Rede Globo* em junho de 2014[33], uma das agências responsáveis pela divulgação dos documentos sigilosos, principalmente os relacionados ao Brasil, Snowden afirmou que suas motivações foram de proteger a liberdade das pessoas que estavam sendo monitoradas pela NSA, pois a vigilância não é algo a ser decidido unilateralmente. Ele ainda ressalta os riscos de uma vigilância global, como sendo uma ameaça à privacidade, à população, à democracia, aos governos e à liberdade de expressão e de comunicação.

Os programas de vigilância apontados por Edward Snowden são referidos em muitos artigos acadêmicos como a ascensão do distópico *1984* de George Orwell (2005), obra na qual o autor retrata um futuro trágico em que um governo totalitário, chamado *Big Brother* (Grande Irmão), fiscaliza e controla as ações de todos os seus cidadãos revogando direitos e liberdades

[33] Disponível em: <http://globotv.globo.com/globonews/milenio/v/sonia-bridi-entrevista-edward-snowden/3389933/> Acesso em 03 jun 2014

individuais. Além de criar uma nova língua (Novilíngua) que impedia qualquer crítica ao regime, de instituir uma severa censura aos meios de comunicação e de obrigar os indivíduos a xingar o traidor da pátria e adorar a imagem do *Big Brother*, o que na realidade se assemelha aos programas de vigilância da NSA é a criação fictícia da *teletela*, um tipo de televisão de duplo sentido que permitia tanto a reprodução de conteúdo quanto a observação e vigilância dos que estão assistindo.

É a partir desse imaginário de uma hipervigilância governamental em que todos estão sendo vigiados e, de certa maneira, controlados e tendo seus direitos e liberdades negados, que partem as principais análises dos programas de vigilância da NSA. Como aponta David Lyon (2015), a visão de Orwell sobre vigilância possui uma conexão clara com as afirmações de Max Weber e Hannah Arendt ao perceber que esta parte de uma racionalidade rígida que toma forma enquanto uma burocracia que acaba tendo efeitos nas relações sociais e proporcionando cada vez mais a expansão dessa vigilância, seja pela alegação da necessidade de tal procedimento, ou pela própria população que passa a acreditar ser essa a única maneira de manter seus direitos assegurados.

O próprio Edward Snowden elaborou comentários acerca dessa comparação da atual situação de vigilância governamental com a obra de Orwell. Segundo ele, o que muda em relação às tecnologias fictícias criadas na obra *1984* é que na realidade atual estas foram transformadas em computadores e celulares com câmeras e microfones ligados a uma rede mundial que os interconectam. Além disso, tendo grande parte dos usuários internalizado o ato do compartilhamento, a vigilância consegue ser ainda mais eficaz que na distopia de Orwell, tornando o mundo "imprevisível e perigoso" (SNOWDEN apud LYON, 2015, p. 141).

O caso Snowden ganhou importância no Brasil devido às espionagens realizadas contra alvos brasileiros. Diversos documentos que dizem respeito ao país revelam que os Estados Unidos interceptaram ligações telefônicas, mensagens de texto e e-mails da Presidente Dilma Rousseff. Além disso, o governo estadunidense e canadense obtiveram informações sigilosas da Petrobrás e ainda hackearam o Ministério de Minas e Energia[34]. Em notícia do portal G1[35], ressalta-se também que cidadãos brasileiros e estrangeiros que visitaram o país tiveram dados coletados, que uma estação da NSA funcionou em Brasília até 2002 e que a embaixada do Brasil nos EUA e a representação na ONU foram monitoradas.

---

[34] Disponível em: <http://globotv.globo.com/globonews/milenio/v/sonia-bridi-entrevista-edward-snowden/3389933/> Acesso em 03 jun 2014

[35] Disponível em: <http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html > Acesso em: 03 jun 2014

Já em relação aos principais programas de vigilância revelados por Snowden estão os chamados: *PRISM* (EUA), *Boundless Informant* (EUA), *X-Keyscore* (EUA), *Tempora* (Reino Unido), *Muscular* (Reino Unido) e *Stateroom* (EUA, Reino Unido, Canadá, Austrália e Nova Zelândia). Além destes programas, diversas análises de Estados, empresas, organizações e indivíduos também foram reveladas, contendo provas de como estes programas agem na coleta de dados através de uma vigilância global.

Importante ressaltar que, apesar de a NSA ser a principal agência fomentadora da vigilância global estadunidense, outros órgãos e agências dos EUA e de outros países também fazem parte desse processo, assim como outros atores aliados. Sabe-se que o Tratado de Segurança EUA-Reino Unido de 1946, com o intuito de compartilhar informações secretas provenientes dos seus respectivos setores de inteligência (NSA, dos EUA, e GCHQ "*Government Communications Headquarters*", do Reino Unido) foi ampliado ao incluir também Canadá (CSEC, *Communications Security Establishment*), Austrália (ASD, *Australian Signals Directorate*) e Nova Zelândia (GCSB, *Government Communications Security Bureau*). Esta rede de vigilância ficou conhecida como *The Five Eyes* (Os Cinco Olhos) e consta nos documentos apresentados por Snowden.

Este acordo, que foi tratado como sigiloso por muitos anos, ainda possui validade e diversos dos programas supracitados são postos em prática através do compartilhamento de informações entre esses Estados e suas agências. Como exemplo, a missão da NSA chamada *Signals Intelligence*, demonstrada anteriormente, funciona através dessa rede de inteligência, informação também revelada pelas apresentações vazadas por Snowden, como demonstrado no Anexo B.

Além do tratado que forma o *Five Eyes*, foi revelado nos documentos vazados por Snowden que a França também possui um acordo de cooperação com os cinco países no que tange a vigilância global. O tratado, conhecido como Lustre, permitiu um relacionamento mais próximo entre o *Direction Générale de la Sécurité Extérieure* (DGSE), a agência de inteligência francesa, e a NSA, proporcionando a transferência de milhões de dados entre as agências[36]

Sendo assim, faz-se necessário uma explanação destes programas, demonstrando como eles funcionam na prática, quais são suas fontes e seus alvos, para assim compreender a dimensão da vigilância posta em prática pelos EUA e seus aliados e as ameaças provenientes deste processo.

---

[36] Disponível em: <http://.lemonde.fr/international/article/2013/10/30/surveillance-la-dgse-a-transmis-des-donnees-a-la-nsa-americaine_3505266_3210.html> Acesso em 30 jan 2016

3.1.1 PRISM

Um dos programas de vigilância da NSA revelados por Edward Snowden foi o chamado *PRISM*. A apresentação interna vazada é datada de abril de 2013 (ver Anexo C) e consiste em uma explanação aos funcionários da maneira pela qual o programa funciona e como utilizá-lo. O *PRISM* pode ser percebido como uma das principais fontes primárias de dados privados e públicos da agência e vem funcionando desde 2007 nesta função.

O que caracteriza esse programa é a possibilidade de funcionários adquirirem dados diretamente de grandes servidores que estão em solo americano. Isso se dá, segundo a apresentação vazada, através de uma parceria com grandes empresas americanas, como as citadas: *Microsoft*, *Yahoo*, *Google*, *Facebook*, *PalTalk*, *AOL*, *Skype*, *YouTube* e *Apple*. Sabe-se que as empresas que agem no ciberespaço armazenam grandes volumes de dados de seus usuários, sejam os dados pessoais entregues diretamente pelo indivíduo (nome, endereço, número de documento, etc.), ou a forma como estes utilizam os serviços oferecidos pelos provedores (fotos publicadas, notícias "curtidas" e compartilhadas, pesquisas em buscadores, etc.). Dessa forma, o governo americano passa a ter uma fonte importante de dados que alguns usuários julgam serem privados.

Essa lista de empresas foi ampliada posteriormente por Glenn Greenwald, incluindo operadoras de telefonia americanas e internacionais (dentre elas a *AT&T*, a *Verizon*, e, no Brasil, *GVT*, *Oi* e *Tim*[37]) e empresas da área de tecnologia e informática que, segundo acusações, produzem hardwares e softwares que facilitam a vigilância pela NSA, tais como a *Qualcomm*, a *Cisco*, a *Oracle*, a *Intel*, a *IBM*[38], dentre outras.

O documento revelado ainda deixa claro a facilidade com que a maioria dos dados trafegados no ciberespaço passa pelas fronteiras estadunidenses, ao afirmar que o tráfego sempre irá procurar o caminho mais barato (passando pelos EUA) e não o fisicamente mais rápido (indo diretamente do ponto A ao ponto B), mesmo que nem sempre seja possível prever esse caminho. Sendo assim, os agentes internos poderiam vigiar seus alvos de duas maneiras: a) ou através do *Upstream*: programa que coleta os dados a partir das redes de fibra óptica e na

[37] Disponível em: <http://www12.senado.gov.br/noticias/materias/2013/09/24/cpi-da-espionagem-vai-ouvir-google-facebook-e-empresas-de-telefonia> Acesso em 30 jan 2016

[38] Disponível em: <http://.washingtonsblog.com/2014/05/direct-nsa-parnters-att-verizon-microsoft-cisco-ibm-oracle-intel-qualcomm-qwest-eds.html> Acesso em 30 jan 2016

infraestrutura enquanto estes estão trafegando; b) ou pelo programa *PRISM*, que, como visto, vai diretamente nos servidores onde os dados privados estão armazenados.

O que chama a atenção no *PRISM* é justamente o fato de o governo estadunidense ter acesso direto aos servidores das empresas que fornecem serviços online tidos como essenciais atualmente. Como descrito nos documentos, os agentes da NSA podem acessar e-mails, conversas (texto, vídeo e/ou voz), vídeos, fotos, dados armazenados, VoIP (serviço de ligação de voz pela *internet*), transferência de arquivos, videoconferências notificações de atividades-alvo (como logins), detalhes das redes sociais dos usuários e podem realizar pedidos especiais, ou seja, demandar dessas empresas outros dados além dos supracitados.

O *PRISM* também teria sido colocado em prática com a cooperação dos *Five Eyes*[39], tendo inclusive provas de espionagens realizadas contra o Brasil pelo Canadá[40]. Além disso, Glenn Greenwald, jornalista do *The Guardian*, afirma em entrevista[41] que estes países realizam espionagens voltadas a interesses econômicos, sob alegação de segurança nacional: “Sem dúvida não estão preocupados com segurança nacional ou terrorismo, como sempre alegam, mas em obter vantagens comerciais para suas empresas" (GREENWALD, 2013).

Sendo assim, percebe-se que a coleta de dados através do *PRISM* possui três fontes principais: os servidores de empresas, a cooperação entre os aliados e o programa *Upstream*. Entretanto, como será aprofundado posteriormente ao analisar-se os discursos que geram o processo de securitização da vigilância da NSA, o governo estadunidense vem alegando que o programa *PRISM* é essencial para a segurança da nação contra ataques terroristas e afirma que os dados coletados são, na verdade, metadados [42] interpretados por computadores que selecionariam possíveis ameaças à segurança nacional, ou seja, a privacidade dos indivíduos estaria salvaguardada pois nenhum agente poderia ter acesso aos seus dados desde que não houvesse qualquer suspeita.

Já as empresas citadas alegam que não possuem qualquer ligação com o programa e que só fornecem dados mediante ordem judicial. Segundo reportagens do *The Washington Post*[43] e

---

[39] Disponível em: <http://www1.folha.uol.com.br/colunas/clovisrossi/2013/07/1308320-cinco-olhos-todos-em-voce.shtml> Acesso em 30 jan 2016

[40] Disponível em: <http://g1.globo.com/politica/noticia/2013/10/ministerio-de-minas-e-energia-foi-alvo-de-espionagem-do-canada.html> Acesso em 30 jan 2016

[41] Disponível em: <http://.cartamaior.com.br/?/Editoria/Internacional/-Governos-dos-EUA-Inglaterra-e-Canada-mentem-o-tempo-todo-/6/29163> Acesso em 30 jan 2016

[42] Metadados são as informações acerca dos dados e não o seu conteúdo em si. Informariam, por exemplo, remetente e destinatário, duração, localização, meio utilizado na comunicação, etc.

[43] Disponível em: <https://.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?hpid=z1> Acesso em 30 jan 2016

do *The New York Times*[44], os dados seriam acessados pela NSA a partir de brechas legais que permitem sua aquisição quando estão relacionados a comunicação com estrangeiros e dizem respeito à segurança nacional. Apesar disso, diversos abusos por parte de funcionários e pessoas com acesso ao programa foram reportados com a utilização da vigilância para fins pessoais[45].

3.1.2 Boundless Informant

O programa *Boundless Informant* (em português, algo como Informante Ilimitado) é outra ferramenta utilizada pelos agentes da NSA e seus aliados no processo de vigilância global. Também foi divulgado pelos vazamentos de meados de 2013 do ex-agente da NSA, Edward Snowden (ver Anexo D).

Trata-se de um programa de computador que consegue interpretar, resumir e demonstrar dados grandes e complexos que seriam impossíveis de decifrar através de programas comuns, o que é chamado de Big Data ou Megadados. Os Megadados são provenientes dos mais diversos servidores e coletados pelos programas de vigilância da NSA e de outras agências aliadas.

O *Boundless Informant* consegue prover diversos resumos da captura de dados ao redor do mundo. Dentre os documentos divulgados, é possível observar a quantidade de dados espionados em diversos países durante um período de 30 dias, dentre eles estão (Anexo D): a) França, cerca de 60 milhões de metadados analisados; b) Alemanha, média de 552 milhões de dados; c) Itália, 46 milhões; d) Holanda, 1,8 milhão; e) Espanha, 60 milhões.

Em outro documento (também no Anexo D), é possível observar ainda outros países dentre dados provenientes de *internet* (DNI) e telefonia (DNR): a) EUA, quase 2,9 bilhões de metadados espionados; b) Irã: cerca de 15,8 bilhões; c) Paquistão, 27,3 bilhões; d) Jordânia, 14,4 bilhões; e) Egito, 9,1 bilhões; f) Índia, 12,6 bilhões. Nesse mesmo período de 30 dias, o documento revela que foram analisados 97,2 bilhões de dados provenientes da *internet* e 124,9 bilhões da telefonia.

Assim como no *PRISM* (e em diversos outros programas), o *Boundless Informant* também coleta dados espionados por outras agências aliadas, principalmente as que pertencem aos *Five Eyes*, além dos próprios programas de vigilância da NSA. Diversas notícias posteriores

[44] Disponível em: <http://.nytimes.com/2013/06/07/us/nsa-verizon-calls.html> Acesso em 30 jan e2016
[45] Disponível em: <http://.foxnews.com/politics/2013/09/27/too-tempting-nsa-details-how-officials-spied-on-love-interests.html> Acesso em 30 jan 2016

aos vazamentos complementaram as informações referentes principalmente aos dados europeus, os quais na verdade teriam sido coletados por agências de inteligência próprias e os dados repassados à NSA[46] [47] [48].

3.1.3 X-Keyscore

O *X-Keyscore* foi outro programa revelado pelos documentos apresentados por Snowden. Datada em 28 de fevereiro de 2008, a apresentação vazada possui diversas informações importantes acerca do que consiste o programa, seu funcionamento e inclusive uma história dos sucessos alcançados com a vigilância (ver Anexo E). Apesar de possuir certa semelhança com o *PRISM* no que tange o acesso a dados privados de milhões de usuários ao redor do globo, o que o difere em grande escala é o uso de servidores próprios em diversos países, mas sem o conhecimento e o aval destes.

Segundo o documento, são mais de 150 sites rastreáveis e mais de 700 servidores espalhados pelo mundo, inclusive no Brasil. A partir destas fontes, os funcionários da NSA ou qualquer outra pessoa que possua acesso a esses servidores, tais como empresas contratadas e agências de outros países, podem ler e-mails de usuários, rastrear seu tráfego em sites, suas buscas e conversas, isso tudo a partir de qualquer computador, em qualquer lugar do mundo e em tempo real[49].

Em entrevista realizada com Glenn Greenwald, que teve acesso a diversos documentos de Edward Snowden que ainda não foram revelados, o jornalista do *The Guardian* afirma que qualquer analista da NSA, até mesmo os que estão hierarquicamente abaixo, pode ter acesso a "qualquer e-mail que quiser, qualquer chamada telefônica, históricos de navegação, documentos do *Microsoft* Word. E tudo é feito sem a necessidade de ir a um tribunal, sem a necessidade de até mesmo obter aprovação do supervisor por parte do analista" (GREENWALD, 2013)[50].

---

[46] Disponível em: <http://.spiegel.de/international/world/german-intelligence-sends-massive-amounts-of-data-to-the-nsa-a-914821.html> Acesso em 30 jan 2016
[47] Disponível em: <https://.rt.com/news/norway-nsa-snowden-spying-us-965/> Acesso em 30 jan 2016
[48] Disponível em: <http://electrospaces.blogspot.com.br/2014/02/dutch-government-tried-to-hide-truth.html> Acesso em 30 jan 2016
[49] Disponível em: <http://ultimosegundo.ig.com.br/mundo/bbc/2013-08-02/ferramenta-de-espionagem-online-dos-eua-permite-monitoramento-em-tempo-real.html> Acesso em 30 jan 2016
[50] Disponível em: <http://abcnews.go.com/blogs/politics/2013/07/glenn-greenwald-low-level-nsa-analysts-have-powerful-and-invasive-search-tool/> Acesso em 30 jan 2016

De acordo com o documento, o *X-Keyscore* é um "Sistema de Exploração DNI / Quadro Analítico", em que DNI significa *Digital Network Intelligence* (Inteligência na Rede Digital), ou seja, é um sistema que almeja encontrar dados de inteligência dentro da *internet*. Dessa maneira, não é um programa com intenções de agir frente um alvo espionado, apenas captar todos os seus dados e armazená-los. Entretanto, ele pode dar início a outros sistemas com funções de defesa e ataque caso seja necessário.

As capacidades de ação do *X-Keyscore* ampliam o poder de busca dos analistas ao fornecer muitos terabytes de informações e dados comuns, ou seja, dados decorrentes do uso diário da rede, e ao conectá-los aos metadados, proporcionando encontrar alvos de forma mais prática. Por exemplo, qualquer pessoa com acesso ao programa pode encontrar diversos dados de um alvo (conversas telefônicas, e-mails, redes sociais, históricos, etc) sabendo apenas seu e-mail, ou até mesmo palavras-chave.

Além disso, o *X-Keyscore* ainda permite procurar o modo de utilização do *Google* Maps, demonstrando buscas suspeitas de lugares; "anomalias", como, por exemplo, a nacionalidade de indivíduos através da língua utilizada na troca de e-mails[51]; detectar indivíduos que utilizem criptografia; encontrar máquinas que utilizem VPN, uma maneira de acessar a rede como se o computador estivesse em outro lugar; rastrear a fonte de documentos que já foram compartilhados diversas vezes; monitorar a rede *TOR*, utilizada para ter acesso ao que ficou conhecido como *Deep Web*[52] [53]; entre outras capacidades.

Ainda segundo a apresentação vazada por Snowden, o *X-Keyscore*, assim como o *PRISM*, possui interação com os *Five Eyes*, sendo realizada uma cooperação entre os países-membro a fim de colocar o programa em prática com a mesma defesa de que sua existência é essencial para a segurança internacional. De acordo com dados apresentados nos slides, o *X-Keyscore* foi responsável pela captura de mais de 300 terroristas; além disso, a facilidade com que se pode vigiar através do programa fez com que os analistas das agências de inteligência se voltassem mais para este tipo de ação, antes extremamente complexa; outro caso que demonstra o uso do *X-Keyscore* foi o rastreio de indivíduos que faziam parte do grupo *Annonymous* na Alemanha[54].

