UNIVERSIDADE D
COIMBRA

Tiago Pedro Vales

AS CONTRIBUIÇÕES DO CIBERESPAÇO PARA OS PROCESSOS DE SECURITIZAÇÃO E DESSECURITIZAÇÃO

Tese no âmbito do Doutoramento em Relações Internacionais – Política Internacional e Resolução de Conflitos, orientada pelo Professor Doutor José Manuel Pureza e apresentada apresentada à Faculdade de Economia da Universidade de Coimbra.

Novembro de 2020

Tiago Pedro Vales

AS CONTRIBUIÇÕES DO CIBERESPAÇO PARA OS PROCESSOS DE SECURITIZAÇÃO E DESSECURITIZAÇÃO

Tese no âmbito do Doutoramento em Relações Internacionais – Política Internacional e Resolução de Conflitos, orientada pelo Professor Doutor José Manuel Pureza e apresentada apresentada à Faculdade de Economia da Universidade de Coimbra.

Novembro de 2020

À minha família,
especialmente à minha avó,
Astolfina (in memoriam).

Agradecimentos

A realização deste trabalho não teria sido possível sem o apoio de várias pessoas que acompanharam todo este processo.

Agradeço aos professores investigadores, profissionais de apoio técnico e colegas da Faculdade de Economia e do Centro de Estudos Sociais da Universidade de Coimbra que sempre solícitos, contribuíram com o apoio institucional e com suas impressões, críticas e considerações desde os primeiros passos deste empreendimento. Mais do que a infraestrutura física e suporte acadêmico, esses centros de investigação tornaram-se símbolos de um período rico em aprendizado e desenvolvimento pessoal.

Agradeço especialmente aos professores titulares e convidados do Programa de Doutoramento em Relações Internacionais - Política Internacional e Resolução de Conflitos que através de muitas discussões e debates dentro do escopo de suas respetivas disciplinas e pelos inúmeros encontros pelos corredores da Universidade de Coimbra e em várias conferências mundo afora, contribuíram de maneira relevante para muitos aspectos deste trabalho. Agradeço aos meus colegas de curso, Isabella, Natália, Luís, Marta, Ana Filipa, por compartilharem esta jornada desde o início. Em especial, agradeço ao professor Daniel Pinéu que, para além de supervisor extraoficial no início deste projeto, tornou-se um amigo, compartilhando de bons momentos de descontração e convívios gastronômicos. Por fim, agradeço ao meu Orientador Prof. José Manuel Pureza que pacientemente, entre suas muitas tarefas, aceitou juntar-se a este desafio e permaneceu sempre atento às necessidades desta tese.

Sou grato aos professores e investigadores das instituições que me acolheram para a realização dos trabalhos de campo. À Piret Pernik, do International Centre for Defense and Security, em Tallinn, ao Professor Giampiero Giacomello, da Università degli Studi di Bologna, aos Professores Mônica Herz e Luis Manuel Rebelo Fernandes, da Pontifícia Universidade Católica do Rio de Janeiro, ao Professor Thomas Renard, do Royal Institute for International Relations – Egmont Institute, em Bruxelas. A seus respectivos modos, me ampliaram o horizonte compartilhando suas impressões e contatos sem os quais esta tese estaria bastante limitada.

Agradeço à Fundação para Ciência e Tecnologia pelo apoio financeiro concedido a este projeto de investigação sem o qual este trabalho não teria sido realizado.

Durante este longo caminho algumas pessoas tornaram-se verdadeiros amigos e merecem todo o destaque. Sinto-me com sorte em ter convivido com a "família" da Residência Universitária Pedro Nunes, que me serviu de lar por anos: a irmã mineira de Coimbra, Raquel do Sêrro, a doce italianinha Ramona, o nobre Roberto, o grande Sérgio Tadeu e sua Teresa, a sorridente Bruna, a determinada Tamara, o inexplicável Joe, o culto Gilvan, e o melhor-amigo-indiano, Agastya. Juntos compartilhamos não só do mesmo teto, mas também de muitas saudáveis noites regadas a risadas, canções de qualidade duvidosa copensadas com bons vinhos, da certeza da brevidade daqueles momentos e de uma amizade que os transcende. Do mesmo modo, para com a crescente família de "Zeromeias", António e Vera, Joana e Nuno, mais do que gratidão, lhes tenho admiração. Por fim, agradeço a Diego Montenegro, cuja amizade e incentivos foram essenciais para suportar a pressão dos momentos finais deste trabalho.

Os agradecimentos mais especiais cabem à minha família que, ainda que um oceano nos separasse, estiveram presentes em todos os momentos desta jornada e compreenderam a minha ausência em tantas circunstâncias durante esses anos. É à minha mãe, Sra. Ivone, ao meu pai, Sr. Deocleci, ao meu irmão Gustavo, à minha tia, Sra. Ilza e meus primos-irmãos Aline, Angélica e Vincent que sou especialmente grato por me ajudarem neste trabalho, que me custou os últimos anos de preciosa convivência na presença da minha avó, D. Astolfina.

Suporte Financeiro

Esta tese de doutorado é uma produção do trabalho de pesquisa desenvolvido no âmbito da Bolsa de Doutoramento SFRH/BD/101482/2014, co-financiado por fundos nacionais através da Fundação para a Ciência e Tecnologia (FCT) e por Fundos Europeus, através do programa QREN - POCH. Agradeço à FCT por esta doação sem a qual essa pesquisa não teria sido possível.

Atentei para todas as obras
que se fazem debaixo do sol,
e eis que tudo era vaidade
e aflição de espírito.

Ec. 1.14

Resumo

Esta tese busca compreender as particularidades dos movimentos de securitização e dessecuritização do ciberespaço. Para tanto, através dos estudos de caso da Estônia e do Brasil, busca-se compreender o papel dos agentes da securitização e dessecuritização situando-os nos respectivos contextos e levando em conta seus objetivos políticos de modo a determinar em que medida esses fatores influenciam e determinam os resultados destes movimentos. A literatura recente das Relações Internacionais, Ciência Política e Ciências Sociais conta da crescente importância da ascensão do ciberespaço e das Tecnologias da Informação enquanto tema emergente em seus respectivos campos, inclusive no enquadramento dos estudos da segurança e de ameaças. Por ser tema recente com muitos desdobramentos em andamento, percebeu-se que há a necessidade de examiná-lo através de lentes e interpretações mais específicas. Neste sentido, observou-se que as teorias da securitização e dessecuritização têm grande potencial em oferecer novas interpretações para a emergência do ciberespaço. Por outro lado, a análise deste tema com base nos preceitos das mencionadas teorias ofereceria contribuições para a própria análise teórica, resultando em sofisticações em alguns aspectos teóricos da securitização. Argumenta-se que os processos de securitização e dessecuritização que envolvem o ciberespaço têm elementos particulares, como objetos de referência pouco delimitados, uma diversidade de agentes da securitização, diferentes objetivos e atores funcionais que adotam uma linguagem própria para os discursos em função do seu contexto e de suas agendas políticas. O contexto e a agenda política dos atores envolvidos na securitização do ciberespaço impõem uma direção que leva a cenários onde as medidas de exceção não prevalecem necessariamente. Deste modo, recorrendo à análise de conteúdo de documentos e discursos oficiais de instituições governamentais e autoridades públicas, analisou-se a securitização no caso dos ataques cibernéticos à Estônia em 2007 e a dessecuritização no caso brasileiro, quando a politização das denúncias de espionagem pelos Estados Unidos acabou por impulsionar a aprovação do Marco Civil da Internet, em detrimento da adoção de medidas de exceção. Compreender esses processos com foco nos seus protagonistas, nos seus papéis, objetivos e contextos em que estavam inseridos contribui não só para uma sofisticação teórica, mas também para a compreensão das implicações da emergência do ciberespaço enquanto objeto dos estudos de segurança.

Palavras-chave: Securitização, Dessecuritização, Ciberespaço, Estônia, Brasil

Abstract

This thesis pursues to understand the particularities of the securitization and desecuritization movements in cyberspace. Taking Estonia and Brazil as case studies, the thesis seeks to understand the role of securitization and desecuritization agents. It evaluates the contexts and he political objectives of the agents in order to determine the influence of those factors in the process and results of the securitization and desecuritization movements. The recent literature on International Relations, Political Science and Social Sciences shows the growing importance of the rise of cyberspace and information technologies as an emerging theme in their respective fields, including in the framework of studies of security and emerging threats. Cyberspace issues being a recent topic with many developments still in progress, we realized that there is a need to examine them through more specific lenses and interpretations. In this sense, it was observed that the theories of securitization and desecuritization have great potential in offering new interpretations for the emergence of cyberspace as a security issue. On the other hand, we aim at offering innovative contributions to the theories of securitization resulting in specific theoretical sophistications. It is argued that the securitization and desecuritization processes that involve cyberspace have peculiar elements, such a lack of accuracy in determining the objects of reference, a diversity of securitization agents portraying different objectives and functional actors who adopt their own language for the speeches depending on their context and their political agendas. The context and political agenda of the actors involved in securitizing cyberspace leads to scenarios where exceptional measures do not necessarily prevail. Thus, using the content analysis of official documents and speeches from governmental institutions and public authorities at both domestic and international level, this thesis considered the securitization approach in the case of cyberattacks against Estonia in 2007 and desecuritization interpretation in the Brazilian case, when the politicization provoked by de denounces of espionage perpetrated by the United States ended up driving the approval of the Civil Framework of the Internet, to the detriment of the adoption of exceptional measures. Understanding these processes and focusing on the leading actors, their roles, objectives and contexts in which they acted, this thesis contributes not only to theoretical sophistication, but also to the understanding of the specific implications of the emergence of cyberspace as an object of security studies.

Keywords: Securitization, Desecuritization, Cyberspace, Estonia, Brazil

Lista de Acrônimos e Abreviações

CCDCoE - Cooperative Cyber Defence Centre of Excellence

CDCiber - Centro de Defesa Cibernética

CERT - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

CERT-EE – Estonia Information System Authority

CGI – Comitê Gestor da Internet

CIA - Central Intelligence Agency

CPI – Comissão Parlamentar de Inquérito

ICANN - Internet Corporation for Assigned Names and Numbers)

IGF – Internet Governance Forum

IP – Internet Protocol

ITU – International Telecommunication Union

MCI – Marco Civil da Internet

NATO – North Atlantic Threat Organization

NetMundial - Encontro Multissetorial Global Sobre o Futuro da Governança da Internet

NSA – National Security Agency

PL – Projeto de Lei

RI – Relações Internacionais

SINGINT – Signals Intelligence

TIs – Tecnologias da Informação

UN/ONU – Organização das Nações Unidas

USA – United States of America

USCYBERCOM - United States Cyber Command

WSIS – World Summit on Information Society

Lista de gráficos, tabelas e figuras

Sumário

Introdução

A ideia desta tese nasceu do interesse pela compreensão do papel dos Estados, instituições internacionais e atores domésticos perante o advento das novas tecnologias de informação. A Ciência Política e as Relações Internacionais têm se dedicado ao estudo das implicações do ciberespaço nas suas respectivas áreas de conhecimento. Contudo, por ser um tema relativamente novo em uma área bastante ampla e dinâmica, há a necessidade de estudos que aprofundem as concepções teóricas na inclusão do ciberespaço enquanto mais um domínio de interação social. Neste sentido, esta tese aproxima as teorias da Securitização e Dessecuritização do campo emergente das tecnologias da informação (TIs) através da análise dos processos nos casos da Estônia e do Brasil, e traz elementos que contribuem para o aprofundamento dos entendimentos teóricos enquanto instrumento de interpretação das Relações Internacionais, das questões de segurança e das implicações políticas do advento das Tis.

Tendo em conta que a concepção da segurança pelas Teorias da Securitização é primeiramente uma identificação de um determinado objeto de referência enquanto tema de segurança, apontando fatores de ameaça a algo que é essencial para o bom funcionamento de uma determinada estrutura. A aproximação natural do tema ascende e populariza as TIs com as questões de segurança e acabou por suscitar movimentos de securitização, tendo o ciberespaço como fonte de ameaças à diversos objetos de referência e atores de securitização provenientes desde o âmbito estatal, acadêmico ou político. Contudo, dada a natureza fluída do ciberespaço, esses movimentos de securitização apresentam especificidades que permitem ampliar o escopo teórico e favorece o entendimento mais amplo dos movimentos de securitização e principalmente da atuação dos atores que deles participam.

Ao mesmo tempo em que é fonte de ameaças, o próprio ciberespaço aparece, como objeto de referência, sendo alvo de políticas de segurança e proteção, já que seu funcionamento regular é fundamental para as diversas atividades da sociedade contemporânea. Sendo assim, é na identificação de elementos particulares nos movimentos de securitização do ciberespaço que ancora a problemática deste trabalho. Através da análise de movimentos de securitização e dessecuritização, este trabalho explora algumas especificidades nos processos de securitização do ciberespaço que contribuem para o aprimoramento do entendimento teórico, e lançam luz sobre os movimentos de

dessecuritização, que atualmente carecem, de forma geral, de estudos empíricos em função de uma sofisticação da teoria.

A análise da literatura sobre a ascensão do ciberespaço na sociedade contemporânea aponta para uma mudança de paradigmas na forma de organização social. O chamado Paradigma da Informação está intimamente ligado à evolução das tecnologias de comunicação e de processamento de dados. As Tecnologias da Comunicação e da Informação (TCIs) e seu crescente e difuso uso diário, a partir da década de 1990, evidenciam um novo aspecto social que não resulta apenas de uma mera evolução ou sofisticação técnica dessas ferramentas. Constata-se que a maioria das atividades sociais atualmente são permeadas, ou mesmo possibilitadas, pelas tecnologias da informação. A simples troca de mensagens através de e-mails ou SMS, WhatsApp, Telegram, Messenger, Instagram, ou qualquer outro aplicativo de mensagens, movimentações bancárias, das triviais às complexas, operações militares controlando, por exemplo, alvos situados a distâncias intercontinentais, operações logísticas comerciais e financeiras ou em cadeias produtivas têm, em sua essência, alguma funcionalidade baseada em Tecnologia da Informação (TI).

Esse novo componente da sociedade contemporânea, amplamente utilizado de maneira quase onipresente, foi suficiente para que alguns autores percebessem essa configuração como uma Sociedade da Informação (Webster, 2007), Era da Informação (Wood, McChesney, & Foster, 1998), Sociedade em Rede (Castells, 2000), ou de Revolução da Informação (Atikinson & Castro, 2008; Eriksson & Giacomello, 2006; Fang, 1997; Greenwood, 1999a; Rayward, 2014). De fato, a velocidade com que as TIs se sofisticaram e sua grande aceitação pela sociedade corroboram essa interpretação. Assim, se consolidando entre os itens de primeira necessidade da população e especialmente nos centros como Europa, Japão, China e América do Norte. O ciberespaço torna-se, então, um relevante tópico para investigação, não só pelos seus aspectos técnicos, mas também suas implicações sociais e políticas.

Observando o contexto da sociedade permeada pelo ciberespaço através das lentes dos estudos de segurança, este trabalho tem, portanto, dois objetivos principais. Inicialmente, mostrar como os movimentos de securitização e dessecuritização do ciberespaço contribuem para as teorias de securitização de modo geral. De maneira complementar, o segundo objetivo deste trabalho é contribuir para a compreensão da relação entre a tecnologia da

informação e os temas de segurança no âmbito das agendas políticas domésticas e internacionais.

Assim, considerando as teorias da securitização como principal parâmetro, a pergunta central desta investigação é: Constitui o ciberespaço um domínio em que o comportamento dos atores políticos se orienta para estratégias de securitização? E, desta pergunta, decorre uma derivada: que especificidade tem o ciberespaço enquanto campo de aplicação de estratégia de securitização. Esta articulação com esta(s) pergunta(s) formula quatro hipóteses.

Propõe-se, então, algumas hipóteses:

1) Os processos de securitização envolvendo o ciberespaço são particulares pois envolvem os movimentos de securitização a níveis domésticos e internacionais. Os atores, sejam eles funcionais ou da securitização, não têm papéis e objetivos previamente definidos que apontem para uma determinada política. Alternam-se entre os papeis de agentes de securitização e atores funcionais, durante os processos de articulação e atuação política em função do contexto que permeia o movimento de securitização e de suas respectivas agendas políticas.

2) Os movimentos de securitização do ciberespaço mantêm-se ligados a um discurso permanentemente renovado e enfatizam a proteção de elementos que variam desde o funcionamento das atividades cotidianas até a proteção de infraestruturas críticas.

3) Quanto mais disseminado o uso das TIs em uma sociedade ou quanto maior a dependência de uma sociedade das ferramentas do ciberespaço, mais eficaz é o discurso da securitização.

4) Os movimentos de securitização e dessecuritização do ciberespaço estão necessariamente ligados a uma agenda política do ator funcional.

A contribuição desta investigação divide-se em duas frentes. A primeira refere-se à abordagem das políticas e estratégias para a promoção do ciberespaço proposta por diferentes agentes sob a lente das teorias da securitização, determinando em quais contextos, discursos ou significados nos quais essas políticas são implementadas e justificadas. A segunda contribuição reside na contribuição teórica para a delimitação ou entendimento dos processos de dessecuritização, ainda dentro desse limite temático do ciberespaço. Os processos de dessecuritização, por outro lado, têm sido preteridos nas análises, inclusive em termos conceituais e de análises empíricas tendo em vista os processos de dessecuritização

(Aradau, 2004; Floyd, 2007, Maulide, 2016). Em suma, a contribuição desta investigação reside na abordagem do ciberespaço através da interpretação proposta pelas teorias da securitização e dessecuritização.

Como já mencionado, a emergência e popularização das Tecnologias de Informação, principalmente a partir da década de 1990, impulsionaram a construção do que Bell (1976) já identificava como uma sociedade baseada em frequentes inovações derivada da acumulação e disseminação de conhecimentos técnicos e teóricos. Ao analisarem as consequências sociais do advento das TIs no começo do século XXI, Castells (1999, 2005; 2009) e Barney (2004) identificaram um novo paradigma que permeava a sociedade contemporânea o qual chamaram de Sociedade em Rede.

O paradigma das TIs, tal como concebido por Castells (2005), é baseado em três características essenciais: a) a informação como matéria-prima; 2) uma alta capacidade de penetração social das tecnologias da informação, e; 3) alta capacidade de adaptação social às complexas interações entre tecnologia e sociedade feitas através de ligações em rede.

Naturalmente, a implicação mais visível desse advento das TIs e do ciberespaço como uma espécie de ágora virtual globalizada, ainda que controversa (Damiris & Wild, 1997), livre das fronteiras tradicionais, é a transformação dos hábitos sociais, não só na facilidade das comunicações interpessoais e nas tarefas cotidianas, mas também expressa no modo como os diferentes atores sociais, desde indivíduos a Estados, instituições internacionais, empresas e representantes do setor privado reagem aos impulsos neste campo. Mais do que isso, o acesso às tecnologias da informação passou a ser considerado sinônimo de desenvolvimento e encorajado por organizações internacionais, como a União Internacional para as Telecomunicações (ITU, 2003). Esse contexto também suscitou mudanças importantes para as questões da segurança, tanto pessoal quanto nacional e internacional.

A partir da década de 2000, surgiu uma percepção mais clara das ameaças propiciadas pelo ciberespaço, uma preocupação crescente com a segurança e para com as atividades nele exercidas e por ele possibilitadas, como por exemplo, a facilitação do financiamento do terrorismo, a atuação de hackers, a possibilidade de espionagem eletrônica conduzida tanto por Estados quanto por indivíduos ou grupos com apurado conhecimento técnico, fraudes financeiras, roubo de dados e propriedade intelectual, entre outros. Neste sentido, de maneira geral, países como os Estados Unidos, o Reino Unido e muitos outros começaram a formular suas estratégias oficiais para a cibersegurança, em um movimento

que aproximava a questão da segurança cibernética das práticas cotidianas e de cenários mais específicos de grande impacto, como, por exemplo, a possibilidade de ataques cibernéticos à infraestruturas críticas, os sistemas de abastecimento de energia, de água potável entre outros setores considerados vitais para a sociedade. No campo da defesa cibernética, registrou-se um reconhecimento por Estados Unidos e Brasil, por exemplo, do ciberespaço enquanto um dos setores específicos da defesa, tal como território, aéreo, marítimo e espacial (Clarke & Knake, 2012).

Neste sentido, embora ainda não haja um consenso acadêmico ou operacional, para o propósito deste trabalho, entendeu-se o ciberespaço tal como definiu o governo espanhol e o governo húngaro na suas respectivas estratégias para a cibersegurança, justamente por sintetizar os níveis técnicos e sociais envolvidos neste ambiente virtual:

> Cyber space is the set of means and procedures based on Information and Communications Technology which is configured for the provision of services. Cyber space consists of hardware, software, the Internet, information services and systems of control that ensure the provision of services that are essential for the socio-economic activity of any nation, especially those that are connected to its critical infrastructure. (Chamorro, Lopez, & Fernandez, 2012: online)

> Cyberspace means the combined phenomenon of globally interconnected, decentralised and ever-growing electronic information systems as well as the societal and economic processes appearing in and through these systems in the form of data and information. (Hungary, 2013: online)

Naturalmente, para além da conceitualização do que seria essa nova dimensão que conjuga a interação social e inovação técnica, os debates acadêmicos têm observado as implicações para a segurança doméstica e internacional em várias frentes. Por exemplo, na questão do uso da tecnologia da informação para a guerra, nos trabalhos de Carr (2012); Clarke & Knake (2012); Green (2012); Harris (2014); Hughes & Colarik (2017); Johnson, (2015); Lindsay (2013); Macedo (2016); Robinson, Jones, & Janicke (2015). Sobre as implicações na questão da vigilância em Karampelas & Bourlai (2017); Landau, (2010) e Lyon (2014). Nas questões da defesa, dissuasão e resiliência cibernética em Jajodia, Cybenko, Liu, Wang, & Wellman (2019); Jari Rantapelkonen & Salminen (2013) Jasper (2017) e Silva, (2016) e a questão da securitização do ciberespaço em Carreiro (2012); Georgieva (2015); Giacomello & Eriksson, (2006); Hansen & Nissenbaum (2009); Hare (2010), Hart (2011); Hjalmarsson (2013); Kasper (2014); Lobato & Kenkel (2015); Stojaković, (2018); Lacy & Prince (2018). E é com foco nesse último debate e com a literatura das teorias da securitização que este trabalho buscou dialogar.

A própria dinâmica do ciberespaço impõe desafios a diferentes áreas das investigações em segurança internacional, tal como se pode verificar em um crescente número de trabalhos publicados sobre o tema. A literatura disponível atualmente permite um bom mapeamento do campo da segurança cibernética. No entanto, há ainda espaço para o desenvolvimento de trabalhos mais específicos para que este mapa deste vasto campo se torne mais nítido, objetivo, e mais eficaz como instrumento de análise para o entendimento da segurança internacional contemporânea. É neste sentido que, embora haja trabalhos que associem as teorias da securitização ao ciberespaço, mantém-se necessário observar as dinâmicas da securitização envolvendo o ciberespaço (Hansen & Nissenbaum, 2009; Hjalmarsson, 2013; Lacy & Prince, 2018; Lobato et al., 2015), levando em conta as dimensões e contextos políticos específicos em que se desenvolvem, o papel e a atuação dos atores políticos envolvidos e seus resultados produzidos a nível doméstico e internacional.

Recursos metodológicos

O primeiro momento desta investigação tem como principal método a pesquisa de bibliografia e análise documental. Neste sentido, a partir do exame de fontes secundárias, tais como artigos acadêmicos e publicações de cunho teórico que vêm a compor o tema proposto, elaboramos o Estado da Arte e enquadramento teórico. Delimita-se, então, o contexto, os atores, a pertinência e a relevância do tema central para uma investigação e explicita-se o quadro teórico, centrado nas Teorias da Securitização. O trabalho, que tem um caráter indutivo, recorre, então, a um conjunto de estratégias metodológicas: análise de conteúdo, análise de discurso, estudos de caso (Estônia e Brasil) e entrevistas semiestruturadas. Essa combinação de estratégias metodológicas permitiu a abordagem dos objetos de estudo de uma maneira multifacetada e permitiu superar eventuais deficiências de uma única estratégia metodológica.

A análise de conteúdo enquanto estratégia metodológica foi escolhida por mostrar-se precisa e ao mesmo tempo flexível para a análise qualitativa dos documentos oficiais, das fontes secundárias e das entrevistas. Neste sentido, o entendimento da metodologia acompanha a definição de Shelley & Krippendorff, (2004) que concebem a análise de conteúdo como uma metodologia que valida e replica as inferências dos textos considerando o contexto em que são inseridos. Tal como apontam Neuendorf & Kumar (2015: 4-5), o uso da análise de conteúdo para interpretar as construções simbólicas e os significados culturais

permitem interpretar textos e documentos de modo a identificar padrões específicos com ênfase nas mensagens políticas das fontes analisadas. A análise de conteúdo ainda se mostrou válida por ser possível aplicá-la, tal como afirma Druckman (2005), a uma grande variedade de comunicações orais e escritas, possibilitando a comparação das fontes e levantamentos bibliográficos utilizando as definições direcionadas pelo marco teórico.

Neste sentido, o que se pretendeu em termos de análise de conteúdo qualitativa ao observar o material de investigação foi estabelecer critérios de buscas, selecionando materiais documentais e fontes secundárias relacionados com as questões da emergência do ciberespaço e as Teorias da Securitização e, dentro desse material, encontrar padrões ou expressões que tornassem possível a análise dos argumentos e objetos de estudo tendo em conta o quadro teórico. Nesse sentido, foi possível determinar e identificar o que foi veiculado, transmitido ou publicado possibilitando, então, a interpretação dos significados políticos referentes ao tema da securitização, tanto em documentos oficiais de governos, relatórios de Organizações Internacionais e instituições de investigação relacionadas com a segurança, em discursos oficiais de autoridades políticas e da administração pública dos países analisados nos estudos de caso, e em artigos e trabalhos acadêmicos.

Tendo em perspectiva os rótulos e a justificativas ligadas à segurança, tal como propõe a Teoria da Securitização, buscou-se identificar os significados presentes nas fontes mencionadas, de modo a estabelecer o contexto em que as decisões dos atores foram tomadas e a que agenda política respondiam. Assim, considerou-se as fontes em que seus autores colocavam o ciberespaço na perspectiva da segurança, trazendo-a para as questões cotidianas, para a necessidade da proteção de temas relacionado à soberania dos seus estados, à segurança dos respectivos governos e o significado que as TIs representavam para aquela determinada sociedade.

Assim, combinou-se a análise de conteúdo com a realização dos dois estudos de caso, Estônia e Brasil, de modo a verificar os significados que a recorrência dos discursos das autoridades em relação à segurança do ciberespaço implicou nos processos de securitização e dessecuritização. Por significados, toma-se emprestado a interpretação de Schreier (2012):

> Meaning is something that we, the recipients, attribute to the words that we hear or read, to the images that we see. This is a complex process in which we bring together our perception of the material with our own individual background: what we know about a topic, the situation in which we encounter it, how we feel at the time, and much more. Meaning is not a given, but we construct meaning. (Schreier, 2012: 13)

O foco da análise de conteúdo neste trabalho reside, em primeiro momento, nos documentos oficiais dos governos estoniano e brasileiro, bem como de Organizações Internacionais (ONU, NATO, ITU) que tratam da questão da segurança do ciberespaço, e outros campos permeados no esteio da securitização do ciberespaço. Os documentos oficiais (Estratégias para a defesa e segurança cibernética, resoluções, projetos de lei, relatórios de agências governamentais e privadas) refletem os objetos de referência que justificam os movimentos de securitização. Parte-se do entendimento de que, a partir do momento em que elementos dos discursos de securitização são traduzidos em forma de documentos oficiais, a securitização ganha um caráter institucionalizado.

Em um segundo momento, mas não menos importante, levou-se em consideração o próprio discurso das autoridades públicas. No caso estoniano, os focos foram representantes do governo durante os ataques cibernéticos, em 2007, nomeadamente o Presidente da República, o primeiro-ministro. Colaboraram para a construção deste quadro os representantes do Ministério da Defesa, Ministério das Relações Externas, Ministério do Interior, Ministério da Economia e Comunicação, da Autoridade Estoniana para Sistemas de Informação, representantes do terceiro setor, nomeadamente e-Governance Academy e representantes de centros de investigação, como o International Center for Defence and Security, CCDCoE, Universidade de Tallinn e Universidade Técnica de Tallinn. Essas últimas menções foram destacadas por estarem envolvidas diretamente com a questão das políticas para o ciberespaço na Estônia, ocupando posições-chave ou desenvolvendo trabalhos relevantes neste campo e por terem experiência *in loco*. Para além das funções que desempenharam ou que hoje ocupam em instituições-chave, as experiências *in loco* são relevantes para o entendimento do contexto social em que se deram os ataques cibernéticos e os processos de tomadas de decisão. Deste modo, cobriu-se também a questão da delimitação do contexto e de seus significados, tal como aponta a estratégia metodológica adotada.

No caso brasileiro, valorizamos as mesmas fontes primárias, porém não na mesma ordem. Os discursos das autoridades proferidos tanto a nível nacional quando internacional, nomeadamente a Presidente da República e notas do Ministério das Relações Exteriores, têm uma relevância central para a análise, visto que é a partir deles que se desenvolvem os argumentos dos parlamentares que aprovaram, posteriormente, o Marco Civil da Internet (MCI). Assim, juntamente com os discursos da Presidente da República, os discursos dos parlamentares constituem a matéria prima mais relevante para este caso, disponibilizados

integralmente em áudio e texto através do portal da Câmara dos Deputados. Naturalmente, documentos oficiais do Governo brasileiro, nomeadamente do Ministério das Relações Exteriores, do Ministério da Defesa, da Câmara dos deputados, como projetos de lei envolvendo a questão da segurança de dados, foram utilizados como fontes primárias e contribuíram para estabelecer o contexto em que se discute a questão da segurança cibernética no Brasil. As entrevistas conduzidas para este caso foram no sentido de estabelecer um entendimento linear e cronológico, focando primeiramente na criação e evolução do projeto de lei do MCI. Neste sentido, foram entrevistados ativistas pela inclusão digital, parlamentares que estiveram ligados à elaboração do projeto de lei, acadêmicos que acompanharam as sessões da Câmara dos Deputados. Para além da sua relação com o projeto de lei, os entrevistados também participaram ou ainda compõem o quadro de colaboradores de instituições relevantes para o tema, nomeadamente, o Comitê Gestor da Internet (CGI), o Ministério da Justiça e Segurança Pública e o Ministério da Defesa. As entrevistas também se estenderam a articuladores de fóruns internacionais que discutiram a questão da participação do Brasil na governança da Internet, nomeadamente a NetMundial e Internet Governance Forum (IGF).

Apesar dos documentos oficiais e discursos figurarem como as fontes primárias mais concretas, as entrevistas têm um peso relevante, pois permitiram não só explorar o contexto particular de cada caso, mas também colher impressões em primeira pessoa de participantes ativos nos processos. A escolha deste método parte do entendimento de que a entrevista estabelecem uma relação social imediata e interpessoal envolvendo o pesquisador e o seu interlocutor, que também é objeto da investigação (Alles, Guilbaud, & Lagrange, 2018: 111). Mais do que aproximar a investigação e o investigador do objeto de estudo, a preparação das perguntas permitiu antecipar problemas e possíveis respostas e assim, aprofundar as questões levantadas. As entrevistas permitiram não só a coleta de dados, mas um debate de ideias e impressões com alguns protagonistas dos eventos em questão.

Considerando esses aspectos, foram realizadas cerca de 20 entrevistas com representantes de setores-chave já mencionados. No caso estoniano, as entrevistas ocorreram principalmente em Tallinn, em duas visitas para trabalho de campo entre 2016 e 2017. Houve certa facilidade tanto em contactar os entrevistados porque há uma proximidade profissional e pessoal entre eles. No caso brasileiro, não houve tal facilidade. Os entrevistados estavam mais dispersos e os contatos e as confirmações deram-se mais por colaboração entre colegas investigadores do que pelas vias institucionais. Entrevistas presenciais ocorreram no Rio de

Janeiro e em São Paulo, sendo que os entrevistados em Brasília, Belo Horizonte e Porto Alegre preferiram colaborar através de redes sociais ou por escrito.

Nos dois casos, atentando para o objetivo de compreender o contexto de forma mais aberta, optou-se por conduzir entrevistas semiestruturadas. As entrevistas semiestruturadas permitem estabelecer um fio condutor centrado no tema e ao mesmo tempo em que possibilitam certa liberdade para os entrevistados complementarem as informações inquiridas com suas experiências in loco, o que é especialmente relevante para a abordagem construtivista deste trabalho.

Por fim, a escolha dos estudos de caso enquanto ferramenta metodológica é uma sugestão do próprio quadro teórico e da própria disciplina das Relações Internacionais. Tal como afirmam Bennett & Elman, (2007), os estudos de caso têm sido um método bastante recorrente nas investigações nas Relações Internacionais por permitirem um envolvimento mais profundo do investigador com o objeto investigado, à medida em que permitem uma combinação de métodos de análise. A opção pela estratégia de estudos de caso foi conduzida de maneira a estabelecer uma visão holística dos movimentos de securitização e dessecuritização acima mencionados. No que tange ao quadro teórico escolhido, Balzacq, (2011) nota que a estratégia tem sido recorrente nas observações empíricas da securitização, embora a metodologia seja variada.

Plano dos Capítulos

Este trabalho dividid0 em quatro capítulos. O objetivo principal do primeiro capítulo é abordar precisamente a relevância das tecnologias da informação e do ciberespaço para a sociedade contemporânea e suas implicações para as políticas de segurança. Entende-se que o advento das novas tecnologias da informação é um processo com múltiplas implicações que apresenta duas dimensões principais que se complementam. Por um lado, as novas ferramentas permitem estabelecer novas configurações sociais e, ao mesmo tempo, fomentam o desenvolvimento de uma nova indústria altamente dinâmica e inovadora. Por outro lado, a centralidade das novas tecnologias suscita cruciais questões de segurança e de defesa e a definição do papel das instituições públicas em meio à emergente sociedade da informação.

O segundo capítulo incide sobre o quadro teórico e tem como lente as teorias da securitização e dessecuritização, buscando trazer as discussões referentes à

segurança do ciberespaço sob este aspecto. Apesar de ter seu início na chamada Escola de Copenhague, as análises das teorias de securitização transcendem os limites da Escola de Copenhague e encontram relevantes contribuições, por exemplo, da chamada Escola Francesa da securitização. Assim, optou-se por não indicar um centro geográfico-acadêmico específico, mas sim sinalizar uma abordagem geral, usando teorias da securitização e considerando a Escola de Copenhague como ponto de partida dos entendimentos acerca da securitização e Relações Internacionais. Os tópicos centrais desta construção são conhecidos: movimento de securitização, agentes da securitização, objetos de referência e atores funcionais. Cada um destes tópicos traz uma abordagem específica em relação à securitização do ciberespaço, repetindo o objetivo de definir um quadro teórico específico para a abordagem através da teoria da securitização bem como apresentar uma revisão de literatura mais específica. No seguimento, à semelhança do proposto acima, apresenta-se uma revisão de literatura com o foco nos processos de dessecuritização. Contudo, esse seguimento tem um caráter mais generalista buscando estabelecer as possibilidades de sofisticação teórica no caso da dessecuritização e entender teoricamente como podem ocorrer movimentos de dessecuritização e como isso acontece em um elemento que permeia ou se sobrepõe, por vezes, os limites de ação dos atores funcionais. Uma vez estabelecida esta base teórica, a verificação empírica dar-se-á nos capítulos seguintes.

O terceiro capítulo é dedicado à verificação dos aspectos da securitização de forma empírica centrando a análise nos ataques cibernéticos à Estônia que ocorreram em abril de 2007, como estudo de caso. O caso estoniano é particularmente importante por terem se tornado uma espécie de emblema ou marco internacional da segurança do ciberespaço. Mais do que um emblema dos recentes esforços para a implementação de políticas de segurança cibernética, o caso estoniano é interessante por ser considerado o primeiro conflito envolvendo Estados em um ambiente cibernético, tanto enquanto modalidade ofensiva, quanto nas respostas técnicas e políticas que, por sua vez, tornam-se mutuamente influenciáveis a certo ponto.

O objetivo do último capítulo é tratar do processo de dessecuritização identificando os momentos e elementos cruciais que levaram o objeto de referência, no caso o ciberespaço e objetos subjacentes, a manter-se regido pelos preceitos normais de conduta, evitando a adoção de situações especiais. Para tanto, toma-se como referência o caso brasileiro e as atuações políticas que levaram o país a aprovar o Marco Civil da Internet e a adotar certas

posturas em âmbitos multilaterais acerca da questão do ciberespaço em fóruns de discussão e decisão.

Vale notar que os eventos abordados em ambos os estudos de caso tem início em ações de atores terceiros: Rússia no caso estoniano e Estados Unidos no caso brasileiro. Essas ações são abordadas de maneira pertinente, ainda que brevemente, para que os casos façam sentido no contexto em que estão inseridos. Visto que, a proposta metodológica tem no contexto, eventos e atores um elemento relevante, a influência desses países, dadas as influências que têm nos casos analisados, passam a ser central para os movimentos de securitização e dessecuritização.

Por fim, a última parte é dedicada a expor as conclusões e especificar as contribuições deste estudo. Trata ainda de algumas dificuldades na realização da investigação e aponta caminhos para outros empreendimentos.

CAPÍTULO 1. A ascensão do ciberespaço: evolução das ferramentas de comunicação e a identificação de novas ameaças no campo da segurança

> "The Internet is the first thing that humanity has built that humanity doesn't understand, the largest experiment in anarchy that we have ever had."
>
> Eric Schmidt

O objetivo deste capítulo é abordar a ascensão das Tecnologias da informação (TIs) nas últimas décadas e identificar os elementos que permitiram que as TIs e o ciberespaço se popularizassem em um lapso temporal relativamente curto, tornando-se centrais para sociedade contemporânea. Entende-se que o advento das TIs é um processo com múltiplas implicações que apresenta duas dimensões principais que se complementam: por um lado, as novas ferramentas permitem o estabelecimento de novas configurações sociais e, por outro, fomentam o desenvolvimento de uma nova indústria altamente dinâmica e inovadora. Com base nestas duas dinâmicas, o texto passa a focar o aspecto das questões de segurança, defesa e o papel das instituições públicas em meio à emergente sociedade da informação.

O capítulo divide-se em três partes principais. A primeira analisa o desenvolvimento do ciberespaço e suas ferramentas de modo a enfatizar a relevância das TIs para a sociedade contemporânea. A segunda parte é dedicada às questões de segurança no espaço virtual focando vários exemplos de episódios particularmente relevantes conjugando ciberespaço e segurança. Por fim, a última parte explora as respostas que governos de diversas partes do mundo têm dado às suas necessidades de proteção ou de promoção da segurança no ciberespaço.

1.1. A transformação do mundo através do ciberespaço e da Internet: desenvolvimentos tecnológicos e implicações sociais.

1.1.1. Da ciência cibernética ao entendimento do ciberespaço: a construção e consolidação de um novo espaço de interação social.

As referências ao ciberespaço tanto na literatura especializada quanto em um âmbito popular são largamente usadas sem que exista a preocupação com a definição exata.

No senso comum, o termo ciberespaço é ligado ao ambiente virtual, possibilitado e moldado pelas interações sociais que ocorrem na Internet e suas diversas ferramentas. Contudo, para os objetivos do presente trabalho um exame mais minucioso do termo faz-se necessário.