---

[51] Disponível em: <http://oglobo.globo.com/infograficos/big-brother-am-latina/> Acesso em 30 jan 2016

[52] *Deep Web* é o termo utilizado para descrever a parte não indexada da *web* em mecanismos de busca como o *Google*, parte esta conhecida como *Surface Web*. É possível elaborar uma analogia com um *iceberg*: a *Surface Web* (indexada) é o lado emerso (visível) e a *Deep Web* (não indexada) sua parte imersa (invisível na superfície).

[53] Disponível em: < http://daserste.ndr.de/panorama/aktuell/nsa230_page-1.html> Acesso em 30 jan 2016

[54] Disponível em: <http://.spiegel.de/international/world/germany-is-a-both-a-partner-to-and-a-target-of-nsa-surveillance-a-916029.html> Acesso em 30 jan 2016

3.1.4 Tempora

Apesar de ser colocado em prática pelo governo britânico, o *Tempora* também foi revelado pelos documentos vazados por Edward Snowden por possuir fortes ligações com a NSA, funcionando em um sistema cooperativo. Esse programa funciona através do GCHQ (*Government Communications Headquarters*) e, segundo relatos de documentos vazados e do próprio Snowden, consegue ser mais eficaz e ir mais fundo na vigilância que o *PRISM*[55]. O projeto teve início em 2008 através de testes, sendo colocado em funcionamente total a partir de 2011[56].

O *modus operandi* do *Tempora* assemelha-se bastante ao *Upstream*, tendo sua principal fonte de dados advinda de interceptações diretas em cabos de fibra óptica que formam o *backbone* que perpassa o Reino Unido e outros cabos espalhados pelo oceano. Segundo reportagem do *The Guardian*[57], o GCHQ implantou interceptadores de dados nesses cabos tanto na entrada quanto na saída das fronteiras inglesas, além dos cabos que interligam o tráfego entre os EUA e a Europa. Sabe-se que nesta área trafegam enormes volumes de dados de todo o mundo, o que propicia uma vantagem geopolítica clara à vigilância cibernética no Reino Unido (assim como nos EUA, seguindo a mesma lógica):

[55] Disponível em: <http://.wired.co.uk/news/archive/2013-06/24/gchq-tempora-101> Aceso em 30 jan 2016
[56] Disponível em: <http://.wired.co.uk/news/archive/2013-06/24/gchq-tempora-101> Acesso em 30 jan 2016
[57] Disponível em: <http://.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa> Acesso em 30 jan 2016

Imagem 1
Fluxo de dados em Mpbs no ano de 2005

Fonte: Diponível em: <http://archive.wired.com/politics/security/news/2007/10/domestic_taps> Acesso em 30 jan 2016

Essa interceptação direta nos cabos se dá através de uma cooperação secreta, forçada ou não, com as empresas responsáveis pela instalação, manutenção e operacionalização destes dutos de dados, o que dá acesso à 10 gigabits por segundo[58]. Isso corresponde a um número de dados exorbitante por segundo, tanto que o GCHQ necessita de auxílio da NSA para conseguir usufruí-los de forma satisfatória, inclusive compartilhando estes dados com a agência estadunidense. Segundo dados apontados pela reportagem do portal Wired[59], cerca de 300 analistas da GCHQ e 250 da NSA trabalham em cima da análise dos dados do *Tempora*.

De acordo com os documentos vazados (ver Anexo F), o *Tempora* funciona a partir de dois componentes principais: o *Mastering the Internet*, MTI (Dominando a *Internet*, em português), e o *Global Telecoms Exploitation*, GTE (Exploração Global das Telecomunicações), sendo o primeiro responsável por coletar dados da *internet* e o segundo pelos dados telefônicos. Há relatos de que o *Tempora* consegue explorar mais dados provenientes de vigilância que o *PRISM* e que não há qualquer distinção entre os dados recolhidos, sejam eles de cidadãos comuns ou alvos pré-estabelecidos[60]. Dentre as informações recolhidas estão e-mails, mensagens, chats, dados de redes sociais, histórico de navegação, chamadas telefônicas, entre outras.

[58] Disponível em: <http://.theguardian.com/uk/2013/jun/21/how-does-gchq-internet-surveillance-work> Acesso em 30 jan 2016
[59] Disponível em: <http://.wired.co.uk/news/archive/2013-06/24/gchq-tempora-101> Acesso em 30 jan 2016
[60] Disponível em: <http://.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa> Acesso em 30 jan 2016

3.1.5 Muscular

O programa *Muscular* é outro sistema de vigilância operado através de uma cooperação entre o GCHQ e a NSA com base no governo britânico. Assim como outros programas supracitados, também possui apoio da rede de inteligência formada pelos *Five Eyes*. Também foi revelado por Edward Snowden em outubro de 2013 e, posteriormente, os conhecimentos acerca do programa foram ampliados por entrevistas com agentes envolvidos[61].

O que chama atenção neste programa é tanto o modo como ele funciona quanto o meio utilizado para chegar a fonte dos dados. Não foram vazadas tantas informações sobre o *Muscular*, mas sabe-se que ele funciona através de uma invasão secreta perpetrada tanto pelo GCHP quanto pela NSA às redes, servidores e centros de processamento das empresas *Google* e *Yahoo*!. Isso acabou dando acesso aos dados das duas gigantes da *internet*, tanto de seus famosos serviços de e-mails quanto aos serviços de nuvem, como armazenamento de arquivos online, editores de textos, apresentações e planilhas online, busca em mapas, entre outros[62].

Por tratar-se de uma invasão secreta, não há qualquer impeditivo de ação das agências principais e aliadas dentro do *Muscular*. Elas possuem acesso direto a vários terabytes de dados sem qualquer preocupação legal na aquisição destes. Segundo o *Washington Post*, o programa consegue duas vezes mais dados que o *PRISM*, tendo até mesmo representado um desafio para a NSA e o GCHQ de como armazenar e vasculhar tantos dados. Apesar de o *Muscular* se delimitar à coleta desses dados privados, existem outros programas como o *Incenser* e o *Turmoil* que são responsáveis pelo processamento das informações recolhidas[63].

Apesar das alegações das empresas de que a maioria dos dados transmitidos em suas redes comunicacionais são encriptados, em um dos slides da apresentação vazada (ver Anexo G), no qual observa-se um desenho de como se dava a coleta de informações pelo *Muscular*, é informado que os dados circulavam sem qualquer tipo de criptografia dentro dos servidores privados do *Google*. Inclusive, o próprio *Washington Post*, que publicou acerca do *Muscular*

---

[61] Disponível em: <https://.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html> Acesso em 30 jan 2016

[62] Disponível em: <https://.washingtonpost.com/news/the-switch/wp/2013/11/04/how-we-know-the-nsa-had-access-to-internal-google-and-yahoo-cloud-data/> Acesso em 30 jan 2016

[63] Disponível em: <https://.washingtonpost.com/news/the-switch/wp/2013/11/04/how-we-know-the-nsa-had-access-to-internal-google-and-yahoo-cloud-data/> Acesso em 30 jan 2016

pela primeira vez, só decidiu realizar a publicação após ver este slide que ainda possui um desenho com um "rosto feliz", demonstrando o sucesso da operação[64].

3.1.6 Stateroom

O programa *Stateroom* faz parte de uma das missões citadas da NSA, o *Signals Intelligence*. Como visto, esta missão "coleta, processa e divulga informações de inteligência de sinais estrangeiros para fins de inteligência e contra-inteligência e para apoiar as operações militares" (NSA, 2011, s/p, tradução nossa). O programa de vigilância é responsável pela interceptação de sinais de rádio em diversos países, telecomunicações e tráfegos de *internet*[65].

Ela está presente em centenas de embaixadas e consulados dos países pertencentes do grupo *Five Eyes*[66] em diversos países e, no caso dos EUA, é conduzida tanto pela NSA quanto pela CIA (*Central Intelligence Agency*), em uma força-tarefa chamada de *Special Collection Services* (SCS)[67]. Segundo os documentos vazados por Edward Snowden (ver Anexo), a prática do *Stateroom* é posta em funcionamento sem o conhecimento de todos os membros das instituições diplomáticas.

De acordo com os vazamentos e com descobertas posteriores, cada membro do *Five Eyes* possui funções específicas no processo de vigilância. Os EUA teriam realizado espionagem nas embaixadas em Atenas, Grécia; Baku, Azerbaijão; Bangkok, Tailândia; Berlim, Alemanha; Brasília, Brasil; Budapeste, Hungria; Frankfurt, Alemanha; Genova, Suíça; Kiev, Ucrânia; Lagos, Nigéria; Madrid, Espanha; Milão, Itália; Moscou, Rússia; Nova Déli, Índia; Paris, França; Praga, República Tcheca; Pristina, Kosovo; Roma, Itália; Sarajevo, Bósnia; Tblisi, Geórgia; Viena, Áustria; e Zagreb, Croácia.

Sabe-se que o Reino Unido também mantém um sistema de espionagem em sua embaixada em Berlim, na Alemanha[68]. Já o Canadá, documentos demonstram que suas

---

[64] Disponível em: <https://.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html> Acesso em 30 jan 2016

[65] Disponível em: <http://.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html> Acesso em 30 jan 2016

[66] Disponível em: <http://.nytimes.com/2013/11/01/world/asia/australia-participated-in-nsa-program-document-says.html?_r=1> Acesso em 30 jan 2016

[67] Disponível em: <http://.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html> Acesso em 30 jan 2016

[68] Disponível em: <http://.independent.co.uk/news/uk/home-news/revealed-britains-secret-listening-post-in-the-heart-of-berlin-8921548.html> Acesso em 30 jan 2016

instituições diplomáticas são utilizadas pela NSA para realizar a vigilância[69], inclusive nas denúncias já citadas de que o Canadá teria espionado o Ministério de Minas e Energia do Brasil. A Austrália é responsável por espionar cidades do leste asiático, como Bangkok (Tailândia), Pequim (China), Hanoi (Vietnã), Kuala Lumpur (Malásia), entre outras[70]. Por fim, alegações apontam que a Nova Zelândia também realizou o mesmo procedimento em Honiara, nas Ilhas Salomão[71].

Grandes revelações mundiais que ganharam evidência nos jornais como as notícias acerca da espionagem da presidente Dilma Rousseff, do Ministério de Minas e Energia e da empresa Petrobrás no Brasil; a vigilância da chanceler da Alemanha, Angela Merkel; a interceptação de comunicações realizadas pelo então candidato à presidência do México, hoje presidente, Enrique Peña Nieto; entre outras, foram realizadas em conjunto com o sistema *Stateroom*, utilizando as representações diplomáticas nesses países.

* * *

Tendo como base essa breve apresentação dos programas de vigilância da NSA e seus aliados, percebe-se o quão avançado está o processo de criação de uma hipervigilância global por parte principalmente do governo estadunidense. Claro que existem diversos outros exemplos de programas de vigilância que estão sendo postos em prática em diferentes Estados e organizações; acusações de espionagem por parte da China, da Coréia do Norte, de Israel e de organizações de *hackers* existem e possuem um importante impacto na segurança internacional. Entretanto, os programas da NSA mostram uma capacidade global ainda não percebida em outros casos, o que os tornam únicos de certo modo.

Como foi possível perceber na apresentação dos programas, essa capacidade só se tornou possível devido à característica de pervasividade do ciberespaço enquanto geradora dos novos espaços sociotecnológicos, arena onde liberdade e vigilância parecem conviver lado a lado. Não haveria vigilância cibernética sem os aspectos demonstrados no primeiro capítulo deste trabalho, pois são eles que permitem essa grande troca de dados em redes que interligam máquinas operadas por humanos em todo o mundo.

---

[69] Disponível em: <http://o.canada.com/news/canadian-facilities-used-for-u-s-spying-efforts-nsa-documents> Acesso em 30 jan 2016

[70] Disponível em: <http://.smh.com.au/it-pro/security-it/australias-asia-spy-network-exposed-20131030-hv2ao.html> Acesso em 30 jan 2016

[71] Disponível em: <http://.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11417762> Acesso em 30 jan 2016

As relações de poder também se tornam aparentes com a clara distinção entre os atores com capacidades de ação mais desenvolvidas que outros dentro da lógica da vigilância cibernética. Neste cenário pouco diplomático, a *cyberpolitik* acaba sendo um reflexo da constituição da ordem sociotecnológica advinda do que ficou conhecido como *cyberpower*, através do qual grupos de atores acabam dominando esta ordem por possuírem um *know how* mais efetivo e gerando consequências para a cibersegurança.

Partindo disto, buscou-se apresentar os programas sem apontar, no momento, os posicionamentos dos principais atores envolvidos em relação às acusações advindas dos documentos de Edward Snowden. Isto deveu-se pela análise posterior, elaborada ainda neste capítulo, acerca do processo de securitização no qual os principais discursos serão apresentados e analisados como formadores de um processo de construção das ameaças percebidas em âmbito internacional, a fim de compreender esse movimento.

Antes de adentrar-se nesta questão, é importante, entretanto, atentar para as principais características dessa vigilância como dimensão-chave na compreensão do seu processo de securitização. Faz-se necessário explorar os aspectos dos programas de espionagem da NSA a partir dos estudos de vigilância levantados no capítulo 2, proporcionando, assim, uma percepção aprofundada do que é esse caso, para quem essa vigilância é colocada em prática e qual o seu intuito, dentro da lógica do panoptismo e do pós-panoptismo.

3.2 Os programas da NSA e os estudos de vigilância

Como visto no capítulo anterior, os estudos de vigilância abarcam uma série de análises que propiciam um vasto apanhado teórico. É possível entender este fenômeno a partir de abordagens positivistas e pós-positivistas que auxiliam em compreensões epistemologicamente distintas, mas que possuem como objetivo final o estudo e a construção de conhecimento acerca dos casos analisados. Sabe-se, entretanto, que a evolução tecnológica acelerada do final do século XX, base do estudo proposto, juntamente com outros fenômenos que vão da arte às ciências biológicas, proporcionaram mudanças paradigmáticas na forma como se pensa a ciência.

Sendo assim, os programas de vigilância da NSA confundem-se, em certo sentido, com essa quebra paradigmática e exigem que novas visões auxiliem em sua compreensão que não exatamente foge da velha análise de sobrevivência estatal e capacidades dos atores, mas deve

enfrentar novas questões que vão além disso. Dessa forma, estudos que busquem examinar o caso juntamente com essas questões contemporâneas nos parecem necessários a fim de ampliar a visão concebida socialmente acerca da vigilância e, especificamente, da perpetrada pela NSA e seus aliados.

Partindo da ideia fundamentada por Foucault (1988) de que a função final da vigilância é o controle da alma a fim de manter o comportamento e o ânimo dos indivíduos que convivem em sociedade, propõe-se aqui duas análises dos programas apresentados que, se certa maneira, se complementam: uma a partir da ideia de um panóptico global que gera uma hipervigilância e um hipercontrole social; e outra que busca inserir nesta visão aspectos da modernidade líquida, concebendo, assim, o papel do indivíduo e da sociedade na vigilância cibernética em um mundo pós-panóptico.

3.2.1 A Hipervigilância dos Programas da NSA

Os programas de vigilância da NSA e de seus aliados vazados por Edward Snowden demonstram uma capacidade de ação dessas agências ainda não observada na história. Com o auxílio de grandes empresas de serviços, softwares e hardwares em todo o globo, com a própria técnica desenvolvida no âmbito do governo e com a construção, ao longo do tempo, de uma logística dos cabos de fibra óptica – que transmitem os dados da rede mundial de computadores – e de telecomunicação favorável aos EUA e à Europa, o mundo se vê interligado, mas dependente e vigiado por esses atores.

Tomando o Panóptico de Bentham e a Sociedade de Controle como ferramenta de análise desta vigilância cibernética, observa-se que os centros de vigilância se confundem com as torres de observação, enquanto um poder visível, mas inverificável, com a função principal de manter sobre controle e disciplinar grande parte da gama de relações que ocorre dentro do ciberespaço, principalmente as que tangem questões de segurança, mas, como observado nas apresentações, não somente estas. Segundo O'Neill:

> Como isso nos ajuda a compreender a questão atual da NSA, *PRISM* e da *Internet*? Isto nos obriga a olhar para a arquitetura da *Internet*. Dando concessão, a *internet* não tem um centro como previsto na prisão de Bentham, mas tem ISPs [provedor de *internet*] e empresas que monitoram (embora eles digam que vagamente) o tráfego da *Internet* e a gestão de metadados. O que vimos com as ações da NSA poderia ser visto como os guardas da prisão, tornando-nos conscientes do poder de vigilância e de sua

> capacidade de assistir e orientar o nosso comportamento; ou seja, os nossos padrões de uso e o conteúdo de nossas pesquisas na *internet* e telefonemas. Ao contrário dos objetivos de Bentham, no entanto, os efeitos de tal vigilância pouco fazem para promover uma sociedade mais justa; em vez disso, gera desconfiança, paranoia e pânico. (O'NEILL, 2015, p. 7-8, tradução nossa)

Logo, assim como Bentham sugeriu a construção do panóptico como uma arquitetura que racionaliza a vigilância e Foucault amplia esta ideia às instituições sociais disciplinares, torna-se possível inferir que a construção do aparato de vigilância cibernética, a partir dos programas apontados, utiliza de forma análoga a mesma racionalização da vigilância encontrada no panóptico, mas em escala global e tendo como alvo não apenas os Estados e governos, mas diversos atores que vão desde os indivíduos até organizações maiores.

Há muito tempo os usuários sabem que são monitorados, mesmo antes das revelações de Snowden. Os vazamentos de fato mostraram a magnitude da vigilância da NSA e deram corpo a ela, mas apenas confirmaram o que já se imaginava, como afirma Lyon (2015). Não é à toa que existem indivíduos que tentam se emancipar dessa lógica, através de programas que escondem a identidade da máquina, da criptografia e até mesmo aqueles que buscam denunciar os programas de vigilância (e outros documentos sigilosos), tais como os grupos *WikiLeaks* e *Annonymous* e o próprio Edward Snowden. Assim como nas relações de poder para Foucault (1988), a soma nunca é zero, logo a vigilância dos espaços sociotecnológicos propicia uma certa emancipação do indivíduo, principalmente por suas características já apontadas neste trabalho.

Observa-se, entretanto, que isto não se aplica a todos os usuários, deixando muitos sob a influência da vigilância e do controle da *internet*. O'Neill ressalta que:

> Isso se reflete nos escritos de Foucault, onde ele argumentou que o Panóptico, ou no nosso caso, a *Internet* foi usada como uma maneira de mudar o comportamento das pessoas […]. Isto nos faz perceber como, através da observação, o corpo e a mente do indivíduo estão constantemente sob interrogatório. Precisamos apenas observar como os usuários de *Facebook* restringem seu comportamento e sua imagem corporal através dos olhos dos outros. Isto impacta nos aspectos da biopolítica da vigilância, mas também, e talvez mais importante, ele tem um impacto sobre a forma como usamos a *Internet* para procurar perguntas para questões que talvez corra o risco de estabelecer a visão dominante da sociedade. Este link com o poder está no coração da relevância de Foucault e das ações da NSA. (O'NEILL, 2015, p. 8, tradução nossa)

Adentrando nos estudos da Sociedade de Controle de Deleuze (1992) e especificamente na análise *tecnófoba* de Bogard (1996), o autor já havia alertado acerca dos aspectos negativos de programas de vigilância como os da NSA. A hipervigilância propicia cada vez mais a ausência de privacidade o que afeta diretamente a vida de indivíduos e outros atores das relações

de poder, sendo esta um instrumento utilizado por quem possui capacidades diferenciadas nessa arena, tais como autoridades (Estado), empresas e *hackers*.

Como visto, entretanto, Shapiro (1999) e Saco (2002) levantam a discussão acerca da eventualidade da existência de uma privacidade total. Seria este um valor pelo qual valeria a pena lutar frente à imposição de um superpanóptico tais como os programas da NSA? Isto não geraria mais incertezas nos espaços sociotecnológicos? Grande parte dos argumentos a favor da vigilância estadunidense trilha este caminho ao afirmar que o mundo seria um lugar menos seguro sem a vigilância da NSA. Mas, apesar disso, questiona-se até que ponto a hipervigilância ao modo NSA seria saudável para as relações entre atores internacionais, tendo em vista que muitos dos alvos não necessariamente são inimigos declarados dos EUA e, em alguns casos, são até mesmo aliados, como os países europeus.

Dessa maneira, a visão da vigilância perpetrada pela NSA como um superpanóptico que a todos vigia e controla acaba gerando um sentimento de desconforto e ameaça dentro do cenário das relações internacionais. Programas como o *PRISM* e o *Muscular* ainda demonstram que nem mesmo as empresas que agem dentro do escopo do ciberespaço e da informática, e que agem em âmbito multinacional, estão fora do jogo da vigilância; o *X-Keyscore* e o *Tempora*, adicionam o perigo às redes de transmissão de dados; e o *Stateroom* ainda levanta suspeitas acerca das representações diplomáticas.

As alegações de que apenas metadados são subtraídos e interpretados, em sua maioria, por máquinas que codificam os indivíduos em busca de elementos que os reconheçam enquanto uma possível ameaça à segurança, também não parece diminuir as tensões a nível internacional, principalmente quando documentos vazados demonstram análises específicas e detalhadas de líderes nacionais, a presidente do Brasil, Dilma Rousseff e o presidente mexicano, Enrique Pieña Nieto (ver Anexo I).

Por essas questões que se percebe uma corrida tecnológica no sentido de superar o déficit das relações de *cyberpower* no sistema internacional. As acusações de Snowden acerca da hipervigilância da NSA levantaram questionamentos se de fato o *Big Brother* de Orwell não estaria sendo colocado em prática pelos EUA. Os investimentos em tecnologia de defesa do ciberespaço, como apontado em tabela no capítulo 1, demonstram esse fenômeno.

Observar os programas da NSA enquanto um superpanóptico que coloca em prática uma hipervigilância global auxilia na compreensão do processo de construção da ameaça vigente e da necessidade dos investimentos como apontado. Entretanto, esta visão não consegue responder a questões como quem está sendo de fato vigiado e analisado ou por que hoje em dia é tão fácil adquirir informações pessoais tidas como privadas em um passado não muito

distante. Não se questiona aqui o poder de vigilância cibernética real da NSA, mas como as mudanças sociais do final do século XX puderam auxiliar, até certo ponto, em sua implementação.

3.2.2 Implicações da contemporaneidade à hipervigilância da NSA

Apesar de se observar características panópticas claras nos programas de vigilância da NSA, como visto anteriormente, é importante também examinar outros aspectos que auxiliam na compreensão desse fenômeno. Segundo Lyon (2014), analisar a vigilância da NSA e de seus aliados apenas como sendo do tipo panóptica é perigoso por gerar um pânico crescente sobre as possibilidades de os indivíduos serem controlados pelos Estados.

Lyon (2014) ressalta principalmente o aspecto de automação da vigilância estadunidense como característica principal de que não é intenção do Estado controlar a todos de forma ininterrupta:

> A automação da vigilância deve também ser vista como um aspecto da forma em que a vigilância ocorre enquanto um procedimento de gestão de rotina. [...] A automação da vigilância é parte dos tipos de exercícios de corte de gastos e eficiência que vem dominando a administração pública há décadas. Longe de ser "um Estado que sabe tudo, o que temos na verdade é uma infinidade de projetos parciais e iniciativas que estão buscando aproveitar as TICs no serviço de conhecer e governar melhor os indivíduos e populações" (RUPPERT, 2012, p. 118). (LYON, 2014, p. 6, tradução nossa)

Logo, se o processo não é panóptico, "então também não é diretamente disciplinar" (LYON, 2014, p.6, tradução nossa). Todavia, o autor não nega a influência que a vigilância perpetrada pela NSA possui na vida dos indivíduos e atores que estão susceptíveis à espionagem, o que ele busca demonstrar é que não é intenção destes programas disciplinar a sociedade nos moldes apresentados por Foucault.

Dentro de uma abordagem pós-panóptica, influenciada pela lógica neoliberal da tentação e da sedução das TICs (como apontado no capítulo anterior), os comportamentos almejados pelos gerenciadores da vigilância da NSA são obtidos muito mais de forma voluntária que imposta. Os perfis dos indivíduos montados pelos programas da agência a partir da aquisição dos metadados partem de códigos muitas vezes doados de forma não coercitiva. Não que a aquisição ilegal dessas informações, como visto na apresentação dos documentos

vazados, seja algo aceito pela sociedade (como será visto posteriormente), mas muitos desses dados já estão a acesso do público e a autovigilância do tipo sinóptica auxilia nesse processo.

Outra questão é que a sedução e a tentação, características sociais marcantes da modernidade líquida segundo Bauman (2001), não estão ligadas apenas no que diz respeito às TICs, mas a quase todos os aspectos da vida social. Portanto, a autovigilância do tipo "faça você mesmo" está intrinsecamente ligada também com questões de segurança. Se ceder informações pessoais, mantendo a autodisciplina, auxilia na manutenção da sensação de segurança, se há um ganho nesse ato, então esta cessão passa a ser vista como algo benéfico e natural pelos indivíduos, mesmo dentro de um ambiente de incertezas, e não como um processo que gera um pânico geral.

Como alertaram Bauman e Lyon (2013), a segurança transformou-se atualmente em um jogo de previsões e a vigilância aos moldes da NSA vem para tentar prever futuras ameaças à segurança nacional dos EUA, algo que Lyon (2014) chamou de "antecipação", comum não apenas na vigilância, mas em tudo o que tange o ciberespaço (antecipação de comportamento, de gostos, de compras, etc.). Didier Bigo (2006) ainda ressalta que a segurança atualmente opera continuamente em qualquer coisa que se mova, seja ela seres humanos, mercadorias ou informações em forma de dados digitais. Perde-se a noção de fronteira e, assim como no processo de globalização, a segurança e a vigilância percorrem todo o globo de forma fluida.

Dessa maneira, atenta-se para as constantes cooperações entre a NSA e outras agências no mundo a fim de alcançar outros patamares de níveis de vigilância. A segurança estadunidense (e também dos outros atores) há tempos não depende mais apenas de uma estrutura firme em suas fronteiras, mas de um sistema global que consiga prever futuras ameaças. Não por acaso, as alegações do governo de Obama ressaltam a necessidade de programas como a NSA a fim de manter a paz, a liberdade e a democracia, o que não deixa necessariamente de ser uma contradição, típica dos tempos líquidos.

Os processos de definição dos alvos da NSA, entretanto, vêm sendo criticados de forma contundente por especialistas. Kundnani e Kumar (2015) chamam a atenção para o fato de que os principais indivíduos catalogados pelos programas da NSA são americanos de origem muçulmana. Em uma lógica ban-óptica, a NSA também vem utilizando as tecnologias de vigilância com o intuito de traçar perfis de indivíduos-alvo, entre pessoas "desejadas" e "indesejadas" a partir de perfis sociais discriminatórios[72]. Segundo os autores, toda a revolta

[72] Sobre a discriminação de muçulmanos: "Na década de 80, mas especialmente depois do 11/9, um processo já estava em curso em que 'Muçulmanismos' eram racializados através da vigilância - outro cenário de produção de tópicos raciais do Estado. Tendo em vista que todos os racismos são socialmente e politicamente construídos em

surgida em 2013 com o vazamento das informações de que todos estariam sendo vigiados não teve a mesma reação eufórica quando descobriu-se que a maioria dos alvos eram muçulmanos, isso porque:

> Enquanto muitos se opõem ao governo dos EUA recolher dados privados sobre pessoas "comuns", os muçulmanos tendem a ser vistos como alvos razoáveis de suspeita. Uma pesquisa de julho de 2014 do Instituto Árabe-Americano descobriu que 42 por cento dos americanos acham que é justificável que as agências de aplicação da lei tracem perfis de americanos-árabes ou americanos-muçulmanos. (KUNDNANI & KUMAR, 2015, s/p, tradução nossa)

Se por um lado características panópticas poderiam gerar sensações de ameaça geral na população, suas características ban-ópticas acabam gerando tais sentimentos em povos específicos, como os árabes. Claro que os receios quanto a uma vigilância nos moldes da NSA são gerais – e isso torna-se perceptível nos principais discursos de atores internacionais como será visto no próximo tópico – mas a partir do momento em que há um foco principal a ser espionado, os discursos passam ser contraditórios, assim como as ameaças. As investidas estadunidenses no âmbito da vigilância passam, assim, a serem fonte também de um agravamento nas relações do ocidente com o mundo árabe, advindas de um histórico problemático que teve seu estopim nos atentados de 11 de setembro.

São muitos os aspectos da contemporaneidade que implicam não apenas no *modus operandi* dos programas da NSA, mas em sua própria formação. Logo, sem esmiuçar os detalhes em cada tópico específico, buscou-se apresentar tais características de forma a permitir uma visão distinta das abordagens clássicas. São essas categorias que nos permitem compreender não apenas o porquê de alguns usuários fornecerem seus dados de forma tão disciplinada e não questionadora, mas também como estes atores adentram e participam do processo de vigilância, sendo eles próprios alvo e vigilante, seja dentro da lógica da vigilância "faça você mesmo", do sinóptico ou do ban-óptico.

Como será apresentado a seguir, tais percepções auxiliam na ampliação de uma abordagem panóptica do caso de vigilância da NSA e de seus aliados e colocam em questionamento uma série de discursos proferidos pelos atores envolvidos no caso. Se por um lado há uma condenação veemente da vigilância cibernética global por parte de alguns agentes, de outro percebe-se um discurso mais *soft* quando tange os principais alvos e a defesa da segurança internacional frente ao terrorismo. Da mesma maneira, muitas vezes são "deixados

---

vez de baseados na realidade de alguma "raça" biológica, é perfeitamente possível que marcas culturais associadas a 'Muçulmanismos' (formas de se vestir, rituais, línguas, etc.) transformem-se em significantes raciais." (KUNDNANI & KUMAR, 2015, s/p, tradução nossa)

de lado" os aspectos que permitiram a formação desses programas em primeiro lugar, propagando discursos de ameaças mas não agindo na base do problema, escondendo falhas internas e programas de vigilância próprios.

Posto isto, uma análise à luz da abordagem de securitização da Escola de Copenhague, auxiliada pelos aspectos levantados até então, parece promover um apanhado do processo de construção das ameaças à segurança internacional no que tange a vigilância cibernética global, com foco no caso dos programas da NSA. A vigilância é vista aqui como uma arma fundamental dentro do novo *front* de conflitos internacionais e analisada conforme as perspectivas da securitização levantadas no capítulo anterior.

3.3 Ameaças vigilantes: a securitização do *Big Brother* global

Percebe-se até aqui que, dentro da lógica da cibersegurança, a vigilância cibernética perpetrada pela NSA apresenta-se como um importante instrumento de ação dos EUA e alguns aliados dentro da nova arena de conflitos sociotecnológica. As respostas dos atores internacionais e a defesa dos programas por parte dos interessados, entretanto, muitas vezes parecem ambíguas no que diz respeito a um consenso internacional acerca das ameaças e virtudes provenientes desse caso.

A fim de examinar se há de fato um processo de securitização da vigilância cibernética global a partir desse caso específico, torna-se necessário investigar os principais discursos securitizadores dos atores envolvidos no processo, sua aceitação e seus respostas frente ao fato ocorrido. Isso dentro da abordagem multissetorial proporcionada pela Escola de Copenhague, a partir de seus setores militar, político, econômico, societal e cibernético, como apresentado no capítulo anterior.

Sabe-se que a militarização do ciberespaço já é uma realidade dentro do contexto internacional e a vigilância da NSA apresenta-se como reflexo deste processo. Já sua politização, pode ser observada a partir dos discursos proferidos internacionalmente, como veremos a seguir. O setor econômico influencia na securitização da vigilância a partir do momento em que grandes empresas tecnológicas são acusadas de fazerem parte das espionagens; seus discursos também influenciam nesse processo. A sociedade apresenta-se como principal alvo da vigilância e também como reflexo da construção de ameaças, através de grupos de direitos civis e comunidades tech.

Por fim, o cibersetor mostra-se de extrema importância neste processo de securitização por permitir uma análise a partir do ciberespaço, arena por excelência do caso estudado. Além disso, os três padrões de segurança apresentados são percebidos de forma clara na vigilância cibernética estadunidense: o efeito em cadeia dos acontecimentos que tiveram início no ciberespaço mas atingiram diretamente outros setores (hipersecuritização); a sensação de insegurança cotidiana por parte dos usuários, o que auxiliou no sentimento de hipersecuritização do caso (práticas de segurança do dia-a-dia); e os discursos técnicos, sejam os da NSA na defesa dos programas, ou da comunidade tech e dos grupos de direitos civis condenando a espionagem, como será visto nesta seção, legitimando ou deslegitimando a vigilância da NSA (tecnificação).

Têm-se, então, como objetos referentes alguns Estados, alvos diretos ou indiretos da espionagem estadunidense. Já como atores securitizadores, somam-se a esse grupo a própria NSA, o governo dos EUA e seus aliados do *Five Eyes*. Por fim, atores funcionais de mesma importância, tais como as empresas acusadas de repassar informações à NSA, a mídia, os grupos de direitos civis e comunidades tech, a população através de manifestações e o próprio Edward Snowden.

3.3.1 Respostas internacionais

A partir da divulgação dos documentos referentes às atividades de espionagem dos EUA por Edward Snowden, diversos Estados e outros atores internacionais buscaram responder às acusações, causando uma série de tensões bilaterais e multilaterais, inclusive entre aliados, como o Brasil, a Alemanha e a União Europeia.

Diversos incidentes mostraram tanto a preocupação dos EUA e aliados, como o grupo *Five Eyes*, em frear a divulgação dos dados sigilosos, quanto as recriminações internacionais ao caso, tais como tentativas de censurar os veículos midiáticos[73], o pouso forçado do avião que levava o presidente da Bolívia, Evo Morales, com suspeitas de estar transportando Edward Snowden[74], o fechamento da empresa responsável pela troca de e-mails de Snowden com os

[73] Disponível em: <http://.huffingtonpost.com/2013/06/28/army-blocks-the-guardian_n_3515374.html> Acesso em 2 fev 2016

[74] Disponível em: <http://g1.globo.com/bom-dia-brasil/noticia/2013/07/aviao-de-evo-morales-e-obrigado-pousar-por-suspeita-de-levar-snowden.html> Acesso em 2 fev 2016

jornalistas do *The Guardian*[75], os impactos financeiros às empresas de tecnologia americanas[76], entre outros.

As principais respostas internacionais seguiram uma linha clara de condenação do caso. Apesar disso, percebe-se três tipos de reações principais entre os atores: o apoio aberto à vigilância da NSA, como o presidente russo, Vladimir Putin, apoiou[77], inclusive alegando que gostaria de possuir um programa semelhante; o choque inicial seguido de condenações ambíguas com o intuito de acalmar os ânimos internos, angariar apoio internacional, mas sem afetar profundamente as relações com os EUA e sem demonstrar total discordância com a vigilância cibernética – tendo em vista que muitos Estados possuem programas semelhantes; e a condenação de fato, mas esta veio principalmente através de outros órgãos ligados aos governos e de grupos não-estatais que diretamente de estadistas.

As reações brasileiras, por exemplo, tiveram que responder a certas pressões. Tornou-se perceptível uma necessidade de um entendimento entre os atores envolvidos devido ao abalo no sistema causado pela divulgação do programa de vigilância e as consequências para a segurança internacional, além da exigência de uma explicação por parte dos EUA acerca dos alvos da espionagem, ao mesmo tempo em que foi necessário pesar o custo/benefício de enfrentar um Estado de grande porte; cresceu também o consenso no meio internacional da necessidade de negociações para a solução dos problemas advindos do uso do ciberespaço, principalmente no que tange à governança da *internet*, nas quais o Brasil se prontificou a tomar os rumos.

Em relação às demandas de um posicionamento da presidente Dilma frente aos EUA, foi visto que ela procurou calcular os custos entre uma reação mais enfática contra um dos seus maiores parceiros comerciais e as perdas que teria internamente caso adotasse uma posição completamente oposta. Ao mesmo tempo em que ela cancelou um encontro que teria com o presidente Obama, demonstrando que não aceitaria a espionagem de seu país, procurou manter um discurso brando em relação aos EUA, como pode ser percebido durante a abertura do Debate Geral da 68ª Assembleia-Geral das Nações Unidas:

> Quero trazer à consideração das delegações uma questão à qual atribuo a maior relevância e gravidade. Recentes revelações sobre as atividades de uma rede global de espionagem eletrônica provocaram indignação e repúdio em amplos setores da opinião pública mundial. [...] Dados pessoais de cidadãos foram indiscriminadamente

[75] Disponível em: <http://.wired.com/2013/08/lavabit-snowden/> Acesso em 2 fev 2016
[76] Disponível em: <http://.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html> Acesso em 2 fev 2016
[77] Disponível em: <https://.washingtonpost.com/news/worldviews/wp/2013/06/13/vladimir-putin-defends-the-u-s-on-spying-programs-drones-and-occupy-wall-street/> Acesso em 2 fev 2016

> objeto de interceptação. Informações empresariais – muitas vezes com alto valor econômico e mesmo estratégico – estiveram na mira da espionagem. Também representações diplomáticas brasileiras, entre elas a Missão Permanente junto às Nações Unidas e a própria Presidência da República do Brasil tiveram suas comunicações interceptadas. [...] imiscuir-se dessa forma na vida dos outros países fere o direito internacional e afronta os princípios que devem reger as relações entre eles, sobretudo, entre nações amigas. [...] Não se sustentam argumentos de que a interceptação ilegal de informações e dados destina-se a proteger as nações contra o terrorismo. O Brasil, senhor presidente, sabe proteger-se. Repudia, combate e não dá abrigo a grupos terroristas. (ROUSSEFF, 2013, s/p)

A presidente ainda continua seu discurso clamando pela não militarização do ciberespaço e por negociações a nível internacional:

> As tecnologias de telecomunicações e informação não podem ser novo campo de batalha entre os Estados. Este é o momento de criamos as condições para evitar que o espaço cibernético seja instrumentalizado como arma de guerra, por meio da espionagem, da sabotagem, dos ataques contra sistemas e infraestrutura de outros países. (ROUSSEFF, 2013, s/p)

Nas negociações da 68ª Assembleia-Geral das Nações Unidas, o Brasil, em conjunto com a Alemanha, formulou um projeto de resolução no qual busca resguardar os direitos à privacidade na era digital, cuja aprovação foi unânime dentre os 193 Estados-membros. Apesar de o documento não ter caráter vinculante, para o Itamaraty isto "demonstra o reconhecimento, pela comunidade internacional, de princípios universais defendidos pelo Brasil", como afirma reportagem da BBC[78].