O termo ciberespaço foi usado pela primeira vez na novela do escritor americano William Gibson, *Neuromancer*, publicada em 1982[1]. Na concepção popularizada pelo novelista norte-americano, o ciberespaço não é um lugar físico, mas funciona como tal, já que há implicações entre os espaços físicos e virtuais.

Segundo Gibson, o ciberespaço é pautado por representações gráficas de dados transferidos através de redes, geradas e manipuladas por computador. Há ainda um componente para além da dimensão essencialmente tecnológica que enquadra questões psicológicas, epistemológicas jurídicas e sistemas sociais (Whittaker, 2004). Seria, de acordo com o romancista, uma espécie de ´alucinação consentida´, compartilhada por usuário e definido a partir de sua relação ao legitimar fontes de poder, que pode ser político, militar, comercial, etc.

> O ciberespaço. Uma alucinação consensual, vivida diariamente por bilhões de operadores legítimos, em todas as nações, por crianças a quem estão ensinando conceitos matemáticos... Uma representação gráfica de dados abstraídos dos bancos de todos os computadores do sistema humano. Uma complexidade impensável. Linhas de luz alinhadas que abrangem o universo não-espaço da mente; nebulosas e constelações infindáveis de dados. Como luzes de cidade, retrocedendo (Gibson, 1992: 67).

À medida em que as TIs se popularizavam, o termo ciberespaço passava a ser entendido, assinala Holloway (2002: 8), como uma metáfora conceitual à qual as pessoas recorrem para que seja possível a familiarização a um universo de termos e ações onipresentes aos quais a sociedade torna-se cada vez mais dependente. Há uma ideia de que o ciberespaço, por não ser um fenômeno físico ou concreto, se limita ao aspecto imaginativo, um mundo 'emulado' ou 'virtual'. Embora os termos supracitados possam funcionar como sinônimos ou complementos para explicar o que vem a ser o ciberespaço, não se pode opor este ao mundo 'real', visto que há uma influência mútua.

[1] O livro de William Gibson publicado no início da década de 1980 trata de um hacker punido pelos ex-patrões por tê-los roubado. A trama traz elementos que combinam uma sociedade decadente, distópica, ambientado primeiramente em uma cidade japonesa e em outras cidades ao redor do mundo. No entanto, os acontecimentos mais relevantes acontecem no ciberespaço que é apresentado por Gibson como um mundo paralelo quase físico. O livro, que inaugura uma trilogia, ganhou vários prêmios e é considerado um dos mais importantes representantes do sub-gênero literário "cyberpunk" que geralmente incorporam temas como inteligência artificial, o submundo hacker, megacorporações em um futuro distópico terrestre.

Apesar de ser uma palavra que se popularizou em um tempo relativamente recente, as origens do termo ciberespaço estão relacionadas às técnicas e os conhecimentos que remontam ao século XIX. O prefixo ´ciber´, refere-se a um conceito ainda mais antigo, proveniente do grego e com raízes próximas aos conceitos relacionados a governo, controle, governança[2]. O termo daí derivado, *cybernetique* foi usado pelo físico francês André-Marie Ampère em 1884 para descrever a ciência de governança civil.

Em perspectiva mais contemporânea, a cibernética relaciona-se, entre outros, às comunicações mediadas por computadores (CMCs), o que pressupõe uma conectividade e interação entre usuários por meio de dispositivos (computadores, telemóveis, *gadgets*[3]) e por meio da interação entre máquinas. Como explica Clark (2010), essa conexão é a que permite a existência ou funcionamento do que se conhece por ciberespaço.

Bell (2001), define o ciberespaço como uma especificação da confluência entre as redes eletrônicas de comunicação, sendo a mais comum delas a Internet. O autor reconhece que uma definição precisa do ciberespaço não é, necessariamente, fácil justamente por agregar vários campos do conhecimento e permear vários segmentos das atividades humanas. Bell (2001: 7) destaca que

> We can define cyberspace in terms of hardware, for example – as a global network of computers, linked through communications infrastructures, that facilitate forms of interaction between remote actors. Cyberspace is here the sum of all those nodes and networks […]. Alternatively, a definition based partly on the 'symbolic' trope could define cyberspace as an imagined space between computers in which people might build new selves and new worlds […]. In fact, cyberspace is all this and more; it is hardware and software, and it is images and ideas – the two are inseparable. (Bell, 2001: 7)

A particularidade do ciberespaço, segundo Bell, está na viabilização da comunicação de pessoal que podem estar dispersas geograficamente a nível global, mas que podem interagir com grande facilidade através da comunicação eletronicamente intermediada. A dificuldade em definir ou delimitar o que se compreende por ciberespaço acaba produzindo definições que se moldam às conveniências ou objetivos do definidor[4].

[2] De acordo com Vallée (2003), o termo ciber vem do grego antigo, 'kubernetike', significando a 'arte de dirigir, conduzir'.

[3] Gadgets são popularmente relacionados a dispositivos eletrônicos portáteis. Através da maioria desses dispositivos é possível acessar à Internet, comunicar-se, entre outras atividades que dependem de uma plataforma digital. Para além de suas funções técnicas os *gadgets* também tem uma conotação de status social.

[4] Tantas são as definições propostas e adotadas para o ciberespaço quantos são os que a definem. A grosso modo, as definições são ligeiramente diferentes, sendo compatíveis com a maioria dos documentos quando se trata de cooperação entre entidades. Contudo, o Centro de Excelência em Cooperação para a Ciber Defesa, da Aliança Atlântica (CCDCOE) mantém uma espécie de glossário com termos derivados do prefixo – ciber bem

Clark (2010), divide o ciberespaço em quatro camadas organizadas hierarquicamente. O modelo evidencia o caráter transdisciplinar do ciberespaço e da cibernética em si. Na primeira camada, a mais importante, estão os usuários. A importância dos usuários se justifica pelo fato de que eles não são meras entidades passivas, pelo contrário, suas ações dão sentido às camadas seguintes: a informação armazenada, transmitida e processada no ciberespaço; os padrões lógicos que dão suporte aos ciberespaço; e as instalações físicas que dão suporte ao elementos lógicos. Em resumo, são as escolhas e atuações, as diferenças e semelhanças culturais e sociais que permitem a existência funcional do ciberespaço, que é suportado por elementos físicos e lógicos.

Esse entendimento é particularmente importante porque outros autores, ao olhar outros fenômenos permeados pelo ciberespaço, perceberam que as tecnologias da comunicação não são necessariamente um ator, mas sim ferramentas. Neste sentido, mais do que melhorar as condições de comunicação, o ciberespaço e ferramentas são dependentes da interação entre os usuários. Ao olhar para as transformações nas relações de poder, Naim (2014) percebe exatamente essa dinâmica:

> Não há dúvida de que a Internet e outras ferramentas estão a transformar a política, o activismo, os negócios e, obviamente, o poder. Contudo, em muitos casos, este papel fundamental é exagerado e compreendido de forma errada. As novas TIs são ferramentas – e, para terem impacto, precisam de utilizadores, que, por sua vez, devem ter objetivos, orientação e motivação. (Naim, 2014: 33)

A percepção quanto a importância primordial dos usuários, ainda antes das ferramentas de TI, torna-se ainda mais evidente em episódios onde são ressaltados o papel das mesmas tecnologias. Um número relativamente grande de trabalhos científicos que se debruçaram sobre os movimentos conhecidos como Primavera Árabe, ou os movimentos chamados Occupy[5], entre outros, apontam as TIs como catalizadora das manifestações, sendo que, mesmo por questões de limites metodológicos, o conjunto político-social em que viviam as respectivas populações não são abordados na mesma medida (para citar alguns

como as definições de ciberespaço adotadas em documentos oficiais no mundo. Disponível em: https://ccdcoe.org/cyber-definitions.html.

[5] Os movimentos que ocuparam as ruas de grandes metrópoles globais como Londres, Madri, Washington, Nova York, entre outras ficaram conhecidos como Occupy e clamava, para além de reivindicações locais, por melhor igualdade social, valores democráticos, entre outros. Para visões sobre o movimento não necessariamente concordantes entre si confira Byrne (2012), Horowitz & Perazzo (2012) e Chomsky (2013). Por Primavera Árabe entende-se os movimentos ou ondas de protestos que iniciaram na Tunísia em 2010 e se ramificaram pelos países árabes do norte da África e Oriente Médio. Com diferentes intensidades e resultados, muitas vezes controversos, os movimentos depuseram regimes instalados a décadas em países como a Tunísia, Egito e Líbia (para uma visão geral sobre a Primavera Árabe, confira Haas & Leech, 2013).

exemplos, Calhoun, 2013; E. Clark & Johansson, 2012; Howard et al., 2011; Stepanova, 2011).

Neste contexto, o resultado da combinação dos motivos para os protestos e a disponibilidade dos meios de propagação da informação levam ao que Clark (2010) aponta como a segunda camada do ciberespaço que seria a informação propriamente dita.

A informação, ou dados, em uma linguagem mais técnica, ganharam uma dinâmica própria no ciberespaço frente ao caráter estático ou passivo de antes. Os sistemas de captura aliados à conectividade de usuários fizeram com que a informação fluísse para além das limitações físicas. O acesso as informações de diferentes tipos são imediatas e globais, a quem dispõe de acesso à rede.

Ao mesmo tempo em que o ciberespaço transcende barreiras físicas, depende delas. Clark (2010), enfatiza que as fundações do ciberespaço são estruturas físicas: computadores, servidores, sensores, transdutores, cabos submarinos, e uma infinidade de outros objetos. Essa camada é a mais fácil de se identificar, uma vez que é a mais comum e visível.

O aspecto físico do ciberespaço é duplamente importante. A função mais evidente é possibilitar as interações entre usuários e o fluxo dos dados, nomeadamente, seu funcionamento. Outra especificidade, entretanto, aparece quando se discute questões de controle e governança do ciberespaço. A questão da infraestrutura da informação tem necessariamente de estar fixada em um território, portanto, sujeito a imposição de leis, regulamentos, controle, sejam eles diretamente ligados ao poder público ou a empresas que, mesmo com presença internacional, devem se reportar aos seus respectivos Estados de origem ou a regulamentações internacionais que porventura se apliquem.

Deste modo, Clark ilustra sua ideia afirmando que o “cyberspace is a real artifact build out of real elements, not a fantastical conception with no grounding” (Clark, 2010: 2). Tanto a dimensão física do ciberespaço, a chamada infraestrutura digital, quanto a aplicação de leis e as regulamentações serão aprofundadas adiante em momentos mais apropriados ao tema, sendo esta uma questão fundamental explorada no quarto capítulo.

Por fim, apesar da importância das estruturas físicas, a natureza do ciberespaço é bem definida em um ambiente lógico. As configurações que tornam possível a existência e o funcionamento do ciberespaço, nomeadamente da Internet, dão-se em um sistema lógico que permite a comunicação entre as estruturas físicas. Essa camada lógica, de linguagens de

programação é a responsável por conjugar os usuários, a informação propriamente dita e as plataformas/estruturas físicas.

Em resumo, o ciberespaço baseia-se sobretudo em estruturas ou plataformas que permitem e são construídas para sua própria evolução ou inovação. Algo que alimenta e se desenvolve a partir de si mesmo, em um processo que tem na colaboração mútua, muitas vezes até anónima, sua principal fonte de evolução (Castells, 2005).

O entendimento do ciberespaço acompanha a flexibilidade do mesmo. Dependente de uma rede complexa de usuários produzindo dados processados por programações lógicas por máquinas amparadas por infraestruturas físicas, o ciberespaço tronou-se uma espécie de universo paralelo ao qual usuários recorrem para facilitar atividades cotidianas. Tais atividades, por sua vez correspondem a alguns aprimoramentos, como ler mensagens pessoais, entretenimento, ou atividades criadas a partir do advento do ciberespaço e ferramentas como a própria lógica de programação, a pesquisas de percepção dos usuários, o desenvolvimento de ferramentas e de hardwares, entre outros.

Em resumo, a ideia de Benedikt ajuda a chegar à forma final do conceito:

> A new universe, a parallel universe created and sustained by the world's computers and communication lines. A world in which the global traffic of knowledge, secrets, measurements, indicators, entertainments, and alter-human agency takes on form: sights, sounds, presences never seen on the surface of the earth blossoming in a vast electronic night. (Benedikt, 2000: 29)

A definição acima consegue conjugar todos os aspectos que compõem a noção de ciberespaço e com ela, é possível visualizar o conceito de maneira completa. Contudo, para atender a uma necessidade prática de trabalhar o ciberespaço em uma perspectiva científica e que ao mesmo tempo seja compatível com os diversos entendimentos políticos de entidades, Estados e instituições, é preciso adotar um entendimento mais específico. Neste sentido, as definições de ciberespaço propostas pelo governo espanhol:

> Cyber space is the set of means and procedures based on Information and Communications Technology which is configured for the provision of services. Cyber space consists of hardware, software, the Internet, information services and systems of control that ensure the provision of services that are essential for the socio-economic activity of any nation, especially those that are connected to its critical infrastructure. (Chamorro, Lopez, & Fernandez, 2012: online)

e pelo governo húngaro:

> Cyberspace means the combined phenomenon of globally interconnected, decentralised and ever-growing electronic information systems as well as the

> societal and economic processes appearing in and through these systems in the form of data and information. (Hungary, 2013: online)

sintetizam o conceito de ciberespaço e se aproxima de maneira mais precisa ao que se pretende considerar por ciberespaço neste trabalho. Não obstante, Medeiros & Goldoni propõem uma definição para o ciberespaço que funciona como uma ferramenta de análise. Após analisarem definições para o ciberespaço provenientes tanto de autores já citados no presente trabalho quanto de documentos oficiais de Estados, nomeadamente Estados Unidos, Brasil, China e Alemanha, chegam ao que chamam de Fundamental Conceptual Trinity of Cyberspace (Medeiros & Goldoni, 2020). Os autores examinam as particularidades do ciberespaço determinadas como desterritorialização, multiplicidade de atores e incertezas e propõem uma definição para o ciberespaço em que sintetizam os entendimentos acima citados:

> cyberspace can be understood as a unique domain of artificial human interaction, disassociated in part from physical elements, which permeates the traditional domains. It exists though the connection of different layers: technological, technical, and personal. It has unique particularities, made possible by its partial immateriality and expansive interconnectivity. Cyberspace is a constantly evolving as technology advances, and is constantly changing as different actors use it, shaping it to meet the most diverse needs.(Medeiros & Goldoni, 2020: 37).

Apesar de reconhecer as nuances das definições conceituais para o ciberespaço, que variam de acordo com necessidades práticas dos autores perante aos seus estudos ou estratégias, no caso de Estados, este trabalho toma as definições sintetizadas acima como significado para o ciberespaço. As implicações do advento do ciberespaço para as questões de poder, na definição do papel do Estado e para a sociedade contemporânea serão então abordadas adiante com base no entendimento proposto.

1.1.2. “O lugar que acontece”

Sendo uma realidade virtual que permeia e exerce influências a planos concretos ao mesmo tempo em que reflete essa mesma realidade, o ciberespaço suscita debates sobre sua própria natureza. As discussões dividem-se em dois entendimentos principais. Por um lado, envolvem a noção geográfica ou territorial, principalmente quando se tenta entender o papel de entidades públicas sobre o ciberespaço, ou se é uma espécie de reunião dos

acontecimentos paralelos permanentes. Por outro lado, Souza & Costa (2006) afirmam que o ciberespaço acontece, ao invés de existir em um determinado local restrito e limitado a fronteiras. Em outra perspectiva, o ciberespaço também é um ambiente. Mais ainda, o ciberespaço através da dinâmica inerente, também é capaz de influenciar e moldar e pautar determinados comportamentos adotados (ou não) por seus frequentadores. Cortes et al. (2012: 3), por sua vez, colocam-se a mesma questão e concluem que o ciberespaço é efetivamente um lugar, não concreto, mas virtual.

A ideia apresentada por Monteiro (2007), propicia uma elucidação do raciocínio acima exposto. A autora descreve o ciberespaço como algo definido a partir de sua condição virtual, não necessariamente limitado a um espaço físico, embora esta dimensão também exista e tenha a sua importância. A ideia da autora é de que o ciberespaço está presente enquanto potência, possibilidade, portanto, existe em uma condição ´desterritorializante´. Esse espaço por existir de forma virtual, não é palpável. Consequentemente, não tem limites necessariamente definidos ou conhecidos, pelo contrário, a condição é a de um permanente estado de possibilidades.

Não é possível nem mesmo dizer que o ciberespaço reside nos computadores ou mesmo nas redes de computadores. O ciberespaço flui entre as ferramentas que os acessa e este caráter fluido que faz com que o ciberespaço tenha essa condição virtual (Monteiro, 2007: 2). De forma simples, Whittaker (2004) afirma que, o "cyberspace is one name for the technological glue that binds many of these elements together".

Whittaker (2004), observando as implicações das TIs para as relações sociais contemporâneas, aprofunda o raciocínio. O autor reafirma algumas ideias trazidas por Monteiro (2007), como a de que o ciberespaço não se classifica como um espaço regular. Contudo, para além disso, citando Dodge e Kitchin, (apud Whittaker, 2004: 23) o autor afirma que o ciberespaço não consiste em um espaço homogêneo, mas sim numa profusão de ciberespaços que interagem e se expandem rapidamente, cada um desses apresenta uma forma particular de comunicação e interação através das ferramentas digitais. Segundo ele, esses espaços que formam o ciberespaço podem ser classificados de acordo com os meios onde ocorrem, que podem ser as tecnologias da Internet, as interações em realidade virtual e ainda as telecomunicações convencionais, como telefones, entre outros, sobretudo porque há uma convergência muito eficiente entre as tecnologias e passaram a ser capazes de comunicar-se entre si, da qual emergem espaços híbridos de comunicação e interação. (Whittaker, 2004: 23)

O ciberespaço, em resumo, tem a capacidade de permear espaços físicos e, de acordo com o que os usuários nele compartilham e compreendem, pode trazer as dinâmicas de uma realidade virtual para algo concreto, com consequências em âmbitos físicos, sociais, entre outros. Essas principais características do ciberespaço - permeabilidade, alto e complexo dinamismo, facilidade de acesso – são as que permitem que os acontecimentos nele "hospedado" possam, dependente ou não do propósito e intenções dos usuários que interagem no ciberespaço, implicar em situações práticas e, em alguns casos, tomar grandes dimensões midiáticas, políticas e sociais.

Talvez o melhor e mais recente exemplo da interação no ciberespaço, implicando em mudanças nos cursos não-virtuais, são as manifestações que tomaram as ruas e praças da cidade do Cairo, no Egito em janeiro de 2011. Atendo-se ao essencial dos fatos para esta ilustração, em 18 dias, manifestantes descontentes com as políticas do governo egípcio, chefiado há décadas por Hosni Mubarack, tomaram a praça Tahrir, ponto central da cidade do Cairo, exigiram e conseguiram a renúncia do mandatário (Attia, Aziz, Friedman, & Elhusseiny, 2011). O fato interessante é que a coordenação dos movimentos foi gestada e permitida, em grande medida, pela interação nas redes sociais virtuais. O governo egípcio tentou impedir o acesso à Internet desligando seus cinco principais servidores, o que não resultou, pois, alguns manifestantes conseguiram organizar-se utilizando as redes e infraestruturas israelenses (Howard et al., 2011; Sutter, 2011). O "papel" do ciberespaço nessa ocasião acabou por alcunhar as manifestações de "Revolução do Facebook" (Vaughn, Gold, & Khamis, 2012).

A análise mais interessante sobre as implicações nas dinâmicas do ciberespaço na condução das questões concretas é feita pelo arquiteto Nezar Alsayyad (2012). O autor, ao olhar para estes eventos na praça Tahrir, constata o surgimento de uma nova dimensão caracterizada por uma espécie de hibridismo que conjuga o real e o ciberespaço em uma mútua influência:

> […] revolutions do not simply happen in cyberspace even if they get their start there. And what the Cairo experience clearly shows is that the real Tahrir Square, with all the sweat and blood that spilled onto it and its messy, disorganized, and ever-changing virtual counterpart, are two sides of the same coin. In fact, I would suggest that today the real Tahrir Square may not continue to possess a meaningful existence without its virtual other, one that could legitimately be called Tahrir2. (Alsayyad, 2012: online)

As implicações dessa permeabilidade e fluidez do ciberespaço vão além das inovações tecnológicas e invadem questões mais tradicionais relativas à segurança,

soberania, domínio e vigência de sistemas legais, entre outros. Por um lado, potencialidade de interação e a capacidade de fluir através das fronteiras físicas e temporais está na essência da Internet; por outro, a inovação tecnológica foi mais ágil que a capacidade dos atores tradicionais em viabilizar respostas e práticas que viabilizassem necessidades de proteção, segurança e controlo que permanecem relevantes ou mesmo decisivas. (Naim, 2014; Nye, 2011).

Os eventos da praça Tahrir podem ser o começo de uma série de transformações nas concepções e ações de atores como os Estados, instituições nacionais e internacionais. As consequências, tanto positivas quanto negativas da expansão do ciberespaço tornam-se cada vez mais evidentes. Não há, entretanto, uma resposta que traduza em termos práticos os termos de posicionamento dos atores sociais e decisores políticos. Essas questões têm importância central para este trabalho e serão devidamente abordadas nas seções seguintes. Contudo, para um entendimento mais coerente do contexto atual e das implicações do ciberespaço, julga-se apropriado trazer as circunstâncias da criação ou desenvolvimento das ferramentas que culminaram na existência do ciberespaço, ainda que de forma breve, sem detalhar tecnicamente os passos.

1.1.2.1. A "criação" da Internet

A partir da percepção e do entendimento que o ciberespaço é uma realidade híbrida, visto que não é algo palpável, mas que tem implicações práticas na sociedade em geral devido a interação de seus usuários, a questão que se levanta é, como isso foi possível? Como se tornaram as inovações tecnológicas da informação tornaram-se tão presentes no cotidiano, principalmente em países ou regiões industrializadas? Mais do que isso, como em alguns casos, tornaram-se tão essenciais às necessidades?

Parte da resposta a essas perguntas relaciona-se com a História da Internet, sua natureza colaborativa e do seu enraizamento na herança proveniente dos movimentos de contracultura muito evidentes na década de 1960. Parte também da evolução da indústria em geral, mas principalmente da indústria bélica a partir do fim da Segunda Guerra Mundial.

As mudanças na economia e em políticas, aliadas ao desenvolvimento tecnológico, deram origem a uma era pós-industrial, centrada em aspectos sociais e de produção que tem base em uma crescente dependência ou valorização de conhecimentos específicos. Como é

sabido, essa nova dimensão das estruturas sociais veio a ser denominada como sociedade da informação (Barney, 2004; Daniel Bell, 1999; Cardoso, 1998; Castells & Borges, 2003).

Interessante ressaltar que o processo de desenvolvimento da Internet deixa evidente a capacidade humana de transcender limites burocráticos, regras institucionais e superar valores. Castells (2004), um dos autores de proa nesta emancipação conceitual da sociedade da informação, examinando este processo através de uma lente sociológica, sustenta que a cooperação e a liberdade de informação, neste processo de criação e desenvolvimento da Internet, favoreceram mais a inovação do que os princípios da concorrência e direitos de propriedade. Contudo, o contexto mais amplo que permitiu os primeiros passos da Internet é permeado pela competição estratégica entre o bloco americano e soviético que competiam estrategicamente por supremacia política e militar (Fernandes, 2014). Assim, se por um lado a criação da Internet tem na colaboração coletiva um dos seus principais pilares, por outro, foi incentivada por um impulso competitivo.

Na impossibilidade de estabelecer uma data precisa, vários autores aceitam que o nascimento da Internet acontece em meados da década de 1960, com a concretização dos trabalhos desenvolvidos pela Agência de Projetos de Pesquisa Avançada do Departamento de Defesa Norte-Americano (ARPA) e pelo Massachusetts Institute of Technology (MIT) (Castells, 2004; Fernandes, 2014; Kleinrock, 2010).

A ideia de criar uma rede de informação guarda relações muito estreitas com o contexto político da Guerra Fria e, consequentemente, da ascensão e desenvolvimento do arsenal nuclear, da consequente corrida armamentista e espacial. O que veio a ser popularizado como Internet surge como parte de estratégias de defesa norte-americana em resposta ao lançamento do satélite russo Sputnik, em 1957. Uma das medidas foi o desenvolvimento da ideia de Paul Baran, da Rand Corportarion[6] de implementar um sistema de comunicação que pudesse resistir a um eventual ataque nuclear, segundo Castells (2005: 55) e também para construir um sistema que permitisse aos investigadores compartilhar recursos e resultados com seus pares (Cohen-Almagor, 2011).

No início da década de 1960, Joseph Linklider, então diretor do *Information Processing Techniques Office*, e Welden Clark, publicaram o artigo "On-Line man

[6] A Rand Corporation (Research ANd Development) é um instituto de investigação sem fins lucrativos, financiado pelo governo americano e capital privado. As investigações ali desenvolvidas voltam-se para o desenvolvimento de tecnologias de informática, inteligência artificial entre outros. Colabora inclusive com o programa espacial americano.

Computer Communication", estabelecendo o que viria a ser o conceito central da Internet, ou "Galactic Network", como classificavam. No artigo os autores exploram rumos e possíveis problemas para os quais se voltariam as investigações. Segundo os autores,

> In associating capabilities [goals and criteria] through [building up a progressively repertoire of procedures without suffering any loss due to interference or lack of use] primarily with human beings and capabilities [of storing large quantities of information with high precision] primarily with computers, we are of course describing the present state of affairs, the technology in which we now must work, and not asserting any essential discontinuity between the domains of human and machine information processing. There is always the possibility that human competence in [storing information] through [computers] can be significantly increased, and it is almost certain that machine competence in [select goals and criteria] through [handling unforeseen and low-probability exigencies] will develop rapidly during the next decades. (Licklider & Clark, 1962: 115)

Nos anos seguintes, alguns institutos, nomeadamente o British National Physical Laboratory, o MIT e a RAND Corporation (Research and Development) pensavam no desenvolvimento desse sistema de redes de informação computadorizada, de modo a desenvolver uma linguagem padrão que permitisse a transmissão e decodificação de dados. Assim, em 1969, estabeleceu-se a primeira rede de computadores, a Advanced Research Projects Agency (ARPANET), lançada por Bolt Beranek and Newman Technologies (BBN). A partir deste marco, Segundo Leiner et al. (1997: 23), vários computadores e redes de outras instituições de pesquisa, militares ou privadas foram adicionadas à ARPANET, não só utilizando-a como rede de comunicação, mas desenvolvendo e aprimorando sistemas para o seu reforço. Pouco tempo depois do estabelecimento da ARPANET, em dezembro de 1970, completou-se o primeiro protocolo host-to-host[7], chamado de Network Control Protocol (NCP), permitindo, então, que os usuários criassem aplicações, desenvolvessem linguagens e outros tipos de aprofundamentos que servissem à própria rede. O protocolo de transmissão de dados entre computadores foi dividido em duas partes, criando o Transmition Control Protocol e Internet Protocol (TCP/IP), que permitiu maior flexibilidade para a comunicação entre redes e entre usuários. Dados os seus benefícios em relação à interconectividade e a robustez das conexões, o TCP/IP tornou-se padrão nas comunicações de computadores nos Estados Unidos na década de 1980.

[7] Na linguagem técnica da informática, um host (um hospedeiro) é um computador ou qualquer outro tipo de dispositivo que, conectado à uma rede, geralmente à Internet atualmente. Oferece recursos, informações, compartilha serviços, a outro hospedeiro ou usuários das redes, os chamados nós da rede (node). Os hosts dispõem sempre de um endereço que os identifica e que lhes permite serem encontrados. O host não é necessariamente uma grande máquina com grande capacidade de armazenamento, pelo contrário, podem ser computadores pessoais.

A abertura tecnológica e a disseminação do conhecimento acerca dessa estrutura permitiram que outras companhias e instituições desenvolvessem redes semelhantes. Ainda na década de 1980 a National Science Foundation (NSF), em parceria com a Internacional Business Machine (IMB), criaram a Computer Science Network (CSNET) com o objetivo de estender os benefícios da comunicação em rede aos departamentos de ciência da computação que não estavam ligados à ARPANET (Denning et al., 1983). Vale mencionar a criação da BITNET (Because it´s time to NETwork), em 1981, que conectava, inicialmente, a University of the City of New York e a University of Yale, na intenção de proporcionar uma forma de comunicação mais rápida e menos dispendiosa para o meio acadêmico. Era utilizada, sobretudo, para fornecer os serviços de correio eletrônico entre os pesquisadores.

Outras redes compunham esse ciberespaço na década de 1980. Muitas delas já haviam sido criadas nas décadas anteriores e existiam de forma paralela à ARPANET, mas usavam-na como principal eixo. Entre essas estão a MERIT, utilizada pelas universidades do estado de Michigan e a CYCLADES, conectando instituições francesas.

A Internet ainda era de difícil acesso à população alheia às instituições e investigadores. Isso foi corrigido com a implementação de um projeto desenvolvido pelo Centre Européen pour Recherche Nucleaire (CERN), com sede em Genebra. Tim Berners-Lee e Robert Recherche coordenaram um projeto que culminou na criação da World Wide Web cujo software (WWW) foi distribuído gratuitamente. As pressões pelo uso comercial privado da Internet cresciam à medida em que os custos de manutenção e disseminação se tornavam mais atraentes. Um passo importante neste sentido veio com o surgimento dos primeiros Browsers (navegadores).

A partir de então, o acesso à Internet e seus serviços registrou em uma progressão geométrica enquanto seus custos de acesso e manutenção diminuíam na mesma velocidade. A associação entre investigadores acadêmicos, o departamento de Defesa dos Estados Unidos e um certo sentimento de contracultura[8] e de popularização do conhecimento nas décadas de 1960 e 1970 acabaram por criar uma sistema capaz de aprimorar a si próprio

[8] As ideologias e mentalidades afloradas de movimentos sociais na década de 1960, como os hippies e a ascensão dos movimentos ambientalistas na década seguinte, tiveram algum impacto no desenvolvimento das TIs emprestando ao processo um caráter voltado para o compartilhamento do conhecimento. Investigações mais profundas sobre este tema podem ser consultadas em Turner (2006).

através da colaboração dos usuários e que, enquanto se desenvolve torna-se mais essencial às atividades sociais.

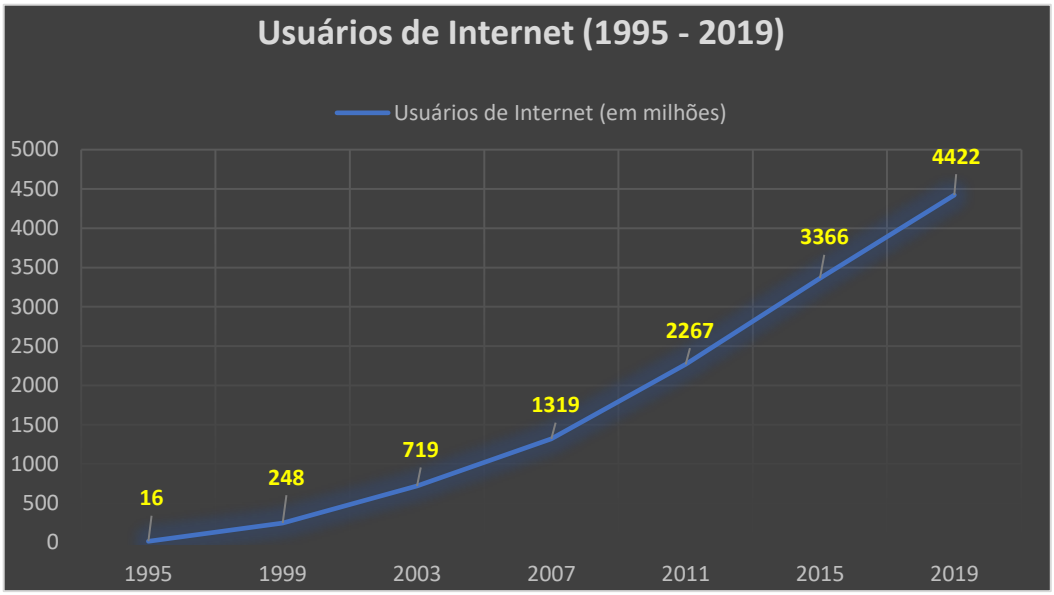
Mas Castells (2004: 36) adverte que a criação da Internet não foi um simples efeito colateral de um projeto de investigação. A Internet foi "idealizada, deliberadamente desenhada e posteriormente gerida por um decidido grupo de informáticos que pouco tinha a ver com as estratégias militares, estava fundamentada no sonho científico de mudar o mundo através da comunicação entre computadores".

Identificados os contornos do nascimento da Internet enquanto suporte do que chamamos ciberespaço, impõe-se agora entender como e o quando o ciberespaço se tonou parte da vida contemporânea. As partes seguintes exploram essa expansão.

1.1.3. O mundo (ou era) digital

O gráfico abaixo oferece a ideia do crescimento dos usuários da Internet desde o início da década de 1990. Em pouco mais de duas décadas, a conexão em rede deixou de ser exclusivo de um pequeno grupo de investigadores e estrategiaS militares, para se tornar uma ferramenta utilizada por quase a metade da população do planeta. Muitos são os usuários, outros tantos são os fins, a rede é usada desde transações econômicas, trabalhos de diversas categorias, investigações e entretenimento, sobretudo para contato e desenvolvimento de relações sociais (Fernandes, 2014: 37). A Internet, suas ferramentas e possibilidades juntaram-se, então, ao conjunto de meios de comunicação de massa (Bargh & McKenna, 2004).

Gráfico 1. Evolução do número de usuários da Internet (1995-2019)



Fonte: Adaptado de Internet Word Stats (2019)

Esses dados revelam ao menos duas implicações sociais importantes que, em uma análise histórico-social, tornaram-se a característica dos anos 1990 e se consolidaram nos anos 2000. A primeira delas é a criação ou popularização de uma nova economia baseada no consumo das TIs. Por outro lado, há também uma implicação nos hábitos não só dos usuários, mas da sociedade como um todo.

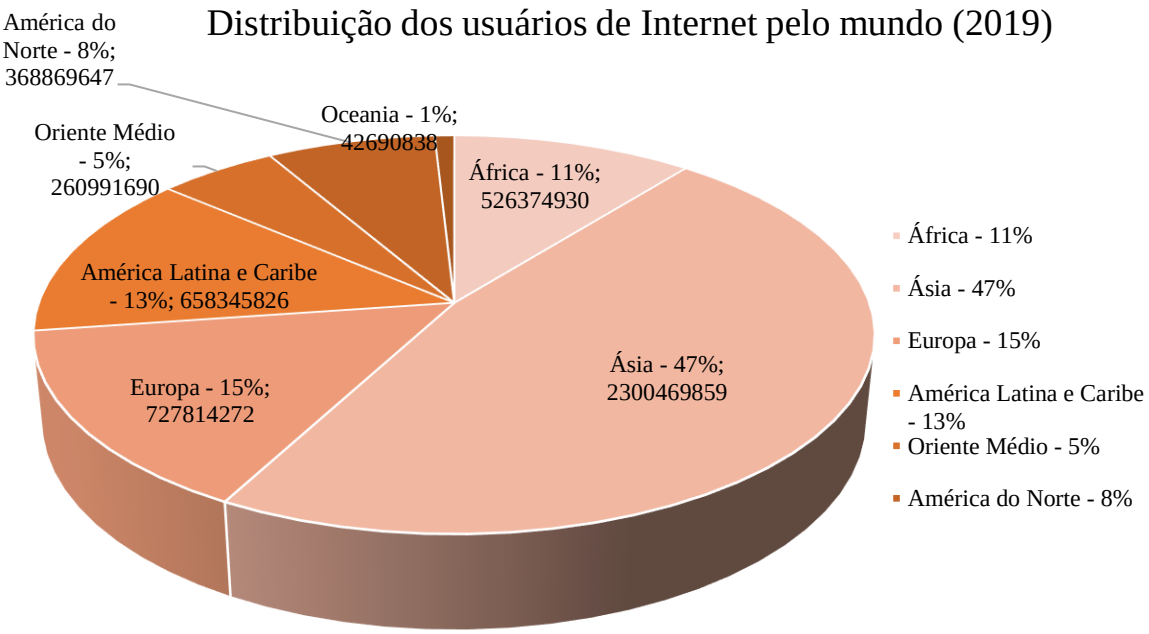
A abertura da informática para a exploração civil e mercadológica e a privatização do acesso à Internet acabou criando um mercado de consumidores de proporções mundiais em um período relativamente curto. Esse potencial não se limita ao número de consumidores que podem passar a fazer parte deste mercado, mas assento também na capacidade de inovação e aprimoramento, no desenvolvimento de produtos e serviços direcionados aos usuários habituais. Esses movimentos são explicados, em parte, pela chamada lei de Moore[9], segundo a qual, a capacidade de processamento de dados das TIs dobra a cada dezoito meses. Esses três fatores: a inovação, a capacidade de atender de forma eficiente muitas das

[9] Gordon Earl Moore, empresário norte-americano, co-fundador e diretor emérito da Intel Corporation, empresa líder no setor de TI e hardware que domina cerca de 60% do mercado. Na década de 1960 Moore trouxe a ideia de que os chips e processadores aumentariam sua capacidade em 100% a cada 18 meses, mantendo o mesmo custo. Inicialmente essa teoria era somente uma opinião, entretanto, a indústria da informática tomou-a como objetivo e meta. Recentemente, entretanto, a Lei de Moore e a indústria começam a necessitar de revisões, visto que engenheiros passaram a desenvolver produtos que não requer tanto dos processadores, não necessitando, portanto, de um constante e padronizado aprimoramento nos processadores.

necessidades sociais e o custo decrescente têm impulsionado o mercado da TI que, por sua vez, tem mantido certo vigor em termos comerciais (Keyes, 2006).

Apesar da constante e expressiva expansão do acesso à Internet e TIs, o acesso a esses serviços ainda é profundamente desigual entre as regiões do mundo. O gráfico abaixo traduz em números absolutos a disposição dos usuários da Internet entre as regiões.

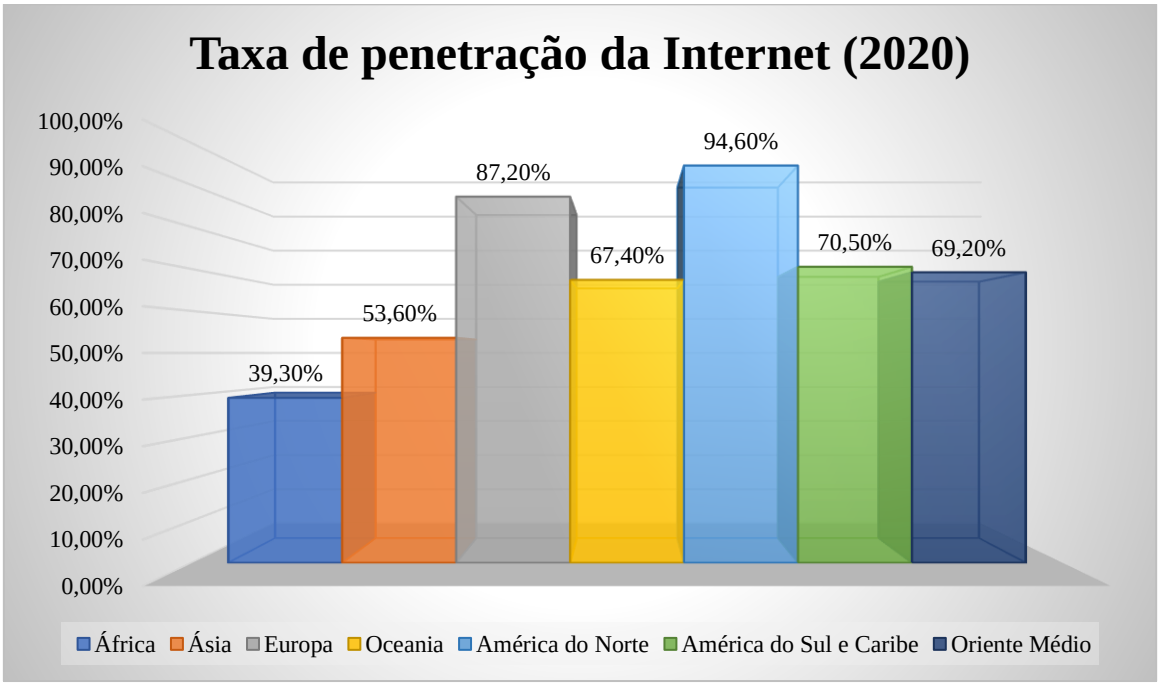
Gráfico 2. Distribuição dos usuários de Internet pelo mundo (2019)



Fonte: Adaptado de Internet Word Stats (2020)

Contudo, a disposição dos usuários não significa, necessariamente, que a Internet tenha mais impacto onde há mais usuários. Percebe-se que, países asiáticos dominam o acesso à Internet em número de usuários, no entanto, é preciso considerar a totalidade da população dessa região para que se possa esboçar hipóteses sobre o impacto da Internet nessas sociedades. Assim, a avaliação da distribuição dos usuários da Internet e das TIs é mais precisa quando se examina o grau de penetração dessas tecnologias em uma determinada sociedade. Como observa Howard (2010), as investigações acerca da Internet são mais eficientes quando se examina o uso da Internet per capita. A diferença de disponibilidade da Internet em função do número de usuários e da população varia de região para região ou até mesmo de países dentro de uma região.

Gráfico 3. Taxa de Penetração da Internet (2020)



Fonte: Adaptado de Internet Society and Internet World Stats (2020)

Comparando os dois planos de dados, percebe-se, por exemplo, na Ásia, embora a região detenha o maior número de usuários (46% do total), a Internet não alcança a maior parte da população, sendo disponível a aproximadamente 35%. Do mesmo modo, embora América do Norte concentre apenas 10% dos usuários totais, a Internet é usada por 85% da população[10].

Interessa ressaltar, não obstante, que as diferenças de acesso à Internet entre as regiões refletem as relações ou diferenças centro-periferia em termos globais. Enquanto cerca de 80% dos cidadãos de países desenvolvidos dispõem de acesso à Internet, pouco mais de 30% dos cidadãos de países em desenvolvimento contam com esse serviço (ITU, 2014). Como é obvio, as diferença de acesso entre países desenvolvidos e em vias de desenvolvimento é conhecido como "digital divide"[11]. Segundo a Organization for Economic Co-Operation and Development (OCDE),

[10] Internet Society oferece um gráfico bem elaborado com dados atualizados e mais precisos sobre a disponibilidade e utilização da Internet por país. Disponível em: http://www.Internetsociety.org/map/global-Internet-report/?gclid=CO7Op8vm2sQCFeoSwwod6mYAaQ

[11] Não há uma expressão que traduza o conceito de "digital divide" para o Português com precisão. Alguns textos que tratam do assunto usam ´exclusão digital´ como sinônimo voltado para temas específicos. Por hora, a expressão ´fissura digital´ parece melhor encaixar para a proposta desse texto, que é comentar as disparidades de acesso à Internet e tecnologias da comunicação que existe entre países desenvolvidos e subdesenvolvidos.

> the term “digital divide” refers to the gap between individuals, households, businesses and geographic areas at different socio-economic levels with regard both to their opportunities to access information and communication technologies (ICTs) and to their use of the Internet for a wide variety of activities. The digital divide reflects various differences among and within countries. (OCDE, 2001: 6)[12]

1.1.3.1. O significado das estatísticas: implicações de uma sociedade digital

A ascensão de uma cultura digital largamente disseminada pode ser considerada mais uma etapa do percurso do ciberespaço enquanto elemento relevante contemporâneo. Mais do que sua estruturação, a popularização da Internet possibilitou a emergência de um novo eixo no qual muitas das necessidades sociais contemporâneas têm relações ou dele dependem. Mais do que isso, a dependência dessas novas tecnologias, devido à sua capacidade de penetração em diversos segmentos sociais, passou a ser vista como uma política ou uma prática a ser incentivada. Deste modo, governos, instituições internacionais, organizações não-governamentais e mesmo as organizações sem fins lucrativos têm se dedicado a formular e a incentivar políticas que permitem a disseminação e o uso de meios digitais sob o entendimento de inclusão social.

A título ilustrativo, é interessante ressaltar que o objetivo alegado da União Internacional para as Telecomunicações (ITU) é a promoção e consolidação da comunicação através das diversas ferramentas a nível global, objetivo inclusive expresso em seu slogan: “Committed to connecting the world”. Sendo assim, há toda uma estrutura que funciona como organização internacional baseada na superação das barreiras referentes à comunicação e para a promoção ou substituição de novos padrões, com ordem, segundo afirmam, na promoção do acesso de usuários (países, indivíduos, empresas) a mercados globais de uma maneira mais equilibrada.

[12] Importante ressaltar que a ´fissura digital´ tem sido um assunto muito debatido internacionalmente. Mais do que isso, existem iniciativas com vistas a diminuí-lo. A própria OCDE funciona como um exemplo dessas práticas. A organização considera que a disparidade do acesso às TIs entre países reflete uma diferença prejudicial para o desenvolvimento social e econômico e que a ausência de medidas para combater essa desigualdade agrava a situação. Neste sentido, a OCDE tem viabilizado programas que atinjam, por exemplo, em nível de cooperação internacional, países que não conseguem desenvolver infraestruturas para as TIs e, em nível interno, tem incentivado políticas que levem essas tecnologias a grupos isolados (comunidades rurais, setores de baixa-renda), a disseminação das tecnologias bem como o treinamento para sua utilização nas escolas. A nível de governo, há uma preocupação com a regulamentação das atividades do setor tecnológico com objetivo de promover a competição econômica e, como já existe em alguns países, o desenvolvimento de práticas de e-government[12] (OCDE, 2004; Ginsburg et al., 2000; Venezky, 2000).

O que se tem incentivado e fortalecido de maneira mais ou menos acordada entre as organizações internacionais e empresas ligadas às TIs é uma cultura digital. Esta seria mais uma etapa do desenvolvimento e implicações do ciberespaço para as questões de ordem social. Contudo, o que se entende por cultura digital é uma ideia que não conta com termos necessariamente definidos ou precisos. Para Gere (2008), mencionar que algo pertence a um domínio faz alusão a uma vasta rede de aplicações e ferramentas de intercâmbio de informações possibilitadas pela ascensão das tecnologias digitais. Esse conjunto de ferramentas e ações por elas possibilitadas geraram respostas culturais através de movimentos (como por exemplo, o *Cyberpunk*), filmes, gêneros literários específicos, como já exemplificados anteriormente. Mais profundo, entretanto, é a criação de uma nova forma de capitalismo mundial dominado por empresas de TI, como a Microsoft e Sony e as empresas outrora chamadas de ´dot.com´, baseadas na Internet, vistas como o modelo de negócio a prosperar no século XXI. Em alguns casos, segundo Gere, tais empreendimentos parecem ter mais flexibilidade e poder de ação que supera o de muitos Estados. Gere (2008) sustenta que as TIs, ao mesmo tempo em que se desenvolvem, se expandem e se tornam úteis, também trazem uma nova definição de maneiras de pensamento:

> Digital refers not just to the effects and possibilities of a particular technology. It defines and encompasses the ways of thinking and doing that are embodied within that technology, and which make its development possible. (Gere, 2008: 17)

E sobrepõe a esta discussão o que Castells (2004) chama de Revolução das TIs. Essa revolução foi possibilitada, segundo ele, por uma estrutura baseada em quatro estratos sobrepostos: a cultura da tecnomeritocracia, a cultura hacker[13], a cultura comunitária virtual e a cultura empreendedora[14].

[13] O termo hacker está relacionado no senso comum aos chamados piratas da Internet. Essa associação é frequentemente utilizada na imprensa não especializada. Os criminosos da Internet são, mais especificamente, denominados crackers. São usuários com conhecimento técnico avançado em programação e redes de comunicação capazes de invadir sistemas privados e então extrair dados que tenham valor financeiro, como acesso a contas bancárias, etc, ou valor político, como segredos de estado, mensagens diplomáticas, entre outros.

[14] Considera-se que a pormenorização da exposição das ideias de Castells sobre essas categorias não acrescentaria grande valor explicativo tanto à proposta da tese como um todo, como também a este ponto específico. Contudo, dada a proposta de organização do autor para o entendimento da evolução de uma cultura digital, opta-se por uma breve apresentação das características principais. Assim, segundo Castells (2005), a característica principal do grupo dos técnicos é o grande conhecimento específico e potencial de criação e inovação em âmbito científico. Geralmente associam-se à vanguarda das inovações tecnológicas amparados por importantes instituições acadêmicas e institutos de investigação. O aspecto meritocrático refere-se ao bem comum que uma inovação tecnológica ali criada e gestada é capaz de proporcionar para uma comunidade. A avaliação da meritocracia a esse modo condiciona o reconhecimento por seus pares e investimentos financeiros. O grupo dos Hackers, apesar de serem popularmente ligados à atividades obscuras e até criminosas, tem seu espaço no desenvolvimento da cultura digital por terem impulsionado o desenvolvimento e inovação das TIs e

A cultura digital também promove uma *skill revolution*. A junção da conectividade com o acesso à informação potencia um aumento do conhecimento dos usuários tanto em temas gerais quanto específicos. Por outro lado, a familiaridade com essas TIs acaba por impulsionar ainda mais o desenvolvimento ou a necessidade de aposta em inovação. Deste modo, a inovação e a capacidade de lidar com ela é um traço marcante da cultura digital (J. Rosenau & Singh, 2002).

Apesar do seu caráter marcadamente individual, a cultura digital abre para a ação digital. No que se refere às questões políticas, de modo mais preciso, as TIs, principalmente a Internet, têm estimulado sentimentos identitários e de pertença, ao mesmo tempo que potenciam interações internacionais e globais. Rosenau vê nessa interação algumas possibilidades de transformações frente a política internacional:

---

das linguagens de programação, inovações que têm base em uma construção coletiva e ou colaborativa entre usuários de grande conhecimento e em uma comunicação continua e livre. Por outro lado, a cultura hacker também serve como um ponto intermediário que viabiliza a comunicação entre a cultura tecnomeritocrática e os projetos empresariais que observam as necessidades sociais enquanto nichos ou possibilidades de mercado. As comunidades virtuais, de acordo com Castells, são o que dá verdadeiro sentido ao ciberespaço, pois transporta para este plano o contexto social concreto, ou seja, traz para o mundo virtual a diversidade e contradições da sociedade. Há, segundo Castells (2004: 76) duas características culturais principais que define esse "estrato". A primeira é a comunicação sem hierarquias e livre, sem ´*gatekeepers*[14]´. Esse atributo permite que os usuários dessas comunidades superem os obstáculos que outrora impediam a comunicação direta e livre a um público geral. Ultrapassam assim, não só os limites físicos (distância e custos, por exemplo) mas os domínios burocráticos de instituições como o Estado e o monopólio das grandes empresas de comunicação. Essa liberdade de expressão tornou-se um dos principais argumentos a favor da disseminação do uso da Internet e uma das principais causas defendidas aos contrários a instituição de regulamentos para a Internet. O segundo valor refere-se à liberdade e possibilidade dos utilizadores em encontrarem seus próprios interesses na rede e associar-se a grupos ou ´comunidades´ direcionadas ou, quando não as encontram, criam eles mesmo seus espaços. É neste ponto que duas das bases da cultura da Internet se encontram. A comunidade hacker, por exemplo, compartilha de um sentimento de pertença a uma comunidade que se reestrutura ao redor de valores comuns que são desenvolvidos e restruturados nessas mesmas redes e comunidades virtuais. Ao mesmo tempo em que é impulsionada pelas inovações das TIs a cultura das comunidade virtuais é a base da cultura hacker. Por fim, o último grupo é guardado às empresas de informática e softwares que têm sido o grande incentivo para a expansão da Internet. É sabido que o desenvolvimento das TIs dependeu em grande parte dos investimentos, sobretudo o de capital de riscos. Os investimentos no setor da informática impulsionaram o que veio a se tornar uma economia globalizada, com novas regras e processos de produção e gestão de produtos oferecidos não só a este meio do ciberespaço, mas que acaba afetando ou tendo implicações importantes para a economia mundial. Outra característica é que esses empreendedores não trabalham necessariamente baseados no que já existe ou nas atuais possibilidades. Pelo contrário, geralmente convencem investidores e o mercado financeiro da capacidade de determinada empresa em inovar determinado setor econômico, ou criar um mercado. A base da cultura empreendedora no ciberespaço está na transformação da visão empresarial conjugada com o conhecimento técnico de inovação em valor financeiro. A cultura empreendedora foi e continua a ser essencial para o desenvolvimento e disseminação da Internet. Segundo Castells, essa dimensão do empreendedorismo digital traz uma caraterística histórica nova que é a de atrair investimentos com base em ideias, e não em produtos. Deste modo, o dinheiro é a mercadoria e a produção material induz o fluxo de capital baseando-se na capacidade de produção e convencimento das ideias. Assim, mais do que homens de negócios, os empreendedores da Era da Informação são mais criadores do que homens de negócios tradicionais. Estão mais próximos da criatividade artística do que da cultura empresarial necessariamente (Castells, 2004: 78 – 82).

> "these individuals enhance public affair skills has also contributed to a major transformation of the global structures that are emerging as instruments of governance in the age of fragmentation" (Rosenau, 2002: 262).

Também nesta perspectiva, Pierre Lévy (1999), sublinha a influência das TIs no municiamento do ativismo dos movimentos sociais em áreas como a democratização, a luta ecológica ou pelos direitos humanos, agilizando o acesso a uma quantidade de informações que antes exigia a presença de um grande número de colaboradores dedicados a análises das mesmas (Lévy, 1999).

Em suma, a ascensão da importância ciberespaço e a crescente utilização da Internet não podem ser consideradas uma mera otimização das técnicas de comunicação. Há questões fundamentais que as diferenciam das inovações da comunicação experimentadas até então. As interações permitidas pelo ciberespaço e Internet acabam por criar e refletir uma cultura própria dessa era da informação. Essa emergência de uma ´cibercultura´, termo aqui emprestado de Lévy (1999) que envolve o comércio eletrônico (e-commerce), a indústria do entretenimento e a comunicação virtual, entre outros aspectos, significa também uma transformação nos costumes, nos sistemas de ensino, na produção industrial, comercial, na organização do trabalho e, naturalmente, implica nas questões de política pública, entre elas, a segurança e o próprio papel do Estado[15]. É este o objetivo da próxima seção.

1.2. O Estado e o ciberespaço: soberania, poder e novas ameaças

1.2.1. Soberania

Uma das primeiras questões levantadas sobre o papel e poder do Estado no ciberespaço é a manutenção da soberania. A permeabilidade do ciberespaço, ou seja, a facilidade e rapidez com que o fluxo de informações parte de um determinado território e torna-se acessível em outro independente da distância sem necessariamente deixar traços de onde veio ou de quem o iniciou é um dos desafios do Estado no século XXI. Há uma boa quantidade de trabalhos de referência que equacionam a ascensão do ciberespaço e a

[15] Dadas as circunstâncias impostas pela pandemia de COVID-19, vale ressaltar um importante aspecto envolvendo as TIs. A necessidade de confinamento e quarentena a um planeta praticamente permeado pela interação virtual, trouxe inovações, novas formas de economia e novas terminologias para caracterizar as atividades sociais. Deste modo, popularizaram-se conceitos como tele-trabalho, tele-medicina, tele-ensino. Compras online, visitas a museus e espetáculos promovidos por artistas através de suporte digital tornaram-se práticas adotadas em massa, com consequências económicas e sociais relevantes que têm suscitado debates públicos e condicionado escolhas políticas de grande repercussão.

aplicação de regras relacionadas à soberania dos Estados e as implicações legais e respectivos ordenamentos jurídicos tanto domésticos quanto no direito internacional (Fleck, 2013; J. Lewis, 2014; J. P. Trachtman, 1998; von Heinegg, 2012). De fato, o processo de formação da Internet não só não levou em conta as tradicionais fronteiras políticas e jurídicas como tinha entre os objetivos evitar precisamente esses limites. Isso fica bastante evidente no discurso de Tim Berners-Lee, o já mencionado criador da WWW (World Wide Web). Segundo ele, a WWW seria um espaço:

> "without a hierarchical bureaucratic government being involved at every step, […]. So where design of the Internet and the Web is a search for set of rules which will allow computers to work together in harmony, so our spiritual and social quest is for a set of rules which allow people to work together in harmony". (T. Berners-Lee, 1998)

Vale ressaltar uma aparente contradição. A afirmação de Berners-Lee revela uma intenção por trás da criação de uma ferramenta que supostamente serviria como um espaço neutro para a ação de seus usuários. Assim, o ciberespaço não poderia ser limitado a uma simples ferramenta e tampouco teria na harmonia entre os usuários uma característica dominante. O primeiro motivo é justamente a intenção de afastar qualquer estrutura hierárquica que pudesse exercer uma influência dominante. E, por outro lado, porque é natural que um sistema anárquico não reflita uma harmonia entre as unidades. Contudo, há autores que sustentam uma neutralidade como característica do ciberespaço em relação à soberania.

Assim, Trachtman & Trachtman (1998) salientam que

> "cyberspace […] is neutral in the contention over the powers of the state. Those who purport to tell us whether cyberspace will, in the course of time, demean or enhance the powers of the state must fail, as this question cannot be answered in general or in advance, but must be answered as we evaluate and build particular institutions over time. In fact, our best hope is that it will be citizens, not scholars, who, by their political acts, will indicate when and how contingent sovereignty will change". (Trachtman & Trachtman, 1998: 565)

Essa ideia de neutralidade se evidencia quando o ciberespaço passa a ser entendido como uma espécie de arena, onde desfilam e atuam vários atores com capacidades e interesses diferenciados. Assim,

> Cyberspace is best viewed as a bulge in the technical production frontier. Our institutions, including contingent sovereignty, determine the extent to which we reach the limits of the technical production frontier. In addition, and more saliently, changes in the technical production frontier, especially in communications, modify the structural production frontier. They do so by modifying the transaction costs of different institutional structures. This means

> that not only does cyberspace facilitate private activity, but, […] it also facilitates government activity. Not only does technology strengthen the tools of government, but it can also strengthen the legitimacy of government through heightened transparency and democracy. (Trachtman, 1998: online)

O ciberespaço colocou, de fato, o Estado como um elemento mais em sua arena onde também estão outros atores com diferentes características e que fora deste espaço pertencem a outras esferas, como indivíduos, grupos diversos. Assim, o poder torna-se mais difuso no ciberespaço, mas isso não significa necessariamente que exista uma igualdade entre os usuários. Naturalmente, essas posições estão em constante debate porque implicam em questões de ordem de governança, de processos jurídicos cíveis e penais.

Não obstante, como já mencionado, o ciberespaço, ao menos por hora, não está necessariamente sujeito às mesmas regras que um território sob leis e domínio do Estado. Contudo, há que se ponderar um certo equilíbrio entre os usuários no ciberespaço o impacto de suas ações em um plano não-virtual. Como afirmam Cavelty & Brunner (2007), computadores, redes e comunicações são produtos das pessoas e estas vivem obrigatoriamente em um espaço físico regido por leis. Deste modo, se por um lado há uma mudança de pensamento e hábitos provocada ou viabilizada pela ascensão das TIs e do ciberespaço, por outro as estruturas de organização tradicionais baseadas em aspectos físicos e políticos não deixaram de existir e ainda exercem ou têm a capacidade de exercer influência, inclusive no ciberespaço. Deste modo, falar em rotular as mudanças como uma revolução das TIs no sentido de rompimento com as estruturas que vigoravam anteriormente é uma distorção da realidade. As estruturas sociais e políticas, embora sob o impacto das novidades do ciberespaço, permanecem em ação a despeito das inovações.

Aceitar simplesmente que há uma revolução da informação não é necessariamente útil para compreender as questões de segurança contemporâneas, uma vez que estruturas como o Estado e instituições como regimes jurídicos nacionais e internacionais ainda permanecem e exercem influência, embora não possam controlar completamente os fluxos de informações. Como afirma Nye (2011), a emergência do ciberespaço e principalmente da Internet entre outras ferramentas não suplantará a soberania do Estado ou mesmo uma alternativa que substitua a importância da convivência e intercambio em lugares físicos pelo contato virtual, pelo contrário, esses novos elementos contribuem para o aumento do leque de atores com os quais o Estado passa a se ocupar. À medida em que o que Nye chama de ´poder informático´, tem ficado mais barato e computadores mais flexíveis e acessíveis, os efeitos da utilização do ciberespaço vão minando as lógicas centralizadoras. Uma

consequência direta e primária deste fenômeno é que o poder sobre a informação está mais disseminado hoje do que há poucos anos. Quando se compara a Internet com os meios de comunicação tradicionais – televisão, rádios, jornais – altamente controlados por suas respectivas direções, percebe-se que a Internet possibilitou uma comunicação quase ilimitada, primeiramente por não ter necessariamente um sistema hierárquico que paute ´artificialmente´ os assuntos comentados e, por outro lado, porque estabelece uma comunicação de indivíduo para indivíduo (através de e-mail e mensagens diretas), de um para muitos (através de blogs, ferramentas de redes sociais), de muitos para um (como as páginas construídas em regime de colaboração voluntária, como o *Wikipedia*) e, talvez o modelo mais importante, o de muitos para muitos (através de salas de chat, redes sociais, fóruns de debates, entre outros).

Esses novos métodos de comunicação possibilitados pelo desenvolvimento da Internet, quando comparados com seus antecessores e paralelos, permitem notar que a grande diferença é de alcance. As mensagens propagadas pela Internet atingem um público muito maior, mais disperso geograficamente ao mesmo tempo em que é mais preciso em relação ao interesse pela mensagem e com menos intermediários. Em muitos casos, a informação passa a garantir um recurso de poder essencial às transformações locais e, ao mesmo tempo, dando resposta a acontecimentos globais.

Naturalmente essa nova dinâmica também se reflete em aspectos nefastos. Este menor controle vertical das informações também permite um aumento da manipulação da informação através da Internet por meio da fabricação de fatos potencializados pelos algoritmos usados na distribuição dessa informação. As denominadas *Fake News* ganharam uma dimensão tão relevante que atualmente são caracterizadas como uma grave ameaça às democracias (Lee, 2019; Muqsith & Muzykant, 2019).

O resultado prático disso é que aa política, incluindo a política internacional, parece estar escapando do âmbito do Estado, dos representantes eleitos ou de uma elite governamental para estar disseminada entre outros atores da sociedade civil: ONGs, grandes e pequenas empresas, organizações terroristas, grupos separatistas, fabricadores de fatos através dos novos meios sociais, entre outros. É verdade que todos esses atores têm agora uma maior possibilidade de influenciar a pauta das discussões políticas em seus países assim como também a nível internacional. Contudo, o Estado não está alheio a essa nova configuração e consequentemente faz-se presente. Essa mesma atuação será alvo de análises em casos mais práticos nos capítulos seguintes.

1.2.2. Poder

A disseminação da informação e da capacidade de produzir informação tem efeito sobre a distribuição do poder. Essa capacidade é distribuída de uma forma mais ampla e menos formal. Outro aspecto importante que contribui para essa disseminação é a velocidade crescente dos fluxos de informação que por um lado chega com maior rapidez à sua audiência e por outro, reduz o tempo de ação dos governos dificultando o controle sobre os tópicos debatidos. Para além de terem de compartilhar os espaços de discursos com outros atores, os governos, e as lideranças políticas terão menor liberdade para escolher os temas a serem discutidos (Nye, 2011: 138).

Sendo os Estados menos capazes de controlar os fluxos de informação que entram nas suas fronteiras e que circulam no seu interior, abre-se um questionamento sobre a capacidade soberana dos Estados sobre o ciberespaço. Naturalmente, os Estados têm controle sobre a parte física que serve de suporte ao ciberespaço. Essas estruturas físicas (linhas de transmissão, servidores, entre outros) estão sujeitos à jurisdição de um Estado. Sendo esses elementos físicos essenciais ao funcionamento do ciberespaço e considerando que eles estão sob a proteção e controle do Estado, alguns autores consideram que a soberania, do modo como é tradicionalmente entendida, pode ser perfeitamente aplicada ao ciberespaço. Assim, para Heinning, (2012: 10), o princípio da soberania territorial e o direito do Estado em exercer sua jurisdição sobre um determinado território se aplica ao ciberespaço enquanto jurisdição sobre as infraestruturas que dão suporte ou que viabilizam o funcionamento do ciberespaço. Esse mesmo sentido se aplica aos indivíduos que, por sua conduta provoquem danos de qualquer natureza. O exercício da jurisdição, segundo o mesmo autor, só é limitado por outras jurisdições soberanas. Ou seja, o Estado pode fazer tudo aquilo que não for assunto jurídico de outro ator no sistema internacional, em termos gerais, o que inclui também atividades referentes ao ciberespaço. É neste sentido que o exercício da soberania territorial e jurídica não encontra obstáculos em tratar de assuntos ligados ao ciberespaço (Heinning, 2012: 10-11).

Contudo, os controles sobre os fluxos de informação permitidos pelo ciberespaço não são tão eficazes quanto o controle das infraestruturas físicas. Mesmo quando o Estado controla as infraestruturas de conexões do país a redes internacionais, desligá-las quando julga necessário pode demonstrar-se prejudicial. As manifestações de 2011 no Egito, já mencionadas anteriormente, servem novamente de exemplo neste caso. Na ocasião, quando

o governo egípcio que controlava os links de acesso à Internet do país a redes internacionais, percebeu que as manifestações que pediam a sua renúncia eram organizadas a partir das redes sociais, tentou desconectar os cidadãos cotando-lhes o acesso à Internet. O *blackout* intencional durou poucos dias e se mostrou ineficaz. Em primeiro lugar, alguns organizadores dos protestos, conhecedores das tecnologias, contornaram o impedimento do governo usando de satélites e outros tipos de conexões mantendo a ligação com o exterior. Em segundo lugar, o corte acabou por limitar e isolar as agências do próprio governo, provocando uma dificuldade interna para a obtenção de informação e inviabilizando a tomada de decisões coerentes, já que, naturalmente, também dificultava a comunicação interna. Em terceiro, a falta de acesso à Internet acabou por chamar mais a atenção de cidadãos que se juntaram à multidão na Praça Tahrir. Por fim, o último efeito indesejado foram as perdas financeiras: o corte da Internet afetou a economia que por ser integrada a fluxos internacionais é muito sensível às interrupções dos fluxos de informação. Após quatro dias do corte da Internet, a economia do país já arcava com um prejuízo de milhões de dólares, sobretudo nas áreas financeiras e de comunicação (Howard et al., 2011).

Em termos gerais, Nye (2011: 141) observa que a difusão do poder experimentada a partir da ascensão do ciberespaço e das participações de vários atores constitui um desafio para o futuro dos Estados. Isso não significa necessariamente que os Estados deixarão de atuar como a principal instituição política mas vão se encontrar um ambiente mais complexo, no sentido em que outros atores, até então pouco expressivos, encontram meios de fazer-se ouvir, ou meios mais eficazes de defender seus interesses que podem ou não coincidir com a política dos Estados. Segundo o mesmo autor, a grande questão relacionada com esse fenômeno, que ele classifica como uma *difusão do poder*, não é a existência continuada do Estado. Há espaço para movimentos contraditórios concomitantes. Esse aspecto não é ao menos uma novidade do ciberespaço, naturalmente as políticas defendidas em um âmbito político da organização estatal já compete com empresas multinacionais, entre outros atores que fogem, de alguma forma e em ao menos alguns aspectos, ao controle das fronteiras e da soberania.

No caso do ciberespaço, a presença e atuação de muitos atores torna a política nacional e internacional mais volátil e menos contida nas células estatais e, em um mundo marcado pela interdependência global, a agenda internacional passa a ser mais vasta, agregando uma diversidade maior de temas e aberta a discussão mais livre de

intermediadores. Ao menos aparentemente, a participação política está ao alcance de um maior número de atores (Nye, 2011: 141).

Essa nova configuração é traduzida em uma forma muito concreta nas atuais discussões sobre a governança da Internet. O atual modelo de negociações, identificado como *multistakeholder*[16], envolve, em um mesmo nível de importância, os Estados, organizações provenientes do setor privado, organizações internacionais, associações da sociedade civil, acadêmicos entre outros grupos de interesses. A própria definição de governança da Internet proposta em um dos principais fóruns internacionais dedicado ao tema, o World Summit on Information Society (2003), não só revela essa diversidade de atores dividindo o poder de decisão sobre a governança da Internet como também a incentiva como o modelo multissetorial

> Governments, as well as private sector, civil society and the United Nations and other international organizations have an important role and responsibility in the development of the Information Society and, as appropriate, in decision-making processes. Building a people-centred Information Society is a joint effort which requires cooperation and partnership among all stakeholders. (WSIS, 2003)

De fato, há o entendimento de que o Estado, por si só, não dispõe de meios eficientes o bastante para tratar da governança da Internet sem que esta descumpra seu propósito de permitir a livre circulação de informações e a comunicação em rede entre usuários. Nesse sentido, Singh resume o impacto da governança da Internet e o papel do Estado na seguinte ideia:

> The rise of information networks thus impacts patterns of governance in three distinct ways: (1) states are no longer the only actors in technological matters globally, (2) we now speak more of technological plurality than of a technological order, and, (3) global advocacy networks, especially among underprivileged groups, are undermining the legitimacy of existing centers of authority. (Singh, 2002: 19)

Não obstante, apesar da crescente participação de atores não-estatais nas questões envolvendo o ciberespaço em fóruns multilaterais, faz-se necessário ponderar, uma vez mais, essa suposta perda de importância do Estado, dado que o ciberespaço, como já foi visto, tem um componente físico, necessariamente situado em uma jurisdição. Assim, a questão da

[16] De acordo com a Internet Society, a ideia por trás do multistakeholdismo é melhor entendida como um modelo de governança que apresenta três componentes característicos: abertura em relação aos temas e à inovação, a descentralização em relação às instituições governamentais e a inclusão como um processo contínuo. Como a mesma associação define: "Individuals and organizations from different realms participating alongside each other to share ideas or develop consensus policy"(Internet Society, 2016: online).

soberania dos Estados tem dois aspectos diferentes. Por um lado, a infraestrutura física do ciberespaço, uma vez sujeita a atores bem definidos já amparados pela estrutura física e jurídica do Estado é mais palpável. O Estado vai continuar sendo o principal ator a decidir sobre as "instalações" do ciberespaço que as viabiliza de acordo com as suas necessidades políticas e econômicas. Por outro lado, o aspecto virtual do ciberespaço suscita desafios mais complexos. Neste sentido, existem iniciativas que tentam promover e reassegurar a soberania do Estado sobre as informações que circulam no ciberespaço. Demchak & Dombrowski (2011), por exemplo, lembram o processo de "reafirmação vestfaliana" que tem o ciberespaço como alvo. Essas fronteiras no ciberespaço têm na alegação da promoção da segurança seu principal suporte político. Nas democracias ocidentais, esse movimento tem se dado a partir da formulação de regras de "comportamento" dos usuários no ciberespaço, com o estabelecimento de penalizações e a atuação do Estado na investigação e combate a crimes no ciberespaço. Mas, mais do que isso, talvez a atuação soberana que tenha mais visibilidade atualmente seja o estabelecimento de filtros de conteúdo. Um dos exemplos é a chamada *China´s Greatest Firewall*[17].

Por outro lado, as democracias ocidentais têm elaborado documentos, muitos deles em cooperação, que pautam o tema da segurança no ciberespaço. Muitos desses documentos usam como base a percepção de ameaças provenientes da Internet e da informação que ali circula. Em geral, estão pautados a proteção das infraestruturas críticas, a proteção de dados de segurança, como contas bancárias, servidores militares e diplomáticos que contenham segredos de estado, a atuação de terroristas pela Internet, entre outros.

A onipresença do ciberespaço abre espaço para uma discussão acerca da necessidade de os Estados celebrarem acordos de cooperação internacional. Os argumentos a favor dos acordos internacionais ancoram-se principalmente na ideia de que, sendo o ciberespaço pouco controlado em termos de fronteiras, as ameaças provenientes desse meio não encontrariam dificuldades em acessar pontos importantes e sensíveis à segurança interna

[17] Atualmente a China é o país que mais se destaca no controle do fluxo de informações e do conteúdo do ciberespaço. O país conseguiu desenvolver uma série de ferramentas para impedir que um usuário da Internet de dentro de seu território não consiga acessar determinadas informações, nomeadamente as que consideram de "conteúdo subversivo ao poder do Estado, atentatórios da unidade nacional (ou) que infrinjam a honra e os interesses nacionais" (Schmidt & Cohen, 2013). A China´s Great Firewall (Firewall, em linguagem da computação, é um dispositivo que funciona como proteção a um determinado computador ou rede), oficialmente chamada de Golden Shields Project, é uma grande rede de vigilância e de censura relativamente eficaz operada pelo Ministério da Segurança Pública. As políticas desenvolvidas neste âmbito acabaram por afastar do mercado chinês grandes empresas da Internet como o Google, Facebook e Twitter, tornando o ciberespaço chinês quase que exclusivo daquele país.

aos Estados. Os defensores da cooperação internacional como resposta aos problemas de segurança do ciberespaço compartilham da ideia de que o que acontece no ciberespaço está subjugado aos Estados, uma vez que esses estão imbuídos na autoridade de tecer acordos intergovernamentais bem como medidas de segurança e defesa.

Os Estados teriam, então, a princípio, as mesmas bases legais para a atuar no ciberespaço contra crimes e ameaças daí provenientes. De acordo com Sofaer (2010), os mesmos acordos Internacionais que têm sido firmados para tratar de assuntos transacionais dos mais variados setores e temas também se aplicam ou podem ser úteis para servir de base para a implementação da regulamentação das atividades no ciberespaço (Sofaer et al, 2010: 180).

Neste sentido, organizações Internacionais como a UIT vêm incentivando ações desse tipo, alegando que as ameaças do ciberespaço não podem ser combatidas por um país contando somente com seus próprios esforços. Como afirma Sánches (2007),

> The world must take action, and it must stand united. This [ameaças provenientes do ciberespaço] is not a problem any one nation can solve alone. A global framework is needed, giving us international principles to match hackers' international range, and allow rapid coordination between countries at the regional and global levels.

Assim, percebe-se, em um entendimento geral, a ascensão da Internet trouxe novos contextos e novas combinações que tem resultado em uma nova interação social em diversos níveis, das pessoas com pessoas, pessoas com instituições, governos e cidadãos, entre muitas outras possibilidades. Trouxe também novas percepções da segurança que, a princípio continuam sendo responsabilidade da tradicional autoridade estatal que, por sua vez, está em busca de melhor definição do seu papel neste contexto onde as fronteiras territoriais e jurídicas nem sempre estão definidas.

É interessante recortar a questão da cibersegurança e analisa-la sob o entendimento de que se vive um advento de uma era da informação que traz implicações para a sociedade em geral e aplicar às questões da segurança e das relações políticas internacionais. Calvelty, ao estabelecer esta ligação, percebe que há dois aspectos a serem pensados. De um lado, mais tecnológico, há um grande apelo para a questão da própria infraestrutura que permite o funcionamento dessas ferramentas. Por outro lado, ao mesmo tempo em que há ameaças contra esse tipo de infraestrutura, também há outras que delas provém. O que está em discussão, segundo a autora, é o que se tem chamado de ´cyberthreats´. Novamente, por

conta de sua abrangência e de uma discussão ainda embrionária sobre o tema, o termo ainda tem uma noção vaga, mas direciona para o uso da informação para más intenções.

O termo não permite distinção sobre os alvos e se aplica tanto às ameaças contra a infraestrutura da informação quanto as ameaças existentes neste meio. Isso tem implicações sobre as medidas a serem tomadas e os atores competentes para tomar decisões.

Mais do que isso, temas caros à segurança ainda aparecem como a atuação de grupos terroristas e o crime organizado ainda não encontraram respostas unificadas ou entendidas entre os atores para a efetivação de medidas através dos sistemas tradicionais de defesa e, no ciberespaço, tende a se complicar ainda mais por conta de outras indefinições de caráter mais simples e prático, como por exemplo, o limite de atuação de um estado ou organização internacional no ciberespaço. Essa indefinição gera debates que, conduzidos por determinados atores visando seus respectivos objetivos, as vezes pouco claros, acaba provocando uma securitização desses meios, fazendo, por exemplo, que organismos como a National Security Agency (NSA) ou agências de inteligência de diversos países atuem com objetivos pouco claros e baseados em medidas de exceção. Provocam, em resumo, uma desconfiança entre os atores que dificulta o processo de tomada de decisão em favor da cooperação.

Levantam-se, diante desse contexto, questões referentes à quais ameaças provenientes do ciberespaço os estados ou instituições responsáveis pela segurança devem se preocupar, ou para qual direção as políticas de segurança têm voltado? O próxima parte discute essas ameaças a partir de alguns fatos ocorridos que suscitaram medidas de segurança e escolhas políticas na intenção de promover não só a segurança mas também a defesa do e no ciberespaço.

1.2.3. Ciberespaço e questões de segurança

Em novembro de 2014 os computadores da Sony Pictures, uma dos maiores grupos do setor de entretenimento, foram acessados por crackers. Há suspeitas que intrusos atuavam há mais de um ano e roubaram cerca de 100 Terabytes de informação. Entre os dados, estavam informações pessoais de empregados da companhia, dados da empresa, desde os financeiros até informações sobre futuros lançamentos de produtos, entre outros (Cook, 2014). O grupo cracker “The guardians of Peace” assumiu a autoria dos ataques pouco tempo depois. Os crackers implantaram um vírus, um *malware* em uma linguagem mais técnica,

chamado *Wiper*, cuja função é apagar os dados dos servidores. Dias mais tarde, outro grupo cracker, os God´sApstls, enviou mensagens aos executivos da Sony exigindo compensações financeiras e, caso não atendidos, ameaçavam com outro ataque e com afirmações de que se o filme fosse lançado, "the world will be full of fear" e que lembraria o 11 de setembro (David & Spargo, 2014).

Alega-se que os motivos para os ataques iriam para além da extorsão e roubo de dados valiosos. Um dos motivos para o ataque e roubo de dados foi atribuído, ao lançamento do filme "A entrevista". Na comédia, dois jornalistas recebem a missão pelo FBI de assassinar o líder norte-coreano Kim Jong-un enquanto o entrevistam. Casas de cinema, então, recusaram-se a exibir o filme temendo ataques. A Sony cancelou oficialmente lançamento do filme. O governo dos Estados Unidos acusou o governo norte-coreano de envolvimento alegando ciberterrorismo (Singer & Perloth, 2014). Tão logo, o governo norte-coreano negou envolvimento com os ciberataques, alegando que as ligações do governo norte-coreano aos ciberataques constituem propagandas para atingir o país (Sungwon, 2014).