Gills Lopes (2013) ainda ressalta que o governo brasileiro, através do Ministério da Defesa e de outros órgãos ligados ao Executivo, também vem buscando ampliar o debate interno acerca de segurança cibernética através de eventos acadêmico-militares. Isto acaba influenciando nas negociações internacionais ao permitirem um maior aparato técnico para o governo. Outra medida adotada foi o aumento nos investimentos em segurança cibernética.

A busca por novas vias que impeçam ou intimidem ações de espionagem e/ou de ataques cibernéticos, entretanto, não é algo novo. Desde o lançamento da Estratégia Nacional de Defesa de 2008[79] que o país já define um fortalecimento do setor cibernético. Outra medida prévia à espionagem americana foi a criação de um projeto em 2011 envolvendo os países do BRICS – Brasil, Rússia, Índia, China e África do Sul – para a ligação destes Estados através de fibra

[78] Disponível em: <http://.bbc.co.uk/portuguese/noticias/2013/12/131218_onu_espionagem_ac.shtml> Acesso em: 08 jan 2014

[79] Disponível em: <http://.mar.mil.br/diversos/estrategia_defesa_nacional_portugues.pdf> Acesso em: 08 jan 2014

óptica, buscando construir uma "nova *internet*" que não dependa exclusivamente dos EUA e da Europa.

Apesar disso, em recente postagem no Twitter, Edward Snowden chama a atenção para o fato de que Dilma Rousseff continua a utilizar telefones não criptografados, como no recente caso de vazamento das escutas obtidas pelo juiz Sérgio Moro nas acusações de corrupção contra o ex-presidente Lula. Em sua conta no Twitter, Snowden afirma que: "'Going dark'[80] é um conto de fadas: três anos após as manchetes de escuta de @dilmabr ela ainda está fazendo chamadas não criptografadas"[81]. Sendo assim, apesar das alegações de investimento em segurança cibernética, o uso de telefone não criptografado por um dos alvos da espionagem americana demonstra uma forte contradição no discurso brasileiro.

Já as reações alemãs trilharam caminhos semelhantes. Condenou-se as acusações de espionagem e exigiu-se respostas do governo americano através do embaixador estadunidense na Alemanha à época dos vazamentos, Philip D. Murphy, não apenas às espionagens referentes ao Estado alemão, mas também a outras instituições e Estados europeus[82].

Como resposta, a Alemanha cancelou um histórico tratado assinado com os EUA, o Reino Unido e a França durante a Guerra Fria, no qual os países ocidentais poderiam pedir da Alemanha informações de vigilância referentes ao período. Ao mesmo tempo, segundo reportagem da BBC[83], a quebra desse tratado não trouxe sérias consequências para as relações entre os países, tendo em vista que ele nunca havia sido invocado. Dessa forma, percebe-se tática semelhante a utilizada pela presidente do Brasil, responder sem necessariamente atacar. Ao mesmo tempo em que acalma os ânimos de uma população que já sofreu com a vigilância durante as ditaduras nazista e o comunista, não se pretendeu cortar as relações de forma enfática com os EUA.

Isso tanto se mostra pelas alegações posteriores aos vazamentos de que a Alemanha auxiliou a CIA no processo de vigilância através da sua agência de inteligência, BND. O programa chamado *Project 6* possuiu o intuito de vigiar cidadãos alemães com o fim de evitar ataques terroristas nos mesmos moldes dos outros programas da NSA apresentados anteriormente. Foram criados perfis de usuários com o intuito de vigiar suas ações online e

[80] A expressão "going dark" refere-se ao uso de criptografia nas comunicações.
[81] Disponível em: "https://twitter.com/Snowden/status/710560657637306368> Acesso em 20 mar 2016
[82] Disponível em: <https://.rt.com/news/germany-summons-us-ambassador-leaks-476/> Acesso em 2 fev 2016
[83] Disponível em: <http://.bbc.com/news/world-europe-23553837> acesso em 2 fev 2016

identificar possíveis informantes jihadistas[84], o que demonstra que não apenas os EUA agem através da vigilância, mas também outros Estados, como a Alemanha.

Em diálogo com o presidente dos EUA, Barak Obama, a chanceler Angela Merkel, inclusive, alertou para a necessidade de cooperação entre os países no que tange a segurança cibernética:

> Falamos sobre questões da *Internet* no contexto da *PRISM*. Conversamos longamente sobre as novas possibilidades e sobre como as novas ameaças que a *Internet* se abre para todos nós. A *Internet* é um novo território, um território desconhecido para todos nós. E também permite acesso aos nossos inimigos. Ela permite aos inimigos de uma ordem livre e liberal, usá-la, abusá-la, trazer uma ameaça para todos nós, ameaçar o nosso modo de vida. E é por isso que valorizamos a cooperação com os Estados Unidos sobre questões de segurança. (MERKEL, 2013, s/p, tradução nossa)

A chanceler, entretanto, também condena a forma como a NSA age, mas sem negar a importância da vigilância:

> Eu também noto, no entanto, que embora nós percebamos a necessidade da aquisição de informações, é necessário que haja a *devida diligência* também no que diz respeito à proporcionalidade. Livres, *democracias liberais vivem de pessoas que possuem um sentimento de segurança*. E é por isso um *equilíbrio justo* deve ser atingido; é necessário que haja proporcionalidade. E isso é algo que nós concordamos, *ter uma livre troca de visões*, entre a nossa equipe, mas também com a equipe do Ministério de Interior dos Estados Unidos e também com o ministro de Interior aqui na Alemanha. E isso vai ser uma batalha em curso. (MERKEL, 2013, s/p, tradução nossa, grifo nosso)

Observa-se, assim, uma resposta ambígua da chanceler alemã. Ao mesmo tempo em que exige a "devida diligência" e afirma que "democracias liberais vivem de pessoas que possuem um sentimento de segurança", demonstrando ressalvas quanto aos programas da NSA, termina afirmando ser necessário "ter uma livre troca de visões" entre EUA e Alemanha, demonstrando abertura para uma possível cooperação na área de vigilância no que diz respeito à segurança.

No que diz respeito à União Europeia, o Conselho Europeu também exigiu respostas aos EUA e alegou que a falta de confiança entre os aliados poderia prejudicar a cooperação. Entretanto, os países não tiveram o mesmo posicionamento, enquanto Alemanha e França focaram nas acusações de espionagem, o Reino Unido, aliado histórico dos EUA e membro do *Five Eyes*, demonstrou maiores preocupações com a traição de Snowden. Já o Parlamento

[84] Disponível em: <http://.spiegel.de/international/germany/cia-worked-with-bnd-and-bfv-in-neuss-on-secret-project-a-921254.html> Acesso em 2 fev 2016

Europeu pediu sanções contra os EUA através da suspensão das negociações de um acordo de livre comércio com o país, mas os líderes das nações europeias negaram tal pedido[85].

De acordo com o relatório de inquérito elaborado pelo Parlamento, a luta contra o terrorismo nunca pode "por si só, ser uma justificativa para programas de vigilância em massa sem alvos, secretos e às vezes até ilegais". Segundo o membro britânico do Parlamento Europeu, Claude Moraes, "privacidade não é um direito de luxo, mas a pedra fundamental de uma sociedade livre e democrática" e ainda complementa ser "muito duvidoso que uma coleta de dados de tal magnitude só seja guiada pela luta contra o terrorismo, uma vez que envolve a aquisição de todos os dados possíveis de todos os cidadãos; logo, aponta para a possível existência de outros motivos, tais como espionagem política e econômica"[86].

A necessidade de tais respostas que busquem calcular ganhos e perdas, internos e externos, parte principalmente da reação condenatória da sociedade e da intensa cobertura dos vazamentos pela mídia que teve papel crucial não apenas na divulgação, mas também foi a ponte entre Edward Snowden e a revelação dos programas, e um dos principais meios de investigação. Sofreram tentativas de censura, tendo o Primeiro Ministro britânico alertado a imprensa que caso não parassem os vazamentos, o governo teria que agir[87]. Vários meios midiáticos tiveram papel de protagonista no caso, tais como *The Washington Post* e *The New York Times*, nos EUA, *The Guardian*, na Inglaterra, *Der Spiegel*, na Alemanha, *O Globo*, no Brasil, *Le Monde*, na França, *El País*, na Espanha, entre outros.

Diversos protestos foram organizados ao redor do mundo, tais como o *Restore the Forth*[88] que reuniu pessoas em mais de 80 cidades estadunidenses em meados de 2013[89]; o *Stop Wacthing Us* (Pare de Nos Assistir), no final de 2013, que teve o apoio de mais de 85 organizações de direitos civis e tecnologia[90]; e o The Day We Fight Back (O Dia em que Nós Revidamos), um protesto digital global no qual mais de seis mil *web*sites publicaram a seguinte mensagem: "Cara *Internet*, nós estamos cansados de reclamar sobre a NSA. Queremos novas

[85] Disponível em: <http://.huffingtonpost.com/2013/10/25/eu-nsa-spying_n_4164559.html> Acesso em 2 fev 2016
[86] Disponível em: <http://.dw.com/en/eu-report-reveals-massive-scope-of-secret-nsa-surveillance/a-17352243> Acesso em 2 fev 2016
[87] Disponível em: <http://uk.reuters.com/article/uk-usa-spying-cameron-idUKBRE99O0K120131028> Acesso em 2 fev 2016
[88] Um jogo de palavras no qual "forth" possui semelhança fonética com "force"; pode ser traduzido como "restaure a quarta", em relação à quarta emenda da Constituição americana que protege a privacidade, mas também pode ter o sentido de "restaure a força".
[89] Disponível em: <http://edition.cnn.com/2013/07/04/tech/web/restore-nsa-protests> Acesso em 2 fev 2016
[90] Disponível em: <https://rally.stopwatching.us/> Acesso em 2 fev 2016

leis que restrinjam a vigilância online. Hoje nós revidamos.", e ainda auxiliaram cidadãos americanos a peticionarem junto a congressistas por novas leis[91].

Organizações não-governamentias de direitos civis, como a Anistia Internacional, a Human Rights Watch, a Transparência Internacional, a Index on Censorship, a Eletronic Frontier Foundation, entre outras, também protagonizaram condenações aos programas e demandaram a proteção de Edward Snowden pelos EUA, além de apoiarem os protestos civis ocorridos.

Por fim, as empresas de tecnologias citadas no programa *PRISM* também responderam às revelações da vigilância da NSA. Todas negaram qualquer envolvimento com o *PRISM* e afirmaram desconhecer o programa. A cessão de informações para o governo só poderia ocorrer através de demandas judiciais e qualquer outra forma deveria ser considerada ilegal. As empresas também alegaram que levam a sério a privacidade e os direitos de seus usuários[92], mas isso não impediu uma queda na receita das companhias envolvidas. Segundo reportagem do *The New York Times*[93], todas tiveram grandes perdas, tendo a *Microsoft*, inclusive, perdido o contrato com o governo brasileiro.

Apesar de não haver uma resposta consensual dos principais atores envolvidos no caso, há certas semelhanças que nos permitem delinear algumas linhas narrativas. A exigência de respostas dos EUA; a condenação da vigilância cibernética aos moldes da NSA; o descontentamento com a espionagem entre nações aliadas; as reações ambíguas quanto a respostas diretas e a instituição de sanções devido à relevância dos EUA; e a descrença acerca de seus fins de combate ao terrorismo, são algumas das respostas mais encontradas até então. A nível internacional, a maioria das reações seguiram nesta mesma linha.

Mesmo com as condenações e o crescimento do receio de ter seus dados monitorados pela NSA, principalmente por parte da sociedade civil, os EUA e seus aliados defenderam os programas de vigilância como essenciais para a segurança nacional e do mundo ocidental. Entretanto, algumas ressalvas foram feitas pelo governo de Obama e mudanças foram colocadas em prática a fim de amenizar os sentimentos de ameaça que cresceram nesse período.

---

[91] Disponível em: <http://thehill.com/policy/technology/197859-thousands-of-sites-to-protest-nsa-spying> Acesso em 2 fev 2016.

[92] Disponível em: <http://techcrunch.com/2013/06/06/google-facebook-apple-deny-participation-in-nsa-prism-program/> Acesso em 2 fev 2016

[93] Disponível em: <http://.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html?_r=0> Acesso em 2 fev 2016

3.3.2 Defesa dos programas de vigilância

A defesa dos programas partiu principalmente da própria NSA, do governo estadunidense e dos seus aliados. Como visto, as principais alegações dizem respeito a questões de segurança frente às ameaças de terrorismo, intensificadas no pós-11 de setembro. Em discurso em janeiro de 2014, Obama alegou que "o programa não envolve a NSA examinando os registros telefônicos de americanos comuns. Pelo contrário, ela consolida esses registros em um banco de dados que o governo pode consultar se ele tem uma pista específica" [94]. Dessa maneira, o presidente dos EUA tentou mostrar que os programas da NSA não estão examinando de forma ininterrupta todos os cidadãos, pelo menos os americanos, apenas quando há suspeitas de envolvimento com o terrorismo.

A controvérsia acerca da aquisição de informações privadas de cidadãos estadunidenses e estrangeiros, entretanto, teve como marco a Lei Patriótica (*Patriot Act*) de 2001. Esta legislação, aprovada nos EUA logo após os atentados contra as Torres Gêmeas, permitiu a interceptação de telefonemas e e-mails de organizações e pessoas que estivessem sob suspeita de ligação com o terrorismo, sem a necessidade de autorização do judiciário. Durante o governo Obama, ela obteve uma extensão de mais quatro anos em 2011, tendo expirado em 2015[95].

No mesmo discurso citado anteriormente, entretanto, Obama alegou que entende as preocupações nacionais e internacionais e que estaria buscando reformar os programas de inteligência, principalmente os que envolvem a vigilância:

> Nos últimos seis meses, eu criei um Grupo externo de Análise de Inteligência e Tecnologias de Comunicações para realizar recomendações para a reforma. Eu consultei o Conselho de Supervisão de Privacidade e Liberdades Civis, criado pelo Congresso. Eu escutei parceiros estrangeiros, defensores da privacidade e líderes da indústria. Meu governo gastou incontáveis horas pensando como abordar a inteligência nesta época de ameaças difusas e revolução tecnológica. (OBAMA, 2014, s/p, tradução nossa)

As reformas de Obama culminaram em uma nova lei, a Lei de Liberdade (*Freedom Act*), contendo legislação semelhante à Lei Patriótica, mas com algumas modificações que

---

[94] Disponível em: <http://.nytimes.com/2014/01/18/us/politics/obamas-speech-on-nsa-phone-surveillance.html?_r=0> Acesso em 4 fev 2016

[95] Disponível em: <http://.npr.org/sections/thetwo-way/2015/05/31/411044789/live-blog-facing-midnight-deadline-the-senate-debates-parts-of-the-patriot-act> Acesso em 4 fev 2016

buscaram proteger liberdades civis ao mesmo tempo em que garantiriam a segurança nacional[96]. Fato é que a defesa da legalidade dos programas de vigilância da NSA partiram principalmente de legislações como a Lei Patriótica que, segundo alegações do governo estadunidense, obteve inúmeros sucessos na luta contra o terrorismo[97]. As pressões advindas das respostas internacionais e internas às revelações dos programas de vigilância, entretanto, possibilitaram mudanças na legislação que exigissem da NSA a demanda de autorização judicial para obter os dados provenientes das interceptações.

As respostas da NSA trilharam caminhos semelhantes, afirmando que os programas não coletam informações acerca dos conteúdos dos dados adquiridos, mas apenas os metadados dessas informações. Para a agência, a coleta é completamente legal, tendo em vista que nem todos os dados armazenados são analisados por seres humanos, e ainda ressalta que esse processo não deve ser categorizado como vigilância, pelo menos até que um agente de fato analise os dados. Segundo o diretor da NSA, General Keith Alexander, "a agência age sob regras que a impedem de investigar os chamados '*haystack of data*'[98] a menos que tenha uma justificação 'razoável, articulável', envolvendo comunicações com terroristas no exterior"[99].

Quanto aos vazamentos realizados por Snowden, o governo americano prontamente classificou o ex-agente como um traidor, pedindo sua prisão imediata. Em discurso, Obama alegou não acreditar que Snowden tenha agido como patriota, colocando toda a nação em estado de alerta e atentando contra a segurança. O presidente dos EUA ainda alegou que Snowden poderia ter utilizado outros canais para alertar acerca dos excessos cometidos pelos agentes da NSA que não colocasse a nação em risco. Obama também acrescentou que os americanos estariam melhor se não soubessem acerca dos programas da NSA e que antes dos vazamentos seu governo já estava elaborando reformas no que tange a vigilância[100].

O Reino Unido, cuja agência de inteligência, GCHQ, aparece nos documentos de Snowden como aliada na NSA, confirmou a troca de dados com os EUA e defendeu que tais programas são importantes na garantia da segurança dos cidadãos e na luta contra o terrorismo. O ministro das Relações Exteriores, William Hague, afirmou que não há o que temer, pois o

---

[96] Disponível em: <http://.usatoday.com/story/news/politics/2015/06/02/patriot-act-usa-freedom-act-senate-vote/28345747/> Acesso em 4 fev 2016

[97] Disponível em: <http://.nytimes.com/2014/01/18/us/politics/obamas-speech-on-nsa-phone-surveillance.html> Acesso em 4 fev 2016

[98] Algo como palheiro de dados, referindo-se à expressão "agulha no palheiro".

[99] Disponível em: <http://.theatlantic.com/politics/archive/2013/10/why-the-nsas-defense-of-mass-data-collection-makes-no-sense/280715/> Acesso em 4 fev 2016

[100] Disponível em: <http://edition.cnn.com/2013/08/12/politics/obama-snowden-whistleblower> Acesso em 4 fev 2016

governo não está escutando ligações nem lendo dados provenientes da *internet* de usuários comuns. Em entrevista, o ministro alegou que:

> Se, na verdade, pudéssemos dizer ao mundo inteiro, ou a todo o país, como fazemos este negócio, eu acho que as pessoas seriam enormemente tranquilizadas e elas veriam que os cidadãos cumpridores dos direitos não têm nada para se preocupar. Mas se nós o fizéssemos, isso iria destruir o objeto. Este é um trabalho secreto... é segredo por uma razão. (HAGUE, 2013, s/p)[101]

O governo australiano também tentou minimizar os impactos dos vazamentos. O ministro das Relações Exteriores, Bob Carr, do partido governista à época, afirmou que o governo iria "examinar cuidadosamente quaisquer implicações no que emergiu para a segurança e privacidade dos australianos". Entretanto, partidos de oposição, como o partido Verde, exigiram maiores explicações do governo acerca de sua participação nos programas de vigilância da NSA[102]. Em reportagem do jornal australiano, Crikey, afirma-se que enquanto o mundo exige respostas dos EUA, "o governo australiano quer que a coisa toda suma e nos diz que não há nada com que se preocupar"[103].

O único líder de governo, fora os EUA, a defender de forma clara a espionagem americana, entretanto, foi Vladimir Putin, presidente da Rússia. Seja pelos conflitos históricos com os EUA, pela força política ou pelo pouco espaço delegado à opinião pública na Rússia, Putin, que deu asilo político a Edward Snowden, alegou acreditar que "todo mundo tem consciência há muito tempo que o *Signals Intelligence* diz respeito à vigilância de pessoas e organizações". Disse ainda que Snowden não revelou nada que eles já não soubessem e que essa prática vem se tornando comum no combate ao terrorismo internacional[104].