A afirmação certeira do governo norte americano tinha base em outra operação de espionagem. Agências de inteligência, como a National Security Agency (NSA) do país espionavam os sistemas norte-coreanos desde 2010. Contudo, os sistemas americanos aparentemente falharam e não foi possível reunir evidências para fazer qualquer acusação pública a tempo (Sanchez, 2015). O ciberataque à Sony foi o maior já levado a público. Causou um prejuízo de ao menos 200 milhões de dólares à companhia e redeu aos Estados Unidos mais um desgaste diplomático nas já conturbadas relações com a Coreia do Norte (Müller, 2014). Por outro lado, o ciberataque levou outras empresas da indústria do cinema a adotar medidas de cibersegurança e evidenciou atos de espionagem e potenciais conflitos que têm o ciberespaço como palco.

Em agosto de 2013 sítios baseados na China, cujo domínio é o .cn, ficaram indisponíveis aos usuários por algum tempo. A razão, novamente, foi um ciberataque que, de acordo com a empresa de segurança na Internet CloudFlare, pode ter sido organizado por somente um indivíduo em qualquer parte do planeta (Mozur, 2013). A notícia do ataque foi divulgada pelo China Internet Network Information Center (CNNIC), uma subdivisão do Ministério da Informação e Indústria responsável pela administração de assuntos ligados à Internet na China. Segundo o CNNIC, os ataques ocorreram em duas fases, a primeira conseguiu isolar alguns sites, a segunda, algumas horas depois aconteceu de modo mais intenso, impedindo o acesso aos sítios chineses.

Os ataques deste tipo são conhecidos como “Denial of Service Attacks” (DDoS) e consistem em, basicamente, sobrecarregar os acessos a sítios através de um esforço coordenado que instrui milhares ou milhões de computadores ao mesmo tempo, espalhados pelo planeta todos (muitas vezes sem que o dono saiba), impedindo, assim, que usuários normais consigam acessar aos serviços (Jose Nazario, 2009).

É interessante, neste caso, observar uma certa ironia dos fatos. Por um lado, a China detém um dos mais sofisticados sistemas de proteção ao fluxo de dados na Internet, um sistema bastante eficiente de controle de domínios (os .cn) e um hábil sistema de controle de conteúdo, que impede acessos de usuários a informações sobre temas sensíveis ao regime. Com todas essas ferramentas, o país não conseguiu impedir os ataques, inclusive o CNNIC veio a público desculpar-se pela falha e prometer aprimoramentos aos seus serviços (Vincent, 2013). Os ataques de DDoS são bastante conhecidos no meio informático. Esse conjunto de ações ficou muito popular ainda na década de 1990 com o desenvolvimento de ferramentas como o *Tribe Flood Network* e *Trinoo* (Nazario, 2009). Por outro lado, a China, para além de ser conhecida como portadora de uma Internet ´quase´ própria, também o é por ser acusada de ser responsável por diversos ciberataques (Vincent, 2013).

Os ataques de DDoS, apesar de já serem bastante conhecidos, têm se sofisticado e se popularizado, sendo utilizado por gangues da Internet para extorsão, ou ativistas reivindicando direitos ou retaliações (Apps, 2014). Outro exemplo foi o episódio que ficou conhecido como Operação Payback, no qual um grupo de ativistas gerenciaram uma ação de DDoS contra o Bank Of America, MasterCard, Paypal, Amazon, Swiss Bank e Visa, entre outras, em retaliação à decisão de bloquearem as doações ao WikiLeaks (Mackey, 2010). Os ataques, cujos responsáveis foram presos mais tarde, causaram um prejuízo de 3,5 milhões de libras às empresas (Turner, 2013).

Os episódios descritos acima servem de ilustração para um problema que se desenvolveu à medida em que as TIs e a Internet se sofisticaram e se popularizaram. Da mesma maneira que a informação ficou ao alcance de um grande número de pessoas, essas mesmas ferramentas viabilizaram ameaças à segurança em geral. Ou seja, sendo o ciberespaço o elemento comum a muitas, talvez todas, as mais importantes atividades humanas, as ameaças à segurança também vão aonde chega o ciberespaço. Mais que do que isso, podem partir de Estados com interesses políticos, de espionagem, de organizações civis, grupos terroristas, ou simplesmente indivíduos com conhecimento técnico o suficiente. Os Estados não estão alheios a esses eventos e possibilidades. Há uma preocupação de diversos

setores públicos e privados com a questão da segurança no ciberespaço. Seguidamente, explora-se como estas preocupações têm se concretizado em ações, documentos, regulamentos e protocolos de cooperação internacional.

Na intenção de entender como a emergência do ciberespaço se cruza com as preocupações da segurança a nível nacional e internacional é preciso levar em consideração dois aspectos importantes. O primeiro relaciona-se com a própria evolução das TIs e suas implicações para questões práticas e a crescente dependência dessas TIs, já discutidas anteriormente. O segundo é uma combinação de fatores: no que se refere às TIs, leva-se em conta sua acessibilidade cada vez menos custosa e mais incentivada, a possibilidade dos usuários terem acesso a informações que outrora seria difícil; do lado do usuário, percebe-se uma melhor qualificação em termos de busca pela informação de acordo com seus interesses e a crescente capacidade dos indivíduos (agrupados ou não) influenciarem desde a questões locais a assuntos que antes estavam restritos aos tomadores de decisões.

A formulação de estratégias para a promoção da segurança desse espaço tem sido uma prática corrente dos Estados e instituições multilaterais focadas na segurança internacional ou doméstica. Tal prática tem sido chamada genericamente de cibersegurança. A definição do termo carece de aprimoramentos, como afirma Radu (2013). Tal indefinição acaba implicando em compreensões bastante gerais do termo, que pode abranger desde o âmbito técnico de programadores e cientistas ligados à Ciências Informáticas às políticas e acordos internacionais para fins de segurança. Adota-se aqui a definição da resolução da ITU (ITU, 2008):

> Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.

A ascensão das TIs somadas ao também crescente número de pessoas com grande conhecimento técnico disperso nos diversos segmentos sociais que, ainda que precedentes à difusão da Internet, ganharam a capacidade de perseguir seus interesses através das redes implicam também em questões de segurança com as quais o Estado e outras instituições tem se preocupado.

Neste sentido, as tecnologias da comunicação e informação têm ajudado, de várias maneiras, a esses atores não estatais maximizarem suas vozes em meio a um cenário que antes predominavam determinados tipos de atores. Alguns autores, inclusive defendem que

as TIs não só ajudam na exposição de atores não estatais, como contribuíram, à medida em que evoluíam e se disseminavam, para a construção dessa diversidade no cenário político internacional.

As questões de segurança também se tronaram mais complexas e os atores, principalmente Estados e Organizações Internacionais têm atuado de forma pontual de acordo com as situações. Não há, ao menos até o momento, uma política definida em temos de consenso em nível multilateral para tratar de assuntos mais sensíveis que vêm à tona e necessitam de respostas. O caso do ciberespaço e as medidas de segurança que terem sido apontadas como necessárias não fogem à regra.

Apesar de existir algum consenso sobre a necessidade de implementar medidas para promover a segurança envolvendo o ciberespaço, as medidas tomadas até então não seguem uma única direção. Documentos de Estados e instituições internacionais apontam uma diversidade grande de atores e caminhos. Assim como não há consenso sobre as medidas a serem tomadas e cada país adota medidas que se voltam para o que julga prioritário, também não há consenso sobre o que é realmente uma ameaça ao ciberespaço capaz de suscitar medidas de segurança.

O Reino Unido, por exemplo, consagrou o entendimento de que a cibersegurança é um esforço para a proteção da infraestrutura, envolve o National Infrastructure Security Co-ordenation Centre, mas tem afetado às agências de inteligência a maior parte dos recursos para a promoção da cibersegurança (UK, 2014; Choucri, 2014). Os Estados Unidos desenvolveram uma estratégia bastante parecida. Para além de considerarem o ciberespaço uma parte da infraestrutura a ser defendida, no documento que estabelece as estratégias para a defesa do ciberespaço, o "National Strategy to Secure Cyberspace", de 2003, atribuem as responsabilidades ao setor privado e aos próprios indivíduos:

> The purpose of this document is to engage and empower Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact. Securing cyberspace is a difficult strategic challenge that requires coordinated and focused effort from our entire society—the federal government, state and local governments, the private sector, and the American people. (US, 2003)

Ainda assim, a proteção do ciberespaço nos Estados Unidos revela um grande viés militar e o envolvimento das agências de Inteligência nesta questão. Primeiramente, as estratégias de defesa do ciberespaço nos Estados Unidos estão em linha com o "Patriot Act", de 2001, aprovado pelo Congresso após os atentados terroristas de 11 de setembro (Congress of United States of America, 2001). No seguimento do desenvolvimento das políticas de

defesa do ciberespaço, foi criado em 2009 o USCYBERCOM (United States Cyber Command, ou CYBERCOM) que, ligado ao Exército e subordinado ao United States Strategic Command, trata as questões relacionadas à guerra cibernética ou o uso do ciberespaço para fins bélicos. Outras agências, como a NSA (National Security Agency) e divisões da Força Aérea também tem competências para promover a defesa e segurança no ciberespaço.

Há, por outro lado, documentos de política nacional de diferentes Estados que assumem a proteção dos dados, ou proteção da informação como prioridade das políticas de segurança para o ciberespaço. Na Finlândia, por exemplo, entende-se que, por ser essencial à promoção da prosperidade econômica e social, há a necessidade de proteger, principalmente, as infraestruturas de comunicação para assegurar o fluxo de informação. Essa política dá-se principalmente pela coleta de informação e também depende dos utilizadores. A Estratégia finlandesa para a segurança do ciberespaço estabelece princípios-guia para a gestão da cibersegurança dos quais dois merecem destaque:

> 3. Cyber security relies on the information security arrangements of the whole society. Cyber security depends on appropriate and sufficient ICT and telecommunication network security solutions established by every actor operating in the cyber world. Various collaborative arrangements and exercises advance and support their implementation.
>
> 4. The approach for the implementation of cyber security is based on efficient and wide-ranging information-collection, an analysis and gathering system as well as common and shared situation awareness, national and international cooperation in preparedness. This requires the establishment of a Cyber Security Centre as well as the development of 24/7 information security arrangements for the entire society. (Finland, 2013: 5)

Em termos de atores, o governo finlandês aponta que a segurança do ciberespaço é de responsabilidade permanente de vários setores da sociedade, desde indivíduos a organizações governamentais. Neste sentido, as políticas de proteção da informação são operadas não só para divisões criadas para esse fim, como também outros que discutem assuntos de outras esferas. Entre eles, o Committee for Data Security, an Emergency Supply Agency, a Communication Regulatory Authority, and Board of Economic Defense (Choucri, 2014: 147).

Os defensores das políticas de cibersegurança voltadas para o fim da proteção das infraestruturas críticas priorizam os danos para a sociedade, economia, etc., que a paralização de um setor causaria, ainda que por pouco tempo. Por infraestruturas críticas entende-se

> a framework of interdependent networks and systems, generally interlinked at many different levels, including industries, institutions and distribution capabilities that provide a flow of products or services. Some infrastructures are becoming essential, if they are not already, for the organization, the functionality and economic stability of a modern developed country. (Halpin, Trevorrow, Webb, & Wright, 2006: 35)

Esses setores podem ser resumidos em cinco grandes grupos: 1) Informação e comunicação; 2) Energia; 3) Setor Bancário e Financeiro; 4) Logística de distribuição; e 5) Serviços vitais; (Halpin, Trevorrow, Webb, & Wright, 2006: 36). Assim, Clemente (2013), olhando para a dependência das infraestruturas críticas do ciberespaço, argumenta em favor do estabelecimento de políticas multilaterais para a promoção da defesa e controle do ciberespaço já que, segundo o autor, este é o sistema nervoso por onde importantes setores críticos nacionais e globais funcionam e se comunicam.

Apontando para outra direção, Rosenfield (2009) argumenta o que se deve temer no caso das ameaças provenientes do ciberespaço não é o potencial de destruição dessas infraestruturas críticas, mas sim a proteção de dados ou das informações, cruciais para o funcionamento de sistemas ligados à rede, como o setor bancário, comunicações militares, entre outros (Rosenfield, 2009: 78). Essa preferência pela proteção dos dados em detrimento da priorização das infraestruturas críticas vem da constatação de que o controle de sistemas que comandam infraestruturas críticas é de acesso extremamente difícil e, por isso, a hipótese de ataques é pouco provável. Assim, não será este o risco principal que oferecem os ataques em redes virtuais. Não é contra as infraestruturas críticas que se dirigem as principais ameaças do ciberespaço. O potencial em termos de danos provocados por ciberataques está na capacidade de estes interromperem a comunicação, ou a oferta de serviços, usando uma tática denominada DDoS (Denial of Service) que, como já exposto anteriormente (Apps, 2014; Jose Nazario, 2009), consistem em impedir que usuários acessem os serviços disponibilizados através de plataformas virtuais. Ataques a dados (roubo de informações ou a implantação de informações, etc.) são mais prováveis e tem maior potencial para causarem danos que ações contra controle de sistemas de infraestruturas.

Eventuais ataques contra a estrutura de dados ou que impeçam o fluxo de informações podem levar a um efeito em cascata, afetando várias atividades, causando prejuízos financeiros e comerciais. Mais do que isso, segundo o autor, uma vez que a sociedade moderna depende cada vez mais de atividades virtuais, os danos em uma rede de comunicação podem ser potencialmente mais abrangentes. Para além disso, há que se considerar um certo *hype* mediático, uma vez que ataques cibernéticos podem não causar os

danos pretendidos, mas seus efeitos são aparentemente maximizados pela atenção dada pelos meios de comunicação.

Essa percepção sobre o que realmente estaria em risco ao se tratar do ciberespaço é determinante para o tipo de iniciativas ou para quais devem ser elaboradas políticas próprias. Por ora, os documentos oficiais publicados por Estados e Instituições Internacionais tendem a oferecer um caráter generalista para as políticas de segurança do ciberespaço. Tentam agregar as questões de forma equilibrada. A priorização de uma ou outra vertente dependerá das necessidades e percepções de ameaças de cada órgão responsável por tomar decisões neste âmbito.

Para além da percepção obvia de que medidas de segurança são necessárias para o funcionamento do ciberespaço, seja para a proteção de dados ou de infraestruturas, a questão da cooperação internacional é essencial ao nível civil, na Europa, por exemplo, a European Network and Information Security Agency (ENISA), criada em 2004, tem cumprido esse papel.

Segundo a própria agência, a necessidade de cooperação internacional dá-se porque as ameaças ao ciberespaço,

> are global in nature and are constantly proliferating, shifting in focus and intensity and exploiting opportunities presented by technology. Adopting mitigation measures is a way to respond to these evolving threats, but it is often the case that technological means need to be accompanied by cross-border collaboration to be effective. Digital boundaries do not coincide with national frontiers, making international collaboration an essential part of the response mechanism. Furthermore, the propagation and implications of threats such as malware (and botnets in particular) illustrate that they are no longer an issue for people to deal with individually, but are increasingly a social and civic responsibility that affects all sectors of the digital society. (ENISA, 2013)

O exemplo mais visível a nível militar vem da NATO (Aliança Atlântica). A instituição criou e mantém em Tallinn, na Estônia, o Cooperative Cyber Defense Center of Excelence, para estudos sobre a ciberdefesa e suas aplicações legais, entre outros aspectos. Também desenvolveu um manual bastante minucioso sobre as dimensões da cibersegurança. Nele estabelece-se que, o principal objetivo do Centro de excelência é,

> to enhance capability, cooperation and information sharing between NATO, NATO Member States and NATO's partner countries in the area of cyber defence by virtue of research, education and consultation. The Centre has taken a NATO-orientated, interdisciplinary approach to its key activities, including: academic research on selected topics relevant to the cyber domain from legal, policy, strategic, doctrinal and/or technical perspectives; providing education and

> training, organizing conferences, workshops and cyber defense exercises, and offering consultancy upon request. (NATO, 2012)

De maneira geral, os documentos exploram quatro ideias principais. A primeira é o reconhecimento de um ambiente permeado por um número crescente de ameaças relacionadas ao ciberespaço; a segunda é a procedência dessas ameaças e a dificuldade de atribuição de um ataque pela falta de mecanismos de monitoramento eficientes; a terceira ideia é de que a segurança no ciberespaço é uma responsabilidade coletiva: civis, militares, setor público e privado têm de adotar medidas de segurança ainda que não apontem claramente quais seriam as responsabilidades de cada setor; por fim, a quarta ideia é a de que as ameaças podem ter variados objetivos (financeiros, criminosos, roubo de dados, terroristas, etc.) e que por isso afetam a todos.

1.2.4 Ciberguerra, Ciberespionagem, Cibercrime

Uma política de segurança para o ciberespaço tem que saber autonomizar três realidades distintas: ciberguerra, a ciberespeionagem e o cibercrime.

O que se entende por cibercrime não é algo preciso o bastante. Mesmo os documentos oficiais que tratam do tema reconhecem que o cibercrime depende do propósito de quem o utiliza. A definição mais comum é a de que cibercrimes é qualquer atividade ilegal cometida com o uso de computadores ou redes (ITU, 2012), ou como define o *National Crime Prevention Council* britânico,

> Cybercrime is any criminal activity involving computers and networks. It can range from fraud to unsolicited emails (spam). It can include the distant theft of government or corporate secrets through criminal trespass into remote systems around the globe. Cybercrime incorporates anything from downloading illegal music files to stealing millions of dollars from online bank accounts. Cybercrime also includes non-money offenses, such as creating viruses on other computers or posting confidential business information on the Internet. (NCPC, 2012)

A imprecisão acaba colocando sob a mesma categoria práticas muito diversas. Contudo, no intuito de estabelecer parâmetros para a atuação de combate ao crime por meios digitais, realizou-se em 2001 em Budapeste a Convenção sobre o Cibercrime, ou simplesmente Convenção de Budapeste. O encontro produziu um tratado assinado no âmbito do Conselho da Europa. O documento estabelece categorias de infrações, tais como o acesso ilegítimo, interceptação ilegítima, interferência de dados, interferência em sistemas, uso

abusivo de dispositivos, falsidade informática, burla informática, infrações relacionadas à pornografia infantil, infrações relacionadas às violações de direito de autor e direitos conexos. O tratado, em vigor desde 2004 e aberto a adesões, é uma tentativa de harmonizar as leis vigentes no âmbito interno dos signatários às práticas criminosas realizadas por meio virtual[18].

Também o conceito de ciberterrorismo não apresenta uma definição precisa, muito menos consensual. Genericamente, como afirma Bogdanoski (2013), o termo refere-se ao uso das TIs por grupos ou indivíduos como ferramentas para atingir seus objetivos, que pode variar entre a organização de ataques contra infraestruturas, redes, sistemas de telecomunicações, roubar ou trocar informações. É perceptível que o conceito se aproxima muito do que se aponta como cibercrime. O que pode apontar uma diferença entre ciberterrostistas e outros criminosos no ciberespaço são dois pormenores. O primeiro relaciona-se com os custos dos ataques e a possibilidade de executar seus objetivos de uma maneira mais anônima. É preciso considerar que grande parte das organizações terroristas têm fundos limitados e por isso as ações por meio do ciberespaço tornam-se atrativas. Primeiramente por não requerer um grandes quantidades de recursos, depois, por não ser necessário um grande número de pessoas, mas recursos humanos com conhecimento técnico. Ainda neste aspecto, outra vantagem das ações terroristas por meios digitais é a possibilidade da permanência no anonimato ou, ao menos, maior dificuldade para identificar os autores. A questão da permeabilidade das fronteiras também se apresenta como um fator favorável ao terrorista, já que ele pode permanecer a quilômetros de distância do seu alvo. Diferente dos 'terroristas tradicionais' os ciberterroristas não precisam de uma base física.

Outro aspecto do ciberterrorismo que vai para além dos objetivos de financiamento e tem a ver com objetivos políticos, é a necessidade de projetar determinada mensagem para populações-alvo e, por fim, recrutar possíveis seguidores ou apoiadores.

> The terrorist organizations also use the Internet to "reach out" their audience, without need to use other media such as radio, television or holding various press conferences. Web pages are used as a way to highlight injustice and to seek support for as the call "political prisoners" wich are "illegaly captured". Typical Web pages will not display any information related to the violent activities and will usually claim to be left with no other choice but to resort to violence. They claim to be persecuted, that their leaders have been targets of assassination and their supporters were massacred. They use this tactic to give impression that they

[18] A Convenção de Budapeste foi ratificada por outros países para além do Conselho da Europa, tal como Israel, Austrália, Japão, Panamá e encontra-se em discussão em outros, tais como Brasil e Egito. O texto pode ser consultado em: http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf

> are weak and to present themselves as outsiders. This public performance is a very easy way to recruit supporters and members. Besides propaganda, on the terrorist organizations Web sites can often be found content and instructions on how to make explosives and chemical weapons. This allows them to identify the most common users that can have sympathy for their cause and because of that this is an effective method for recruiting. (Bogdanoski, 2013)

Projetar mensagens e ganhar apoiantes para as causas não é algo necessariamente difícil e pode ser feito de maneira relativamente anônima, tal como angariar fundos para tais fins. Embora haja investigações e equipes especializadas em rastrear atividades suspeitas mesmo em lugares mais escondidos do ciberespaço, é relativamente fácil acessar a parte não mapeada da Internet, a chamada Deep Web[19] ou Hiden Web e fazer transações financeiras anônima usando criptomoedas[20], como o BitCoin, LiteCoin, DarkCoin, Dash, BackCoin, DigitalNote, ou qualquer outra similar, chamada *cripto-currencies*.

Organizações Internacionais e Estados têm adotado medidas de prevenção e combate ao ciberterrorismo em diversas frentes. A NATO, por exemplo, desenvolve várias medidas para a proteção contra o terrorismo no ciberespaço através do NATO Cyber Terrorism Program. Envolve, para tanto, várias das subdivisões, como NATO Information Assurance Operations Centre (NIAOC) e NATO Computer Incident Response Capability (NCIRC) tanto para autoproteção, quanto para desenvolver medidas aplicáveis aos estados-membro.

O terceiro conceito essencial é o de ciberespionagem. Para além das ameaças do ciberterrorismo, a espionagem possibilitada pelo ciberespaço também aparece como um problema de segurança do ciberespaço e tem refletido em dificuldades no estabelecimento de acordos de cooperação.

[19] Deep Web é um conceito que se refere, em termos gerais, ao conteúdo informático público não indexado pelas ferramentas de busca como o Google, Yahoo!, entre outros, e por isso necessitam de um software específico para serem acessadas. Segundo revistas especializadas em informática, grande parte do conteúdo da Deep Web é de páginas inacabadas, abandonadas, uma espécie de descarte virtual, no entanto, há uma enorme quantidade de sítios e atividades que requerem ou preferem o anonimato como venda de armas e drogas, contratação de pessoas para cometer crimes, contratação de hackers, entre outros muito graves, recrutamento e arrecadação de fundos para organizações terroristas.Esta parte, especificamente, é chamada de Dark Web. No entanto, o ´submundo´ da Internet – que segundo a Wired, revista especializada, representa 90% de tudo que existe na Internet – não é feito só de criminosos. Há fóruns de discussões que tratam de praticamente todos os assuntos, desde política a inovações científicas, organizações não-governamentais de defesas de minorias, de animais, entre outros. A atuação de ativistas na Deep Web ajudou a popularizar, por exemplo, o Weakleaks.

[20] Criptomoedas, ou moedas virtuais são uma espécie de dinheiro digital desenvolvidos e disponibilizados dentro de comunidades virtuais e, ao invés de terem algum controle de qualquer baco central, as operações são controladas pelos desenvolvedores e pelo mercado criado em torno dessas operações. Um aspecto sempre importante é que as moedas virtuais permitem o anonimato de quem as usa e onde as usa. Há várias moedas virtuais e algumas delas já são utilizadas fora do ambiente virtual. Entre as mais conhecidas, está o BitCoin, que é aceito em várias transações, desde a clínicas veterinárias a hotéis.

Os ataques partindo da China que têm acessado computadores de organismos importantes nos Estados Unidos, como o U.S. Transportation Command, órgão responsável pelo deslocamento de soldados e equipamentos pelo mundo (Paletta, Yadron, & Valentino-Devries, 2015), ou sistemas de medição do tempo e redes de satélites (Flaherty, 2014) ou a presença de hackers russos nos computadores do Departamento de Estado nos Estados Unidos (Perez, 2015) são relevantes de práticas de ciberespionagem que suscitam respostas de segurança.

A espionagem cibernética, principalmente a que envolve suspeitas de participação de Estados tem colaborado com ataques, têm suscitado, ainda que de forma indireta, uma espécie de corrida armamentista para as capacidades bélicas dos Estados no ciberespaço. Alguns autores (Lewis, 2010; Clarke, 2012; Saalbach, 2014; Fernandes, 2014; Singer and Friedman, 2014) afirmam que está em ascensão uma espécie de ciberguerra. O conceito não é consensual e nem mesmo a ideia de que o ciberespaço será um campo de batalha.

Diferente dos que chamam a atenção para a emergência das ameaças do ciberespaço, Rid (2012), levantando definições teóricas sobre a guerra de pensadores clássicos do tema, principalmente Clausewitz, argumenta-se que os ataques com base nas tecnologias ancoradas no ciberespaço, provenientes de governos ou outros atores, não se enquadram nas definições de guerra. Os ataques (espionagem, sabotagem, inserção de códigos maliciosos em aplicações estratégicas), correspondem somente a um dos requisitos, que é a motivação política. Segundo aquele autor, os exemplos de ciberataques não correspondem aos critérios necessários para serem identificados como atos de guerra, apesar de que tais iniciativas podem vir dar suporte a estratégias militares.

Carreiro (2012), compartilha da ideia de que é um exagero dar conotações de atos de guerra a ciberataques. Carreiro critica a ideia de levar os problemas e ameaças ao ciberespaço ao nível de securitização dos conflitos internacionais. Mesmo na incidência de crimes no ciberespaço com consequências físicas no mundo real, ainda que esses crimes ou ataques contem com a cumplicidade de Estados, chamar tais atividades de ciberguerra, parece, para o autor, um exagero. Assim, a presença militar no ciberespaço em nome da defesa dos interesses nacionais é um excesso, incentivado em grande parte pela imprensa não especializada. Segundo Cavelty (2012: 144), estratégias militares identificam os ciberataques como uma modalidade nos conflitos em que somente a força militar não seria suficiente para fazer frente a essas ameaças. E, nesse sentido, torna-se necessário, então, assegurar o domínio da informação através de processos de militarização do ciberespaço.

Ainda neste sentido, recentemente o Comandante da NSA e U.S. Cyber Command, Michael Rogers, afirmou que as regras de um estado de guerra também se aplicam à ciberguerra:

> "[…] anything we do in the cyber arena … must follow the law of conflict. Our response must be proportional, must be in line with the broader set of norms that we've created over time. I don't expect cyber to be any diferente" (Tucker, 2015: online).

Considerando a adaptação de conceitos como a guerra, tradicionalmente ligados a questões militares ou de equilíbrio de poder, às especificações do ciberespaço ou era da informação, nota-se que existe uma preocupação com a crescente capacidade dos países em relação a capacidade de atuar no ciberespaço. Assim, o ciberespaço também surge como uma nova dimensão do poder e das questões de segurança para o século XXI.

Apesar de incidentes cibernéticos envolvendo Estados[21], não há, até o momento um evento que causasse consequências consideradas sérias o suficiente para desencadear reações mais violentas, onde há perda de vidas ou danos a infraestruturas críticas. Ainda assim, há uma grande movimentação em torno da segurança do ciberespaço, principalmente no âmbito militar e estratégico, onde quase todos os países já elaboraram suas respectivas estratégias para o ciberespaço.

Neste sentido, Rid (2012, 2013a), argumenta que uma guerra no ciberespaço não ocorreria necessariamente porque as operações levadas a cabo no ciberespaço não justamente por não produzirem danos suficientemente graves para serem classificados como atos de guerra, isto é, envolvendo violência física concomitante com uma orientação política bem definida. O argumento é baseado na observação empírica constatando que os incidentes envolvendo o ciberespaço não acarretaram em respostas ou retaliações que fossem muito além do limite retórico das vítimas (Rid, 2012b, 2013).

Valeriano & Manness (2015) concordam com o argumento acima. Para eles, há, por ora, especulações sobre as possibilidades de exploração das vulnerabilidades das

[21] É possível apontar alguns exemplos de envolvimento de Estados em ataques cibernéticos. Um dos primeiros casos é o denominado Dossie Farewell, que detalhava como os Estados Unidos responderam a uma tentativa de espionagem industrial por parte da Rússia, ainda no início da década de 1980. Segundo Weiss (1996) e Reed (2005), os americanos adulteraram chips que foram posteriormente entregues aos soviéticos. A utilização destes chips em gasodutos causou uma explosão e um dano econômico relevante à Rússia. Outro episódio envolvendo os dois países ficou conhecido como Moonlight Maze, em 1998 (Healey, 2013). O episódio estava novamente relacionado a tentativas de espionagem pela Rússia contra bases militares norte-americanas. Em 2009, Israel e Estrados Unidos conseguiram infectar com o vírus Stuxnet o sistema de centrífugas de uma central nuclear iraniana, provocando danos e prejuízos (Falliere, Murchu & Chien, 2010; Kelley, 2013, Zetter, 2014).

conexões e da dependência das tecnologias informacionais. Ao mesmo tempo, embora concordem que os incidentes no ciberespaço não evoluiriam para guerras, salientam que há particularidades nos conflitos do ciberespaço que merecem ser estudadas e explicadas em termos teóricos (Valeriano & Mannes, 2015). Os autores sustentam que, em termos estratégicos, o ciberespaço pode vir a somar-se a outras ferramentas do arsenal da diplomacia ou de interação internacional, assim como outras formas de pressão, ameaças e dissuasão, no campo defensivo e ofensivo, em suma, mais um objeto do poder estatal, ao que aparenta, entendido como algo hibrido, entre a diplomacia e o uso da força (Valeriano & Mannes, 2015). Giacomello e Eriksson (2005, 2007) apresentam uma visão semelhante. Segundo os autores, as tecnologias da comunicação permitirão uma espécie de ciberguerra que viria a anteceder antes de ações tradicionais em situação de hostilidade. Semelhante à apreciação de Valeriano e Manness, as tecnologias de informação podem funcionar como mais uma ferramenta no conjunto das estratégias de ataque ou defesa, mas não são capazes, por agora, de caracterizar um campo de hostilidade relativo a um conflito armado (Giacomello, 2005; Giacomello & Eriksson, 2007).

Ventre (2011), por sua vez, aproxima os conceitos de guerra cibernética e armas cibernéticas aos entendimentos aos recursos bélicos contemporâneos (Ventre, 2011: 203-208). Para ele, preocupações com o ciberespaço, quando se tratam de conflitos neste ambiente, elevam-se a um nível maior do que a atuação de hackers ou indivíduos usando tecnologias da informação como armas. Envolvem, mais do que isso: a atuação de Estados com intenções agressivas ou defensivas ainda que não levem necessariamente a uma resposta bélica. Limita-se, não obstante, a a uma espécie de corrida armamentista no ciberespaço

> "We are moving on from the concept of "computer hacking" to cybernetic "attacks" (the term is much more aggressive). We are moving away from risk management to the battle against major threats, from questions on crime to questions on the act of war, from the difficulty of protecting ourselves from cybercriminality to the somewhat impossibility of protecting ourselves against major threats. We are no longer dealing with looking for information domination on the battlefield, with an extreme weakness in the whole system […]. We are finally departing from a discourse on threats, towards one dealing with a global or invisible threat. Foreign intrusions into systems had, of course, been denounced in the past […], but statistics show a high rise in cybernetic attack during the last years of 2000, occasionally lightly mixing statistics on cybercrimes with intelligence operations". (Ventre, 2011: 210)

A ideia de Ventre pressupõe uma diferença teórica entre atos considerados criminosos cometidos no ciberespaço apresentados anteriormente e ofensivas de Estados ou instituições estatais, como agências de inteligência. Karatzogianni (2008) entende a

dinâmica dos conflitos no ciberespaço como provenientes de tensões pré-existentes ou conflitos propriamente ditos em situações reais e, neste sentido, em determinadas situações a condição de hackers são indissociáveis já que na prática o ativismo político no ciberespaço pode ser atrelado às atividades hackers ou estes podem estar ligados a grupos, como a autora exemplifica, étnico-religiosos ou terroristas. Tais exemplos, segundo ela, são elucidativos para demonstrar uma relação de complementaridade entre um ambiente real e virtual (Karatzogianni, 2008: 167). Assim como outros autores, Karatzogianni também enfatiza a condição de ferramenta das tecnologias da informação, uma vez que elas também são aplicadas não só como um facilitador de conflitos, mas também para a resolução dos mesmos[22]. Assim, segundo ela,

> "the term cyberconflict is used to refer to conflicts of the real world spilling over to cyberspace. Typical of cyberattacks is the use by opposing parties of either Information Technology as such or IT as a weapon […] to attack the other side" (Karatzogianni, 2008: 94).

Assim como é particular dos termos que envolvem o ciberespaço, a compreensão dos conflitos no ciberespaço é demasiada flexível. Essa pouca precisão do termo "ciberconflitos" não é necessariamente um problema das investigações realizadas ou de pouca atenção ao tema, mas sim da sua abrangência que é característica do campo do ciberespaço. Aparentemente, esse caráter genérico deve-se a duas razões ligadas às características do próprio ciberespaço. Sendo as tecnologias da informação ferramentas disponíveis e aplicadas a diversos setores o estabelecimento de limites claros sobre suas capacidades parece ser não só difícil, como também não produtivo quando o objetivo é produzir conhecimento de realidades diferentes. Esta primeira impressão leva à segunda razão, sendo esta a necessidade de explorar diferentes casos envolvendo diferentes atores em interação que também é particular do campo.

Na intenção de determinar o que se entende por ciberconflitos neste trabalho, dois aspectos devem ser ressaltados para além das definições já exploradas. A primeira parte dos meios utilizados e, neste aspecto Karatzogianni, (2009) é muito precisa:

> Typical of cyberattacks is the use by opposing parties of either Information Technology as such or IT as a weapon – for example, worms, Distributed Denial

[22] A bibliografia associada à utilização das tecnologias da informação na resolução de conflitos geralmente centra-se em cenários prospectivos e previsões como em Schmidt & Cohen (2013), na prevenção de conflitos Mancini (2013) e na utilização de ferramentas participativas para mapemaneto de conflitos e focos de violência.

> of Service attacks (DDoS), Domain Name Service attacks (DNS) or unauthorized intrusions – to attack the other side. (Karatzogianni, 2009)

Em paralelo, sem prejuízo dos limites conceituais apresentados a noção explorada por Valeriano & Mannes (2015), também pode se aplicar ao propósito deste trabalho. Assim, os conflitos no ciberespaço se referem ao

> use of computational technologies, defined as the use of microprocessors and other associated technologies, in cyberspace for malevolent and/or destructive purposes in order to impact, change, or modify diplomatic and military interactions between entities. Unpacking this definition more, cyber conflict must occur in cyberspace through the use of computational technologies. (…) What must be clear is that cyber conflict remains in the realm of conflict, which is a disagreement on preferred outcomes. (Valeriano & Mannes, 2015: 32)

Importante ressaltar que os atores envolvidos nos conflitos no ciberespaço não se limitam necessariamente ao âmbito estatal. Pelo contrário, a própria natureza do ciberespaço faz com que essa divisão entre os níveis estatais e não-estatais não sejam claramente delimitadas. Mais do que isso, o Estado, como explica Harris (2014), frequentemente recorre a entidades privadas ou a especialistas para tratar de questões de segurança no ciberespaço.

Dadas as condições e dimensões do ciberespaço enquanto ambiente ou plataforma de interação de múltiplos atores, os Estados têm voltado as atenções a esse espaço visto que o potencial de conflitos que emanam do ciberespaço deve ser considerado nas equações das políticas de segurança, entre outras. Essa preocupação fica bastante evidente a partir da década de 2000, quando vários países começaram a estabelecer o ciberespaço e a segurança cibernética como uma de suas prioridades. Essa concepção relaciona-se com o reconhecimento de uma nova dimensão da segurança nacional e dos limites da soberania.

Como Lin (2013) percebe que, existe uma espécie de campo de batalha no ciberespaço onde os conflitos e a exploração são vistos como uma ameaça permanente aos Estados. Mais do que isso, quando se verifica a dinâmica própria do ciberespaço, a dinâmica dos conflitos tem de ser vista para além dos níveis estatais, como lembra Srikanth (2014: 66),

> "there are no clear lines between the civilian and military, as civilian computer systems may be used to launch offensive cyber-war against an "enemy" state". (Srikanth, 2014: 66).

A autora ainda sustenta que, diferente das situações tradicionais onde a dissuasão pode funcionar, sendo esta preferível em detrimento dos meios ofensivos e defensivos,

quando se trata de conflitos no ciberespaço a tendência é ter um sistema de defesa em funcionamento constante, principalmente porque neste campo em específico a identificação dos agressores e a atribuição de responsabilidades não são necessariamente claras:

> "the difficulty is determining the perpetrator (which could be state or non-state actors) adds to the confusion in determining the legal course of action once a cyber-attack is discovered" (Srikanth, 2014: 66).

Neste sentido, é natural é natural que surjam iniciativas com vistas a ações estatais no âmbito da segurança. A tendência de incorporação de uma dimensão cibernética nos conflitos e nos assuntos militares é perceptível em alguns exemplos. Como nos embates militares internacionais durante a crise da Geórgia e Rússia, em 2008 (Arquilla, 2013; Healey, 2013; Mazanec, 2015) e novamente em 2014 na crise russo-ucraniana (Zetter, 2016). Também os Estados Unidos, tal como discorre Harris (2014: 12-20), combinaram estratégias militares com tecnologia da informação no Iraque. Através de programas que monitoravam redes sociais e sites de propaganda da Al-Qaeda e outros dispositivos que conseguiam monitorar a comunicação de líderes de grupos insurgentes através das redes de telemóveis, criou-se, como aponta o autor, uma espécie de "*cyberwarriors*", juntando a força com a inteligência em um campo de batalha. Da mesma forma, a Rússia, dados os exemplos de atuação em conflitos que lhe têm sido atribuídos (Karatzogianni, 2010), tem empregado formas diferentes das tradicionais, o que vem sendo chamado de "hybrid warfare*"*. Este termo, apesar de carecer de melhores definições e estudos, refere-se ao emprego de ataques cibernéticos juntamente com ataques físicos. Segundo um relatório do Netherlands Institute of International Relations, analisando a postura russa em conflitos recentes em que a componente cibernética está presente,

> The term [hybrid warfare] is confusing as Moscow itself is not conducting war in a classical sense but applying a wide set of confrontational instruments. It would be more appropriate to use the term hybrid threat or hybrid intervention, which consists of a mix of non-military and military elements, applying both 'soft power' and 'hard power'. (Drent, Hendriks, & Zandee, 2015)

Assim, as TIs têm adicionado um elemento complementar aos conflitos e métodos tradicionais. Naturalmente, ao avaliar as possibilidades de conflito, as potencialidades de eventuais oponentes, os Estados têm de levar em conta essa capacidade cibernética dos seus pares. Mais do que isso, a princípio, essas capacidades não se restringem a entidades estatais ou organizações internacionais relevantes.

Ao analisar as diferentes tipologias de conflitos no ciberespaço, tanto envolvendo atores estatais quanto indivíduos ou determinados grupos, Chroucri percebe que

> "each type reflects diferente values, leading to diferente forms of policization of players and positions. Each represents, implicity of explicity, different principles and political values as well as visions of preferred futures" (Choucri, 2012: 127).

A preocupação de Estados e decisores com a emergência de ameaças provenientes do ciberespaço tem suscitado, segundo alguns autores e veículos de comunicação, uma espécie de corrida armamentista no ciberespaço (Craig & Valeriano, 2016a, 2016b; Paletta et al., 2015; Riley & Vance, 2011).

> Many countries appear to be seeking to enhance their cyber warfare capabilities by establishing cyber command units and hiring teams of professional hackers, and these actions may be symptomatic of what is increasingly being referred to as the "cyber" arms race. (Craig & Valeriano, 2016: 22)

Naturalmente, as perceções de ameaças levam os Estados a adotarem estratégias que sirvam de proteção, incrementando, então, seus respetivos aparatos de defesa. Quando se trata do ciberespaço e das tecnologias da informação essas medidas tendem a ser relacionadas a uma espécie de higiene cibernética como, por exemplo, recomenda o Serviço Secreto Norte Americano (U.S. Department of Homeland Security, 2016). Contudo, uma corrida armamentista no campo da segurança cibernética afasta-se do caráter defensivo e de práticas de segurança e se aproxima de um âmbito de práticas ofensivas (Craig, 2015; J. A. Lewis, 2013).

Neste cenário, o desenvolvimento de armas para o ciberespaço passa por dois campos que se complementam. Primeiramente, há uma militarização do ciberespaço que é visto como mais um domínio militar, juntamente com ar, mar, território e espaço. Neste sentido, de acordo com Deibert (2011), o exemplo mais visível destes movimentos é a criação do *Cyber Command* (USCCYBERCOM) nos Estados Unidos. Não obstante, essa construção de uma força cibernética capaz de organizar operações ofensivas vai para além do investimento direto em conhecimento e presença militar no ciberespaço, passa também pela contratação de mão de obra altamente especializada (Craig, 2015). Análises das políticas de diferentes países corroboram o entendimento de que os investimentos em segurança cibernética, inclusive no que se refere a atividades mais ofensivas, são direcionadas pela perceção das ameaças. Apesar das desconfianças, países têm demonstrado, ao menos do ponto de vista formal, em cooperar para estabelecer regras que evitem esse tipo

de comportamento, estabeleçam mecanismos de confiança e governança para o ciberespaço (Fleck, 2013; Yannakogeorgos & Lowther, 2013).

Operações cibernéticas ou situações de conflitos no ciberespaço perpetradas por Estados também denotam uma espécie de "continuação da diplomacia por outros meios". Apesar dos exemplos de conflitos envolvendo o ciberespaço e todas as precauções tomadas, Estados não estão, em geral, dispostos a entrar em um conflito cibernético (Rid, 2013), contudo, adotam ou fomentam práticas consideradas ofensivas no ciberespaço como uma ferramenta diplomática, de modo a tratar de assuntos que não poderiam ser tratados na diplomacia tradicional, ou que, por outros modos, trariam riscos e custos que o Estado não estaria disposto a bancar (Valeriano & Mannes, 2015). Assim, os conflitos envolvendo o ciberespaço, ao menos por hora, têm sido mantidos no âmbito da baixa política, inclusive porque as respostas a agressões no ciberespaço não têm sido levadas a uma escala militar ou mais agressiva.

Essa proximidade de hostilidades digitais com a política diplomática de alguns países acaba por revelar um perfil regionalista dos conflitos no ciberespaço. Ao buscar um padrão para os ciberconflitos, Valeriano e Mannes percebem que as dinâmicas regionais ou contexto de rivalidades, com suas contradições diplomáticas, exercem uma grande influência sobre a incidência de ciberconflitos ou de operações ofensivas no ciberespaço (Craig & Valeriano, 2016a; Valeriano & Mannes, 2015):

> "Most rival interactions in cyberspace will have a regional context connected to the issue of territorial considerations or disputes since most rivalries start due to territorial concerns" (Valeriano & Mannes, 2015: 66).

Essa concepção, explica o frequente envolvimento de países como Rússia e China que contabilizam um número razoável de ataques cibernéticos iniciados contra vizinhos (China – Japão; China – Índia; China – Coreia do Sul; Rússia – Estônia; Rússia – Geórgia; Rússia – Ucrânia) ou antagonistas no cenário internacional (Rússia – EUA; EUA – Irão; Israel – Irão, entre outros).

Essas dinâmicas apresentam dois aspectos. O primeiro deles refere-se à facilidade e aos riscos. Ações ofensivas, desde a negação de serviços, a propaganda política, a atos de espionagem perpetrados através das tecnologias da informação oferecem um risco relativamente pequeno ao agressor, justamente por causa de uma das grandes dificuldades

impostas pelos ataques no ciberespaço que é o problema da atribuição de responsabilidades. A atribuição da responsabilidade por um ataque cibernético é algo difícil de ser realizado efetivamente, de forma incontestável. Em segundo lugar, ainda que não cause grandes danos, ataques cibernéticos provocam um efeito psicológico negativo nos usuários. Isso é especialmente problemático quando o ciberespaço e as tecnologias de informação são parte relevante para o funcionamento de serviços essenciais, como bancos e controle de infraestruturas críticas que, baseiam-se em uma relação de confiança nos sistemas informáticos. Os ataques cibernéticos causam uma desconfiança dos usuários em relação aos administradores de sistemas informáticos e das políticas de defesa e de segurança de determinado alvo. Esse receio vem a ser bastante frutífero para processos de securitização no ciberespaço.

Para além da questão básica da segurança, da quebra de confiança, o próprio papel dos Estados contribui para um movimento de securitização, uma vez que há uma participação, ou ao menos uma coparticipação de atores estatais em todos os temas acima citados até este ponto. Além disso, somente a presença do Estado em uma contenda cibernética e capaz de classificá-la como ciberconflito, naturalmente, somadas a outras características. Assim, um conflito no ciberespaço pode vir de um movimento de securitização e estar bastante próximo com o contexto regional e social característico de um determinado Estado.

Há, naturalmente, assim como em outros setores, uma competição entre os atores de diversos níveis acerca de aprimoramentos e desenvolvimento de melhores capacidades e eficiência nas ferramentas de comunicação. Isso fica bastante evidente no ciberespaço, principalmente quando este torna-se um elemento de desconfiança e um espaço frutífero para o fomento de uma ´corrida para ter o melhor arsenal cibernético´.

Deste modo, o ciberespaço, a Internet e as redes de conexões talvez sejam a criação humana mais presente entre os diversos setores sociais e que mais envolva soluções para as necessidades sociais em um espaço especial que guarda semelhanças com o que existe no mundo real, mas que tem as vantagens e limitações de uma comunidade virtual. Das facilidades às dificuldades, das desconfianças às liberdades, o ciberespaço e a Internet tornaram-se o elemento que os permeia.

1.2.5 Cibersegurança e Ciberdefesa

As discussões sobre a questão de segurança no ciberespaço têm sido traduzidas em políticas implementadas em diferentes níveis de análise. Desde as questões de segurança interna, como a questão de crimes cibernéticos, até à intenção da construção de uma rede de governança internacional baseada em uma estrutura multissetorial, as propostas de densificação de estratégias de ação protetiva no ciberespaço apresentou intensidades variadas.

Neste sentido, faz-se necessário delimitar fronteiras entre os conceitos de cibersegurança e defesa cibernética, ou ciberdefesa, outra política de responsabilidade principal do Estado e das instituições militares.

Essa distinção é importante para delimitar não só o que se entende por uma e por outra, já que se sobrepõem em atividades, e meios de ação. Embora correlatas e por vezes sobrepostas, cibersegurança e ciberdefesa não tem necessariamente as mesmas intenções, objetivos e aspectos estratégicos.

Silva (2016) define a defesa cibernética como um conjunto de práticas desenvolvidas sob a égide militar, parte de uma estratégia que abrange a segurança das estruturas e capacidades cibernéticas através de meios militares e com objetivos estratégicos definidos. Sob as políticas de defesa cibernética estariam, por exemplo, o aprimoramento das capacidades de um Estado em termos de resiliência, no aprimoramento técnico e material para fazer frente as ameaças cibernéticas e eventualmente se posicionar à frente de seus pares. Avulta, pois, no conceito de ciberdefesa um componente estratégico com o objetivo de assegurar o uso dos recursos cibernéticos de segurança da maneira mais efetiva possível em proveito nacional. Daí o foco em elementos como as infraestruturas críticas, a criação e aprimoramento de capacidades estratégicas no campo cibernético, como o a criação e fortalecimento da capacidade de resiliência frente a ataques e ameaças.

Mais do que a pura capacidade de resiliência frente a ataques, Galinec, Možnik & Guberina (2017) lembram que o Departamento de Defesa dos Estados Unidos incorporou entre as estratégias de defesa cibernética o conceito de Defesa Cibernética Ativa, que busca desenvolver uma capacidade sincronizada tratando de instrumentos para reconhecer, detectar, analisar e mitigar ameaças e vulnerabilidades. E referem três subcategorias a serem consideradas. Primeiramente, há uma referência à proatividade, capaz de manter uma alta eficiência à medida em que fortalece a defesa no ciberespaço. Depois, uma dimensão ativa

com a intenção de limitar eventuais danos causados por alguma atividade hostil. Por fim, uma capacidade reativa, com o intuito de reconstruir e restabelecer a eficiência dos sistemas depois de um eventual ataque cibernético bem-sucedido. Esses três aspectos atuam como um processo contínuo integrado às outras ferramentas de segurança cibernética.

Na última ratificação da Estratégia de Cibersegurança dos Estados Unidos, em 2018, o Departamento de Defesa americano apresentou um entendimento bastante claro da necessidade de implementar as questões de defesa nacional no ciberespaço e resumiu sua atuação em missões específicas: a defesa do próprio sistema, redes e informações, a defesa dos interesses nacionais contra ciberataques, o apoio operações militares e planos de contingência (USA, 2018). Nota-se, portanto, que o Departamento de Defesa tem um papel ativo na questão cibernética, já que as práticas e a própria missão denotam um escopo maior do que a mera reação a possíveis ameaças ou a implementação e sofisticação dos mecanismos de resiliência.

Naturalmente, o entendimento sobre a relevância da defesa cibernética também está é replicada no âmbito da NATO. Contudo, a visão da NATO da defesa cibernética é bastante menos proativa e, como é próprio de uma organização de segurança coletiva, há um reforço nas ideias de cooperação entre aliados:

> Allies recognised cyberspace as an operational domain, joining land, air and sea. This will enable the Alliance to better protect its networks, missions and operations, with more focus on cyber training and planning. NATO's cyber posture remains defensive, but this is a clear sign that the Alliance is strengthening its collective defence in all areas. Allies also pledged to strengthen their own cyber defences and share more information and best practices as a matter of priority. (NATO, 2017: online).

O conceito de defesa cibernética, assim como as próprias práticas e definições de cibersegurança, variam conforme os limites e interesses de quem os define para si. Mais do que isso, na prática, não há uma linha específica que delimite a fronteira entre defesa cibernética e segurança cibernética, já que, muitas vezes a defesa dos sistemas de informações e redes vale-se de métodos próprios de cibersegurança. Contudo, para o presente trabalho a necessidade de delimitar esses conceitos se impõe, já que é necessário delimitar os níveis de análise e atores. Toma-se, então, emprestada a delimitação apresentada por Viegas et al. (2018: 47):

> "ciberdefesa" [ou defesa cibernética] para referir questões de segurança no contexto da utilização de meios eletrónicos que envolvam a segurança do próprio Estado – abrangendo a segurança das várias dimensões que o compõem: povo, território e poder político –, reservando-se a expressão "cibersegurança" para

> todas as demais questões de segurança no contexto da utilização de meios eletrônicos. (Viegas et al., 2018).

É importante reconhecer que a diferenciação dos conceitos de defesa cibernética e segurança cibernética é uma discussão em andamento. Para os efeitos específicos, entendemos que o aprofundamento dessa discussão não traria maiores benefícios para o tema central da nossa investigação, privando a discussão da profundidade com a qual necessita ser tratada. Por isso, o entendimento acima exposto parece-nos ser suficiente, já que permite separar de maneira objetiva o escopo da ciberdefesa e cibersegurança.

CAPÍTULO 2. Teorias da Securitização e Dessecuritização e a questão do ciberespaço

O objetivo deste capítulo é abordar as teorias que tratam da securitização e dessecuritização e aplicá-las na interpretação do ciberespaço enquanto objeto de referência da securitização.

O argumento central deste capítulo é de que a securitização do ciberespaço tem diversos focos. Por ter uma natureza permeável e extremamente fluída, a securitização do ciberespaço não tem como objetivo o elemento todo, mas sim aspectos específicos que passam a ser tratados por agentes especializados tecnicamente. A partir destes elementos, como eixos de segurança, o acesso de agências de segurança governamentais, entre outros atores, atingem setores comuns aos usuários sem que haja uma discussão política sobre os limites desses agentes. Esses processos partem de um discurso baseado em ameaças e apontam para técnicos, geralmente ligados a instituições de inteligência e/ou militares, como os únicos responsáveis pelas decisões de segurança no ciberespaço. Este contexto permite interpretar a teoria da securitização de uma forma mais completa e sofisticada. Também no que se refere à dessecuritização, a análise de medidas que regulamentam a Internet, bem como os papeis, funções e responsabilidades dos atores que convivem nesse espaço, podem ser fonte de um aprofundamento no conhecimento desses movimentos e, igualmente, sofisticar a teorização neste aspecto.

2.1 Das visões tradicionalistas às Teorias da Securitização: diferentes visões sobre a segurança internacional

É amplamente aceite que o que se entende por segurança, tanto para as questões domésticas, mas principalmente em nível internacional passou por uma modificação significativa. Apesar de não ter um início específico que se possa datar, as ampliações da agenda internacional para a segurança são mais visíveis a partir do final da Guerra Fria. Da década de 1990 em diante, com a ascensão e consolidação de uma nova ordem mundial, muito mais próxima e adepta do multilateralismo e que dava maior peso ao papel das instituições internacionais, a segurança internacional passou a ser um assunto coletivo, ou o que Nasu (2011) chama de sistema coletivo de segurança.

Segundo o citado autor, as leis prevalecentes na prática e na promoção da segurança internacional têm se fundamentado no Artigo 2(4) da Carta das Nações Unidas (United Nations, 1945: 6) que diz que "Todos os Membros deverão evitar em suas relações internacionais a ameaça ou o uso da força contra a integridade territorial ou a independência política de qualquer Estado, ou qualquer outra ação incompatível com os propósitos das Nações Unidas" e na atuação do Conselho de Segurança, naturalmente, o órgão com mais importância.

A institucionalização da segurança coletiva dependeu, no entanto, não só do objetivo central, que é dar respostas às necessidades de segurança em um mundo cada vez mais integrado, mas principalmente da necessidade de atender a uma conjuntura que se ajustasse aos interesses soberanos das principais potências da política internacional e até então continua a servir à manutenção do *status quo* da política internacional. Deste modo, a emergência da segurança coletiva não pode ser vista dissociada de uma vontade soberana dos países. Como resume Nasu (2011: 15) "Collective security provides institutionalized procedures for legalizing collective response, designed at least originally to address traditional, military-oriented threats to the maintenance of international peace and security".

Observa-se, no entanto, que a soberania estatal, bem como as medidas ou políticas nela centradas tem enfrentado diversos desafios derivados de situações ou elementos que, entre outras coisas, são capazes de permear os limites estatais, tanto no âmbito jurídico, quanto em termos mais tradicionais como questões territoriais (Baylis, Smith, & Owens, 2016). Esse fenômeno, observado com maior nitidez no período pós-Guerra Fria, tem como enquadramento contextual o crescimento ou a emergência de atores não-estatais, como grandes corporações, grupos terroristas, questões referentes ao meio ambiente e à exploração de recursos limitados e, mais recentemente, maior e mais fluida comunicação e troca de informação entre grupos com os mais variados objetivos, uma opinião pública mais consciente e mais especializada[23], para os quais antigos arranjos internacionais forjados a partir da soberania estatal para tratar de problemas coletivos, não tem conseguido formular respostas eficientes. Essa nova dinâmica tem, então, colocado alguma pressão sobre os

[23] Por opinião pública mais especializada entende-se o sentido que Rosenau (2006) emprega. Indivíduos, de uma forma geral, tem sido capazes de entender e lidar com problemas ou assuntos que antes eram tratados somente por conhecedores exclusivos ou especialistas. O acesso à informação e a facilidade de comunicação tem permitido às pessoas tornarem-se de certo modo mais cientes de determinados ou em vários assuntos, inclusive em temas exclusivos a autoridades estatais e suas respectivas condutas e decisões.

entendimentos e meios tradicionais para tratar da segurança fazendo repensar os conceitos e um ajuste institucional de modo a acompanhar as novas necessidades (Nasu, 2011: 15-17).

A visão tradicionalista da segurança internacional, ligada a um entendimento de base realista enquanto enquadramento teórico hegemônico nas Relações Internacionais, e atribui um peso essencial dos objetivos militares e à identificação de ameaças a este setor ou a objetos de referência sob a proteção essencialmente militar, como a soberania estatal, o território, a segurança do regime político e do sistema de governo. Assim, a segurança é tradicionalmente entendida como a ausência de ameaças militares e, deste modo, seu estudo limitava-se, como aponta Walt (1991), à identificação das ameaças e do uso da força e controle militar. Essa noção tradicional entrou em crise após o fim da Guerra Fria (Villa, 1999). St. Jean (2007) afirma que a visão tradicional da segurança limitou-se demasiado ao centrar-se no papel do Estado e aponta quatro principais dificuldades desse entendimento.

A primeira das dificuldades é que os limites tradicionais focam no Estado enquanto unidade de análise e não oferece um enquadramento amplo o suficiente para abranger a análise de ameaças dos Estados a seus próprios cidadãos. Essa preocupação com o indivíduo é o começo de uma discussão que virá a assumir a segurança humana como um dos objetivos estatais ou de entidades responsáveis pela manutenção da segurança não só a nível internacional como em instâncias domésticas. Este ponto também chama a atenção para o que o St. Jean (2007: 5) classifica como a segunda dificuldade da visão tradicional que é o foco limitado às ameaças externas. Sendo o Estado a única unidade de análise, as ameaças à sua existência ou integridade poderiam vir somente de outra entidade similar ou unidade política, como prefere (Waltz, 1978). Assim, ignoram ou descartam as ameaças à segurança provenientes de fatores domésticos, como repressão política, conflitos civis, entre outros.

A terceira insuficiência da visão tradicional diz respeito à falta de foco nas ameaças de longo prazo ou potenciais. Estão em causa questões que se afastam das questões militares e envolvem outras instâncias sociais, como questões sanitárias, ambientais, aspectos que envolvem segurança societal, etc. A importância de dar a atenção a ameaças que parecem pouco prováveis ou distantes temporalmente articula-se ainda com a ascensão da segurança humana (Floyd, 2007).

Por fim, o quarto problema da visão tradicional é o foco na maximização das capacidades militares unilaterais como solução para ameaças à segurança. Essa centragem exprime um elemento central das Teorias Realistas: a desconfiança própria da natureza anárquica do Sistema Internacional que, por sua vez, não permite que os atores saibam ou

estejam certos das intenções de seus similares seguindo as teses do dilema de segurança, os Estados, neste contexto, são obrigados, então, a preparar-se para eventuais defesas ou construir meios de dissuasão. Deste modo, os acordos de cooperação feitos no âmbito da segurança constituem-se sempre em oposição a um suposto inimigo comum. Essa visão traduzia o contexto político da Guerra Fria. Com a dissipação das tensões ao fim da Guerra Fria e seguido de uma institucionalização da segurança, essa visão perdeu força enquanto aspecto teórico de análise das relações internacionais (St. Jean, 2007: 2-5).

Ao dar-se conta das insuficiências das teorias tradicionais para a compreensão do sistema internacional emergente, marcado por uma variedade de atores e pela complexidade de suas relações, diversos autores adotaram perspectivas alternativas para a análise da segurança. Villa (1999) propõe uma abordagem que entende que as análises de segurança pensada a nível global e multidimensional. Essa nova percepção da segurança, ao invés de limitar, agrega temas e novas preocupações à agenda de segurança, no entanto, como aponta Baldwin (1997), não significa, necessariamente, que o conceito de segurança tenha sofrido mudança substantiva.

A nova interpretação da segurança veio justificar um debate que já vinham sendo delineado antes da década de 1990. Opõe-se duas visões identificadas, segundo Sulovic, (2010: 5) como "*traditionalists*" e "*wideners*". Assim como todas as proposições teóricas que enxergam a segurança como algo que vai para além das questões militares, sendo muito mais discutida politicamente e afetando diversos setores, é no campo dos 'widerners' que se inserem as teorias da securitização e dessecuritização.

Barry Buzan e Ole Weaver, na principal obra que traduz o que denominam securitização - *Security, a New Framework to Analysis* - desafiam o conceito tradicional de segurança em dois sentidos principais. Primeiramente, vendo de uma maneira mais horizontal, argumentam justamente em favor de uma ampliação de conceitos de segurança propondo um compromisso multidimensional ou multisetorial da segurança. Assim como é amplamente aceite que os temas de segurança deixaram de ser tratados essencialmente por atores tradicionais ligados às questões militares (Baldwin, 1997), há também um entendimento de que a abordagem da segurança em temas divididos por setores reflete uma crise do pensamento realista (Villa, 1999). Assim, as práticas envolvidas na segurança ultrapassam o limite essencialmente militar. Este setor, então, vem a somar-se a outros: político, econômico, societal e ambiental.

Para além da ampliação dos temas ou focos de estudo, em termos metodológicos, essa compreensão multisetorial da segurança admite abordar a segurança em diferentes padrões, permitindo traçar comportamentos diversos ao mesmo tempo que não se desliga de uma visão geral da segurança como explicam Buzan et al. (1998: 8-9):

> The use of sectors confines the scope of inquiry to more manageable proportions by reducing the number of variables in play. Thus, the economists looks at human systems in terms that highlights wealth and development and justify restrictive assumptions, such as the motivation of behavior by the desire to maximize utility. The political realist looks at the same system in terms that highlights sovereignty and power and justify restrictive assumptions, such as the motivations of behavior by the desire to maximize power. The military strategist looks at the systems in terms that highlight offensive and defensive capability and justify restrictive assumptions, such as the motivation of behavior by opportunistic calculations of coercive advantage. The environmentalist looks at the systems in terms of the ecological underpinnings of civilization and the need to achieve sustainable development. In the societal, the analyst looks at the systems in terms of patterns of identity and the desire to maintain cultural interdependence. Each is looking at the whole but is seeing only one dimension of its reality. (Buzan et al., 1998: 8)

Esta abordagem multissetorial da segurança é uma das dimensões dos estudos de segurança que distingue a Escola de Copenhagen. Albert & Buzan (2011) retomam esse aspecto e apontam que a divisão dos estudos da segurança em setores, conjugada com a diversidade possível de objetos de referência, implica a possibilidade do surgimento de outros setores, sem que haja necessariamente um limite conceitual. Um eventual estabelecimento de um novo setor da segurança dependeria, então, da eficiência dos discursos dos agentes da securitização ao apontarem um objeto de referência e convencerem uma determinada audiência sobre a urgência em se efetivar medidas para fazer frente às ameaças a este objeto. Também não se impõe limites ou critérios para especificar os setores para além dos que se estabeleceram através dos discursos. Os que foram sugeridos pela Escola de Copenhague são produtos de observações empíricas, mas o elenco é aberto.

Deste modo, juntando as duas dimensões cujas dinâmicas acompanham sua contextualização, entende-se que os temas referentes à segurança são socialmente construídos, a partir de um discurso voltado para determinada audiência que o interpreta como digno de mobilização de entidades competentes para fazer frente a ameaças a um valor ou elemento que é caro à mesma. Os objetos da segurança não são independentes, pelo contrário, sua existência depende de uma construção social subjetiva. Em resumo, temas de segurança são aqueles que alguém assim classifica como tal e encontram uma audiência que desta maneira o entende.

Este é precisamente o ponto de partida das teorias da securitização. Essa nova interpretação argumenta que a segurança não se refere à ausência de ameaças, mas sim à sobrevivência: "security is about survival" (Buzan et al., 1998: 21). A classificação de um determinado tema como objeto de segurança, ou seja, que precisa ter sua sobrevivência assegurada, implica uma atenção especial a este assim como a tomada de medidas extraordinárias para tratar das ameaças.

A natureza especial que carrega o termo segurança e a evocação deste tema envolvendo um objeto de referência acaba por justificar ou legitimar, como constatam Buzan et al., (1998: 21), o uso da força ou a mobilização das forças do Estado (em termos gerais, mas nem sempre, sendo aberto a outras entidades ou instituições tanto a nível interno quanto internacional), ou servir como justificativa para a adoção de comportamentos não previstos pela conduta normal dentro das regras socialmente estabelecidas: "Tradicionalmente, ao mencionar 'segurança' um representante do estado declara uma condição emergencial, requisitando, então, o direito de usar quaisquer meios necessários para bloquear ameaças" (Buzan et al., 1998: 21).

Neste sentido, colocar um tema sob a alçada da segurança acaba por tirá-lo do âmbito da normalidade político e colocá-lo, necessariamente, em uma instância especial, apartada das regras comuns. Como consequência, são tomadas as medidas de emergência ou de exceção que se entendem necessárias para tratar das ameaças a estes objetos. Assim como o termo segurança, esse movimento ou processo é uma das chaves para o entendimento da proposta das teorias da securitização.

Em um entendimento mais generalizado sobre a segurança proposto pela Escola de Copenhagen há, primeiramente, uma politização da questão. Inicia-se um processo que leva um assunto geralmente não discutido publicamente, ou ao menos com uma visível ênfase, a uma situação altamente comentada, tornando-se alvo de discussões e de políticas públicas e por isso logo passam a requerer algum tipo de decisão ou posição governamental. Através dessa politização, na qual determinada situação ou objeto de referência é apresentado como algo ameaçado, leva-se a questão ao âmbito da securitização. Através dessa politização de uma ameaça a um objeto de referência, passa-se a requerer medidas de emergência. Os discursos que embasam essa politização, por sua vez, passam a ser elementos de justificação para ações fora do regime normal dos procedimentos políticos.

Em resumo, um processo de securitização tem três fases como representado na seguinte sequência:

Não-politização → Politização → Securitização

De maneira mais específica, um processo de securitização exitoso apresenta elementos que variam de acordo com as especificidades de cada tema, de cada contexto, de cada audiência, dos elementos discursivos, entre outros. Como apresentam Buzan et al., (1998: 25) "a definição e critérios exatos de securitização são constituídos pelo estabelecimento subjetivo de uma ameaça existência relevantes o suficiente para ter efeitos políticos substanciais". Essas questões foram aprofundadas posteriormente por Williams (2003), Balzacq (2005, 2011), Albert & Buzan (2011), Weaver (2012), além de outros autores que aplicaram a teoria a casos específicos, a serem abordados posteriormente em uma revisão bibliográfica.

Uma sistematização eficiente da teoria da securitização que articula tanto os pressupostos originários da Escola de Copenhague como os aprimoramentos da chamada Escola de Paris encontram-se na forma como Balzacq define a securitização:

> an articulated assemblage of practices whereby heuristic artefacts (metaphors, policy tools, image, repertoires, analogies, stereotypes, emotions, etc.) are contextually mobilized by a securitizing actor, who works to prompt an audience to build a coherent network of implications (feelings, sensations, thoughts, and institutions), about the critical vulnerability of a referent object, that concurs with the securitizing actor´s reasons for choices and actions, by investing the referent subject with such an aura of unprecedent threatening complexion that a customized policy must be undertaken immediately to block its development (Balzacq, 2011: 3).

A securitização, tal como originalmente proposta, apresenta um padrão de elementos a serem compreendidos e delimitados em um processo de securitização. Enquanto processo, há quatro componentes que envolvem a securitização: "o ator da securitização (securitizing actor), o objeto de referência, (referente object), a audiência e o ator funcional (functional actor). O processo todo é iniciado pelo que os autores chamam de movimento de securitização (securitizing move). Os próximos tópicos abordam esses elementos e, à medida em que se aborda a teoria, apresenta-se um estado da arte referente a cada elemento. O objetivo principal é delimitar o quadro teórico usando como estrutura os próprios elementos propostos pela teoria da securitização. À medida em que se abordam os elementos teóricos, abordam-se estudos específicos onde tais aspectos foram abordados em uma revisão da

literatura tanto em casos gerais, como no que se aproxima da securitização do ciberespaço, tema central deste trabalho.

2.2 O movimento de securitização

Segundo a proposta da Escola de Copenhagen, os processos de securitização iniciam-se a partir de um movimento de securitização. Inicia-se sempre a partir de um discurso que identifica uma ameaça existencial a um segundo elemento. A existência desse elemento tem de ser entendida por uma audiência como sendo algo essencial a si ou para a configuração normal do respectivo contexto no qual se situa audiência.

Neste início do processo há dois aspectos que merecem destaque por sua função. O primeiro é o ato discursivo que usa uma linguagem e uma gramática própria com o objetivo de conferir urgência a uma determinada situação e, com isso conseguir justificar a tomada de decisões e mobilização de recursos para fazer frente a uma situação entendida como urgente. Assim, segundo Buzan et al., (1998: 25) diferentemente do que propunham as interpretações tradicionais da segurança, o objeto ameaçado convoca, por si só, o imperativo da sua defesa, precisa de um movimento de securitização ancorado em um discurso coerente para que seja alçado a esta categoria. Na essência, reside neste aspecto a grande contribuição teórica da securitização: o que se entende por segurança tem alvos dinâmicos, é o que se convence como sendo questão urgente e excepcional. Neste entendimento, a linguagem vem a tornar-se um elemento essencial. É através da linguagem, que faz referência ao contexto e aproxima os objetos de referência e a audiência a contextos específicos e subjetivos, que se constrói o movimento de securitização.

Esse sublinhado da centralidade da da linguagem aproxima as proposições das teorias da securitização da interpretação construtivista das relações sociais. A linguagem aqui é vista como um instrumento que serve a vários objetivos nas interações sociais diárias. Como resume Ferreira (2010) a linguagem é o produto final de uma interpretação subjetiva de agentes em interação.

A linguagem, dentro do escopo das teorias da securitização, funciona como um instrumento que transmite a intenção dos agentes em um determinado contexto(Balzacq, 2011; Ferreira, 2010). O movimento de securitização inicia-se em um ato discursivo que

clama atenção especial para determinado objeto de referência. Essa atenção especial dá-se especificamente quando o termo ´segurança´ é empregado. Ou, como argumenta Weaver,

> The process of securitization is a speech act, not interesting as a sign referring something more real: it is the utterance itself that us the act, *by labelling something a security issue, it becomes one* – issues aren´t security issues in themselves and then afterwards possibly talked about in terms of security. (Weaver, 2012: 52)

Esse ato discursivo com o qual se inicia um processo de securitização divide-se, segundo o teórico da linguagem John Austin (1962), em três níveis. O primeiro, chamado de locucionário, apresenta um termo ou expressão-chave que permite um determinado sentido a uma situação, no caso de um movimento de securitização. Emprega-se, naturalmente, expressões que conferem sentido de urgência, sendo o mais apelativo, ou assim entendida, como visto, o termo segurança. O segundo nível relaciona-se com a articulação de uma informação. Aprofundando o entendimento, Searle (1976)[24] estabelece classificações para os atos ilocutórios que indicam assertividade do discurso, do comprometimento do locutor a uma causa ou à defesa de seus argumentos. Esses atos indicam ainda o compromisso com futuras ações que, em certa medida, podem pautar a mudança da realidade em acordo com as afirmações propostas. Por fim, o ultimo nível, o ato perlocucionário, diz respeito às transformações visadas quando se empregam elementos, como a evocação de sentimentos ou a referência a símbolos, que fazem sentido a uma determinada audiência (J. Austin, 1962). Um ato discursivo, dentro desse campo da securitização não é o mero ato de dizer, mas sim empregar a linguagem em um discurso em busca de transformações em um determinado contexto.

O ato discursivo configura-se, então, como um aspecto muito relevante das teorias da securitização. Contudo, aprofundamentos teóricos sugeridos por (M. C. Williams, 2003) sugerem que o foco nos atos discursivos enquanto único elemento de análise para a securitização acabam por limitar o alcance das explicações teóricas. Segundo o autor, o foco nos atos discursivos não é suficiente para englobar todos os elementos que influenciam as questões de segurança. Por consequência, se a intenção é considerar as questões empíricas e

[24] Sugere-se que para um aprofundamento nas teorias dos atos discursivos se leve em conta duas obras principais: Searle, J. (1975) "A Taxonomy of Illocutionary Acts", in: Günderson, K. (ed.), *Language, Mind, and Knowledge*, Minneapolis, (7); Searle, J. (1976) "A Classification of illucutionary acts". *Language and Society*. 5(1), 1-23) e Austin, J. (1962) How To Do Things with Words. Oxford: Oxford University Press. Por agora para o desenvolvimento do texto, não se aprofunda nesta discussão por entender-se que, embora tenha um papel importante para o entendimento dos movimentos de securitização, pertence a outro campo de estudo, o das teorias da comunicação.

não apenas os discursos sobre elas, a teoria da securitização deve desenvolver um entendimento mais amplo dos meios, estruturas, e instituições que estão envolvidas no contexto onde se dá a comunicação política contemporânea (Williams, 2003: 512).

Seguindo o raciocínio, Williams (2003: 512-513) argumenta que o foco no ato discursivo em detrimento de outros aspectos acaba por limitar a teoria da securitização. O foco no ato discursivo não permite agregar ao conjunto das possibilidades de assuntos securitizados aqueles temas que não passam necessariamente pelo discurso ou que dependem mais de outros elementos de entendimento. Esses constrangimentos operam em três aspectos. Primeiramente, na amplitude ou abertura do processo de securitização. Sendo o movimento de securitização, como afirma a teoria, um processo aberto a todos os atores, a securitização depende da capacidade desses mesmos em fazer-se ouvir e convencer uma determinada audiência, usando elementos empíricos para embasar seus argumentos. Nem todos os fatores, contudo, são socialmente relevantes. Os processos dependem também das condições de propagação da mensagem e da capacidade de convencimento dos atores da securitização. Assim, os processos de securitização dependem da competência do ator em usar os recursos disponíveis e os entendimentos internos da audiência que o locutor se dirige a tentar convencer das necessidades de implementar medidas especiais de segurança. Os processos de securitização são por isso também dependentes de fatores externos, do contexto e dos elementos sociais que confiram sentido no contexto empregado já que servirão para suportar uma posição da qual o ato na securitização pode ser executado. Em segundo lugar, própria efetividade do movimento de securitização: Nem todos os discursos são efetivos para se criar um movimento de securitização. Igualmente, nem todos os atores da securitização dispõem de competência suficiente para os gerar e desenvolver. Assim, um ato discursivo para ser efetivo no plano da securitização tem de observar duas exigências: primeiro, as especificidades linguísticas e gramaticais que correspondem ou que sirvam de entendimento para uma determinada audiência e a adequação ao contexto social ao qual o discurso se baseia para marcar sua posição e justificar seus argumentos.

Por fim, em terceiro lugar, as bases para outros movimentos de securitização são um outro aspecto a ter em conta. Ainda que os contextos empíricos e as reivindicações assumidas em um dado movimento de securitização não tenham resultado na securitização de determinada questão, eles ainda servem como base retórica para outros movimentos.

Para além dos discursos baseados na linguagem falada, (Williams, 2003: 514) ainda argumenta em favor do alargamento dos elementos que constituem os movimentos de

securitização. O autor afirma que os atos discursivos da securitização não se reduzem a um ato puramente verbal ou a uma retorica linguística. Mais complexo que isso, constitui-se de um ato performativo que se forma através de uma variedade contextual, institucional e recursos simbólicos para ter efeito. Neste sentido, considerando a infinidade de maneiras com que se transmite uma ideia ou mensagem, levar em consideração as imagens é importante para o entendimento de um movimento de securitização. Contudo, incluir essa dimensão significa uma série de complexificações teóricas para a análise dos casos.

Os diferentes meios de comunicação não são neutros em seus atos/discursos. As condições para a produção e recepção dos atos de comunicação são fundamentalmente afetadas pelos meios pelos quais são transmitidos. Essa nova dimensão a ser considerada traz o foco, por exemplo, para como as comunicações televisivas causam impacto sobre as diferentes audiências, e para as consequências desse ato para a securitização. Analisar a segurança por esse lado também requer novas técnicas para a compreensão dessas retóricas. Tais abordagens focam não só no significado desses discursos (imagens) mas também no impacto que essas diferentes opções políticas influenciam as práticas de segurança. Deste modo, é preciso um maior e melhor entendimento das retoricas de securitização (Williams, 2003: 525-528).

Neste sentido, considerando que os movimentos de securitização são ancorados em determinado contexto para provocar e convencer determinada audiência em aceitar medidas especiais para tratar de uma situação que requer uma atenção especial por envolver questões de segurança, Balzacq (2005a) argumenta que os processos de securitização são, na realidade melhor entendidos se forem acatados como uma prática estratégica, que envolve certo pragmatismo e cálculo de quem inicia o movimento de securitização. Essa estratégia assenta, por sua vez, na configuração das circunstancias em que acontece, que envolve o contexto político, as disposições culturais da audiência e, naturalmente, a aceitação do ator pela audiência e do poder que gera esta interação (Balzacq, 2005a).

Ao integrar a dimensão estratégica e pragmática no movimento de securitização, Balzacq coloca definitivamente a teoria da securitização no âmbito do contexto social onde encontra elementos fundamentais que devem ser considerados, como o exercício de poder e de convencimento que os atores da securitização fazem ao tentarem aproximar as questões de segurança ao entendimento da audiência em busca de apoio para uma mobilização.

Assim, concordando com Ferreira, (2010), o estudo dos processos de securitização que pretenda examinar determinada situação de forma mais completa deve focar em um ato

momentâneo, ou aquele preciso momento onde se tomou a decisão de securitização de um tema, mas também deve-se levar em conta o contexto no qual o ator da securitização se baseou para tomar suas respectivas decisões.

Na maioria das vezes, segundo Buzan et al. (1998), é uma autoridade pública que inicia o movimento de securitização. Contudo, como já visto, o papel do ator da securitização é aberto a qualquer instância, condicionado à sua competência em agregar credibilidade ao ato discursivo. Neste sentido, há vários exemplos de discursos proferidos por autoridades que visam a securitização de determinada questão e que já foram analisados pelas teorias da securitização. A questão climática e ambiental por exemplo, tornou-se um assunto bastante politizado principalmente a partir das décadas de 1990 e 2000. O discurso que identifica as mudanças climáticas como ameaça à humanidade, às seguranças nacionais e internacional vem dos últimos anos da década de 2000. Segundo Scott (2012), em 2006 a ex-secretária de Assuntos Estrangeiros do Reino Unido, Margareth Backett, assumiu a liderança nessa associação entre mudanças climáticas e segurança internacional em fóruns multilaterais. Pouco tempo depois, com a ênfase discursiva na questão da segurança, a questão climática foi debatida pelo Conselho de Segurança das Nações Unidas não só como uma ameaça, mas como um elemento multiplicador de ameaças (Scott, 2012: 222). Essa noção já estava sendo delineada a partir de outros estudos, por exemplo, os que argumentavam que as mudanças climáticas poderiam provocar Estados falhados (Campbell, 2008; Podesta & Ogden, 2007). Há, posteriormente, investigações que associam as mudanças climáticas à ascensão ou fortalecimento de células terroristas (Lytle, 2017).