Ao mesmo tempo em que não condenou o uso da vigilância, todavia, Putin elaborou uma crítica direta ao *modus operandi* dos EUA:

> [...]pelo menos na Rússia, você não pode simplesmente ir e grampear uma conversa por telefone de alguém sem um mandado emitido por tribunal. Isso é mais ou menos a forma como uma sociedade civilizada deve agir na luta contra o terrorismo com a tecnologia moderna. Enquanto ela é exercida dentro dos limites da lei que regula as atividades de inteligência, está tudo bem. (PUTIN, 2013, s/p)[105]

---

[101] Disponível em: <http://.telegraph.co.uk/news/politics/william-hague/10108560/Nothing-to-fear-from-GCHQ-says-William-Hague.html> Acesso em 4 fev 2016

[102] Disponível em: <http://motherboard.vice.com/blog/surveillance-for-all-foreign-governments-responses-to-the-prism-scandal-are-enlightening> Acesso em 4 fev 2016

[103] Disponível em: <http://.crikey.com.au/2013/06/14/australias-supine-reaction-to-our-surveillance-planet/> Acesso em 4 fec 2016

[104] Disponível em: <http://motherboard.vice.com/blog/surveillance-for-all-foreign-governments-responses-to-the-prism-scandal-are-enlightening> Acesso em 4 fev 2016

[105] Disponível em: <http://motherboard.vice.com/blog/surveillance-for-all-foreign-governments-responses-to-the-prism-scandal-are-enlightening> Acesso em 4 fev 2016

Sendo assim, percebe-se que a defesa dos programas da NSA teve sempre como base a condenação dos atos de Snowden; a definição da vigilância enquanto arma de combate ao terrorismo internacional; a afirmação de que cidadãos que não estão vinculados a atividades ilegais, principalmente o terrorismo, não estão sendo vigiados (porém, seus metadados armazenados); e a tentativa de amenizar as ameaças geradas através principalmente de discursos apaziguadores.

Provas documentais de que as alegações da defesa são verdadeiras, entretanto, não foram apresentadas até então[106], apenas a modificação da Lei Patriótica para a Lei de Liberdade é apontada como tomada de decisão a fim de diminuir a ameaça da vigilância global. Críticas acerca da quebra da legislação americana no processo de espionagem demonstram, todavia, que muitos dos argumentos são apenas atos de fala que não condizem com a realidade.

Segundo editorial do *The Atlantic*[107], é possível apontar 5 falhas na defesa dos programas de vigilância: 1) ela não está de acordo com a lei de grampo dos EUA, que o define como tal a partir de sua aquisição e não de sua leitura por um indivíduo; 2) é inconstitucional por desrespeitar a quarta emenda que proíbe mandados genéricos, ou seja, que não descrevem lugar, pessoas e/ou coisas a serem apreendidas; 3) não há legislação que defina quando, como, onde e por quanto tempo o governo pode ter acesso ao cotidiano das pessoas; 4) os dados armazenados podem ser hackeados por ataques externos, mesmo que a NSA afirme que mantém a segurança, não há garantias, e Snowden está aí para provar isso; 5) a história mostra que a reação dos seres humanos quando estão em posição de poder, no caso, os funcionários da NSA, pode ser perigosa.

Além disso, a noção de terrorismo internacional também faz parte de uma construção social e não há um consenso global acerca desse fenômeno, tendo sido diversas vezes modificado dentro do contexto da Guerra ao Terror dos EUA. Sendo assim, afirmar que a NSA apenas espiona os dados de indivíduos que possuem ligação com o terrorismo é um discurso amplo, não há uma noção clara do que os defensores querem dizer ao alegar tal condição. Se um pesquisador árabe da área, por exemplo, realiza constantes buscas na *internet* acerca do tema, tem relações com outros pesquisadores internacionais e mantém uma comunicação online, o que garante que seus dados não serão analisados? Se máquinas são responsáveis pela

---

[106] Disponível em: <http://.theatlantic.com/politics/archive/2013/10/why-the-nsas-defense-of-mass-data-collection-makes-no-sense/280715/> Acesso em 4 fev 2016

[107] Disponível em: <http://.theatlantic.com/politics/archive/2013/10/why-the-nsas-defense-of-mass-data-collection-makes-no-sense/280715/> Acesso em 4 fev 2016

filtragem dos metadados coletados, tal hipótese torna-se completamente possível e o pesquisador terá seu direito à privacidade subtraído.

Somando-se isto às denúncias de Snowden de abusos por parte dos funcionários da NSA, já citados neste trabalho, percebe-se que de fato há uma linha tênue entre o que se armazena e o que se vigia dentro dos programas apresentados. Os discursos internacionais que condenam a prática e exigem respostas do governo estadunidense não perdem força, assim, frente às repostas elaboradas por seus defensores.

3.3.3 Uma ameaça vigilante

Dentro de uma lógica panóptica, os discursos apresentados no meio internacional, tanto de resposta ao caso quanto de defesa, demonstram que há um sentimento de ameaça aos direitos individuais, principalmente por parte da sociedade e de organizações civis que vêm se manifestando contra os programas da NSA. A aceitação dos discursos securitizadores veiculados por Estados-alvo, pela mídia e por outras organizações, vem apresentando respaldo internacional, principalmente através dos altos investimentos em segurança cibernética (como visto no quadro 1) e pelo crescimento do tema nas agendas de debates internacionais.

Casos como o dos programas de vigilância da NSA fizeram com que temas como direito à privacidade, respeito aos direitos humanos e cibersegurança ganhassem cada vez mais espaço nas agendas de debate, além de trazerem o Estado e a sociedade civil de volta ao centro das discussões, colocando em cheque o próprio modo pelo qual a *internet* funciona, através de um regime privado imposto por Washington. Fóruns internacionais como o *Internet Governance Forum* (IGF), organizado pela ONU, e o *NETmundial*, que serve de preparatório para as reuniões do IGF, vêm debatendo amplamente o tema, tendo inclusive suas duas últimas edições ocorridas no Brasil, o primeiro nos dias 10 a 13 de novembro de 2015, em João Pessoa-PB, e o segundo nos dias 23 e 24 de abril de 2014, em São Paulo-SP. Tais debates, acabam por politizar as questões de segurança do ciberespaço e do seu uso como ferramenta de vigilância global.

Tal como apresentado no capítulo anterior, o processo de securitização não exige que as ações em resposta às ameaças sejam necessariamente através do uso da força, logo, os debates internacionais e os diálogos bilaterais com os EUA vêm sendo amplamente utilizados na tentativa de solução dos danos advindos da vigilância global. A militarização do ciberespaço, entretanto, vem se mostrando como algo real através de ataques por vírus, *DDoS*, *worms* e/ou

vigilância cibernética, e os investimentos em cibersegurança comprovam que há uma preocupação latente com as ameaças advindas dessa nova arena.

A participação das empresas também vem se mostrando fundamental na formulação das ameaças vigilantes. A acusação de que grandes corporações tecnológicas são as principais responsáveis na coleta de dados acaba por torná-las um dos alvos centrais dos atores que buscam espionar tais informações. Mesmo que as companhias citadas no *PRISM* não tenham de fato participação no programa, o que se mostra pouco provável devido às evidências, elas foram as responsáveis pela cessão de diversos dados sigilosos que apenas deveriam ter sido repassados por ordem judicial.

Utilizando os conceitos apresentados por Hansen e Nissenbaum (2009), percebe-se que a vigilância perpetrada pela NSA atingiu um nível de hipersecuritização ao extrapolar as ameaças geradas em âmbito cibernético para diversos outros setores da sociedade. Isto, somado aos receios da população em ter seus dados vigiados, mesmo que muitas vezes cedam tais informações de modo voluntário, e aos discursos de entidades de direitos civis e de tecnologia, o que acabou tecnificando o caso, resultam em uma legitimação das ameaças vigilantes.

Os aspectos da contemporaneidade na hipervigilância da NSA, entretanto, parecem trazer outras questões importantes ao debate da securitização do tema. As tentações e seduções da sociedade atual, conforme Bauman (2001) demonstrou, apontam para uma noção ambígua acerca dos benefícios e malefícios de uma vigilância que promete uma sensação de segurança confortável nos padrões atuais, pelo menos para os povos ocidentais. Os discursos políticos contraproducentes de parte dos Estados-alvo também parecem legitimar uma visão de que a intenção real não é buscar soluções para a vigilância global, confortável também para os Estados que temem o terrorismo e que possuem programas semelhantes, mas apenas demonstrar força política.

A disciplina advinda de mini-panópticos individuais, típicos de indivíduos ávidos por mais tecnologias e formas de compartilhar seus feitos em redes sociais, e que geram as contradições apresentadas aqui, não parecem, entretanto, diminuir a necessidade de se manter um devido processo legal na aquisição de informações, uma transparência, que lhes permitam conhecer em qual terreno estão pisando. Não há nas manifestações civis e estatais qualquer negação da importância do programa enquanto arma contra o terrorismo, mas uma exigência em manter o ciberespaço transparente e livre de ameaças não visíveis, pelo menos entre seus "iguais". Essa visão corrobora com o ban-óptico de Bigo (2006) e com a análise de Kundnani e Kumar (2015) ao demonstrarem um teor discriminatório nos programas da NSA quando

observaram que 42% dos entrevistados americanos concordam ser necessário a criação de perfis digitais de árabes-americanos.

Isso entretanto, não nega os receios da sociedade frente ao ciberespaço como ele se encontra hoje: uma arena hipersecuritizada, militarizada e politizada. Como aponta Bruce Schneier (2013):

> Ao ceder à NSA a capacidade de conduzir uma vigilância ubíqua em todo mundo, cedemos a ela uma enorme quantidade de controle sobre nossas próprias vidas. Uma vez que a NSA pega uma cópia de seus dados, você já não os controla. Você não pode excluí-los. Você não pode mudá-lo. Você pode até mesmo nem saber quando as regras segundo as quais ela usa seus dados mudam. E até o momento em que Edward Snowden vazou os documentos que mostram o que a NSA está fazendo, você nem sabia que o governo os tinha tomado. (SCHNEIER, 2013, s/p, tradução nossa)

Sendo assim, as ameaças vigilantes, com todas as suas características ban-ópticas, contradições e ambiguidades, mostram-se não apenas verdadeiras, mas ainda em curso, gerando uma série de consequências para a segurança internacional refletidas tanto em debates que envolvem Estados, agências burocráticas, corporações e sociedade, quanto na militarização de sua arena por excelência. Observa-se alguns ensaios que buscam amenizar as sensações de ameaça, mas o fim da vigilância cibernética não parece ser um objetivo dos principais atores envolvidos. A defesa da necessidade de programas como os da NSA afasta essa hipótese.

CONSIDERAÇÕES FINAIS

A influência dos novos espaços sociotecnológicos nas relações sociais, em todas as suas áreas, já é um fato incontestável nos diversos campos das ciências humanas. Nas Relações Internacionais não é diferente e, apesar das análises sobre o tema ainda serem incipientes, elas vêm se apresentando como ferramentas necessárias não apenas para a ampliação dos debates, mas também na compreensão de como essa nova arena digital gera efeitos e impactos no meio internacional. Tais estudos são importantes para a compreensão da sociedade atual – que vê seus padrões mudarem em consonância com o desenvolvimento tecnológico – ao delinearem perspectivas de como ela vem lidando com esse fenômeno ao perceber o surgimento de novas questões, tais como os programas de vigilância da NSA.

Não é possível afirmar, todavia, que há um determinismo tecnológico em ação atualmente, no qual as TICs apontam os caminhos que a sociedade deve tomar. O que ocorre é um processo de co-construção social, a partir das demandas cotidianas ou da criação de novas necessidades. É esse processo de gera significados às TICs, o que os novos dispositivos *são* e o que eles *passam a ser* depois de apropriados socialmente através do seu uso diário. O *Facebook* e o *Twitter* não foram imaginados para o fim de organizar revoluções políticas. Os sistemas bancários digitais também não surgiram com o intuito de ampliar fraudes. Assim como a forma pela qual a *internet* funciona não foi gerada necessariamente para a criação de um sistema de vigilância cibernética global tal como o perpetrado pelos EUA.

Nesse sentido, o presente trabalho buscou contribuir para o debate acerca da vigilância cibernética, ao apontar perspectivas de como o processo de apropriação da *internet* para fins de vigilância e espionagem influencia no cotidiano das relações humanas, principalmente no que diz respeito à construção de ameaças intersubjetivas e, consequentemente, à sensação de segurança em um ambiente digital global com pouca ou nenhuma ordenação jurídica a nível internacional. Dessa maneira, com o intuito de compreender se há um *Big Brother* global, nos moldes da vigilância perpetrada no distóptico *1984* de George Orwell, buscou-se delinear dois processos: 1) tanto o de formação do ciberespaço através de suas principais características; 2) quanto o de apropriação deste para fins de vigilância, exemplificado pelos programas da agência estadunidense, e a consequente geração de ameaças no meio internacional.

Para alcançar tais objetivos e responder às indagações, entretanto, uma série de outras etapas foram elaboradas no percurso. Como variável comum às áreas do estudo proposto, foram apresentadas primeiramente as principais características do ciberespaço que proporcionaram o

surgimento dos programas de vigilância da NSA, visto aqui como um espaço aberto e pervasivo que se infiltra pelos mais diversos tecidos sociais, gerando espaços sociotecnológicos aptos à interação dos indivíduos através de diferentes meios e trocas de informação.

Isso, claro, tem impacto também nas Relações Internacionais que não deixam de ser uma área das relações humanas. Dentro de uma nova lógica interacional chamada por Rothkopf (1998) de *cyberpolitik* – que modifica a estrutura, devido à relativização do tempo e do espaço nos meios digitais, mas não as relações de poder – observa-se, entre efeitos positivos e negativos, o crescimento dos conflitos digitais – dentre os quais ressalta-se a vigilância cibernética para fins deste trabalho – que colocam em risco a segurança internacional e dão base à formação do conceito de cibersegurança.

A fim de compreender o papel da vigilância como dimensão-chave do ciberespaço securitizado, realizou-se um apanhado dos estudos panópticos de Foucault (1988), que enxerga na vigilância uma ferramenta de disciplina e controle social; desenvolveu-se essa análise a fim de transportar os estudos panópticos para a sociedade informacional, através dos conceitos de Deleuze (1992), Bogard (1996), Shapiro (1999) e Saco (2002), demonstrando, assim, que a sociedade atual consegue fomentar através das TICs uma hipervigilância dentro de um superpanóptico digital.

Apontou-se também as abordagens de Bauman e Lyon (2013) acerca das características da contemporaneidade, da modernidade líquida, e como elas influenciam na vigilância cibernética. Os estudos pós-panópticos demonstram como a vigilância hoje sai da lógica do controle centralizado e espalha-se pelas mais diferentes brechas da sociedade, podendo estar presente no próprio ser humano (ao internalizar as características da modernidade líquida), nas instituições, ou a quilômetros de distância em alfândegas e aeroportos.

Quando aplicados estes conceitos à segurança internacional, optou-se por uma abordagem da Escola de Copenhague por permitir a manutenção das importantes análises de Foucault e Bauman, ao mesmo tempo em que propiciou observar o espaço cibernético como uma arena securitizada e a formação de ameaças, enquanto processo intersubjetivo, a partir dos discursos dos diversos agentes envolvidos nos sistemas de vigilância cibernética, servindo, dessa maneira, como base teórica para o estudo do caso dos programas de vigilância da NSA. Logo, buscou-se apreender como essa vigilância cibernética em nível global foi fomentada e securitizada no sistema internacional.

Foram apresentados seis programas de vigilância cibernética da agência estadunidense: *PRISM*, *Boundless Informant*, *X-Keyscore*, *Tempora*, *Muscular* e *Stateroom*. A partir desse levantamento, observou-se que estes possuem características técnicas avançadas, que o escopo

de ação da vigilância abrange uma grande parte dos fluxos de dados no mundo e que operam fundamentados em um híbrido *vigilância + segurança*, a fim de prever ameaças futuras e prevenir que elas ocorram. Suas características panópticas e pós-panópticas também apontam para uma estrutura construída com o objetivo de vigiar qualquer indivíduo independente de sua localização e, mesmo que não seja intenção da NSA perpetuar uma vigilância de todos e de forma ininterrupta, apenas a possibilidade de que isso ocorra já pode ser visto como um gerador de ameaças ao indivíduo, ainda que este muitas vezes compartilhe dados pessoais de forma voluntária na lógica contemporânea das redes sociais.

Dessa maneira, considera-se que a hipervigilância global da NSA atingiu um nível de hipersecuritização ao extrapolar a arena digital e adentrar em outros setores como o militar, o político, o econômico e o social. Em uma abordagem panóptica, observa-se que os discursos securitizadores dos principais agentes, o que inclui Estados, organizações, empresas e grupos civis, apresentados no trabalho, acabaram gerando um sentimento de ameaça no que diz respeito ao receio de ter dados privados vigiados por agências de inteligência ao redor do mundo. Já através de perspectivas pós-panópticas, nota-se que, apesar das contradições existentes nos discursos, não há, na verdade, uma negação da importância da vigilância fomentada pela NSA e seus aliados no que diz respeito à segurança, mas a sensação de que o ciberespaço transparente, livre e pervasivo, enquanto valores da cibercultura, está sendo ameaçada por casos como este.

Não foi intenção da pesquisa, entretanto, apontar caminhos para a manutenção desses valores ou para o fim da vigilância cibernética global nos moldes em que se encontra. Antes, compreender como tais aspectos geram sentimentos de ameaças no meio internacional que terão consequências principalmente nos debates sobre segurança. Como visto, o vazamento dos programas da NSA já motivou a constituição de novas reuniões internacionais e o fortalecimento de antigas organizações que tratam do assunto com o intuito de ampliar as discussões e encontrar um caminho cooperativo que minimize as ameaças. Diálogos bilaterais, principalmente com os EUA, também apontam para o mesmo caminho.

Tendo o corpo do trabalho explicitado a argumentação acerca da vigilância cibernética como dimensão-chave da segurança, cabe retornar à questão central do tema proposto: há *de facto* atualmente um *Big Brother* global em ação? Importante ressaltar que não se trata aqui do governo nos moldes do *Big Brother* e seu Partido, uma ditadura totalitária disfarçada, como apresentado por George Orwell em *1984*. Antes, a analogia pretendida por este trabalho diz respeito à vigilância, ao controle e à perda da liberdade, problemas que, apesar de ligados a

estruturas políticas totalitárias, ainda convivem dentro de democracias sob alegações de perigos externos e outros discursos que conquistam "corações e mentes".

"*Abaixo o Big Brother!*" é a primeira frase que Winston escreve em seu diário, instrumento utilizado para expressar aquilo que jamais poderia falar em público acerca do partido, ao qual era filiado. Escondia-se em um "ponto cego" de seu apartamento enquanto escrevia, onde não poderia ser captado pela *teletela* e vigiado pela *Polícia do Pensamento*. "*Abaixo a NSA!*" poderia ter sido a primeira frase de Edward Snowden, que por um certo tempo também escondeu-se nos "pontos cegos" do ciberespaço a fim de revelar e derrubar uma instituição que utiliza a vigilância e a quebra da privacidade para alcançar seus objetivos.

O uso da espionagem por ambos os países – a fictícia Oceania (onde se passa a obra) e os EUA – também possuem fins semelhantes: o de angariar informações acerca da população (local e estrangeira) para evitar ataques à nação, seja uma revolta contra o partido do *Big Brother*, seja um ataque terrorista contra os norte-americanos. O que difere principalmente são os meios para conquistar o controle e a aceitação: enquanto o *Big Brother* impõe as normas do partido de forma ditatorial, os EUA buscam através de discursos convencer a opinião pública de que programas como os da NSA são essenciais na manutenção da segurança nacional e dos Estados aliados.

Em uma sociedade líquida ávida por segurança, a aceitação da vigilância pelo Estado não parece algo a ser descartado. Ainda é possível ir além: em uma sociedade voyeurista e espetacularizada, na qual público e privado confundem-se com facilidade, observar e ser observado já não é algo definido e imposto por governos, mas intrínseco às relações sociais. Não é por menos que o distópico *Big Brother* de Orwell tornou-se o nome de um *reality show*[108] no qual participantes são vigiados 24h por dia e o público pode interferir no andamento do programa através da interatividade.

Logo, é possível considerar *1984* como uma previsão da vigilância dos tempos atuais, pelo menos no que diz respeito à quebra da privacidade. A tecnologia a favor da vigilância invadiu computadores pessoais, *smartphones*, *tablets*, câmeras de segurança, detectores corporais, leitores biométricos, cartões de crédito, entre outros. Como afirmou Snowden, o mundo atual parece ser até mais imprevisível e perigoso que o governo do Big Brother (LYON, 2015), no qual nada além das imposições, da censura e da vigilância através da *teletela* era esperado. Claro que o indivíduo poderia ser *vaporizado* (desaparecer, nos termos da obra) por pensar diferente, mas no que tange a privacidade, nem mais um "ponto cego" para se esconder

[108] Programas de televisão baseados na vida real e com participantes não ficcionais.

a sociedade atual parece encontrar. O que Orwell não previu, todavia, foi que muitas dessas ameaças vigilantes seriam, na verdade, consentidas.

REFERÊNCIAS

AMARAL, Inês. **Jornalismo, self media, media sociais e a realidade dos "prosumers"**. 2009. Trabalho apresentado ao Seminário de Ciberjornalismo do Mestrado em Ciências da Comunicação da Universidade do Porto, Porto, 2009.

ASSANGE, Julian. **Cypherpunks:** Liberdade e o futuro da *internet*. São Paulo: Boitempo Editorial, 2013.

BAUMAN, Zygmunt. **Modernidade líquida**. Rio de Janeiro: Jorge Zahar Ed., 2001.

BAUMAN, Zygmunt; LYON, David. **Vigilância líquida**. Rio de Janeiro: Jorge Zahar Ed., 2013.

BECK, Ulrich. **O que é globalização?** Equívocos do globalismo: respostas à globalização. Tradução de André Carone. São Paulo: Paz e Terra, 1999.

BIGO, Didier. Globalized (in)security: the field and the ban-opticon. In: SAKAI, Naoki; Solomon, Jon (Orgs.). **Traces 4:** Translation, Biopolitics, Colonial Difference. Hong Kong: Hong Kong University Press, 2006.

BOGARD, William. **The simulation of surveillance – hypercontrol in telematic societies**. New York: Cambridge University Press, 1996.

BUZAN, Barry; WAEVER, Ole; WILDE, Jaap. **Security:** a New Framework for Analysis. Boulder and London: Lynne Rienner Publishers, 1998.

CANABARRO, Diego Rafael; BORNE, Thiago. Ciberespaço e *Internet*: Implicações Conceituais para os Estudos de Segurança. In: **MUNDORAMA**, 2013. Disponível em: <http://mundorama.net/2013/05/19/ciberespaco-e-*internet*-implicacoes-conceituais-para-os-estudos-de-seguranca-por-diego-rafael-canabarro-e-thiago-borne/> Acesso em: 08 jan 2014.

CASTELLS, Manuel. **A Sociedade em Rede**. Tradução de Roneide Venâncio Majer. 6. ed. v. 1. São Paulo: Paz e Terra, 1999.

CEPIK, Marco; CANABARRO, Diego; BORNE, Tiago. A securitização do ciberespaço e o terrorismo: uma abordagem crítica. In: SOUZA, André; NASSER, Reginaldo; MORAES, Rodrigo (Orgs.). **Do 11 de Setembto de 2001 à Guerra ao Terror:** reflexões sobre o terrorismo no século XXI. Brasília: IPEA, 2014.

CERVO, Amado Luiz; BUENO, Clodoaldo. **História da Política Exterior do Brasil**. 4. ed. Brasília: Editora UnB, 2011.

CHARAUDEAU, Patrick. **Discurso das mídias**. São Paulo: Contexto, 2009.

CHOUCRI, Nazli. **Cyberpolitics in International Relations**. Cambridge: The MIT Press, 2012.

CRUZ, Sebastião C. Velasco e. **Globalização, democracia e ordem internacional:** ensaios de teoria e história. Campinas: Editora da UNICAMP; São Paulo: Editora Unesp, 2004.

DELEUZE, Gilles. **Conversações**, 1972 – 1990. Rio de Janeiro: Ed. 34, 1992.

DUQUE, Marina Guedes. **A teoria da securitização e o processo decisório da estratégia militar dos Estados Unidos na Guerra do Iraque**. 2008. 181 f. Dissertação (Mestrado em Relações Internacionais) - Instituto de Relações Internacionais, Universidade de Brasília, Brasília. 2008.

FOUCAULT, Michel. **Microfísica do poder**. Rio de Janeiro: Graal, 1988.

_____. **Vigiar e punir:** nascimento da prisão. Petrópolis: Vozes, Ed. 25, 2002.

GREENWALD, Glenn. Entrevista. In: ARAÚJO, Elizângela. **"Governos dos EUA, Inglaterra e Canadá mentem o tempo todo".** Brasília: Carta Maior, 2013. Disponível em: <http://.cartamaior.com.br/?/Editoria/Internacional/-Governos-dos-EUA-Inglaterra-e-Canada-mentem-o-tempo-todo-/6/29163> Acesso em 30 jan 2016.

_____. Entrevista. In: REA, Kari. Glenn Greenwald: Low-Level NSA Analysts Have 'Powerful and Invasive' Search Tool. ABC News, 2013. Disponível em: <http://abcnews.go.com/blogs/politics/2013/07/glenn-greenwald-low-level-nsa-analysts-have-powerful-and-invasive-search-tool/> Acesso em 30 jan 2016.

HANSEN, Lene; NISSENBAUM, Helen. Digital Disaster, Cyber Security, and the Copenhagen School. **International Studies Quarterly**, n. 53, p. 1155–1175, 2009. Disponível em: <https://.nyu.edu/projects/nissenbaum/papers/digital%20disaster.pdf> Acesso em 30 jun 2015.

HARDING, Luke. **The Snowden Files:** The Inside Story of the World's Most Wanted Man. New York: Vintage Books, 2014.

ITU. Overview of cybersecurity. Geneva: ITU, 2009. Disponível em: <https://.itu.int/rec/T-REC-X.1205-200804-I> Acesso em 8 mar 2015.

_____. **Understanding cybercrime:** Phenomena, challenges and legal response. Geneva: ITU, 2012 Disponível em: <http://.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf> Acesso em 8 mar 2015.

JENKINS, Henry. **Cultura da convergência**. São Paulo: Aleph, 2008.

JORDAN, Tim. ***Cyberpower*:** The Culture and Politics of Cyberspace and the *Internet*. London: Routledge, 2003.

KEOHANE, Robert; NYE, Joseph. **Power and interdependence:** world politics in transition. Boston: Little, Brown and Company, 1977.

KUNDNANI, Arun; KUMAR, Deepa. Race, surveillance, and empire. **International Socialist Review**, n. 96, 2015. Disponível em: <http://isreview.org/issue/96/race-surveillance-and-empire> Acesso em 2 fev 2016.

LAKATOS, Eva M.; MARCONI, Marina. A. **Fundamentos de Metodologia Científica**. São Paulo: Atlas, 1991.

LATOUR, Bruno. **Ciência em Ação:** como seguir cientistas e engenheiros sociedade afora. São Paulo, Editora Unesp, 2000.

LEMOS, André. Cidade e Mobilidade. Telefones Celulares, funções pós-massivas e territórios informacionais. **Matrizes, Revista do Programa de Pós-Graduação em Ciências da Comunicação**, São Paulo, v. 1, n. 1, p. 121-137, 2007. Disponível em <http://.facom. ufba.br/ciberpesquisa/andrelemos/Media1AndreLemos.pdf>. Acesso em: 06 mar 2012.

LEMOS, André; LÉVY, Pierre. **O futuro da *internet*:** em direção a uma ciberdemocracia planetária. São Paulo: Paulus, 2010.

LEMOS, André; PALACIOS, Marcos (Orgs.). **Janelas do ciberespaço:** comunicação e cibercultura. 2. ed. Porto Alegre: Sulina, 2001.

LÉVY, Pierre. **A inteligência coletiva:** por uma antropologia do ciberespaço. 3. ed. São Paulo: Loyola, 2007.

_____. **As tecnologias da inteligência:** o futuro do pensamento na era da informática. Tradução de Carlos Irineu da Costa. Rio de Janeiro: Ed. 34, 1993.

LOBATO, Luísa; KENKEL, Kai. Discourses of cyberspace securitization in Brazil and in the United States. **Rev. bras. polít. int.** Brasília, v. 58, n. 2, jul-dez, 2015. Disponível em: < http://.scielo.br/scielo.php?script=sci_arttext&pid=S0034-73292015000200023&lng=en&nrm=iso&tlng=en> Acesso em 30 jun 2015.

LOPES, Gills. BRICS Cable: levando a cabo uma resposta brasileira à espionagem internacional?. In: **MUNDORAMA**, 2013. Disponível em: <http://mundorama.net/2013/ 09/28/brics-cable-levando-a-cabo-uma-resposta-brasileira-a-espionagem-internacional-por-gills-lopes/> Acesso em: 08 jan 2014.

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

LUCERO, Everton. **Governança da *Internet*:** aspectos da formação de um regime global e oportunidades para a ação diplomática. Brasília: FUNAG, 2011. Disponível em: <http://.funag.gov.br/biblioteca/dmdocuments/0514.pdf> Acesso em 10 jul 2014.

LYON, David. Surveillance, Snowden, and Big Data: Capacities, consequences, critique. **Big Data & Society**, p. 1-13, jul–dez, 2014. Disponível em: <http://bds.sagepub.com/content/spbds/1/2/2053951714541861.full.pdf> Acesso em 30 dez 2015.

_____. The Snowden Stakes: Challenges for Understanding Surveillance Today. **Surveillance & Society**, v. 13, n. 2, p. 139-152, 2015. Disponível em: <http://.surveillance-and-society.org/> Acesso em 30 dez 2015.

MANOVICH, Lev. **The language of new media**. Cambridge: The MIT Press, 2001.

MARCONDES, Valéria. Poder, vigilância e ciberespaço. **Sessões do Imaginário Cinema Cibercultura Tecnologias da Imagem**, Porto Alegre, ano 10, n. 13, p. 72-79, 2005. Disponível em: <http://revistaseletronicas.pucrs.br/fo/ojs/index.php/famecos/article/viewFile/864/651> Acesso em: 20 dez 2014.

MARTÍN-BARBERO, Jesús. Globalização comunicacional e transformação cultural. *In:* MORAES, Denis de (Org.). **Por uma outra comunicação:** mídia, mundialização cultural e poder. 5. ed. Rio de Janeiro: Record, 2010.

MATHIESEN, Thomas. The viewer society: Michel Foucault's panopticon revisited. In: **Theoretical Criminology**, v. 1, n. 2, p. 215-234, 1997.

MERKEL, Angela. Remarks by President Obama and German Chancellor Merkel in Joint Press Conference. Berlim, 2013. Disponível em: <https://.whitehouse.gov/the-press-office/2013/06/19/remarks-president-obama-and-german-chancellor-merkel-joint-press-confere> Acesso em 2 fev 2016.

NSA. **About NSA**. Washington: NSA, 2011. Disponível em: < https://.nsa.gov/about/> Acesso em 30 jun 2015.

NYE, Joseph S. **O paradoxo do poder americano.** Por que a única superpotência do mundo não pode prosseguir isolada. São Paulo: Editora UNESP, 2002.

O'NEILL, Timi. **Michel Foucault and the NSA Panopticon**. 2015. Disponível em: <https://.academia.edu/9290473/Michel_Foucault_predicts_the_NSAs_cyber_Panopticon> Acesso em 30 jan 2016.

OBAMA, Barak. **Obama's Speech on N.S.A. Phone Surveillance**. Washington, 2014. Disponível em: <http://.nytimes.com/2014/01/18/us/politics/obamas-speech-on-nsa-phone-surveillance.html> Acesso em 4 fev 2016.

ONUF, Nicholas. Worlds of Our Making: The Strange Career of Constructivism in International Relations. In: PUCHALA, Donald J. **Visions of International Relations:** Assessing an Academic Field. Columbia: University of South Carolina Press, 2002.

ORWELL, George. **1984**. 29ª ed. São Paulo: Ed. Companhia Editora Nacional, 2005.

PAIT, Heloisa & PINHEIRO, Ruan. Vazamento de informações: um ritual democrático na era da comunicação em rede. In: **Cadernos Adenauer: Cibersegurança**, Rio de Janeiro, n. 4, p. 09-32, 2014.

RABAÇA, Carlos Alberto; BARBOSA, Gustavo. **Dicionário de Comunicação**. Rio de Janeiro: Campus, 1995.

ROTHKOPF, David J. Ciberpolitik: the changing nature of power in the Information Age. **Journal of International Affairs**, v. 51, 1998.

ROUSSEFF, Dilma. **Discurso da Presidenta da República na abertura do Debate Geral da 68ª Assembleia-Geral das Nações Unidas**. Nova York: ONU, 2013. Disponível em: <http://www2.planalto.gov.br/acompanhe-o-planalto/discursos/discursos-da-presidenta/discurso-da-presidenta-da-republica-dilma-rousseff-na-abertura-do-debate-geral-da-68a-assembleia-geral-das-nacoes-unidas-nova-iorque-eua> Acesso em 8 jan 2014.

RUDZIT, Gunther. O debate teórico em segurança internacional: mudanças frente ao terrorismo?. **Civitas**, Porto Alegre, v. 5, n. 2, p. 297-323, jul-dez. 2005.

RUPPERT, E. The governmental topologies of database devices. **Theory, Culture and Society**, n. 29, p. 116–136, 2012.

SACO, Diana. **Cybering Democray:** public space and *Internet*. London: Electronic Mediations, 2002.

SCHJOLBERG, Stein. **The History of Global Harmonization on Cybercrime Legislation** – The Road to Geneva. 2008. Disponível em: <http://cybercrimelaw.net/documents/cybercrime_history.pdf> Acesso em 08 mar 2015.

SCHNEIER, Bruce. **Why the NSA's Defense of Mass Data Collection Makes No Sense**. The Atlantic, 2013. Disponível em: <http://.theatlantic.com/politics/archive/2013/10/ why-the-nsas-defense-of-mass-data-collection-makes-no-sense/280715/> Acesso em 4 fev 2016.

SEIB, Philip. **Real-time Diplomacy:** politics and power in the social media era. Nova York: Palgrave Macmillan, 2012.

SHAPIRO, L. Andrew. **The control revolution:** how the *internet* is putting individuals in charge and changing the world we know. New York: A century foundation book, 1999.

SILVA FILHO, Edison; MORAES, Rodrigo (orgs.). **Defesa nacional para o século XXI:** política internacional, estratégia e tecnologia militar. Rio de Janeiro: Ipea, 2012. Disponível em:<http://.ipea.gov.br/portal/index.php?option=com_content&view=article&id=15955> Acesso em: 4 fev 2016.

STOCKINGER, Gottfried. A interação em ciberambientes e sistemas sociais. In: LEMOS, André; PALACIOS, Marcos (Orgs.). **Janelas do ciberespaço:** comunicação e cibercultura. 2. ed. Porto Alegre: Sulina, 2001.

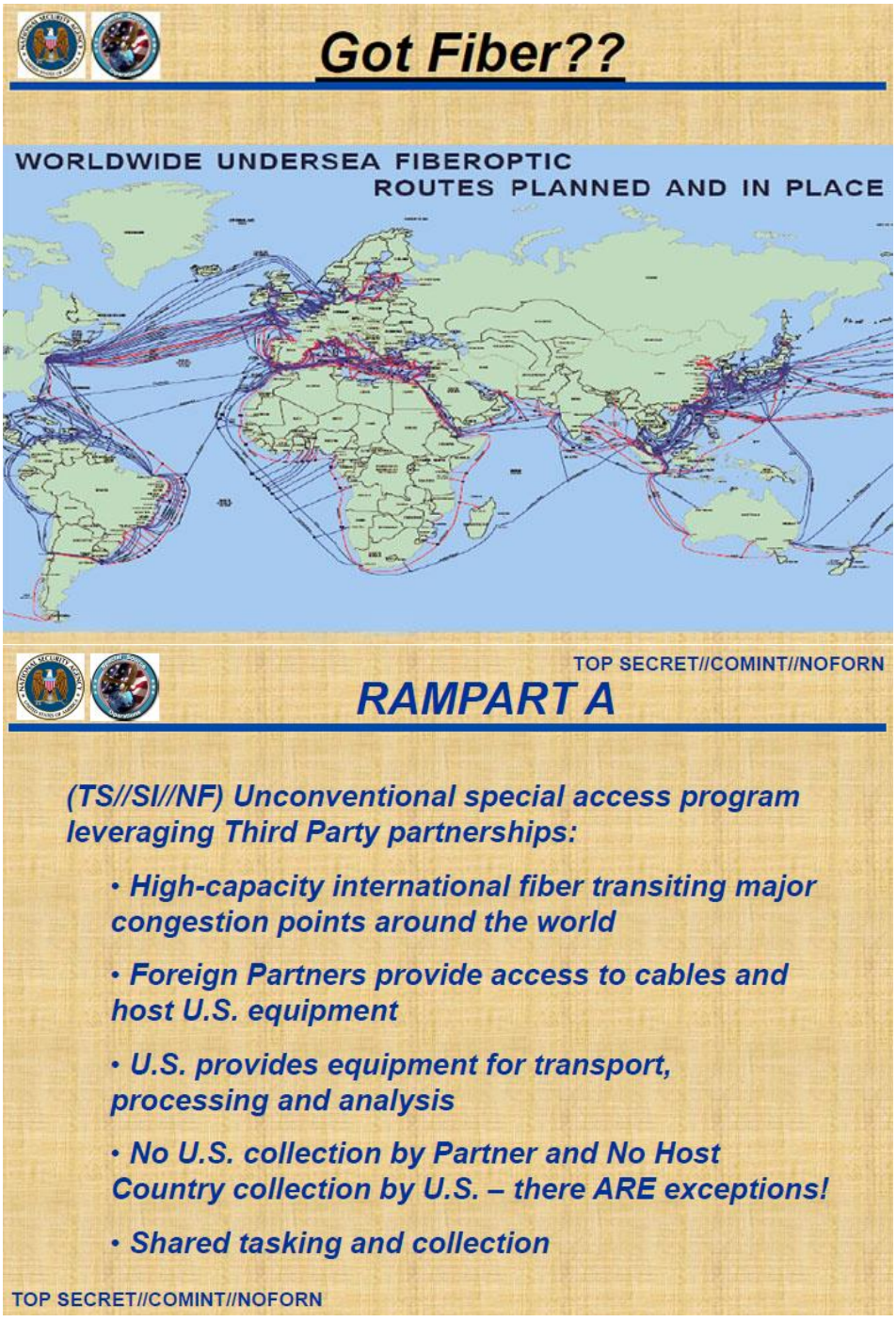
VALENTE, Leonardo. **Política externa na era da informação:** o novo jogo do poder, as novas diplomacias e a mídia como instrumentos de Estado nas Relações Internacionais. Rio de Janeiro: Revan, 2007.