O terrorismo, como é sabido, passou a ser um tema largamente politizado após os atentados de 11 de setembro de 2001 nos Estados Unidos. Após os atos e as imagens que circularam em todo o mundo instantaneamente, foi fácil aos atores da securitização colocar o tema do terrorismo como a principal ameaça securitária a exigir medidas especiais e a supressão das condições de normalidade. Assim, o então presidente norte-mericano, George W. Bush, proferia:

> "Tonight we are a country awakened to danger and called to defend freedom. Our grief has turned to anger, and anger to resolution. Whether we bring our enemies to justice, or bring justice to our enemies, justice will be done."
>
> […]
>
> "On September the 11th, enemies of freedom committed an act of war against our country. Americans have known wars - but for the past 136 years, they have been wars

> on foreign soil, except for one Sunday in 1941. Americans have known the casualties of war - but not at the center of a great city on a peaceful morning. Americans have known surprise attacks - but never before on thousands of civilians. All of this was brought upon us in a single day - and night fell on a different world, a world where freedom itself is under attack."
>
> […]
>
> "I ask you to uphold the values of America, and remember why so many have come here. We are in a fight for our principles, and our first responsibility is to live by them". [25]

Os discursos que se baseiam no terrorismo como ameaça, principalmente este proferido pelo então líder da nação mais poderosa do mundo em um momento de grande sensibilidade, são organizados de uma maneira que permitem a fácil visualização dos elementos descritos pelos autores da teoria da securitização. Por exemplo, no trecho acima selecionado, é claro o ênfase dramático em valores básicos ("freedom") ameaçados pelos terroristas, e o imperativo de tomar medidas para tanto ("justice will be done"). É também imperativo um apelo a uma memória agregadora ("America have known war...") para convocar o apoio almejado ("we are in fight for our principles, and our first responsibility is to live by them"). Naturalmente, em um sistema mundial altamente globalizado onde a tecnologia permite o acompanhamento dos acontecimentos instantaneamente, as imagens dos atentados exaustivamente transmitidas ao mundo deram um largo apoio à credibilidade do discurso e à justificação das medidas que se seguiram, ou seja, um aumento das medidas de segurança em geral, o que inclui, por exemplo, a supressão de algumas liberdades essenciais, como a privacidade ou a liberdade de movimento, entre outros, para alegadamente preservar esses próprios valores. Esse aspecto só vem a corroborar as propostas sobre a inclusão das imagens entre os elementos de análise dos movimentos de securitização e sobre a importância do contexto e da estratégia discursiva dos atores da securitização (Balzacq, 2005a e 2011; Williams, 2003).

No que a segurança do ciberespaço, especificamente diz respeito percebe-se que os principais argumentos a favor dessas medidas que poderiam tornar-se marco do início do movimento de securitização, são articulados por mandatários ou autoridades

[25] Discurso do presidente George W. Bush ao Congresso Norte Americano referindo-se aos atentados terroristas que atingiram os Estados Unidos em 11 de setembro. O discurso na íntegra está disponível em: http://www.theguardian.com/world/2001/sep/21/september11.usa13.

governamentais, como o presidente Obama. Em 2009, após constatar e expor a dependência da sociedade norte americana do ciberespaço, Obama declara que

> "It's the great irony of our Information Age, the very technologies that empower us to create and to build also empower those who would disrupt and destroy. And this paradox -- seen and unseen -- is something that we experience every day" (White House, 2009: online)

Mais adiante, relaciona temas já consolidados enquanto questões de segurança com o ciberespaço:

> Our technological advantage is a key to America's military dominance. But our defense and military networks are under constant attack. Al Qaeda and other terrorist groups have spoken of their desire to unleash a cyberattack on our country -- attacks that are harder to detect and harder to defend against. Indeed, in today's world, acts of terror could come not only from a few extremists in suicide vests but from a few key strokes on the computer -- a weapon of mass disruption (White House, 2009: online)

E conclui que

> "cyber threat is one of the most serious economic and national security challenges we face as a nation" and that "America's economic prosperity in the 21st century will depend on cybersecurity" (White House, 2009: online).

Um outro exemplo, em várias ocasiões, o Ministro das Comunicações e Tecnologias da Informação indiano, Kapil Sibal, expôs sua preocupação com a segurança do ciberespaço inclusive com a possibilidade de ameaças provenientes de outras nações e a necessidade de promover políticas de segurança e defesa para este espaço:

> "Now, what is happening today is that we know for a fact that nations have organised themselves to indulge in cybercrime. We know for a fact that they work sometimes through individuals far removed from them" (India Times, 2013: online).

> "We believe in the complete freedom of cyber space, but there should be a de facto recognition of threat,"

> "[…] the Internet world today does not allow us to find where the attack came from and who attacked us, nor does it allow us to disclose the identity of the attackers. We need to develop global rules for that. We need a global accord for that and we then need a system of cyber justice," (DNAIndia, 2013)

O ministro enfatizou a necessidade de estabelecer políticas para a defesa e segurança do cyberespaço:

> "No nation can fight cybercrime or secure its cyberspace in isolation. Increased and focused cooperation among key players, governments, industry and international bodies, is essential to create a secure cyber space" (Economic Times, 2012).

Em outra ocasião, anuncia medidas que vão neste sentido: “We are working on a cyber security policy... we need more work to curb cybercrimes” (IBN Live, 2013).

As justificativas para a implementação de políticas voltadas para a securitização do ciberespaço residem principalmente no fato de que as infraestruturas críticas, ou seja, aquelas das quais depende o bom funcionamento dos serviços básicos dos Estados, são permeadas pelas TIs e são vulneráveis a ameaças provenientes do ciberespaço. Recorremos agora ao exemplo italiano. Como apontado pelo Sistema de Informações pela Segurança da República da Itália,

> La sicurezza del cyberspace è oggi una delle esigenze principali di chi opera a garanzia degli interessi nazionali di un Paese. Per garantirla però è necessaria una vera e propria politica di cyber security che non si confronti solo con la componente tecnica e tecnologica del problema, ma che sia in grado di coglierne gli aspetti sociali, legali ed economici[26] (SISR, 2013: online).

2.3 Objetos de Referência

O processo de securitização apresenta, logo em seu início, um objeto de referência. Como explica Buzan et al., (1998: 36) trata-se objetos ou elementos que são vistos como existencialmente ameaçados e cuja existência justifica moral e legalmente a adoção de medidas para sua defesa. A indicação de determinado objeto de referência é dada pelos agentes da securitização ao apontar determinado aspecto como algo ameaçado.

Diferente do que propunha o pensamento tradicional sobre segurança, os objetos de referência, segundo as teorias da securitização, não se limitam às questões estatais, à soberania, e a outros aspectos ligados a cada Estado. Pelo contrário, a securitização, segundo sua lógica, possibilita que muitas outras realidades sejam tomadas como objeto de referência. Assim, cabe a questão colocada por Baldwin (1997: 12) que propõe uma análise das questões de segurança perguntando-se para quem seriam as medidas a serem tomadas, ou ainda como aponta Huysmans (1998) “in whose name security operation is conducted?”.

Partindo de uma agenda mais ampla, o escopo da segurança se complexifica ao ser aberto a qualquer elemento, como aponta Williams (2003). Os estudos da segurança já não

[26] Tradução livre: A segurança do ciberespaço é hoje uma exigência principal de quem opera a garantia dos interesses nacionais de um Estado. Para garanti-la, faz-se necessária uma verdadeira e própria política de cibersegurança que não se confronte somente com os aspectos técnicos e tecnológicos do problema, mas que esteja ao nível de acolher os aspectos sociais, legais e econômicos.

possuem um elemento-alvo pré-determinado, mas passam a abordar uma infinidade de possibilidades de ameaças ao elemento identificado como digno de proteção urgente. Mais do que isso, por outro lado, esses elementos ameaçados são construídos através do ato discursivo, e não existem independentemente da iniciativa de quem o aponta. Fica evidente, então, o fundo construtivista da Escola de Copenhague e, automaticamente, das teorias da securitização por ela desenvolvidas. (Sulovic, 2010)

Interessa ressaltar que, nessa lógica teórica sugerida pelas teorias da securitização, indivíduos podem desempenhar um papel duplo nos processos de securitização sendo atores da securitização e ao mesmo tempo objetos de referência. Os agentes da securitização, assim, podem apontar a existência de ameaças a si mesmos, ou à sua coletividade, sociedade, etc. A possível centralidade de questões subjetivas nesta agenda de segurança alargada traz também para ela a consideração dos contextos, a pertença a um grupo, a uma sociedade, a uma maneira de viver, a valores centrais, a liberdades específicas, entre muitos outros. Segundo Buzan et al., (1998: 36-37), os objetos de referência que envolvem o sentimento de pertencimento, o "nós", são construções sociais que funcionam a partir da interação de pessoas. O principal critério para os processos de securitização que usam desse apelo, ainda segundo o autor, é a formação de uma comunidade interpretativa baseada em contextos particulares nos quais os princípios de legitimação ganham sentido partilhado.

Neste sentido, os processos de securitização que envolvem a proteção a um determinado local ou modo de vida têm mais chances de tornarem efetivos. Os processos de securitização que envolvem questões de imigração são bons exemplos desse aspecto pois parte deles ancoram seus argumentos na unidade cultural ou a estabilidade da unidade política. Por exemplo, Dijck (2006) ao observar o processo de securitização da imigração na União Europeia, percebe que os objetos de referência variam de acordo com o contexto e a conveniência circunstancial, ao mesmo tempo que dependem do funcionamento da estrutura de bem estar social promovida pelos Estados. São apontados como alegadamente ameaçados o sistema de saúde, o sistema econômico, a livre circulação de pessoas dentro do espaço da União, entre outros. Essas políticas também fazem referência a outros níveis como o pacto de integração, a estabilidade da União Europeia e, dependendo do ator da securitização, declaram-se ameaçados ora os Estados Membros, especificamente, ora estados do sul europeu. A securitização nesses termos procura legitimar uma política que dificulte a entrada de imigrantes e a burocratização das condições legais para a admissão (Dijck, 2006: 25-27).

Huysmans (2000), ao se debruçar sobre o mesmo tema anos antes, percebia a existência de um discurso que aponta a migração como um elemento supostamente desestabilizador ou um desafio a ser tratado principalmente pelos países da Europa ocidental:

> The development of security discourses and policies in the area of migration is often presented as an inevitable policy response to the challenges for public order and domestic stability of the increases in the number of (illegal) immigrants and asylum-seekers […] In this analysis the security problem triggers the security policy. The policy is an instrument to protect the state, its society and the internal market against the dangers related to an invasion of (illegal) immigrants and asylum-seekers. In other words, the problem comes first and the policy is an instrumental reaction to it. (Huysmans, 2000: 753).

Mais do que isso, e aproximando da pauta do sentimento de pertença, o autor argumenta que há um discurso de teor conservador que identifica o multiculturalismo, enquanto resultado de uma migração alegadamente descontrolada, como a pretensa causa de desintegração social. A migração é identificada como um dos principais fatores que ameaçam ou enfraquecem a tradição e a homogeneidade nacional (Huysmans, 2000: 758). Esse discurso estabelece uma divisão entre o "nós" e "nosso modo cultural" e "eles" que, com suas particularidades, põem em risco a sobrevivência ou a existência dos "nossos" valores, das "nossas" tradições, etc.

O contexto nacional ou cultural é, pois, ao mesmo tempo o objeto de justificação do discurso perante a uma determinada audiência e também o objeto de referência, carente de proteção e de medidas efetivas para garanti-la.

As justificativas baseadas no contexto nacional são bastante amplas, permeando muitos objetos de referência. Essa mesma amplitude em seu alcance indica, primeiramente, que as questões de segurança ainda se voltam em grande parte para a ação estatal em busca de medidas para tratar o que se entende serem ameaças. Embora argumente que a segurança seja um assunto aberto, Buzan et al. (1998) defendem que geralmente se espera do Estado ou sistemas estatais a resposta para tais questões. Não se nega ou diminui, portanto, a importância que o Estado guarda perante as questões de segurança. Um exemplo neste sentido é a securitização das capacidades energéticas. Özcan (2013), argumenta a este respeito que, dado a importância estratégica que a disponibilidade de energia tem no cenário internacional contemporâneo, a energia passou por um processo de securitização. Neste cenário, segundo o citado autor, os objetos de referência não são o sistema energético em si ou a disponibilidade de energia, ou ainda as fontes de energia, mas sim a sobrevivência estatal e o desenvolvimento econômico e social que depende de energia para seu sustento.

Para além disso, há também uma dimensão internacional, já que a energia passou a ser moeda de troca na política internacional. Como alguns países utilizam de sua abundância de recursos energéticos para implementar suas posições em meio aos players internacionais, a ideia de escassez de energia, principalmente o petróleo e gás, ameaça existencialmente a sobrevivência de Estados no sistema global e, automaticamente suas respectivas economias entre outras necessidades. É claro que a questão energética não se tornou um elemento relevante na política internacional com o movimento de securitização. Segundo Özcan (2013), esse processo já era uma realidade e foi utilizado pelos atores da securitização para justificar seus argumentos, principalmente após a primeira crise do petróleo no início da década de 1970, tornando-se, então, assunto da alta política, saindo do escopo da agenda normal da política e chegando a ser explicitamente assumido como justificação principal de eclosão de conflitos internacionais.

Assim, como explica o autor,

> […] energy is taken out of the 'agenda of normal politics', and the 'breaking of the established rules of the game' have been justified to prevent any danger posed if no prevention had been taken.61 In other words, energy has started to be perceived in terms of existential threats, and in such a context, political rather than economic dimensions of energy have become significantly more considerable with the securitization of energy: therefore, energy relations consist of transactions such as 'export', 'import' and 'the transit' of energy. Security of demand holds importance according to the energy producers (export), and as the fossil fuels would deliberately continue to play a dominant role in the energy sector, they have approached the domination status and used their energy industry as a weapon for their own political interest. In terms of the energy consumers (import), they have used political and military power to maintain their energy needs as less expensive and more reliable. (Özcan, 2003: 12)

Os objetos de referência superam o campo restrito do objeto securitizado. O alvo da securitização da energia, por exemplo, não é a energia em si, mas algo maior, que depende da energia para a sobrevivência. O mesmo pode ser aplicado no caso da securitização do ciberespaço. Não é a existência dele que está ameaçada, e tampouco o ciberespaço é visto como uma ameaça que deve ser extinta para que um objeto de referência seja poupado. São as ameaças dele provenientes ou nele possibilitadas que são o alvo da securitização. Nota-se, entretanto, que o ciberespaço é apontado como objeto de referência por alguns autores. Sua existência não é entendida como uma ameaça, mas se pondera como uma ferramenta disponível a atores que podem, então, ser compreendidos como ameaça. Assim, tornar o ciberespaço mais seguro e disponível a quem faça bom uso deste é o que tem sido alegado pelas discussões de securitização.

Alguns textos já citados no capítulo anterior apontam com bastante clareza os objetos de referência do movimento de securitização do ciberespaço. Entende-se que retomar estes textos em uma exploração com vistas à securitização do ciberespaço é útil ao aprofundamento do raciocínio proposto.

O Estado, tal como foi abordado no início do capítulo, tem sido tradicionalmente o objeto principal de segurança, alegando a defesa da soberania ou, a integridade identitária como elementos sob ameaça. Contudo, as análises feitas a partir da teoria da securitização permitem ampliar este aspecto, considerando que os agentes de securitização podem referir-se a qualquer elemento ou aspecto de um determinado contexto enquanto objeto de referência. São vários os exemplos de securitizações que ultrapassam o limite dos Estados e restrições no âmbito militar. Entre esses está o conceito de segurança humana cujo discurso de defesa se baseia na securitização das necessidades básicas (Watson, 2011). Do mesmo modo, o discurso da segurança assentado na securitização dos equilíbrios ecológicos e da preservação dos ecossistemas essenciais como forma de prevenir ameaças quer à existência humana (Brauch, 2008), quer à própria sobrevivência física do planeta.

Restringindo ao tema da cibersegurança e analisando alguns dados e estratégias de alguns países, bem como a análise empírica de alguns episódios, Geers, Kindlund, Moran, & Rachwald (2013) e Weingartl et al. (2005) apontam a soberania nacional como objeto de referência. Defendem ainda a ideia de que governos em diferentes contextos e regiões já usam de estratégias veiculadas ao ciberespaço para defender sua soberania nacional, para além de desenvolver instrumentos para a projeção de poder. Segundo estes autores, os ciberataques são mais do que um fim em si mesmo, ou seja, são meios para atingir objetivos políticos, militares ou econômicos. Geers (2013), por fim, ainda cria um conceito para ilustrar a ideia de um advento de um possível conflito mundial a ter lugar no ciberespaço: *World War C*.

Choucri, (2012: 125-130) também identifica a segurança nacional, ainda que de forma genérica, como alvo de ameaças no ciberespaço. Essa alegação vem da percepção de que a Internet pode ser usada como arma para conseguir objetivos políticos ou informações privilegiadas de maneira ilegal ou não consentida. Para além das questões ligadas ao conceito de soberania, de maneira mais específica, outro aspecto que gera preocupações é a vulnerabilidade das infraestruturas críticas: sistema bancário, sistemas de abastecimento de bens essenciais, controle de fluxos aéreos, entre outros, largamente dependentes de tecnologias ligadas em rede. A autora considera que a militarização do ciberespaço está

emergindo como um requisito essencial para as políticas de defesa e isso é visto como um desenvolvimento natural, dadas as necessidades que o novo ambiente impõe (Choucri & Ridgeway Center, 2012). Há uma série de investigações, documentos e relatórios que, olhando para a dependência das infraestruturas críticas do ciberespaço, principalmente no que se refere à sua administração e logística, identifica-as como alvo de ameaças provenientes do mesmo ciberespaço (Clemente, 2013; Department of Homeland Security, 2013; Karabacak, Ozkan Yildirim, & Baykal, 2016; Martin, 2013; Olive, 2013; Rosenzweig, 2013; Rudner, 2013; Stoddart, 2016). Por exemplo, Clemente (2013) argumenta, em favor do estabelecimento de políticas multilaterais a nível internacional para a promoção da defesa e controle do ciberespaço e rejeita a noção de que o ciberespaço é um setor com pouca importância estratégica, contrapondo a constatação de que este espaço pode ser visto como um sistema nervoso essencial para que setores críticos funcionem e se comuniquem entre si. O autor faz uma série de recomendações para um novo entendimento das necessidades de proteção e defesa do ciberespaço. Segundo ele, é preciso estabelecer novos parâmetros do que constituem as infraestruturas críticas e adaptá-las dentro de uma hierarquia organizacional que facilite respostas a riscos emergentes. A questão da proteção das infraestruturas críticas é uma constante e parece ser um consenso na política de proteção do ciberespaço.

Apontando para outra direção, Rosenfield (2009) sustenta que a preocupação mais séria no caso das ameaças provenientes do ciberespaço não é seu potencial de destruição dessas infraestruturas críticas mas sim o potencial de isolamento das mesmas. É a interrupção dos fluxos de comunicação que, em uma sociedade pós-industrial altamente dependente desta estrutura, pode causar gravosas consequências econômicas e sociais. O controle de sistemas que comandam infraestruturas críticas é de acesso extremamente difícil e, por isso, a hiótese de ataques a estes é pouco provável. Com alguns exemplos, o autor acaba por sinalizar que as consequências também não são tão preocupantes e de fácil e rápida recuperação. Assim, não é este o risco que oferecem os ataques em redes virtuais. Para ele, não é contra as infraestruturas críticas que se dirigem as principais ameaças do ciberespaço. O potencial em termos de danos provocados por ciberataques está na capacidade de estes interromperem a comunicação, ou serviços, usando uma tática denominada DDoS (Distributed Denial of Service) que consiste em impedir que usuários acessem os serviços disponibilizados através de plataformas virtuais. Ataques a dados (roubo de informações, implantação de informações, etc) são mais prováveis e têm maior potencial para causar

danos de que ações contra o controle de sistemas de infraestruturas. Ataques contra dados podem resultar em um efeito cascata de falhas e de informações e redes de comunicação e impor sérias ameaças à sociedade moderna, cada vez mais dependente de estruturas construídas e viabilizadas no ciberespaço. Os ataques a sistemas de controle podem ser mais abrangentes no sentido de que ganham maior atenção da mídia, mas os ataques contra sistemas de dados e o impedimento de acesso são muito mais frequentes, fáceis e por isso mais ameaçadores.

De maneira um pouco mais assertiva, McGraw (2013) argumenta que o potencial de conflitos no ciberespaço está em expansão, acompanhando o crescimento da dependência de tecnologias vulneráveis cada vez mais difundidas. O autor afirma que, contrariamente ao que acreditam os decisores sem o devido conhecimento técnico, os sistemas modernos apoiados no ciberespaço são desafiados frequentemente por apresentarem sistemas de segurança vulneráveis. Tais vulnerabilidades acabam por tornar possíveis ataques relativamente fáceis. Há inúmeras como a ciberguerra, ciberespionagem e cibercrime que constituem desafios fundamentais à reflexão sobre a segurança.

Importante ressaltar que não há um consenso no que se refere às ameaças, ou aos objetos de referência ao menos quanto às prioridades entre eles, nem mesmo se o ciberespaço constitui alguma ameaça aparente. Assim, por exemplo, em contraste com os que chamam a atenção para a emergência das ameaças do ciberespaço, Rid (2012) entende que atos de guerra tendo o ciberespaço como foco não são viáveis. Regressando a definições teóricas sobre a guerra de pensadores clássicos, principalmente Carl von Clausewitz, o autor sustenta que os ataques com base nas tecnologias ancoradas no ciberespaço, provenientes de governos ou outros atores, não se enquadram nas definições de guerra, baseadas em atos de força, violência e alcance letal. Quando muito, os ataques (espionagem, sabotagem, inserção de códigos maliciosos em aplicações estratégicas), correspondem somente a um dos requisitos, que é a motivação política. Analisando os casos mais comuns de ciberataques, o autor desconstrói a ideia de que os ataques à Estônia, ao Pentágono, e às instalações nucleares sírias, todos em 2007, constituem atos de guerra. Segundo ele, tais ataques não correspondem aos critérios necessários para serem identificados como atos de guerra, apesar de que tais iniciativas podem vir dar suporte a estratégias militares.

A literatura sobre a questão da segurança do ciberespaço não é, pois, consensual em relação aos objetos de referência. Mesmo quando coincidem sobre o alvo das políticas de proteção, divergem sobre o que seria prioridade entre eles. Contudo, mesmo os que não

concordam que a questão levará a consequências tão trágicas quanto se expôs, concordam que a questão da segurança do ciberespaço é relevante. É neste espaço que se situa uma oportunidade para um movimento de securitização. É no momento em que a sociedade e os governos se dão conta de que há uma dependência crescente do bom funcionamento das tecnologias da informação já que assim as necessidades contemporâneas e cotidianas exigem, que se começa a pensar em políticas de segurança. Naturalmente, esse pensamento não se limita, como se pode perceber, a um mero sistema de governança. Pelo contrário, o que se percebe através de documentos oficiais e iniciativas de governos, é que para além das iniciativas de governança, há também iniciativas que ultrapassaram a fase de politização da questão e assumem um caráter mais securitizado, como uma militarização do ciberespaço e a preparação para uma eventual guerra cibernética. Contudo, as decisões para que tais iniciativas se realizem não dependem somente do convencimento coletivo de suas necessidades. A securitização depende da ação crucial do que os teóricos chamam de atores funcionais, que serão explorados no próximo tópico.

2.3 Atores funcionais

A definição de Buzan et al. (1998: 36), sobre os atores funcionais é bastante precisa. Segundo os autores, um ator funcional no processo de securitização é aquele que consegue ou tem a capacidade de afetar as dinâmicas de um determinado setor, ou, como explica Balzacq (2011: 178), aqueles cujas ações ou atividades têm significativo impacto na mobilização de medidas de segurança.

Buzan et. al. (1998: 36), no entanto, afirmam que não há troca de papeis entre os elementos da securitização. Para ele, os atores funcionais não podem figurar como agentes da securitização em um mesmo movimento de securitização. Não participam, portanto, do convencimento ou das justificações para a adoção de medidas de segurança. No entanto, convém pontuar que, ao menos nos casos analisados a serem abordados nos próximos capítulos, essa linha de separação não é necessariamente clara. Por vezes os atores funcionais, antes de tomarem suas decisões que levariam à securitização adotam os discursos e compartilham das ideias de um movimento de securitização intencionando, por vezes, direcionar as decisões para um determinado sentido.

O ator que desempenha um papel funcional em um processo de securitização varia de acordo com a natureza e os temas e setores que envolvem o processo. Neste sentido, as

Organizações Não-Governamentais aparecem como atores funcionais quando defendem alguma medida ou decisão já tomada por um Estado, atores determinantes nos processos de securitização que envolvem o meio ambiente (Hughes, 2007). Assim, a Alliance of Small Island States, por exemplo, figura-se como uma coalizão de países voltada para a segurança, já que seu discurso relaciona as mudanças climáticas com algo que ameaça diretamente a sobrevivência e a segurança dos 32 países que representa. Faz isso em fóruns multilaterais, fazendo uma espécie de lobby para que os países industrializados tomem medidas mais efetivas na tentativa de amenizar o que entendem como ameaça, nomeadamente, o aumento do nível dos oceanos (Hughes, 2007: 50-52).

No setor militar, como lembra Duque (2009: 483) os atores funcionais tendem a ser os atores que guardam o poder de força ou têm determinar o uso da força. Naturalmente, o primeiro exemplo neste sentido são as Forças Armadas e suas subdivisões, polícias e forças de segurança. No entanto, há um relevo crescente do setor privado que tem oferecido soluções para a segurança, inclusive, ou sobretudo, com a permissão dos Estados. A empresa americana Academi, anteriormente designada por Blackwater, tem desenvolvido o que chamam de soluções para questões complexas de segurança. Segundo os próprios,

> "No firm in the world is more proven when it comes to supporting governments as they resolve hard security problems. With 7000 acres dedicated to training and preparing government clients and our own staff to operate in every possible environment, ACADEMI is unsurpassed" (Academi, 2018: online).

Esse campo não está limitado, entretanto, às instituições com poder militar, mas se estende também a *think tanks* ou qualquer instituição que consiga exercer influência na condução da política externa de um determinado país. Assim, o Council of Foreign Relations, que conta com uma grande dimensão e influência nas decisões do governo norte-americano, é um exemplo neste sentido. Isso mesmo é mencionado em sua missão divulgada, que é ser,

> a resource for its members, government officials, business executives, journalists, educators and students, civic and religious leaders, and other interested citizens in order to help them better understand the world and the foreign policy choices facing the United States and other countries. (Council of Foreign Relations, 2018: online)

Ainda no setor militar, há um grande papel desempenhado pela indústria de armamentos. Neste caso, para além dos armamentos de guerra tradicionais ou para o uso policial, há uma aproximação com as questões de segurança do ciberespaço. Assim,

Boulanin (2013) sustenta que, com o desenvolvimento e disseminação das ferramentas de tecnologia da informação, houve um crescimento do mercado da proteção, tanto devido a atuação individual quanto das medidas de segurança que envolvem a inteligência e instrumentos militares no ciberespaço. Assim, o setor público, mas principalmente o setor privado constituem atores funcionais nos movimentos de securitização do ciberespaço.

Choucri (2012) também identifica o Estado como ator funcional no caso da cibersegurança. Também abordando a questão da cooperação para a promoção da cibersegurança, a autora trata da emergência de cooperação a nível nacional e internacional como a criação de políticas e instituições para a governança de segurança e identificação de ameaças no ciberespaço (Choucri, Madnick, & Ferwerda, 2014). Para este efeito, explora o papel do Estado enquanto incentivador de políticas para suporte de direitos o desenvolvimento de normas e condutas e para a consolidação das regras já existentes.

O próprio Joseph Nye (2011:135) também oferece pistas que permitem caracterizar o Estado como ator funcional como tomador de decisão e executor das iniciativas para a segurança do ciberespaço. Para Nye percebe que a emergência das novas tecnologias da informação baseadas na Internet e no ciberespaço tem consequências nas dinâmicas de poder, deixando o controle exercido pelo Estado mais difuso entre muitos atores. No entanto, o Estado continua a ser a entidade que mantém as capacidades de intervir decisivamente nestes processos. Mesmo com o fortalecimento das atividades e ferramentas do ciberespaço, o Estado continuará a manter sua capacidade de influir.

Os Estados têm atuado, mesmo que muitas vezes no âmbito normal da política, ou seja, sem que exista um ambiente securitizado, na construção e implementação de ferramentas para a segurança e até mesmo a governança do ciberespaço. De fato, há importantes movimentos neste sentido dada a atuação dos Estados em âmbito internacional ou multilateral para desenvolver acordos que visam a promoção da segurança do ciberespaço. Assim, Estados Unidos e Índia assinaram, em 2011, um Memorando de Entendimento a fim de promover uma aproximação entre os dois países na questão da cibersegurança (Arora & Kaura, 2017). Há também uma iniciativa entre os governos brasileiro e argentino, que concordaram em promover o tema da cooperação para a cibersegurança no âmbito da União das Nações Sul-Americanas (UNASUL) (El Nacional, 2013).

O governo brasileiro tem tentado implementar uma política internacional a respeito da segurança no ciberespaço. A ex-presidente brasileira, Dilma Rousseff, na Assembleia

Geral das Nações Unidas sinalizou a adoção de medidas e instou a própria ONU a se empenhar em função da regularização do uso deste espaço:

> A ONU deve desempenhar um papel de liderança no esforço de regular o comportamento dos Estados frente a essas tecnologias e a importância da Internet, dessa rede social, para construção da democracia no mundo. Por essa razão, o Brasil apresentará propostas para o estabelecimento de um marco civil multilateral para a governança e uso da Internet e de medidas que garantam uma efetiva proteção dos dados que por ela trafegam (Itamaraty, 2013)

Assim, os Estados não são as únicas entidades relevantes entre os atores funcionais para o caso da segurança do ciberespaço. Embora com menor destaque e com menor hipótese de efetivarem seus discursos por dependerem das decisões dos Estados, as instituições internacionais também protagonizam estratégias de influências nas dinâmicas da segurança. A este respeito, vale ressaltar, entretanto, o papel que tem desenvolvido a NATO enquanto agência de segurança. A instituição criou um centro de excelência, o Cooperative Cyber Defense Center of Excelence, para estudos sobre a ciberdefesa e suas aplicações legais, entre outros aspectos. Também desenvolveu um manual bastante minucioso, detalhado os elementos e dimensões da cibersegurança. De acordo com o Manual, o principal objetivo do Centro de excelência é

> to enhance capability, cooperation and information sharing between NATO, NATO Member States and NATO's partner countries in the area of cyber defence by virtue of research, education and consultation. The Centre has taken a NATO-orientated, interdisciplinary approach to its key activities, including: academic research on selected topics relevant to the cyber domain from legal, policy, strategic, doctrinal and/or technical perspectives; providing education and training, organizing conferences, workshops and cyber defense exercises, and offering consultancy upon request. (NATO, 2012)

2.4 O Discurso e a Audiência

As etapas que constituem um processo de securitização dependem basicamente de dois elementos principais: a formulação do discurso e a identificação de uma audiência com esse discurso. Como argumentam Buzan et al. (1998: 31) os processos de securitização não acontecem fora de um âmbito onde não haja participação de uma determinada audiência. A securitização não é decidida, segundo os autores, somente pelo agente da securitização, mas antes, pela audiência do qual esse agente desenha o seu discurso.

A importância da audiência, segundo Roe (2008) reside na sua capacidade de garantir ao ator da securitização ou ator funcional a anuência e o apoio para atuar para além

das regras normais. Contudo, em casos onde haja uma securitização institucionalizada, o papel da audiência tende a ser marginalizado ou até mesmo excluído. Os casos de securitização institucionalizada não estão muito desenvolvidos do ponto de vista conceitual pelos teóricos da securitização. A securitização institucionalizada aparece quando a identificação de um determinado tipo de ameaças e as respostas a ele são corporizados por um mecanismo institucional (Buzan et al. 1998: 27).

Tanto no caso dos processos de securitização como no aparecimento ou consolidação de uma securitização institucionalizada, o discurso ou os atos discursivos desempenham um papel importante. Segundo Adamides (2012), para que a institucionalização da segurança aconteça, é preciso que exista um discurso ativo, persistente e reiterado que clama pela necessidade de proteção especial de um dado objeto de referência e que, para o efeito, apele à necessidade urgente de medidas excepcionais.

Uma vez criados os mecanismos para responder a essa determinada ameaça e, dado o caráter contínuo das mesmas, tem-se uma securitização institucionalizada. Neste ambiente, segundo Adamides (2012: 85), quando a securitização já é institucionalizada, não há mais a necessidade de convencer a audiência que a este ponto estaria convencida de que as ameaças já estão internalizadas e entendidas. Assim, os atos discursivos funcionam de duas maneiras diferentes perante a uma determinada audiência em um contexto de securitização permanente. Primeiramente, o discurso é necessário para perpetuar a atmosfera da securitização, lembrando a audiência da justificação para as ações do ator funcional e, em segundo lugar, mantêm o sentido de iminência e urgência para determinado tema (Adamides, 2012: 86).

O convencimento da audiência, no entanto, não se refere necessariamente à opinião pública. Os atos discursivos não precisam necessariamente de ser dirigidas às massas, em um sentido mais abrangente. De acordo com Weaver (in Roe, 2008: 619), o papel da audiência, e automaticamente, o discurso a ela direcionado, varia de acordo com o sistema político e a natureza das questões envolvendo a segurança. Balzacq (2005: 34) acrescenta dois novos aspectos no papel da audiência. Segundo o autor, a audiência oferece ao ator funcional um suporte de caráter moral e outro de caráter formal. Os dois aspectos podem ser combinados e isso possibilita a efetivação de um processo de securitização.

Como explicar a não-adoção de medidas extraordinárias mesmo após o êxito no convencimento da audiência? Segundo Collins (in Roe, 2008: 620-621) há duas respostas possíveis. A primeira está relacionada com o caráter da solução proposta. Ainda que se

convença uma determinada audiência que inclui a elite política, mesmo que seja aceite por ela a urgência de um determinado assunto configurado como questão de segurança, a solução pode não passar por medidas extraordinárias, sendo então propostas soluções dentro do sistema político. A segunda resposta identifica o discurso da securitização como algo com uma ambição ou alcance mais amplo que a securitização em si, mas que sinaliza uma vontade política em adotar medidas excepcionais para tratar do assunto. Ou seja, criar uma plataforma que confia legitimidade à adoção de medidas emergenciais é uma parte do processo que pode não se concretiza em medidas efetivas por diversos motivos, inclusive falta de interesse político nessa questão, ou o interesse em mudar o curso das políticas em andamento em um determinado contexto. Dito de outra forma, o discurso securitizador pode ter um objetivo meramente retórico que não busca o êxito do processo como um todo, mas tão só alterar o curso das discussões.

Fica evidente assim que, em qualquer aspecto ou etapa do processo de securitização, o discurso da securitização e a audiência são elementos-chave. E que nem toda audiência corresponde necessariamente à opinião pública, mas pode ser direcionado aos atores que possuem a capacidade de mobilizar recursos ou de justificar medidas que alterem as regras normais de conduta, na política ou em órgãos institucionais capazes de adotar medidas excepcionais.

2.5 Dessecuritização

Do mesmo modo que os processos de securitização apresentam elementos e etapas, é possível identificá-las no processo que tem a dessecuritização como fim. Contudo, , nem sempre é possível identificar o movimento de dessecuritização como um processo simétrico à securitização. A dessecuritização é, assim como a securitização, um processo de construção de um novo entendimento acerca de ameaças ou a desconstrução do processo que levou à percepção dessas mesmas ameaças. Contudo, o contexto, o discurso, os interesses, os atores e as audiências impõem particularidades aos processos de dessecuritização, obrigando a repensar estratégias, mudanças no discurso e outros aspectos que, por vezes, não permite uma volta às condições iniciais pelo mesmo caminho. A dessecuritização é uma nova construção discursiva apontando para objetivos antagónicos do que apontava o processo de securitização.

De acordo com Weaver (1995), a dessecuritização deve ser o principal objetivo a ser buscado em um contexto securitizado. Ou seja, a dessecuritização segundo Weaver (1995: 59 – 60), é o processo em que se desmobiliza as medidas especiais ou emergenciais adotadas para fazer frente a ameaças a um determinado objeto de referência e traz as questões de segurança para serem tratadas no âmbito normal da política. Transforma-se, como afirma o autor, ´threats into challenges and security into politics" (Weaver, 1995: 60).

O certo é que os processos de dessecuritização ainda estão pouco teorizados. Essa falta de um marco teórico mais robusto é uma percepção comum entre os trabalhos que tentam explorar o conceito através de experiências empíricas, como se vê em Acikmese (2013), Aradau (2003), Roe (2004), Huysman (1995), Campana (2013), e Biba (2013). Mesmo Weaver (1995; 1998), enquanto principal formulador da teoria e outros autores da Escola de Copenhague (Buzan et al. 1998) não se dedicam a explorar teoricamente o tema da dessecuritização com a mesma intensidade com que trabalham sobre a securitização. Os processos dessecuritização contam, ainda assim, com alguma teorização que sugere pautas de dessecuritização ou tentam abordar possibilidades para a dessecuritização que serão abordadas mais adiante. Entretanto, uma aparente consequência dessa pouca teorização é a aplicação da teoria em diversos setores ou contextos de uma maneira aberta, sem determinações teóricas que limitariam, em alguns casos, o entendimento dos contextos enquanto processos de dessecuritização.

Weaver aponta três caminhos para a dessecuritização. Uma primeira estratégia seria evitar o discurso que caracteriza a securitização, ou evitar tratar determinados assuntos em termos de segurança. Segundo Biba (2013: 10) essa estratégia tem sido identificada como uma não-securitização. Sugere, então que os processos de dessecuritização não dependem necessariamente de um contexto securitizado, mas a dessecuritização pode, a sua vez, ser aplicada a processos de securitização em curso. A segunda estratégia consiste numa gestão de uma situação securitizada para evitar uma securitização cíclica, ou seja, uma (re)securitização do objeto de referência. Finalmente, a terceira é a que mais se aproxima de um movimento contrário à securitização. Emprega-se um discurso direcionado a trazer o contexto securitizado a um âmbito normal da política. Esse movimento tem sido chamado de estratégia de transformação (Roe, 2004).

Hensen, por sua vez, vê a possibilidade de dessecuritização em quatro maneiras diferentes. Segundo a autora (Hensen, 2012: 529 – 544) os movimentos de dessecuritização podem apresentar-se na forma de mudanças de uma questão securitizada rumo à

estabilização, por exemplo, quando um assunto securitizado passa a ser tratado em outros termos fora do âmbito da segurança mesmo que ainda vigore um contexto securitizado. A ascensão de um processo de securitização em detrimento de outro também pode ser entendida como um processo de dessecuritização. Um tema securitizado pode deixar de sê-lo ao dar lugar a outro entendido como mais grave ou mais urgente, dependendo, sempre, do discurso, contexto e audiência. Há aqui um processo de reposição onde uma determinada ameaça toma o lugar de outra que deixa de fazer sentido ou não oferece um risco tão grande quanto a que toma seu lugar. Os temas securitizados podem ser rearticulados. Neste sentido, a observação de Hensen (2012: 541 – 542) não vai muito além das segunda e terceira proposta de Weaver, expostas acima. Basicamente, a rearticulação de uma questão securitizada envolve sua remoção do âmbito da segurança oferecendo soluções políticas para as ameaças tratando-as como desafios.

Por fim, a dessecuritização pode ocorrer através de um silenciamento. Interessante ressaltar que essa estratégia envolve mais do que o simples desaparecimento do discurso que leva à securitização, mas envolve medidas que impeçam ou que enfraqueçam os atores da securitização em seu discurso ou adotar medidas que invalidem ou desfaçam as ações do ator funcional.

Mcdonald (2008) observa que o foco que a Escola de Copenhague tem dado ao discurso e na linguagem, no estudo da dessecuritização, limita o entendimento desses processos, já que a dessecuritização também pode ocorrer através de outras instâncias que não visam necessariamente um discurso de convencimento, como as burocracias ou, como sugere Biba (2013), num viés mais realista, o equilíbrio de poder, quando aplicado a relações entre países.

Também Balzacq contribui para ampliar a visão sobre os processos de dessecuritização. Validando o mesmo argumento usado para alargar o entendimento dos processos de securitização, ou seja, levando em conta a dependência dos contextos em que se desenvolvem os processos de securitização, sublinha que a dessecuritização é tão dependente do meio em que se desenvolve quanto a securitização. Mais do que dependente do contexto, a dessecuritização, segundo Balzacq também depende das dinâmicas de poder e, como igualmente, centra-se em uma determinada audiência. Para ele, os processos de dessecuritização podem ocorrer ou começar através de duas formas: de um processo argumentativo ou através de dispositivos específicos que a traduzem em práticas (Balzacq, 2012: 22).

O exame da bibliografia sobre a dessecuritização ou focada no objetivo de fornecer bases teóricas para o conceito sugere que, diferente dos processos de securitização, onde há elementos determinantes, como objetos de referência, atores funcionais, atores da securitização e foco no discurso, os processos de dessecuritização são mais abertos. Não há, necessariamente, uma lista de elementos que precisam constar ou precisam atuar para que haja um movimento de dessecuritização. O simples esquecimento da questão securitizada pode ser entendido como dessecuritização. Isso não significa que as participações ativas são desnecessárias, pelo contrário, não só são importantes, como levam em conta uma infinidade de elementos presentes no contexto em que ocorre ou se almeja a dessecuritização.

O processo de dessecuritização pode ser mais simples do que a securitização, no sentido de exigir menos esforço por parte dos atores mas, por outro lado, pode exigir a compreensão de uma realidade bastante complexa. Esse escopo amplo da dessecuritização dificulta o estabelecimento de regras ou de elementos necessários para o êxito ou o simples funcionamento do processo. Assim, olhar para a realidade onde sucede a dessecuritização, através de estudos de casos particulares ou até mesmo utilizando metodologias de análise de discurso, entre outras, é uma forma eficiente de entender os processos de dessecuritização e sofisticar teoricamente a dessecuritização bem como, pelo estudo do contexto em que se desenvolvem, ajuda a entender diferentes realidades e papeis dos atores nelas envolvidos.

Neste sentido, é interessante abordar alguns trabalhos que exemplificam as variadas dinâmicas de dessecuritização, para então, tendo em mente que os resultados não são universais e nem pretendem sê-lo, sugerir uma base teórica com elementos específicos para o estudo da securitização e dessecuritização envolvendo o ciberespaço.

Assim, Acikmese (2013), examinando o caso da securitização e dessecuritização das minorias curdas na Turquia ao fim da década de 1990, sugere que a dessecuritização tem ao menos dois aspectos-chave. O primeiro é o papel da União Europeia como agente externo que exerce pressão sobre a gestão turca desse dossiê. A pretensão da Turquia em tornar-se membro da União Europeia impõe, para Bruxelas, uma transformação na política interna,

> European membership conditionality has been an important mechanism for Turkey to undertake such democratic reforms that have undoubtedly contributed to the ongoing desecuritization processes; however, since security-speak on the Kurdish issue and Islamic activism has not faded away, the EU's desecuritizing role has remained limited (Acikmese, 2013: 302).

Mais do que isso, outro fator chave em determinada fase histórica foi a retirada do discurso que mantinha a securitização com o afastamento do governo e suspendendo as

restrições à liberdade de expressão. Isso propiciou uma mudança momentânea no contexto com maior pujança dos movimentos em favor da democracia.

O processo de dessecuritização das minorias curdas na Turquia e também em relação ao extremismo islâmico, identifica a União Europeia como um agente dessecuritizador neste processo. Esta dessecuritização foi, porém, muito limitada no tempo, pois que a subida ao poder de Erdogan e a relação que a União Europeia aceitou ter com o seu governo – designadamente no quadro do conflito na Síria e gigantescos fluxos de refugiados nele originados – trouxeram de volta uma intensa securitização do assunto Curdistão, que permanece até os dias de hoje.

Campana (2013), vê uma reconsideração do discurso ao redefinir as ameaças no caso das relações do governo russo com os chechenos e o islamismo extremista. A autora reconhece que o processo de dessecuritização neste caso não está concluído devido a dificuldades de articulação e coordenação do próprio discurso em diferentes governos (Dimitri Medvedev e Vladimir Putin).

A estratégia dos dois presidentes, após a segunda guerra da Chechenia, já na década de 2000, foi de mudar o discurso que via o terrorismo, proveniente de grupos da região, como uma ameaça, portanto, uma questão de segurança nacional. Como aponta o autora, o discurso elencando o terrorismo e medidas contra terroristas era um elemento que criava e sustentava a ideia de emergência. A estratégia passou pela modificação do discurso empregando termos-chave.

> "The focus of discourses has slowly changed from security threats and responses to a diagnosis highlighting structural factors. The link between socio-economic difficulties and violence dates back to Putin's second term as President. […] [o discurso empregado] began to broaden its approach, and the Regional Development Ministry was put in charge of designing a socio-economic plan for the region's development […] This new strategy intended to raise the effectiveness of counterterrorism operations: given the failure of repressive measures to prevent, deter and destroy "terrorist" groups, the focus was put on actions aimed at diverting potential recruits from joining terrorist ranks" (Campana, 2013: 463)

Esse discurso veio acompanhado de medidas práticas que são, segundo Campana, uma expressão das intenções de dessecuritização. Poucos meses depois do fim da guerra e das operações contra terroristas, o presidente Medvedev anunciou novas orientações que visavam tratar de questões estruturais que, de acordo com o discurso do governo, estavam mais ligadas às causas da violência. As medidas passaram a dissociar a região dos terroristas,

adotando uma perspectiva mais inclusiva dos cidadãos, enquanto combatia o terrorismo localizado.

Outro elemento de dessecuritização foi a mudança do discurso sobre o extremismo islâmico, fazendo com que este passasse de ameaça a um aliado no combate ao terrorismo. Neste sentido, a estratégia foi mobilizar os líderes religiosos para esse efeito, já que estes representantes desempenhavam um papel-chave no diálogo entre governos, setores da sociedade e esses grupos identificados como extremistas religiosos.

O processo de dessecuritização dos chechenos na Rússia é muito relevante porque evidencia o papel do governo em três frentes. Primeiramente enquanto ator securitizador quando apontava a urgência de medidas para fazer frente a uma questão de segurança cujo objeto de referência era a segurança nacional. Em segundo lugar, no processo de dessecuritização, o governo atua como ator da dessecuritização, quando começa adotar um discurso que visa a normalização da situação securitizada e, por fim, como ator funcional da dessecuritização, quando adota medidas para tanto. Importa ressaltar, porém, que embora tenha havido uma intenção clara de dessecuritização na interpretação da autora (Campana, 2013), não se pode afirmar que o processo tenha tido o êxito, já que como lembra, faltou um alinhamento nos discursos dos presidentes. Essas ambiguidades ou falta de alinhamento permite interpretações ambíguas que, ao fim do processo, como sugere a autora, dificulta a dessecuritização ou abre caminhos para uma ressecuritização dos objetos de referência.

Em suma, os processos de dessecuritização assumem uma condição particular em cada contexto e por isso estão abertos a diversas possibilidades, sempre em função dos instrumentos e atores envolvidos. O discurso e a audiência, tal como sucede nos processos de securitização, tem grande relevância, pois o processo em si continua a ser uma construção intersubjetiva. Contudo, nem sempre se percebe a participação ativa ou passiva das agências e audiências. Na falta de uma teoria que aponte os elementos básicos para a dessecuritização, a melhor maneira de construir um quadro conceitual consistente, bem como contribuir para seu aprofundamento é a análise de estudos de caso. É neste sentido que a parte seguinte examina a bibliografia existente centrada na questão do ciberespaço e também esse o sentido do estudo do caso brasileiro adiante apresentado.

2.6 Securitização e dessecuritização do ciberespaço

A crescente preocupação com as questões de segurança no ciberespaço, contribui, por si só, para um movimento de securitização. Documentos, a formulação de determinadas políticas, discursos e decisões de autoridades tem demonstrado e oferecido ferramentas para uma interpretação do ciberespaço como um objeto de securitização.

Em primeiro lugar, verifica-se a construção de um entendimento baseado em receios sobre futuros ataques ou atitudes ofensivas. Como alguns autores já mencionados apontaram, muitas das políticas para o ciberespaço assentaram em percepções ou antecipações do que pode ocorrer em termos de ameaças (Dunn Cavelty, 2013; Myriam Dunn & Elgin, 2007; Rid, 2012; Valeriano & Mannes, 2015). É claro que destacar que o fator psicológico caracterizado pelo reconhecimento da necessidade de proteção tem valor fundamental em um primeiro nível dos processos de securitização. Como apontam Craig e Valeriano (2016b),

> The role that psychology plays is especially important to factor into the study of the cyber domain given the fact that we have yet to witness a catastrophic computer network attack. Craig e Valeriano (2016b: 24)

Mais do que o aspecto psicológico individual e generalizado, a securitização do ciberespaço talvez ancore primeiramente em preocupações de segurança individual. A partir dela, gera-se um campo fértil para pressões políticas sobre os decisores ou atores funcionais. Como observa Buzan, (2008: 50),

> Most threats to individuals arise from the fact that people find themselves embedded in a human environment which generates unavoidable social, economic and political pressures. Societal threats come in a wide variety of forms, but there are four obvious basic types: physical threats (pain, injury, death), economic threats (seizure or destruction of property, denial of access to work or resources), threats to rights (imprisonment, denial of normal civil liberties) and threats to position or status (demotion, public humiliation). These types of threat are not mutually exclusive in that the application of one (injury) may well carry penalties in another (loss of job). (Buzan, 2008: 50)

De fato, os discursos e documentos que tratam de medidas ou políticas para a segurança do ciberespaço levantam, por exemplo, as possibilidades de interrupção de serviços essenciais controlados ou inteiramente dependentes da tecnologia da informação. As justificativas geralmente colocam as infraestruturas críticas como um grande conjunto que inclui várias vertentes essenciais, incluindo formas diretas de segurança mas também o funcionamento econômico, ou o bem estar social:

> systems and assets, whether physical or virtual, so vital to the [US] that the incapability or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. (Department of Homeland Security, 2013)

Deste modo, tendo um alvo que engloba tantos elementos dos quais há uma grande dependência e grande permeabilidade, a justificativa da proteção e do tratamento desses assuntos como uma questão de segurança nacional, eventualmente implementando medidas especiais torna-se mais factível. Pouco preciso ao mesmo tempo em que é abrangente, as políticas que apontam para a necessidade da implementação de medidas de segurança cibernéticas para as infraestruturas críticas tem sido um dos elementos que mais contribuem para um processo de securitização do ciberespaço justamente pela sua capacidade de envolver múltiplos setores entre os itens ameaçados. Naturalmente, nota-se que há uma disseminação dessa percepção de ameaças e da vulnerabilidade dos setores dependentes da tecnologia e, consequentemente, dos usuários e dependentes dos serviços que desempenham.

Neste sentido, cabe enfatizar outro aspecto central dos pressupostos da securitização. Faz-se notar que tantos os documentos oficiais quanto os pronunciamentos de autoridades relativamente a implementação de políticas de segurança no ciberespaço apresentam-se em um discurso alinhado, que apela a dois grupos de fatores ligados à segurança. O primeiro refere-se justamente à disseminação da ameaça, levando a ideia de que as ameaças do ciberespaço são elevadas à um nível generalizado de preocupação, já que dizem respeito a serviços e dependências comuns a toda a população. O segundo refere-se diretamente à segurança nacional ou a necessidade de proteção da soberania. A partir de então, os discursos apontam para uma tendência de especificação que concorda com o interesse de quem então porta-se como ator da securitização.

Mais do que apontar para processos de securitização, esses discursos refletem uma intenção, direcionada a um determinado objetivo. Tanto um aspecto mais generalista quanto o outro mais específico enquadram-se em uma perspectiva que inclui uma dimensão estratégica no discurso. Essa questão levantada por Balzacq (2005), na qual equaciona uma intenção estratégica e pragmatismo no ato discursivo, adiciona à securitização a ideia de estabelecer políticas ou medidas que conjuguem a necessidade de determinada audiência ao interesse do ator da securitização:

> […] the idea that securitization is a sustained strategic practice aimed at convincing a target audience to accept, based on what it knows about the world, the claim that a specific development […] is threatening enough to deserve an immediate policy to alleviate it. (Balzacq, 2005: 173)

A especificação de objetivos e interesses dos discursos e das políticas implementadas para questões do ciberespaço veem-se, aparentemente, refletidas nas diferentes configurações dos conflitos envolvendo o ciberespaço. A gramática utilizada nos discursos, a escolha do vocabulário usado na justificação e, naturalmente, as possibilidades de ação diante de uma situação de conflito no ciberespaço passam por uma influência mútua.

As aproximações entre a teoria da securitização e o ciberespaço já vêm sendo mencionadas por alguns autores. Buzan et al. (1998), referem-se à emergência do ciberespaço enquanto uma nova dimensão de análise de conflitos no século XXI. Contudo, limitam-se a citar os trabalhos de Der Derian (apud. Buzan et al. 1998: 137) e Nierop (apud Buzan et al. 1998: 163 – 164) para sustentar a argumentação de que as dinâmicas da globalização ainda estão ligadas a questões de segurança tradicionais, como o território e a militarização. Contudo, com o desenvolvimento tecnológico e a crescente dependência dessas tecnologias dos diversos setores sociais e infraestruturas, houve a necessidade de se estabelecer políticas e estratégias de segurança para o ciberespaço, o que coloca novamente este tema na pauta dos formuladores de políticas e decisores.

Buzan e Hansen (2009: 228), voltam a tratar o ciberespaço como um elemento de preocupação de segurança ligando-o ao contexto da segurança internacional após os ataques terroristas de setembro de 2001. Argumentam nesse sentido que a percepção de ameaças iminentes em diversos setores da segurança acaba também implicando uma espécie de securitização do ciberespaço e isso resulta em formulação de políticas específicas para este espaço. A ligação terrorismo-ciberespaço tornou-se, então, prioridade dos Estados na formulação das estratégias nacionais de defesa.

As políticas de promoção da segurança para o ciberespaço apresentam, por vezes, elementos que se aproximam o bastante de preocupações militares e de segurança econômica. Há, no entanto, uma gramática própria do setor da cibersegurança e especificam um processo de securitização. Segundo Hensen e Nissembaum (2009) , a securitização do ciberespaço apresenta três elementos essenciais: a) hipersecuritização: a tendência de exagerar as ameaças, para além dos elementos hipotéticos presentes em qualquer processo de securitização, e adotar medidas excessivas de segurança; b) as práticas de segurança cotidianas que mobilizam os atores da securitização usando a identificação da segurança do ciberespaço a problemas cotidianos, tornando os argumentos da hipersecuritização mais plausíveis e c) tecnificação, ou seja, construção da ideia de que o domínio deste campo está ligado a quem tem conhecimento técnico sobre o mesmo, sendo esses os responsáveis pela

segurança. Em resumo, o discurso da tecnificação acaba por legitimar a ideia de que "if cyber security is so crucial it should not be left to amateurs (2009: 1167). Nesse sentido, há uma aproximação do ciberespaço a questões técnico-militares. Cavelty (2012) argumenta que a delegação desse assunto aos militares acaba por imputar um sentido de urgência, mesmo que haja uma percepção não muito acurada dos riscos oferecidos por diversas ameaças.

Essa visão é reforçada pelo crescente avanço e complexificação dos ataques a estruturas do ciberespaço, por um crescente e cada vez mais sofisticado ativismo hacker ou espionagem virtual e pela atividade de Estados como a China que, de acordo com Ball (2011), classifica o ciberespaço como um domínio estratégico e tem feito esforços para equiparar seus recursos de defesa deste espaço ao dos Estados Unidos.

Assim, a militarização do ciberespaço relaciona-se com a securitização ao menos em duas formas. 1) A militarização decorre da securitização: quando a percepção de uma ameaça – ao ciberespaço ou deste proveniente – é entendida como uma questão de segurança nacional. 2) Quando a militarização do ciberespaço se aproxima da dimensão técnica da securitização do ciberespaço apontada por Hensen e Nissembaum (2009), como por exemplo, o US Cyber Command, do Exército estadunidense.

Levando em conta essa dimensão militar, Hare (2010) sugere que a securitização do ciberespaço tem relações com a coesão sociocultural de determinados Estados. O sistema elaborado pelo autor permite argumentar, por exemplo, que estados militarmente fracos e com pouca coesão social, ou seja, aqueles que não tem um setor militar suficientemente organizado e tampouco dispõe de uma população que compartilhe dos mesmos entendimentos quanto aos ocupantes do poder político, são mais propensos a securitizar o ciberespaço em comparação com os Estados militarmente fortes e socialmente coesos, com instituições internas eficientes. O modelo teórico de análise é interessante e poderia ser aplicado a diversos casos, no entanto, o autor opta por não o fazer.

A dessecuritização no ciberespaço é apenas mencionada em dois trabalhos. Assim, Erikson e Giacomello (2007: 71) ao sustentarem que não houve um movimento para a dessecuritização do ciberterrorismo durante o governo de Bill Clinton, nos Estados Unidos, porque não houve propriamente um movimento de securitização da questão. E Giacomello (2005) sugere que as iniciativas dos Estados Unidos e França, influenciados por interesses de setores comerciais, em regularizar o uso de softwares de encriptação por usuários comuns seria uma espécie de ´desecuritizing move´:

> […] The advocates of national security interests (law enforcement and intelligence agencies, the military) in both countries [United States and France] had warned against allowing individuals to use or freely distribute encryption software. In pursuing the implementation of restrictive policies for cryptography with policy-makers and government leaders, however, champions of national security met an unexpected and influential alliance of private business, consumer protection, and civil liberties organizations"

Tanto os textos que abordam a securitização do ciberespaço quando as menções sobre a dessecuritização carecem de uma sistematização teórica que dialogue com as bases propostas pela teoria da securitização em termos de identificação dos ´funcional actors´, ´securitizing moves´ e, em uma vertente mais sociológica, como o contexto e os interesses de diversos atores influem na securitização do ciberespaço.

A questão do discurso é necessariamente importante na avaliação da politização das questões do ciberespaço por duas razões essenciais. Primeiramente porque os atos discursivos figuram entre os as metodologias principais das Teorias da Securitização. Depois porque é também é um elemento do campo em si. Sendo um elemento etéreo, real, mas não físico ou visível de forma imediata, as justificativas para as políticas tendem a contar somente com a lógica discursiva. Neste sentido,

> It is not yet clear whether political discourse via cyber venues consists of a parallel mode of discourse or, alternatively, whether political discourse is assembled first in real venues and then exported or steered toward the cyber domain. Another hypothesis holds that the discourse is interactive across real and virtual domains and that the cumulative effects, if any, will be observed if they shape the outcomes of political behavior in real institutional contexts. (Choucri, 2012: 12)

Esses elementos e características dependem necessariamente do contexto em que são percebidos bem como das capacidades dos agentes da securitização de operacionalizá-los e dos atores funcionais em articular medidas de exceção. Assim, o entendimento da securitização do ciberespaço tem necessariamente de ser contextualizado em um determinado caso, apontando autores, contexto histórico e desdobramentos. É precisamente este o objetivo dos estudos de caso dos capítulos seguintes.

CAPÍTULO 3. O ciberespaço e a securitização: o contexto, o papel dos atores e o discurso no caso estoniano.

We live in a bad neighbourhood.
Being invaded by a big neighbour
to the east is scary ...
(Thomas Hendrik Ilves,
ex-presidente estoniano)

O foco deste capítulo é a análise do ataque cibernético à Estônia em 2007 interpretando-o através dos pressupostos teóricos das Teorias da Securitização, na intenção de que a análise de um caso empírico possa trazer elementos que testem – e eventualmente reforcem – a consistência desses mesmos pressupostos teóricos.

O caso estoniano não é só relevante por ser considerado um símbolo da equação segurança-ciberespaço emergente nas discussões acadêmicas contemporâneas. É também relevante porque é rico em termos de materiais e possibilidades de análise, já que o grande espaço que foi dedicado pelos média à sua cobertura, a importância atribuída pelas organizações internacionais e entidades ligadas a políticas de defesa e segurança, bem como as decisões e atuação do governo estoniano, proporcionam uma significativa fonte de elementos de análise do ponto de vista da política internacional e da disciplina de Relações Internacionais. O caso estoniano aparece frequentemente citado nos mais diversos trabalhos relacionados com o ciberespaço e a segurança internacional. Esta associação deve-se, em primeiro lugar, aos ataques cibernéticos sofridos pelo país em 2007. A imprensa chegou a caracterizar os ataques como "a primeira guerra cibernética", dados o relativo ineditismo e a visibilidade alcançada (Aaviksoo, 2010; Davis, 2007; Kaiser, 2015; Mansfield-Devine, 2012). Há, obviamente, discussões sobre o verdadeiro alcance dos ataques, sobre as motivações, sobre a gravidade e sobre a atribuição de responsabilidades (Karatzogianni, 2010). Não obstante, uma análise sob o ponto de vista das teorias da securitização requer uma análise que aponte não só os resultados, traduzidos em medidas, decisões e documentos, mas também os elementos considerados cruciais para a avalição de um processo de securitização.

Neste sentido, o que se impõe analisar no caso estoniano são justamente por esses elementos, ou seja, o contexto em que o país estava envolvido, as características sociais em relação à experiência da utilização das tecnologias da informação, os atores relevantes que

protagonizaram o incidente dos ataques bem como suas respectivas decisões, as relações externas com aquele que é tido como o responsável dos ataques (a Federação Russa) e, finalmente, os resultados dos ataques para as questões de segurança e de política externa. Com isso, cobre-se os aspectos propostos pela teoria, isto é, contexto, movimento de securitização, atores da securitização e atores funcionais.

O principal argumento que desenvolvemos neste capítulo é que o caso estoniano apresenta elementos de securitização em algumas medidas, mas não chega a configurar um caso pleno de securitização tal como propõe a teoria, algo que decorre da sutileza de ações pontuais. Essa "sutileza da securitização" aparentemente é uma característica deste processo no ciberespaço em lugares que não preveem juridicamente algum tipo de cerceamento do tráfego de dados e da informação. Na verdade, o caso estoniano parece indicar que a securitização do ciberespaço tende a ser incompleta em países que não securitizam a informação em si. Naturalmente, há outros elementos que dificultam o estabelecimento de um processo de securitização pleno e esses aspectos também serão analisados adiante.

No plano metodológico, considerámos como fontes primárias os documentos emitidos pelo governo estoniano e outras instituições internas. Sendo uma situação muito estudada no campo acadêmico, considerámos também os estudos e discursos tanto da comunidade acadêmica como da imprensa especializada e empresas de segurança cibernética. Analisámos ainda os documentos publicados, antes dos ataques de 2007. Mas, sendo neles patente que não se assumia a possibilidade de que ocorresse algo com o alcance e a gravidade que se vieram a registar, e sendo assim manifesto que teriam uma contribuição quase nula para o estudo a que nos propomos, entendemos não os considerar em termos finais.

3.1. Da "E-stonia" à Moscow Cyberwar

Desde o início da década de 1990, a Estônia começou uma política de desenvolvimento de sistemas eletrônicos que deixaria os serviços públicos e privados mais próximos e acessíveis aos seus cidadãos. Essa disseminação de recursos eletrônicos e a disponibilidade de serviços privados e estatais através dos meios digitais permitiria uma economia de recursos financeiros e humanos, sendo que estes últimos são especialmente difíceis em um país que conta com pouco mais de 1.300.000 habitantes (Estonia, 1998; European Comission, 2015; Vassil, Solvak, Vinkel, Trechsel, & Alvarez, 2016).

O resultado dessa política foi que, em pouco mais de duas décadas, a Estônia tornou-se uma das nações com maior número de usuários e serviços funcionando no ciberespaço em termos percentuais. Cerca de 98% das transações bancárias são feitas através da Internet, sendo a mesma largamente utilizada para pagamentos diversos, consulta de boletins médicos, e até mesmo eleições para o Parlamento Estoniano são realizadas parcialmente pela Internet. (Aaviksoo, 2010, Estônia, 2014).

Mas a dimensão dessa informatização e a grande penetração das tecnologias da informação nos serviços públicos e privados acabaram por ser também um causa de fragilidade para a Estônia. Como resumem Tikk, Kaskae Vihul (2010: 18),

> The high availability of public e-services and wide Internet accessibility that the Estonian population enjoys have, as negative side effect, also made the country more attractive target for cyber-attacks. The dependency of the population on easily accessible online services has made the society more vulnerable to large-scale disruptions in the availability of Internet access.

De fato, como o desenvolvimento digital tende a apontar prioritariamente para a eficiência em detrimento da segurança, a infraestrutura digital estoniana acabou por revelar uma vulnerabilidade imprevista e tornou a Estônia num dos Estados mais dependentes e, neste sentido, vulnerável, em termos de segurança das suas estruturas básicas.

Esses elementos já foram sistematizados por Valeriano e Maness em uma tabela onde se pode observar e comparar a capacidade cibernética em função da dependência da tecnologia, das capacidades de cibersegurança e da capacidade ofensiva de inflicção de ataques no ciberespaço. Os dados na Tabela que se segue foram obtidos através do número de menções desses Estados em diálogos envolvendo conflitos cibernéticos.

Tabela 1. Capacidades cibernéticas gerais entre Estados selecionados

País	Ciber Ofensa	Ciber Dependência	Ciber Defesa	Pontuação total
Irã	4	5	3	12
Grã-Bretanha	7	2	4	13
Estônia	**3**	**1**	**9**	**13**
Coréia do Sul	6	4	4	14
Coreia do Norte	3	9	2	14
Alemanha	7	2	6	15
Israel	8	3	4	15
Estados Unidos	10	2	5	17
China	8	4	5	17
Rússia	7	3	8	18

Fonte: Adaptado de Valeriano e Mannes (2015: 25)

Essa comparação é especialmente útil por dois motivos. Primeiramente, de forma geral, porque permite uma comparação entre os países em função das suas capacidades de defesa cibernética. Depois, no que diz especificamente respeito à Estônia, permite comparar sua posição não só em relação a outros Estados, mas também em termos internos, já que o país aparece ao mesmo tempo muito vulnerável (já que é bastante dependente dos recursos cibernéticos), mas ao mesmo tempo tem uma grande pontuação (a maior entre os Estados comparados) em capacidade de defesa. Esse retrato, segundo autoridades do Ministério do Interior Estoniano (*Siseministeerium*), reflete uma realidade posterior aos ataques já que a Estônia incrementou suas capacidades de defesa e cibersegurança, transformando-as em um elemento de excelência do país[27].

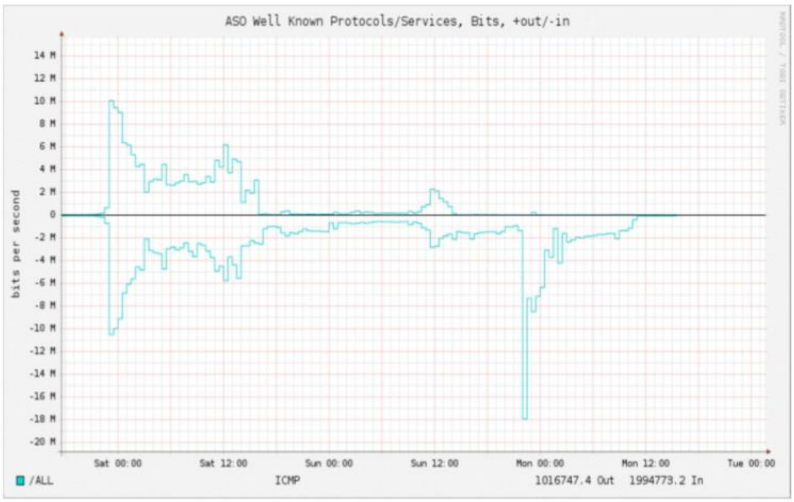
Foi neste contexto que, entre abril e maio de 2007, os sistemas cibernéticos estonianos foram atacados através de operações cibernéticas coordenadas e planejadas e atribuídas de maneira não conclusiva à Rússia (Kozlowski, 2014).

[27] Entrevistas realizadas a representantes do Ministério do Interior e da Defesa estonianos.

Por várias semanas, os estonianos ficaram privados do acesso a serviços e produtos que costumeiramente já se faziam através de plataformas digitais. De acordo com Hassan e Saleem (2009: 2), os ataques atingiram desde páginas de órgãos oficiais do governo e ministérios, a agências de notícias, bancos e a infraestrutura de comunicação. Entre os órgãos do governo diretamente afetados estavam o sítio oficial do Governo, o do Primeiro Ministro e do Presidente, do Parlamento, Tribunal de Contas, agências governamentais como a Polícia, todos os ministérios[28]. Entre os serviços privados, o mais afetado foi o setor bancário (SEB, Eesti Ühispank, Hansapank), das telecomunicações, incluindo fornecedores de serviços de Internet (Elion Ettevõtted, Elisa Andmesideteenused, Starman, ee.ee, Zone.ee), e a imprensa (Postimees, Delfi, EPL, Baltic News Service (Tikk et al., 2010: 22).

Os ataques seguiram a estratégia da negação de serviço, ou DDoS, já mencionada anteriormente. Ou seja, utilizando computadores infectados mundo afora, os autores dos ataques conseguiram inundar os servidores estonianos mencionados acima de modo a provocar uma sobrecarga da capacidade dos mesmos impedindo o funcionamento. Os estudos de Hassan e Saleem (2009: 3), que recorrerem essencialmente a dados técnicos quantitativos, permitem uma percepção visual do ataque. É importante ressaltar que os ataques não foram contínuos, mas aconteceram em fases o que Tikk et al. (2010) chamam "fases" (I e II) e "ondas" (4 delas na fase II)

Gráfico 4. Evolução do tráfico de dados no período dos ataques cibernéticos de 2007



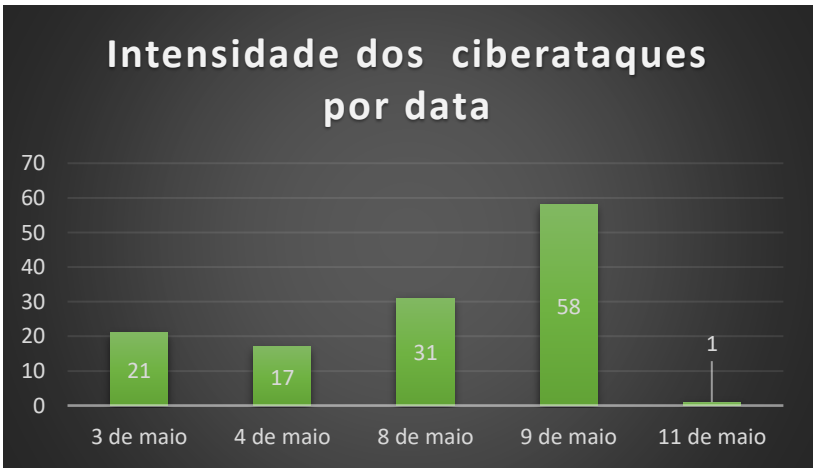
Fonte: (Hassan & Saleem, 2009: 3)

[28] Curiosamente os ataques pouparam o Ministério da Cultura.

A monitorização do tráfico de dados na primeira fase dos ataques (27 a 30 de abril de 2007) mostra um acentuado aumento no número de acessos aos servidores estonianos, o que sobrepôs sua capacidade de resposta. Esta fase, de acordo com Tikk et al. (2010) caracterizou-se por ataques relativamente simples e pouco organizados, apesar de terem sido eficientes em impedir o funcionamento de páginas do governo estoniano. Investigações posteriores identificaram que instruções para os executar eram fornecidas em fóruns de origem russa, ou de língua russa. Também eram oferecidos os códigos e ficheiros necessários para processar os ataques.

A segunda fase dos ataques ocorreu entre os dias 30 de abril a 18 de maio de 2007. Diferente da anterior, nesta fase os ataques revelavam uma coordenação mais eficiente, sendo programados para afetar os sistemas em determinadas horas, gerando um volume maior de acessos. Algumas características dessa fase contribuíram para sua atribuição à Rússia. Assim, a organização, coordenação e eficiência dos ataques apontam para uma estrutura grande o suficiente para executá-los. Embora o recurso de distribuir códigos e divulgar instruções através de fóruns se tenha mantido, a articulação dos ataques denotou uma coordenação dos horários e volume de acessos. Em certos momentos de caráter simbólico, como o dia 9 de maio (Dia da Vitória, na Rússia), os ataques remetiam para o horário de Moscou. Esta data é também a que contabiliza o maior número de ataques. Os gráficos abaixo oferecem um perfil dos ataques cibernéticos na segunda fase (Beatrix Toth, n.d.; Jenik, 2009; Kozlowski, 2014; Jose Nazario, 2007; José Nazario, 2009; Reigas, 2008; Tikk et al., 2010).

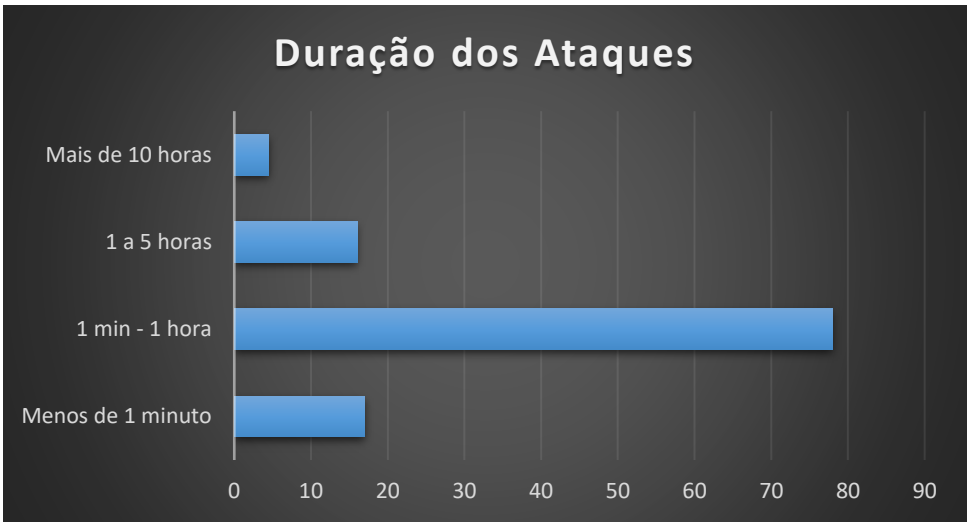
Gráfico 5. Intensidade dos ciberataques por data



Fonte: Adaptado de (Hassan & Saleem, 2009; Jose Nazario, 2007)

A duração dos ataques também é determinante para a compreensão da dimensão e da complexidade dos recursos utilizados e indica uma coordenação eficiente.

Gráfico 6. Duração dos ataques cibernéticos



Fonte: Adaptado de (Hassan & Saleem, 2009; José Nazario, 2009)

As respostas aos ataques vieram de, pelo menos, duas frentes. A primeira, com um caráter técnico, veio do Computer Emergence Response Team (CERT-EE) ou Estonian Information Response Team[29]. A estratégia consistiu, em primeiro lugar, em aumentar rapidamente a capacidade dos servidores informáticos estonianos, depois identificar e separar os acessos reais dos que estavam sendo usados para inviabilizar o sistema e, por fim, neutralizar os acessos invasores. Nesta última etapa, a resposta exigiu a cooperação com organismos internacionais e principalmente técnicos altamente capacitados da comunidade internacional, nomeadamente os Vetted[30]. Em operações conjuntas entre o Riigi

[29] O sistema CERT (Computer Emergence Response Team) é um grupo de especialistas responsáveis por tratar de incidentes ligados à segurança cibernética e prestam serviços tanto a instituições públicas quanto a empresas privadas, inclusive pode ser uma divisão interna de ambos as esferas. Podem ser requisitados quando ocorre uma emergência ou pode ser um grupo formalizado entre as instituições de segurança de um determinado país. No caso Estoniano, o CERT-EE, atende sob o nome de Riigi Infosüsteemi Amet (RIA), ou Information System Authority foi organizado como uma divisão estatal em 2011 e está ligado ao Ministério dos Assuntos Econômicos e das Comunicações, que passou a ser responsável pelas questões relativas à informação eletrônica. O RIA coordena o desenvolvimento e administração da informação estatal, organiza atividades relacionadas à segurança da informação, presta assistência em caso de incidentes informáticos e presta consultoria e cooperação externa. (Information System Authority, n.d., Entrevista com representante do RIA)

[30] The Vetted, um pequeno grupo de informáticos responsáveis por 13 servidores localizados em diferentes partes do globo capazes de direcionar o tráfico de dados mundial. Os Vetted têm a capacidade e autoridade para identificar dispositivos informáticos intrusos e removê-los do tráfico mundial. Coincidentemente, segundo Ruus, (2008) três membros desse grupo, um americano e dois suecos, encontravam-se em Tallinn na ocasião dos ataques. (Davis, 2007; Poulsen, 2007, Entrevistas a membros do RIA, Ministério da Defesa e Centre for International Defense Studies)

Infosüsteemi Amet (RIA) e participantes internacionais, o tráfico de dados foi controlado, permitindo inviabilizar os acessos intrusos e normalizar o acesso a serviços (Dubroff, 2009; "Estonia hit by 'Moscow cyber war,'" 2007; Joubert, 2012; Poulsen, 2007; Ruus, 2008, Entrevistas realizadas a respresentantes do Information System Authority, Ministério da Defesa, Ministério do Interior, Centre for Internationa Defense Studies).

A segunda frente de resposta teve uma natureza eminentemente política. Uma das primeiras decisões foi tornar a extensão e a gravidade dos acontecimentos em algo público e, com isso, fomentar uma discussão mundial sobre as direções e necessidades de políticas para a defesa e segurança cibernética e com isso, pressionar aliados a estabelecerem novos princípios para uma mudança de doutrina e para a cooperação multilateral. Isto porque, como classifica o Ministro da defesa Estoniano, Jaak Aavikso, embora os ciberataques de 2007 não tenham sido os primeiros, são significativos por serem sofisticados e politicamente orientados (Aaviksoo, 2010).

Foi assim possível forçar um debate sobre políticas envolvendo a cibersegurança, desde a criação ou aprimoramento de sistemas de defesa até sanções a Estados que se envolvessem em ataques a estruturas digitais de outros Estados. Nesse contexto, chegou a ser considerada a invocação, pelo ministro da Defesa, Jaak Aviksoo, da aplicação do artigo 5 do Tratado de Washington[31] ao ciberespaço (Davis, 2007), sendo depois descartada, uma vez que os danos não foram considerados substanciais o suficiente (Wolff, 2014).[32] Um ano mais tarde, em abril de 2008, a NATO adotou a Política para a Ciberdefesa, criando, em Bruxelas o Cyber Defense Management Authority (CDMA)[33.] Em agosto desse mesmo ano, a capital estoniana passou abrigar o NATO Cooperative Cyber Defense Centre of Excellence (CCD-COE)[34].