WALLERSTEIN, Immanuel. A reestruturação capitalista e o sistema-mundo. *In*: GENTILI, Paulo (Org.). **Globalização excludente:** desigualdade, exclusão e democracia na nova ordem mundial. 4. ed. Petrópolis: Vozes; Buenos Aires: CLACSO, 2000.

WENDT, Alexander. Collective identity formation and the international state. **American Political Science Review**, Los Angeles, v. 88, n. 2, p. 384-396, jun. 1994.

ANEXOS

ANEXO A – Rotas dos cabos de fibra óptica

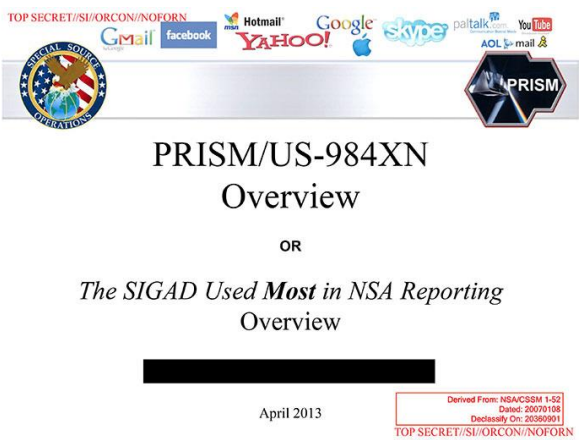


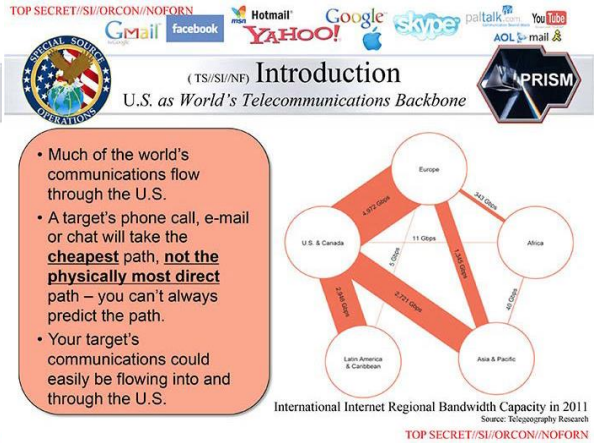
FONTE: Disponível em: <https://theintercept.com/2014/06/18/nsa-surveillance-secret-cable-partners-revealed-rampart-a/> Acesso em 20 fev 2016

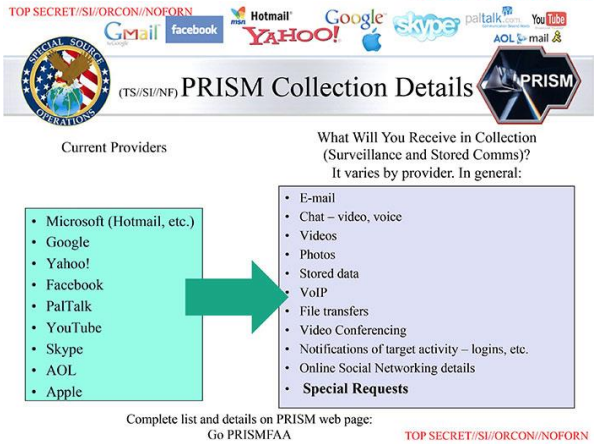
ANEXO B – Parceiros da NSA nos programas de Vigilância

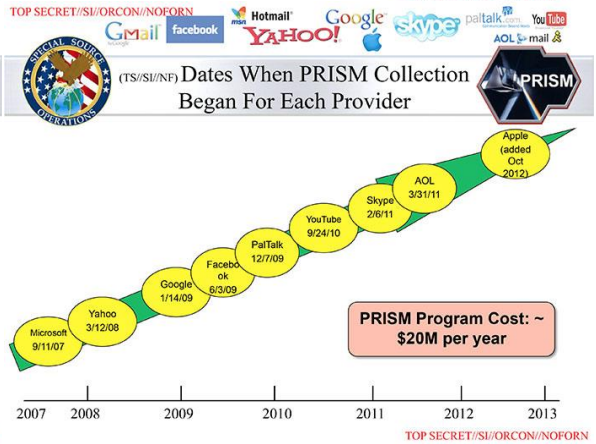
FONTE: Disponível em: <https://theintercept.com/2014/06/18/nsa-surveillance-secret-cable-partners-revealed-rampart-a/> Acesso em 20 fev 2016

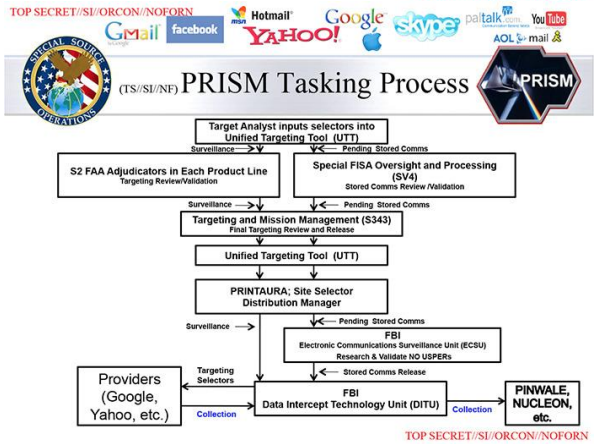
ANEXO C – Documentos do *PRISM*

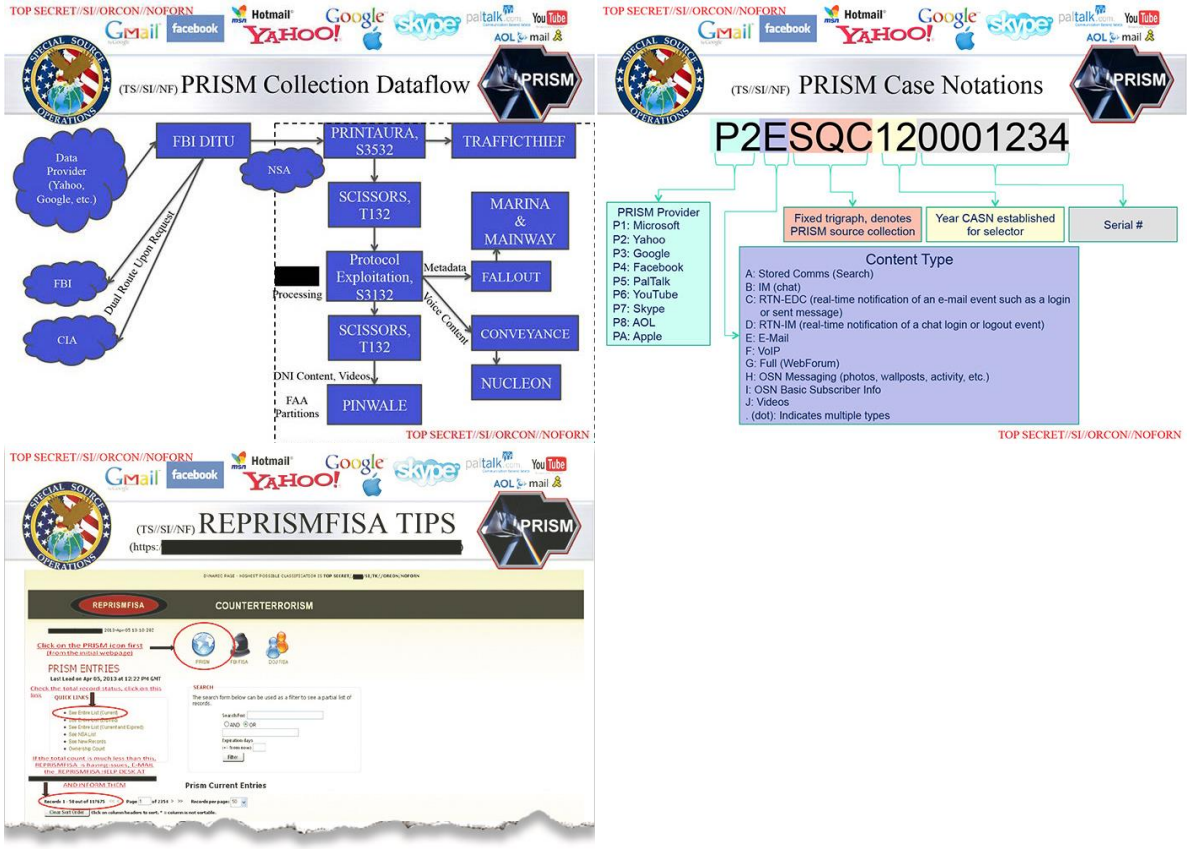










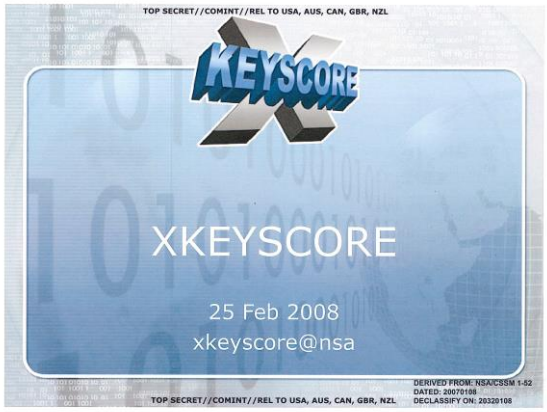


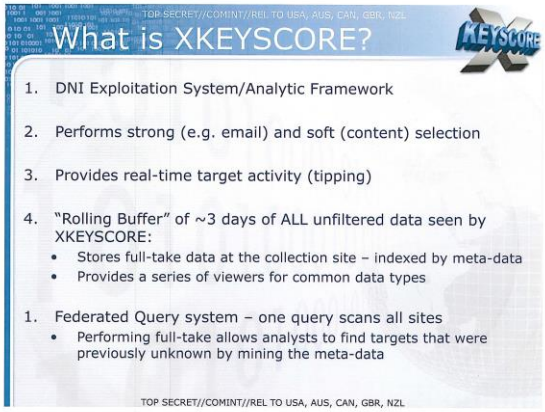
FONTE: Disponível em: <https://pt.scribd.com/doc/213627960/NSA-PRISM> Acesso em 20 fev 2016

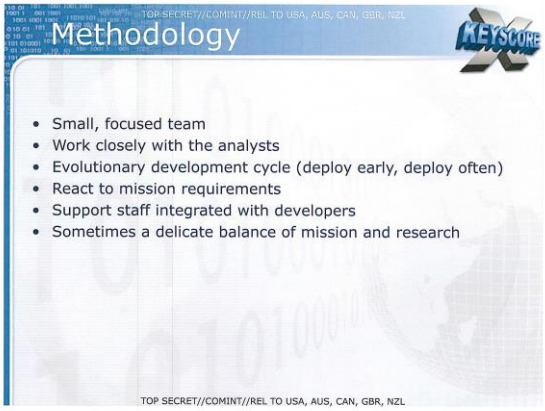
ANEXO D – Documentos do *Boundless Informant*

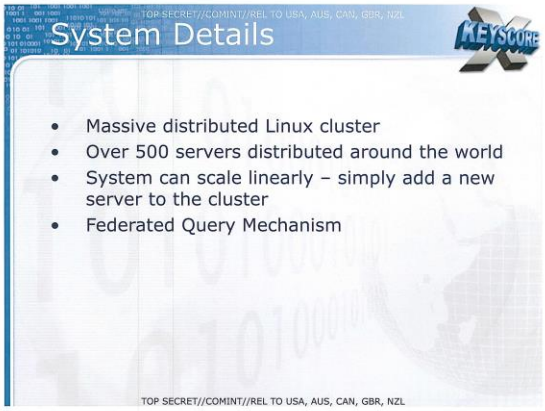
FONTE: Disponível em: <https://leaksource.info/2013/06/13/nsa-files-verizon-prism-boundless-informant-fisa-702-xkeyscore-whistleblower-edward-snowden-interview/> Acesso em 20 fev 2016

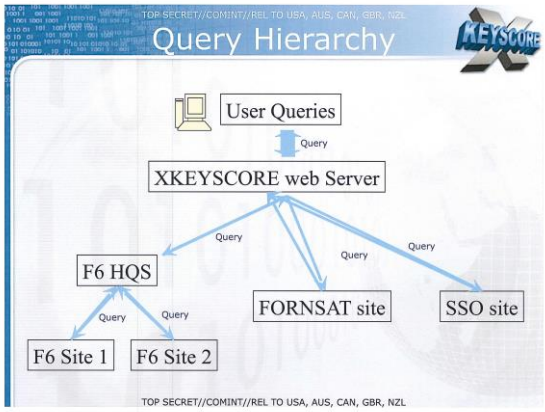
ANEXO E – Documentos do *X-Keyscore*

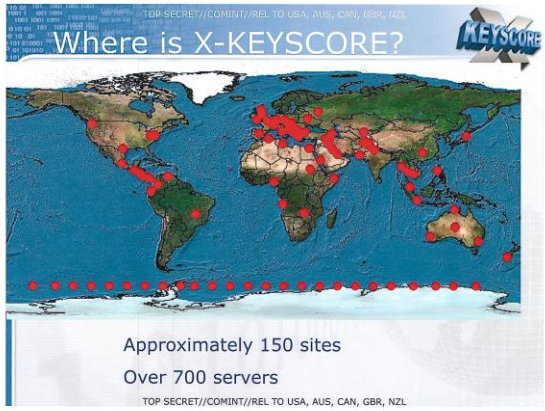


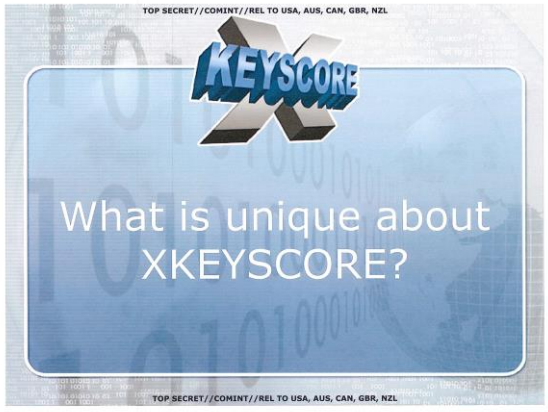


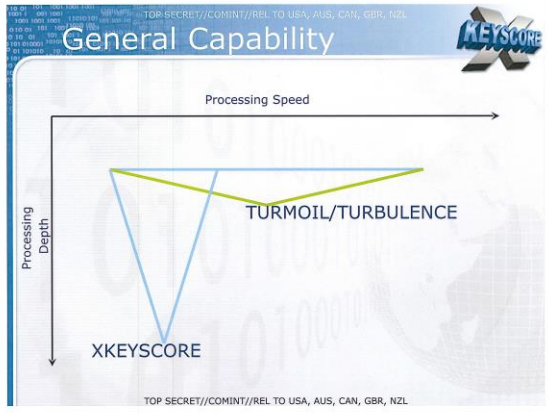












Why do shallow

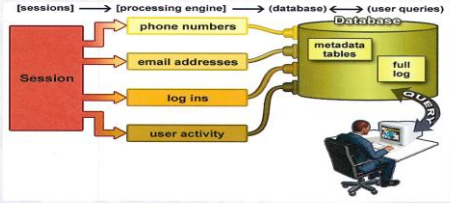
- Can look at more data
- XKEYSCORE can also be configured to go shallow if the data rate is too high

Why go deep

- Strong Selection itself give us only a very limited capability
- A large amount of time spent on the web is performing actions that are anonymous
- We can use this traffic to detect anomalies which can lead us to intelligence by itself, or strong selectors for traditional tasking

What XKS does with the Sessions

Plug-ins extract and index metadata into tables



Plug-ins

Plug-in	DESCRIPTION
E-mail Addresses	Indexes every E-mail address seen in a session by both username and domain
Extracted Files	Indexes every file seen in a session by both filename and extension
Full Log	Indexes every DNI session collected. Data is indexed by the standard N-tupple (IP, Port, Casenotation etc.)
HTTP Parser	Indexes the client-side HTTP traffic (examples to follow)
Phone Number	Indexes every phone number seen in a session (e.g. address book entries or signature block)
User Activity	Indexes the Webmail and Chat activity to include username, buddylist, machine specific cookies etc.

What Can Be Stored?

- Anything you wish to extract
  - Choose your metadata
  - Customizable storage times
  - Ex: HTTP Parser

[redacted]

```
GET /search?hl=en&q=islamabad&meta= HTTP/1.0
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-
application/msword, application/x-shockwave-flash, */*
Referer: http://www.google.com.pk/
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Host: www.google.com.pk
[redacted]
Connection: keep-alive
```

No username/strong selector

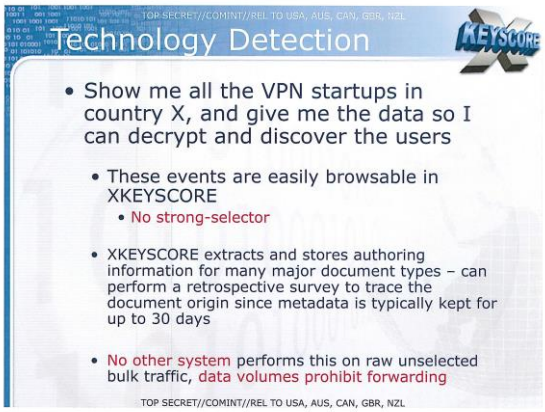
What can you do with XKEYSCORE?

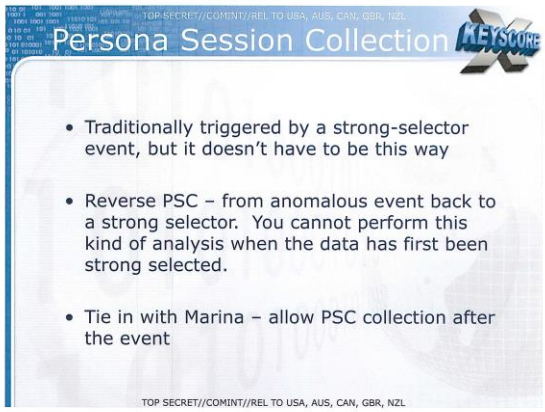
Finding Targets

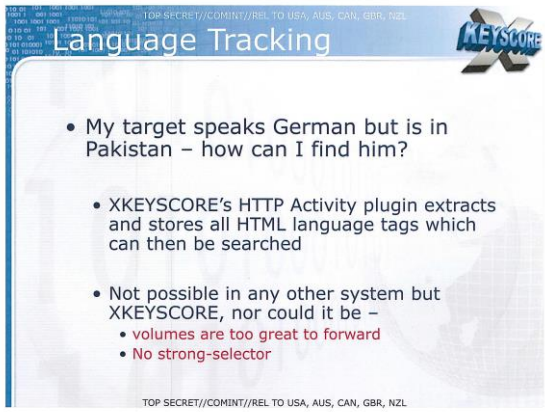
- How do I find a strong-selector for a known target?
- How do I find a cell of terrorists that has no connection to known strong-selectors?
- Answer: Look for anomalous events
  - E.g. Someone whose language is out of place for the region they are in
  - Someone who is using encryption
  - Someone searching the web for suspicious stuff

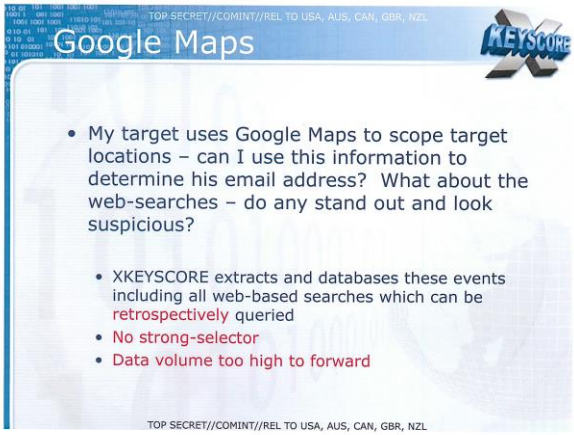
Encryption

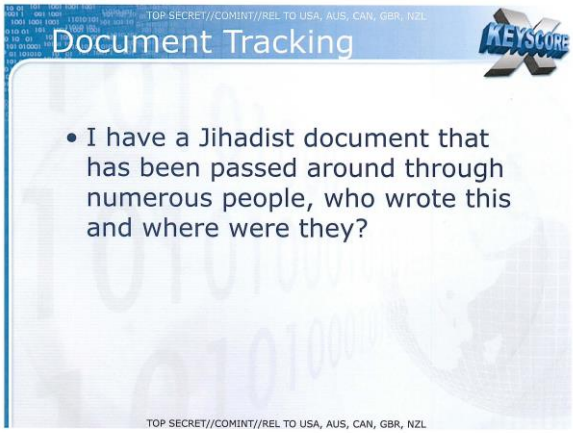
- Show me all the encrypted word documents from Iran
- Show me all PGP usage in Iran
  - Once again – data volume too high so forwarding these back is not possible
  - No strong-selector
  - Can perform this kind of retrospective query, then simply pull content of interest from site as required

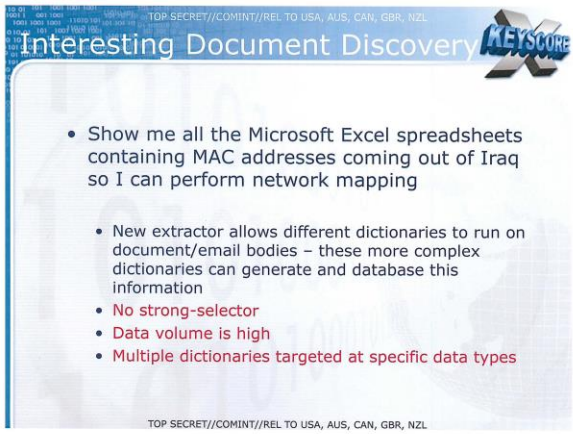

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL
Technology Detection
• Show me all the VPN startups in country X, and give me the data so I can decrypt and discover the users
• These events are easily browsable in XKEYSCORE
• No strong-selector
• XKEYSCORE extracts and stores authoring information for many major document types – can perform a retrospective survey to trace the document origin since metadata is typically kept for up to 30 days
• No other system performs this on raw unselected bulk traffic, data volumes prohibit forwarding
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

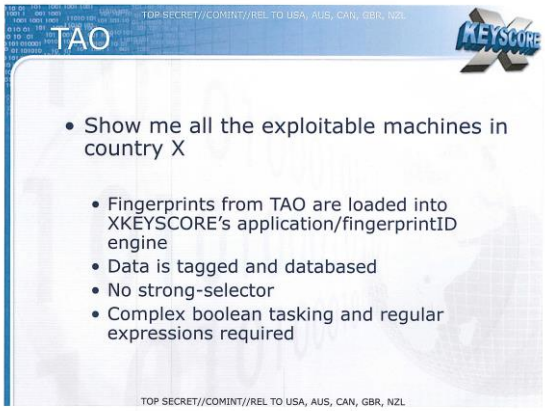

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL
Persona Session Collection
• Traditionally triggered by a strong-selector event, but it doesn't have to be this way
• Reverse PSC – from anomalous event back to a strong selector. You cannot perform this kind of analysis when the data has first been strong selected.
• Tie in with Marina – allow PSC collection after the event
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL


TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL
Language Tracking
• My target speaks German but is in Pakistan – how can I find him?
• XKEYSCORE's HTTP Activity plugin extracts and stores all HTML language tags which can then be searched
• Not possible in any other system but XKEYSCORE, nor could it be –
• volumes are too great to forward
• No strong-selector
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

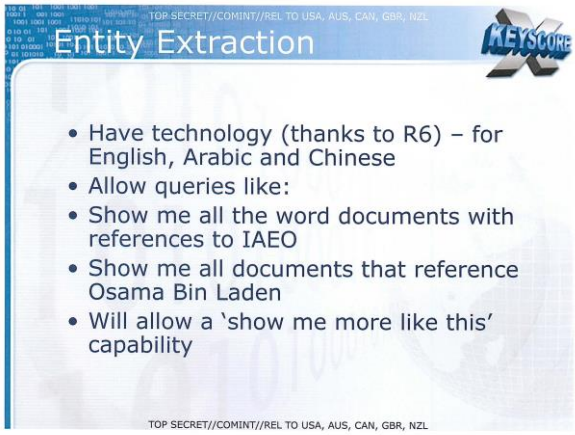

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL
Google Maps
• My target uses Google Maps to scope target locations – can I use this information to determine his email address? What about the web-searches – do any stand out and look suspicious?
• XKEYSCORE extracts and databases these events including all web-based searches which can be retrospectively queried
• No strong-selector
• Data volume too high to forward
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

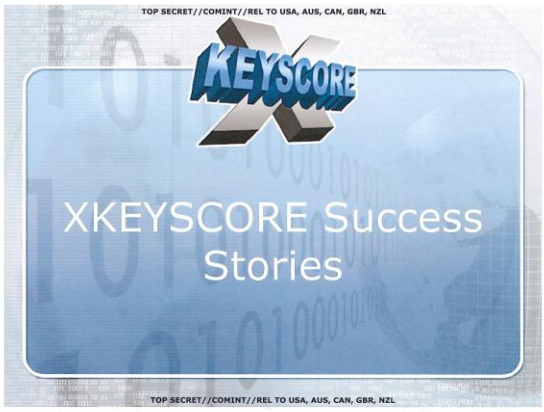

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL
Document Tracking
• I have a Jihadist document that has been passed around through numerous people, who wrote this and where were they?
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

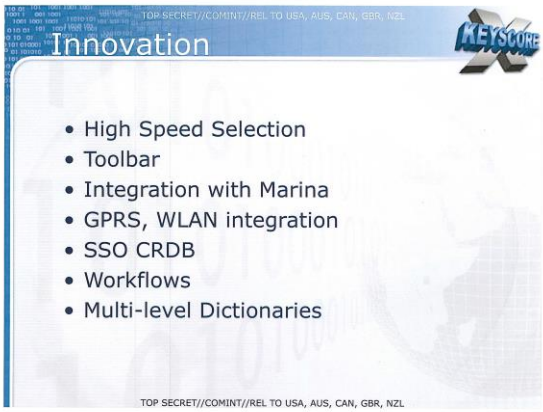

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL
Interesting Document Discovery
• Show me all the Microsoft Excel spreadsheets containing MAC addresses coming out of Iraq so I can perform network mapping
• New extractor allows different dictionaries to run on document/email bodies – these more complex dictionaries can generate and database this information
• No strong-selector
• Data volume is high
• Multiple dictionaries targeted at specific data types
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

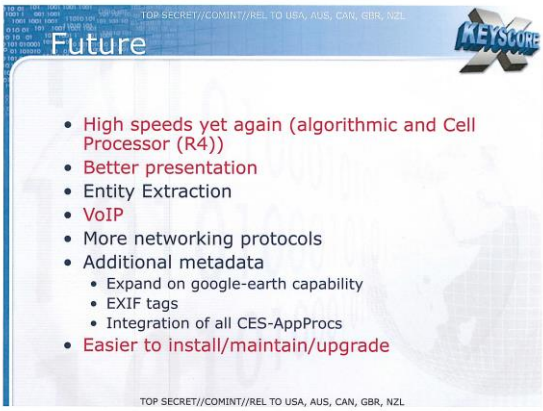

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL
TAO
• Show me all the exploitable machines in country X
• Fingerprints from TAO are loaded into XKEYSCORE's application/fingerprintID engine
• Data is tagged and databased
• No strong-selector
• Complex boolean tasking and regular expressions required
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL


TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL
Discovery of new target web services
• New web services every day
• Scanning content for the userid rather than performing strong selection means we may detect activity for applications we previously had no idea about
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL





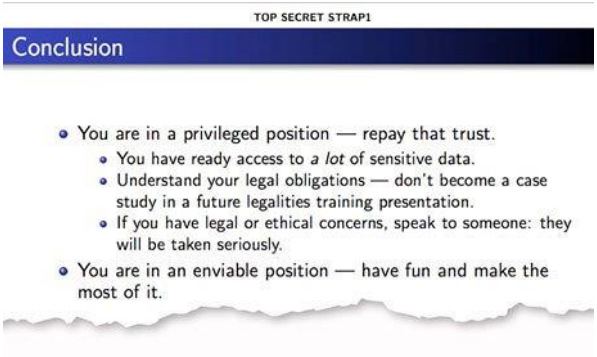




FONTE: Disponível em: <https://leaksource.info/2013/06/13/nsa-files-verizon-prism-boundless-informant-fisa-702-xkeyscore-whistleblower-edward-snowden-interview/> Acesso em 20 fev 2016

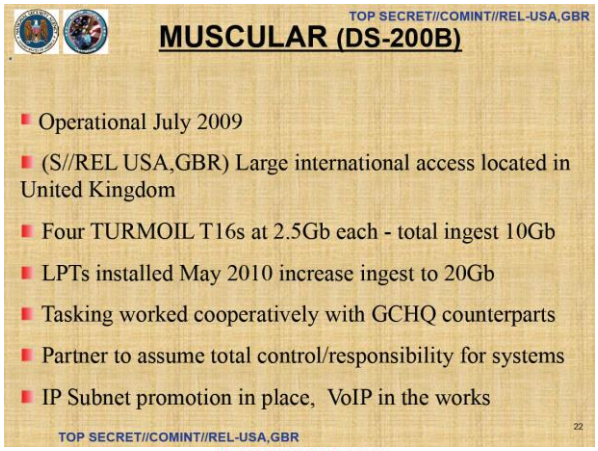
ANEXO F – Documentos do *Tempora*

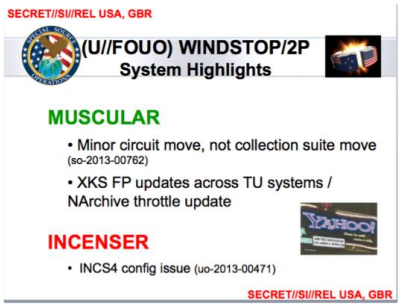
FONTE: Disponível em: <http://.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa> Acesso em 20 fev 2016

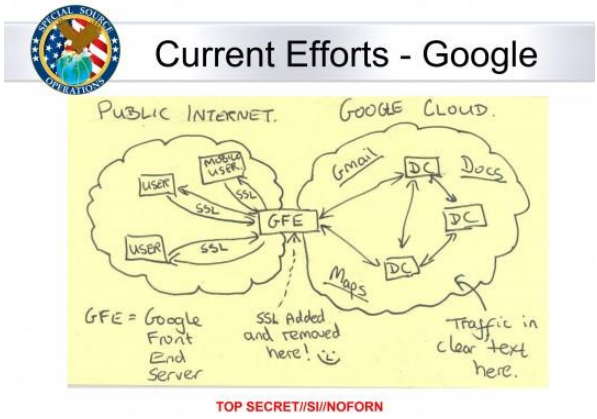


FONTE: Disponível em: <http://.theguardian.com/uk/2013/jun/21/gchq-mastering-the-*internet*> Acesso em 20 fev 2016

ANEXO G – Documentos do *Muscular*

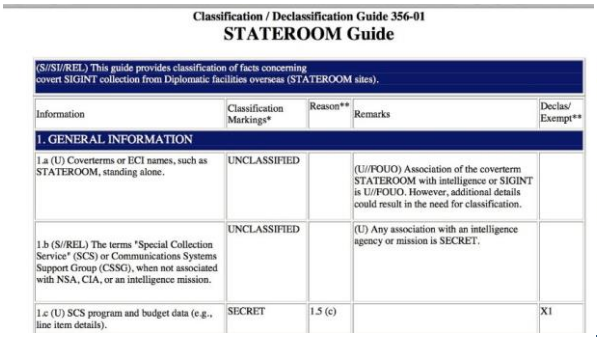






FONTE: Disponível em: <https://leaksource.info/category/nsa-files/> Acesso em 20 fev 2016

ANEXO H – Documentos do *Stateroom*

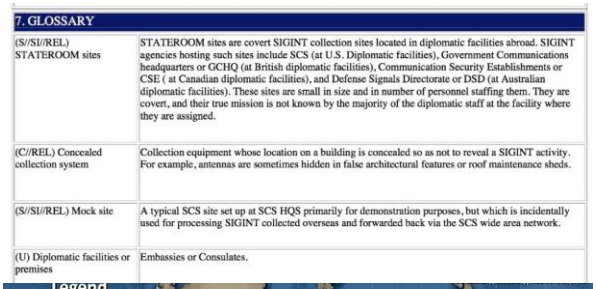


Classification / Declassification Guide 356-01

STATEROOM Guide

(S//SI//REL) This guide provides classification of facts concerning covert SIGINT collection from Diplomatic facilities overseas (STATEROOM sites).

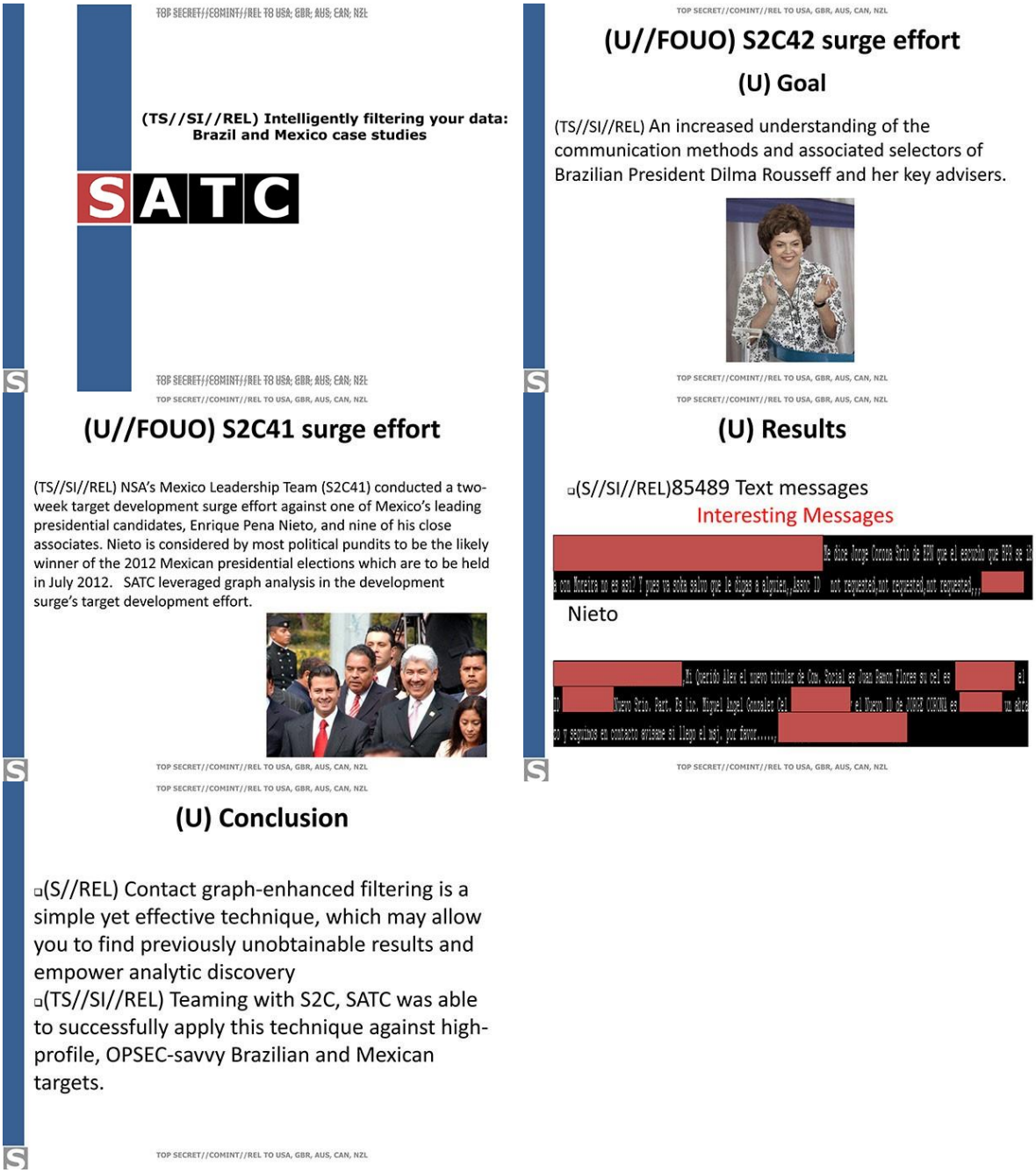
Information	Classification Markings*	Reason**	Remarks	Declas/ Exempt**
1. GENERAL INFORMATION				
1.a (U) Coverterms or ECI names, such as STATEROOM, standing alone.	UNCLASSIFIED		(U//FOUO) Association of the coverterm STATEROOM with intelligence or SIGINT is U//FOUO. However, additional details could result in the need for classification.	
1.b (S//REL) The terms "Special Collection Service" (SCS) or Communications Systems Support Group (CSSG), when not associated with NSA, CIA, or an intelligence mission.	UNCLASSIFIED		(U) Any association with an intelligence agency or mission is SECRET.	
1.c (U) SCS program and budget data (e.g., line item details).	SECRET	1.5 (c)		X1



7. GLOSSARY	
(S//SI//REL) STATEROOM sites	STATEROOM sites are covert SIGINT collection sites located in diplomatic facilities abroad. SIGINT agencies hosting such sites include SCS (at U.S. Diplomatic facilities), Government Communications headquarters or GCHQ (at British diplomatic facilities), Communication Security Establishments or CSE (at Canadian diplomatic facilities), and Defense Signals Directorate or DSD (at Australian diplomatic facilities). These sites are small in size and in number of personnel staffing them. They are covert, and their true mission is not known by the majority of the diplomatic staff at the facility where they are assigned.
(C//REL) Concealed collection system	Collection equipment whose location on a building is concealed so as not to reveal a SIGINT activity. For example, antennas are sometimes hidden in false architectural features or roof maintenance sheds.
(S//SI//REL) Mock site	A typical SCS site set up at SCS HQS primarily for demonstration purposes, but which is incidentally used for processing SIGINT collected overseas and forwarded back via the SCS wide area network.
(U) Diplomatic facilities or premises	Embassies or Consulates.

FONTE: Disponível em: <https://leaksource.info/category/nsa-files/> Acesso em 20 fev 2016

ANEXO I – Documentos de espionagem: Brasil e México



FONTE: Disponível em: <http://g1.globo.com/fantastico/noticia/2013/09/veja-os-documentos-ultrassecretos-que-comprovam-espionagem-dilma.html> Acesso em 20 fev 2016