Os ataques perpetrados contra a infraestrutura estoniana representam um marco relevante para as estratégias de defesa contemporâneas. Ainda que o país não conte com

[31] Através do Artigo 5 do Tratado de Washington, os países-membro da Aliança Atlântica concordam que um ataque militar direcionado a um dos membros é considerado um ataque a toda organização. Essa qualificação legitima a tomada de ações coletivas, invocando o artigo 51 da Carta das Nações Unidas que reconhece o direito de legítima defesa a um país atacado. (NATO, 1949)

[32] Contudo, segundo informação coletada em entrevista a representantes do Ministério da Defesa, a evocação ao artigo 5 nunca foi necessariamente cogitada pelo Ministério da Defesa, mas sim chamar a atenção para uma situação que na altura não estava contemplada pelo Tratado de Washington.

[33] O CDMA é um esforço em conjunto na intenção de funcionar como um centro coordenador para respostas dos estados-membros a cyber ataques. Entre as funções desenvolvidas ali, os estados-membros podem contar com monitoramento em tempo real para identificar e compartilhar conhecimento sobre ameaças provenientes do ciberespaço (Hughes, 2009).

[34] A criação e o papel do CCDCoE será explorada com maiores detalhes adiante, quando se aborda as consequências práticas dos ataques cibernéticos à Estônia.

grande representatividade em termos de população ou de peso econômico, os ciber-ataques tornaram-se um ponto de inflexão na política estratégica de defesa tanto da União Europeia, quanto da NATO. A Estônia, tornou-se, de fato, referência nesta área para os demais países tanto da NATO quanto da UE em vários aspectos. Essa postura deve-se, em parte, à atitude do governo estoniano em adotar uma conduta de transparência pública em relação aos ataques, principalmente na política externa, em assumir um papel de pioneirismo e excelência nas questões de segurança cibernética.

3.2. ...a combinar com os russos...[35]

Os eventos envolvendo os ataques cibernéticos sofridos pela Estônia em 2007 não puderam ser traçados ao ponto de identificar quem esteve por trás dos mesmos, com provas suficientemente consistentes para iniciar algum tipo de medida mais coercitiva ou de retaliação. De fato, um dos grandes problemas da criminalidade perpetrada em ou através de tecnologias da informação é a clara atribuição e a devida responsabilização de um ato hostil a um perpetrador concreto (Brenner, 2007; Rid & Buchanan, 2014; Ron Keys, Solutions, Winstead, & Simmons, 2010). Há sempre pistas deixadas pelos agressores, mas estas nem sempre levam aos verdadeiros iniciantes dos ataques. Assim, ainda que não seja possível traçar com nitidez o caminho de ciberataques, uma análise do contexto político e social pode oferecer informações mais relevantes para o apuramento de um determinado evento. Ainda que pistas de ciberataques levem a computadores administrados por entidades governamentais, a atribuição de culpa ou responsabilidade ainda é vaga, já que criminosos cibernéticos podem mascarar a identidade de suas redes. Assim, mesmo o *Tallinn Manual of International Law Applicable to Cyberwarfare*, aponta que

> The mere fact that a cyber operation has been launched or otherwise originates from governmental cyber infrastructure is not sufficient evidence for attributing the operation to the State**,** but is an indication that the State in question is associated with the operation**.** (Schimidt**,** 2013: 34)

[35] No mundial de 1958, o treinador da seleção brasileira preparou um plano um tanto complicado e de difícil execução contra a seleção russa, com a qual disputaria uma partida decisiva. Ao ouvir a explicação do técnico, o jogador Garrincha, uma das estrelas da equipe à época, avaliando a impossibilidade de êxito da estratégia perguntou ao técnico: "mas o senhor combinou com os russos?" Desde então, a expressão tem sido usada em referência a algo bem planejado, mas que certamente não funcionaria devido à sua complexidade.

No caso estoniano, as movimentações, as características dos ataques, as investigações policiais e o envolvimento histórico-político apontam para uma participação da Rússia nos ataques, ainda que por circunstâncias técnicas não tenha sido possível comprovar completamente, com a devida eficiência, o seu envolvimento. Consideramos, no entanto, relevante ressaltar alguns elementos pelos quais foi possível a associação da Rússia aos ataques à Estônia. Esse passo é especialmente importante para uma análise sob o ponto de vista da securitização, já que os movimentos de securitização valem-se de diversas associações, entre elas políticas e culturais (Balzacq, 2005a).

A Estônia, não só por sua localização geográfica, mas também pelo seu histórico recente, apresenta uma considerável proximidade relação à Rússia, embora, como é sabido, tenha se distanciado a partir da década de 1990. Uma das heranças da inclusão na União Soviética é justamente o fato de uma porção considerável da população ter o russo como primeira língua. Essa população soma mais de trezentas mil pessoas[36], ou seja, aproximadamente um terço da população estoniana e guardam, para além da língua, estreitos laços culturais com o vizinho (Dougherty & Kaljurand, 2015; Zakem, Saunders, & Antoun, 2015). Esses laços culturais têm resistido às tentativas do governo estoniano em melhor integrá-los na sociedade através de modelos de integração baseados no estreitamento das relações entre os grupos étnicos através de diálogos, com certa ênfase na integração linguística e estratégias de comunicação (Włodarska-Frykowska, 2016). A verdade é que essas políticas colidem, por vezes, com a política externa da Rússia e suas estratégias de *soft power*, que inclui a mobilização de minorias étnicas e compatriotas russos que vivem para além das fronteiras da Federação. Este exercício continuado de soft power inscreve-se, como tem sido abundantemente estudado [37], numa ação mais ampla de política externa da Rússia a partir do fim da União Soviética, mais evidente a na década de 2000 em diante, com uma busca por fortalecer sua área de influência sobre as antigas repúblicas soviéticas, hoje estados independentes que geralmente apresentam resistência às configurações políticas do passado. Essa postura da Rússia ganha linhas bastante definidas com a anexação da Criméia em 2014, mas apresenta-se também de outras formas, ora mais dura, ora mais suave (Casula, 2014, 2017; Wijk, 2015). E é nesse esforço para a reconquista da influência em regiões onde fora hegemônica que se inclui a ênfase nos laços culturais remanescentes da era soviética.

[36] De acordo com o instituto de estatística estoniano, em 2016 o país contava com 330.263 cidadãos de etnia russa, número que, estatisticamente, tem decrescido no último quinquénio, ainda que levemente, acompanhando uma tendência geral da população estoniana (fonte: Eesti Statistika, www.stat.ee).
[37] Alguns trabalhos de referência neste assunto são: Freire (2009, 2015); Freire & Kanet (2012); Laenen (2012); Loftus & Kanet (2015); Simão (2011, 2012)

Uma das maneiras de implementar sua zona de influência é projetar ou resgatar a imagem de grande potência dominante em um nível primeiramente regional, mas com objetivos globais.

Como Zakem et al. explicam,

> In seeking to influence the former Soviet region, Russian compatriots can be useful to Moscow in many ways. Their very existence strengthens Russia's argument that there is a "Russian world" (Russkiy mir) larger than Russia itself that lends legitimacy to both Russia's great power status and its regional aspirations. To the extent that they identify with Russia not only culturally but also politically, Russian compatriots can amplify Russia's political influence in the former USSR and provide political, economic, and military intelligence. Where they are alienated from governments in their countries of residence—a condition to which Moscow can contribute—their alienation from their own governments creates latent potential for unrest and another possible lever. Protecting compatriots is also politically useful both at home, to rally support, and internationally, where it can benefit Russia's public diplomacy. (Zakem et al., 2015)

Ora, no caso específico, esse aspecto não só esbarra na política de outros Estados, principalmente os que estavam sob a esfera de influência da antiga União Soviética, como têm ligações diretas com os ataques cibernéticos à Estônia em 2007. No que se refere à Estônia, essa política de fortalecimento da identidade e aproximação dos compatriotas russos têm nos ciberataques de 2007 e no contexto que envolve essa operação uma das suas faces mais visíveis.

As entrevistas que efetuámos junto a autoridades ligadas a instituições e autoridades que se relacionam à segurança cibernética estoniana, entre outras de caráter mais político, como o Ministério dos Negócios Estrangeiros, indicaram que as investigações sobre os ataques apontavam para o vizinho russo. Ouve-se comumente uma outra pergunta como resposta: "Quem mais poderia ter sido?". Embora alguns dos entrevistados reconhecessem a dificuldade de atribuição dos ataques, consideram que as provas são suficientemente fortes para que eventuais dúvidas sejam mitigadas. Mais do que isso, os entrevistados do Ministério do Interior, do CERT-EE e de Centros de Investigação, como a Universidade de Tallinn e o Centro de Estudos para a Defesa e Segurança dão conta de que, dias antes, havia certa movimentação em blogs de origem russa comentando a possibilidade de ataques. Ainda segundo alguns entrevistados das entidades mencionadas, alguns rastreios permitiram verificar que havia computadores do governo da Rússia sendo utilizados nos ciberataques. Por sua vez, as autoridades russas se recusaram a cooperar quando chamada a colaborar para

as investigações, de acordo com os entrevistados. Negaram também qualquer responsabilidade para com os ataques e se negaram.

De fato, essa atribuição que os entrevistados fazem à Rússia vem ancorada em algumas percepções ligadas ao contexto estoniano. Ruus (2008) apresenta um breve contexto do momento imediatamente anterior aos ciberataques. Neste momento, já se percebia um movimento que previa oposições e choques entre medidas do governo estoniano e a posição da Rússia. Ainda que não houvesse indícios de posições mais agressivas, o caráter simbólico da ocasião parece ter sido suficiente para desencadear manifestações, tumultos e posteriormente os ciberataques.

> […] in the early months of 2007, as Moscow started becoming more combative toward the EU, notably over gas supplies, Tallinn's Unknown Soldier started to become a focal point for anti-Estonia activists – often angry and violent. Alarmed by the trend, the Estonian government decided that a military cemetery would be a more appropriate place to memorialize the Red Army dead. After extensive public debate, the statue was relocated there at dawn on April 27th.
>
> […]
>
> The attack on Estonia's Internet systems began in the hours before midnight on April 26, 2007. Estonian-Russian relations had been brewing with bitter tensions for weeks, and that morning rioting had erupted in Tallinn […] The man who started Cyber War I was not a Russian rioter or hacker, but a bronze statue in the old city center. […] A symbol of foreign occupation, it was never popular: Estonians dubbed it the Unknown Rapist. It was a gathering place for Red Army soldiers and their compatriots in the 400,000-strong minority community of ethnic Russians, sometimes for boisterous occasions celebrating Soviet holidays. But over the decades, Estonians tolerated the downtown monument on the grounds that the Russian community also needed a place to commemorate their fallen. (Ruus, 2008)

Sublinhe-se que, desde os ataques cibernéticos à Estônia, a Rússia tem sido apontada como a principal responsável por outros ciberataques, principalmente os perpetrados contra as ex-Repúblicas soviéticas. A tabela abaixo ilustra o histórico de acusações de envolvimento russo em ciberataques a países a vizinhos.

Tabela 3. Acusações de envolvimento russo em ciberataques

País	Ano	Tipo de ataque	Alvos
Bielorússia	2008	DDoS	- Empresas de comunicação (Radio Free Europe)
Estônia	2007	DDoS	- Órgãos governamentais - Bancos - Imprensa - Comunicação governamental - Sistemas de pagamentos
Georgia	2008	DDoS Injeção de SQL[38]	- Websites governamentais - Imprensa - Instituições financeiras - Empresas - Instituições Educacionais
Letônia	2013	Cyber Vandalismo[39]	- Websites do governo - Sites de empresas de comunicação
Lituânia	2008	DDoS Cyber Vandalismo	- 300 websites entre governamentais e comerciais
Quirguistão	2009	DDoS	- Servidores de Internet - Comunicação
Ucrânia	2015 - 2017	DDoS	- Infraestruturas críticas (Sistemas de energia)

Fontes: Arquilla, 2013; Ashmore, 2009; Fisher, 2017; Hales, 2008; Kozlowski, 2014; "Lithuania cyber attacks: Round two," 2008; Markov, 2009; McLaughlin, 2008; Press, 2013; Stephens, 2008; Sytas, 2016; Thorne, 2017; Wirtz, 2015; Zetter, 2016

Apesar de existir um padrão nas denúncias, geralmente apontando instituições que promovem um certo afastamento dos países da zona de influência da Rússia, como é o caso da Bielorrússia (Ashmore, 2009; Associated Press, 2013; Stephens, 2008), ou de tensões que levantam questões de identidade, como a própria Estônia e Lituânia (Hales, 2008b, 2008a; McLaughlin, 2008), ou ainda como complemento a operações militares, como na Ucrânia (Wirtz, 2015; Zetter, 2016) e Geórgia (Arquilla, 2013; Kozlowski, 2014), a Rússia ainda é

[38] Injeção de SQL ou *SQL Injection,* é uma tipo de ação que aproveita-se das falhas de segurança em sistemas que compartilham dados. O perpetrador do ataque consegue inserir códigos através da manipulação de dados por meio de uma aplicação.

[39] O vandalismo cibernético é caracterizado por ataque a sites impedindo seu funcionamento através de ataques de negação de serviço (DDoS), adulteração de sites, entre outras ações não específicas que impedem o bom funcionamento das infraestruturas de comunicação digital.

acusada de praticar operações cibernéticas contra os Estados Unidos[40] (Nakashima, 2016; Schmidt & Sanger, 2016) e, igualmente, à França[41] (Borger, 2017; Satter, 2017).

A grande motivação da Rússia para os ataques à Estônia não foi, obviamente, uma simples retaliação pelo ato da mudança de uma estátua símbolo da Rússia do centro de Tallinn para um lugar menos nobre. Pelo contrário, reflete uma estratégia histórica de tentar desestabilizar governos que se tentam se distanciar da esfera de influência da Rússia. Como percebe Blank,

> "By disrupting and possibly unhinging the Estonian government and society, and by demonstrating NATO's incapacity to protect Estonia against this novel form of attack, the cyber attacks aimed to compel Estonia to consider Russian interests in its policies". […] In Estonia, […] the attack may have reflected not only an effort to correct Estonia's behavior or influence its orientation but also a desire to punish it and deter others from following suit by making it an example of the risks to anyone who crosses Russia (Blank, 2017: 86).

Ainda que não se possa indicar precisamente os perpetradores de ataques cibernéticos, por um lado, mesmo que se considere um suposto filtro de interesse dos governos afetados por ciberataques em culpar os russos, nota-se que há um grande número de elementos, desde questões de identidade à uma política externa mais agressiva, que os coloca como primeiros suspeitos, seja por promover os ciberataques ou por não coibir essas práticas. Tais fatos deixam claro que ataques cibernéticos com alvos específicos tem se tornado rotina no atual cenário e, consequentemente, objeto de análise para as Relações Internacionais e analistas de política externa.

É possível perceber que, de acordo com as incidências de ataques cibernéticos atribuídos à Rússia, na tabela acima, há uma espécie de "conflito suave", em que não há o emprego de força.

---

[40] Recentemente, com as eleições presidenciais nos Estados Unidos, o comitê do Partido Democrata, que perdeu o pleito, acusou os russos de invadir seus computadores e divulgar informações que vieram a favorecer o candidato opositor, Donald Trump, vencedor da disputa. Em resposta, enquanto presidente americano, Barack Obama, mostrou sua insatisfação através de procedimentos e sanções diplomáticas. Tal ação, na ocasião, foi ignorada pelo governo russo.

[41] O caso francês, apesar de ainda encontrar-se em investigação, teve menor repercussão. Diferente do americano, o grupo atacado foi o vencedor das eleições. O ato chamou atenção para a atuação do governo russo, ainda que não fosse comprovadas as ligações, foi acusado de ter patrocinado o vazamento de cerca de 20 mil emails relativos à campanha de Emmanuel Macron que se defendeu afirmando que os emails foram adquiridos e disseminados de maneira fraudulenta e que entre eles foram adicionados documentos falsos com o intuito de desinformar(AFP, 2017: online).
Não obstante, com as denúncias de invasões e vazamentos de dados, o governo holandês decidiu que a contagem dos votos em suas eleições seria através da tradicional contagem manual (Chan, 2017) e o governo alemão decidiu reforçar suas estruturas de defesa cibernética alegando abertamente um receio de ataques russos (Barker, 2017).

Essa diferenciação entre os ciberataques russos, de um lado, e a simples intensificação/dramatização de uma diferença étnica ou um conflito tradicional, do outro, está patente no caso dos ataques à Estônia em 2007.

Primeiramente, apesar de existir, como foi exposto, uma minoria étnica de origem russa com importante representação na Estônia, essa relação não tem gerado problemas que conduzam a conflitos internos. Pelo contrário, apesar de essas minorias guardarem estreitos laços com suas origens, há, como já referimos, esforços por parte do governo estoniano em formular políticas de inclusão dessas minorias, em vários aspectos sociais (Institute of International and Social Studies, 2008), desde o final da década de 1990 (Poleshchuck, 2009). Para além disso, esses segmentos da população estoniana, no geral, exprimem uma aprovação em relação às instituições de defesa e segurança (Kivirähk & Jermalavicius, 2014). Apesar dos esforços do governo, essas diferenças étnicas foram ressaltadas no episódio da remoção do monumento do Soldado de Bronze do centro de Tallinn, ainda que, segundo a percepção de autoridades e funcionários de instituições públicas que entrevistámos para esta dissertação, essas diferenças não configuram um elemento crítico para o estabelecimento de um conflito. Apesar dos ciberataques e os distúrbios serem eventos correlacionados em um quadro mais amplo, os esses últimos foram entendidos pelo governo e pelas instituições de segurança como um episódio pontual[42].

Por outro lado, os ciberataques são abertamente reconhecidos como conflitos pelos entrevistados. Ao mesmo tempo, os entrevistados reconhecem que o conflito obedece a certos aspectos que o fazem especial, já que, em primeiro lugar, não há o emprego de armas de destruição, não se pode atribuir as ações ao governo russo, nem ao menos verificar se houve o apoio direto do governo russo. Mais do que isso, não houve a exposição de um objetivo claro que justificasse tal posição. Por outro lado, a coordenação dos ataques, a recusa dos russos em colaborar tanto com as investigações em relação aos ciberataques quanto em relação às ameaças e agressões que a embaixada estoniana em Moscou estava sofrendo ao mesmo período dos ataques.

De todo o modo, apesar do problema da atribuição, o nível de organização dos ataques, a precisão e a duração revelam um planejamento estratégico bastante centralizado. Assim, devido ao contexto histórico e diplomático entre Estônia e Rússia ligam-se as agressões digitais a uma ação estratégica do governo russo que se aproveitou das datas

[42] Entrevistas concedidas por funcionários designados pelo Ministério dos Negócios Exteriores e pelo Ministério do Interior Estoniano.

comemorativas e de uma ação específica aparentemente de pouca importância – a transferência de um monumento - tomada pelo governo estoniano e da opção estoniana em adotar um estilo de vida que recorre quase que completamente à entrega de serviços eletrônicos para lançar um ataque profundamente desestabilizador do Estado e da sociedade estonianos.

Naturalmente, a classificação de um ataque digital como um conflito internacional ainda é um tema em discussão e os documentos que pretendem estabelecer os requisitos para a classificação de um conflito cibernético, como por exemplo, o *Tallinn Manual on the International Law Applied to Cyberspace* (Schimidt, 2013), por hora não contam com o reconhecimento oficial de organizações internacionais tampouco de países. Contudo, a classificação dos ciberataques à Estônia como um conflito cibernético servem a este país como uma alavanca de inserção internacional. De fato, várias das autoridades estonianas por nós entrevistadas classificam como uma decisão acertada do seu respectivo governo (em alguns casos, dizem guardar até um certo orgulho) em tratar a questão de uma forma aberta e indicar o conflito no ciberespaço como um tema de emergência para a segurança internacional, no qual a Estônia assumiu algum protagonismo. Em suma, os elementos que envolvem o ciberataques à Estônia em 2007 não só permitem entendê-lo como um ciberconflito como também facilita sua compreensão em termos estratégicos e de análise de política externa.

A soma desses elementos – desentendimentos diplomáticos, o apelo à identidade, a necessidade e a dependência do bom funcionamento das tecnologias da informação e o entendimento dessas falhas como uma questão que ameaça a segurança nacional – favorece um discurso de securitização. Esses movimentos de securitização na Estônia serão analisados a seguir.

3.3. A securitização através dos discursos: desdobramentos e objetivos

Voltemos um pouco atrás. Como salientámos no capítulo 2, os atos discursivos constituem uma peça-chave para os movimentos de securitização. Os discursos, por sua vez, levam em conta os elementos presentes no contexto de modo a criar uma narrativa coerente que sirva de base para, ao fim, levar à adoção de medidas especiais ou de exceção. Para que

seu fim seja cumprido, ou seja, para que o convencimento de uma audiência alargada tenha lugar, é essencial que os discursos deem o destaque devido aos elementos mais sensíveis do contexto no qual se insere.

Ora, o que pretendemos argumentar, tendo em conta o caso concreto dos ciberataques à Estônia em 2007, é que nem sempre as medidas de exceção são o objetivo dos atores da securitização e tampouco do agente funcional. Esse aspecto é central nas elaborações teóricas da Escola de Paris da Securitização. Há nelas um distanciamento das medidas de exceção em favor do entendimento da construção do objeto de referência. Assim como percebeu Balzacq (2005; 2011), os discursos securitizadores nem sempre têm como objetivo a constituição de medidas de exceção. Deste modo, um movimento de securitização pode ser a base ou um instrumento para atingir objetivos ou justificar uma agenda em que não seja pretendida uma quebra da ordem.

É, por isso, fundamental analisar os eventos dos ciberataques não só até sua resolução imediata, mas também seus desdobramentos e contabilizar os direcionamentos e ganhos para a política interna e externa estoniana. Para tanto, faz-se necessário levar em conta pronunciamentos de autoridades estonianas e altos quadros ligados ao tema da cibersegurança no país.

Com este objetivo em mente, alguns elementos devem ser considerados como guias para avaliar os discursos que se seguem. Primeiramente, busca-se identificar elementos propostos pela teoria da securitização: os discursos devem ser claros ao apontarem os elementos essenciais, como os agentes funcionais e os objetos de referência – como os discursos vêm de autoridades estonianas com poder de tomar decisões, podem ser eventualmente tomados como agentes funcionais, contudo, são limitados ao papel de agentes da securitização. Em segundo lugar, para além desses elementos propostos pela formulação teórica, busca-se também analisar as referências ao contexto estoniano nos discursos e a que audiências foram direcionados. Em terceiro e último lugar, outro elemento derivado que será considerado é a identificação das ameaças que fechariam o ciclo apontando para o já mencionado objeto de referência. Deste modo, tem-se um leque de identificação de cinco elementos principais: a) objeto de referência; b) agentes da securitização; c) contexto da formulação do discurso; d) ameaças; e) eventuais soluções para os problemas.

A urgência provocada pelos ataques cibernéticos foi resolvida recorrendo a especialistas em tecnologia da informação, sendo estes do campo técnico. Tal postura, vem a corroborar o que Hensen & Nissenbaum (2009), identificaram como “tecnificação”, um

espaço criado e restrito a um discurso técnico e especializado. Neste caso, antes mesmo de discursos que pudessem justificar qualquer determinação política, houve primeiramente a ação direta de interveniente técnicos, na expetativa de que o problema gerado pelos ataques fosse tecnicamente resolvido.

No entanto, superando claramente essa "tecnificação", o episódio de 2007 suscitou debates com um alcance muito mais amplo, tornando-se objeto concreto da política de defesa e da política externa, colocando a Estônia não só como vítima de um ataque internacional, mas também como um país capaz de fazer frente a esses novo desafios. Neste sentido, o próprio discurso do então ministro da defesa estoniano, Jaak Aaviksoo, ao falar para uma plateia de especialistas e autoridades em segurança internacional, em 2008, demonstra e resume esse caminho:

> The aim of cyber-attacks as well as its unprecedented size can thus be defined as an attack against an Estonian way of life. It is clear that without having applied timely and imminent countermeasures the situation could have turned much worse and posed a significant risk to our national security. In essence, cyber-attacks against Estonia demonstrated that Internet already is a perfect battlefield of the 21st of century. Our globally increasing dependence on Internet, on-line services and on critical information infrastructure makes us all also more vulnerable. As demonstrated by events in Tallinn, an effective political propaganda can motivate a significant number of people to launch a massive cyber-attack almost instantly thus inflicting potential damage to critical information infrastructure even in case of *ad hoc* and amateur level attacks. (Aavksoo, 2008)

É interessante ressaltar que o discurso do ministro refletiu, relativamente pouco tempo depois dos ataques, vários elementos correspondentes a um movimento de securitização, desde logo, o objeto de referência ameaçado. Tanto de uma maneira genérica (como "risco significante à segurança nacional"), quanto de uma maneira mais abrangente de modo a identificar uma escolha comum aos estonianos (como "um ataque ao modo de vida estoniano"). Mais do que isso, o ministro trouxe o problema das ameaças cibernéticas de um âmbito técnico para um âmbito comum, já que "há uma crescente dependência global das tecnologias da Internet e de serviços online" dos quais todos, de uma maneira geral, guardam alguma dependência e, portanto, estão vulneráveis.

Este trecho do discurso revela ainda algo que escapa do limite da tecnificação teorizado por Hensen e Nissenbaum (2009), já que, como aponta o ministro, não são só os códigos e a obstrução do sistema que importam na segurança cibernética, mas também o fato de que "uma propaganda politicamente orientada é capaz de motivar pessoas a cometer tais ataques". Assim, a preocupação com a segurança cibernética passou para um campo essencialmente político, em que as tecnologias da informação funcionam como uma simples

ferramenta. Assim, os problemas de ordem técnica passaram a ser olhados como consequências de ações tomadas em ambiente não-virtual e não como as principais causadoras dos problemas.

O discurso do ministro propõe depois uma espécie de novo pressuposto para uma agenda de segurança que serviria não só a nível local, mas como uma preocupação geral:

> "as we try to come to grips with this new battlefield there are certain aspects that in my opinion immediately stand out. First is the issue of dealing with cyber defense, in general. It is worth to ask ourselves whether it would not serve our common purpose better to start acknowledging the impact of cyber defense on our civilian as well as military affairs more clearly. I think we all agree that our military command and control, ISR and precision strike capability rely on ensured access to the electronic spectrum. It is also clear that losing the freedom of action in the cyberspace domain is not an option. At the end of the day, all the data in our national or international neural networks is relatively useless unless it can be protected" […] I fear that if do not start answering these hard questions soon, we will not be able to deal with future effectively. (Aaviksoo, 2008)

Novos objetos de referência aparecem que remetem ao próprio meio, ambiente, ou seja, a rigor, ao próprio ciberespaço que deve ser protegido ao mesmo tempo que o mesmo também é um instrumento para a proteção de outros objetos de referência. Assim, o "campo de batalha" ao qual se refere o ministro estoniano deve ser mantido sob constante observação suscitando uma política de defesa e de cooperação internacional em torno desse assunto. Por fim, apesar de não apontar nenhuma medida específica a ser tomada, o discurso do ministro aponta que a situação pede alguma resposta com certa urgência, já que a segurança do ciberespaço é um assunto presente com consequências para o futuro não muito distante.

Naturalmente, um único discurso cinge-se ao momento ao qual foi proferido e não necessariamente um padrão de ideias a ser replicado. Contudo, a ideia de trazer o tema da cibersegurança para um plano prioritário também apareceu em um artigo escrito pelo mencionado ministro dois anos depois, quando era responsável pela pasta da Educação e Investigação da Estônia. Na ocasião, o ministro sustentou que,

> Our societies´ vulnerabilty extends beyond a mere threat to critical infrastructure. Information societies depend on trust and open communication. Undermine these, and you can spread panic, destabilize democratic governments, and destroy massive amounts of wealth. Cybersecurity and defense is often spoken of alongside other so-called ´new threats´ like energy security, climate change, or population movements, but cyber is more than a security and defense problem, a change in the structure of our societies, economies, and relations. Instead of talking about cybersecurity and cyberdefense, we need to speak of security and defense as a whole in cyberworld.
>
> Cyberattacks can be combined with the conventional and intelligence capabilities available to states, magnifying their impact. While as not as terrifying as all-out

> nuclear war, cyberattacks can damage physical infrastructure, cause loss of life, and sow widespread fear and panic that can quickly destabilize networked societies. In short, full-scale cyberwar could bring modern life to a halt. (Aaviksoo, 2010: 14, 18)

Desta vez, interessa destacar que o governante alça o tema da cibersegurança entre os outros temas de segurança que gozam de maior reconhecimento e apelo internacional, como a questão ambiental e as migrações. Mais do que isso, tratar da questão da cibersegurança e defesa cibernética implica redefinir os instrumentos institucionais e as capacidades com as quais os Estados hoje contam. Aparentemente, o ministro quis evidenciar que o aparato bélico hoje existente, por exemplo, não é de grande utilidade contra ameaças do ciberespaço. Estas ameaças, em sua perspectiva, têm o potencial de causar danos similares aos dos aparatos bélicos tradicionais. Os discursos apontam sempre para uma contextualização com temas cotidianos, aproximando a importância da segurança do ciberespaço da audiência para a qual dirige seu discurso, neste caso, ao mesmo tempo que se restringe a profissionais da área e interessados no assunto, compartilham da mesma necessidade dos demais cidadãos por, com obviedade, situarem-se na mesma sociedade.

Agrega valor ao discurso o fato de o locutor não só ser uma autoridade governamental testemunha direta dos ciberataques de 2007, mas alguém que esteve à frente de um programa de digitalização e de inclusão digital enquanto ministro da Educação, ainda na década de 1990 (EURACTIV, 2004). Além disso, sendo o Ministro da Defesa na ocasião dos ataques, coube-lhe a tarefa de formular e articular respostas, o que lhe confere um peso bastante significativo enquanto referência para as questões de segurança cibernética. No entanto, o ministro da Defesa não foi a única autoridade a se pronunciar sobre o tema, e aparentemente os discursos se afinam no que se refere às apreciações do episódio.

Relativamente pouco tempo depois dos ciberataques, o então presidente estoniano, Toomas Hendrik Ilves, levou a questão da segurança do ciberespaço à 62ª Sessão da Assembleia Geral das Nações Unidas. Nestes termos:

> [...] Cyber-attacks are a clear example of contemporary asymmetrical threats to security. They make it possible to paralyze a society, with limited means, and at distance. In the future, cyberattacks may in the hands of criminals or terrorists become a considerably more widespread and dangerous weapon they are at present.
>
> […]
>
> Cyber-attacks are a threat not only to sophisticated information technological systems, but also to a community as a hole. For instance, they could be used to

> paralyze a city´s emergency medical services. The threats posed by cyber warfare have often been underestimated since, fortunately, they have so far not resulted in the loss of any lives. Also, for security reasons, the details of cyber attacks are often not publicized. In addition to concrete and technical and legal measures for countering cyber attacks, governments must morally define cyber violence and crime, which deserve to be generally condemned just like terrorism or the trafficking in human beings. Fighting against cyber is in the interests of us all without exception. This fight requires both appropriate domestic measures as well as international efforts. (Estonia, 2007)

Nota-se que o discurso proferido pelo presidente estoniano ao mesmo tempo que deu o tom das comunicações referentes ao tema repetiu quase literalmente um discurso comum já em vigor no que se refere às questões de segurança cibernética não só na Estônia, mas também noutros países e organizações internacionais, alguns deles já citados anteriormente. Os elementos comuns presentes ao chamar a atenção para a questão da segurança cibernética permanecem sendo a crescente dependência que a sociedade moderna tem em relação às tecnologias da informação e ao ciberespaço de maneira geral e a ameaça contra esse estilo de vida uma vez que essa tecnologia possibilita seu próprio mau uso por grupos criminosos. Há ainda um recurso à associação a grandes temas de segurança internacional. Frequentemente o crime organizado e, no caso, o terrorismo internacional, são indicados como problemas que podem ser somados e amplificados quando conjugados com a segurança cibernética. Por fim, outro padrão nos discursos é a socialização do problema em dois aspetos. Primeiro, a natureza global do tema, já que, por natureza, o ciberespaço não dispõe de fronteiras definidas. Segundo, a noção de que a ameaça não é só a um estilo de vida mas a uma multiplicidade de objetos de referência, desde a gestão eficiente de serviços essenciais, geralmente associados às infraestruturas críticas, até aos problemas convencionais de segurança, identificados pelas conceções tradicionais. Com isso, os discursos apontam para uma solução que envolve iniciativas coletivas.

Neste aspecto, a audiência do presidente estoniano foi de especial relevância, já que era composta por altos representantes estatais e de organizações internacionais, ou seja, a todo modo, atores funcionais, com capacidade, ao menos teórica, de articular medidas, incentivar políticas, assumir posições com consequências práticas tanto em uma esfera doméstica , quanto a nível internacional. Assim, mais adiante, Ilves aconselha sua audiência sobre o que deveria ser feito para fazer frente às ameaças e articular a cibersegurança:

> We should move ahead and create a truly international framework to combat these vicious acts. The global Cybersecurity Agenda of The International

> Telecommunication Union[43], launched by the Secretary-General in May, is a very important initiative for building international cooperation in this field. Estonia Also agrees with the assessment of the specialists of the United Nations Institute of training and Research, that a globally negotiated and comprehensive law Cyber-Space is essential, and that the UN can provide the neutral and legitimate forum for this talk. (Estonia, 2007).

Ressalta-se que o discurso, sendo parte de um movimento de securitização também faz referência aos atores funcionais. Neste caso, tais atores constituem um grupo legitimamente reconhecido e apto, ao menos, a tomar direções que levassem a medidas excepcionais. Obviamente, dada a complexidade do tema que envolve várias discussões em outros níveis (domésticos, multilaterais), nos quais a influência do locutor não é suficiente, o presidente estoniano não identificou medidas que fossem para além do que já havia sido mencionado tempos antes, que, por sua vez, vem a corroborar suas posições àquela audiência.

Naturalmente, o discurso proferido naquela ocasião não teve diretamente um impacto direto na implementação de medida de exceção. Essas medidas de exceção dependeriam não só da persuasão daquela audiência, formada por eventuais atores funcionais, mas também da sua capacidade de incorporar o discurso e articulá-lo em suas respectivas esferas de ação. Essa dinâmica levaria, então a uma possibilidade de outros movimentos de securitização variados e ligados necessariamente aos possíveis atores funcionais que formavam a audiência do presidente estoniano.

Os elementos pontuados pelo presidente Ilves repetem-se em vários de seus discursos, e não só quando o assunto limita-se ao assunto da cibersegurança. Mesmo as entrevistas que o presidente concede a periódicos, tanto com um viés mais generalista quanto aos essencialmente acadêmicos, expressam fundamentalmente a mesma mensagem.

[43] A Agenda para a Cibersegurança mencionada pelo presidente Ilves foi publicada em maio de 2007 pela União Internacional para as Telecomunicações. O principal objetivo da iniciativa foi fortalecer mecanismos de confiança entre entes da sociedade da informação. O mesmo conteúdo do discurso do presidente para as Nações Unidas já estava presente no documento e serve para justificar-se na intenção de criar espaço para o desenvolvimento e incremento da segurança cibernética. O discurso do presidente Ilves é muito semelhante ao disposto no documento, inclusive alguns termos se repetem: "The rapid growth of ICT networks has created new opportunities for criminals to exploit online vulnerabilities and attack countries' critical infrastructure. Governments, firms and individuals are increasingly reliant on the information stored and transmitted over advanced communication networks. The costs associated with cyberattacks are significant – in terms of lost revenue, loss of sensitive data, damage to equipment, denial-of-service attacks and network outages. The future growth and potential of the online information society are in danger from growing cyberthreats. Furthermore, cyberspace is borderless: cyberattacks can inflict immeasurable damage in different countries in a matter of minutes. Cyberthreats are a global problem and they need a global solution, involving all stakeholders" (ITU, 2007).

Outra característica é uma certa atemporalidade da mensagem. No trecho a seguir, por exemplo, o apelo às questões de segurança do ciberespaço aparece uma década após os ataques de abril de 2007, de uma forma bastante similar aos pronunciamentos feitos à altura:

> in today's world the more modern and the more digitized you are, the more vulnerable you are. Thus, high dependence on digital services and networked infrastructure makes Estonians more vulnerable than other countries that do not use Internet services in everyday business. At the same time, we are more secure than the majority of countries that use less robust security measures.
>
> […]
>
> raising awareness about cyber threats as well as developing skills and knowledge to use technology safely have become a central aspect of ensuring cybersecurity in Estonia. After all, the technology itself doesn't create risks—they occur from the malicious, rather than intended, use of technology. The more aware we are about the possibilities of technology, the more we can predict threats and prevent detrimental consequences.
>
> […]
>
> Estonia cannot ignore that we are located next to Russia, which uses aggressive rhetoric, is constantly developing its cyber attack capabilities, and for whom activities directed against other states in cyberspace are merely an instrument to increase its influence and accomplish its objectives. On the other hand, attacks in the cyber domain pay no attention to geography. Politics pays attention to geography, electrons and bits do not. […] In addition to Russia, our cyber threat analyses cannot ignore the need to take into account terrorists and hostile cyber activists. Thus, we need to be aware what is going on in cyberspace worldwide, not only in Russia. (Ilves, 2017)

Apesar da repetição da mensagem, inclusive repetindo muitos dos mesmos elementos ou objetos de referência, cabe destacar a presença de um novo elemento que é a acusação textual de que a Rússia foi responsável pelos ataques. Esse reconhecimento serve ao menos dois propósitos no discurso. Primeiramente identifica um agente ofensivo, uma ameaça presente e bastante definida aos objetos de referência. Depois reforça a ideia de que a segurança do ciberespaço deve ser pensada constantemente, já que o presidente reconhece primeiramente que, obviamente, a Rússia é uma presença constante na política estoniana, mesmo por questões geográficas e, mais do que isso a Rússia, segundo o presidente, tem adotado uma postura mais agressiva no ciberespaço como uma forma de pressionar e influenciar a política de outros Estados. Deste modo, juntamente com o desenvolvimento concomitante das ameaças cibernéticas e das formas de contê-la, questões tradicionais de política e diplomáticas vem contribuir para uma espécie de *movimento de securitização contínuo*.

Percebe-se que o discurso e o conteúdo prevalecem mesmo anos depois do episódio. Mesmo trocando o interlocutor. Uma década, depois dos ataques, em fevereiro de 2017, o ex-primeiro-ministro estoniano, Andrus Ansip, na ocasião da Cybersecurity Conference, em Munique, reafirma o conteúdo dos discursos. À sua audiência, diferente daquela que acompanhava o presidente estoniano nas Nações Unidas, formada, desta vez, essencialmente por técnicos e especialistas na área, Ansip expõe que:

> you do not need me to tell you about the global threat posed by cybercrime. I think it is enough to say that today, people – and companies – no longer think about if they are going to be hacked, but when it will happen. Or maybe worse, if they are not sure if they may already have been hacked. Are they prepared to deal with it? Are we? Will businesses survive? Is Europe as a whole prepared? At the moment, I would say: unfortunately not. We are working hard to do something about it. Cyber threats evolve as quickly as technology, which plays an increasing part in our daily lives. All these devices, systems and services are connected, exposed and vulnerable. An attack might come from a hacker for political goals. Or one with financial motives. It might be a threat made through ransomware, a hybrid threat or even nation-state cyber-espionage. Or it might have no obvious objective other than to 'disrupt' for the sake of it. (Ansip, 2017a)

O conteúdo da mensagem não é novidade, pelo contrário, reforça um padrão que vinha sendo repetido em vários outros pronunciamentos. Mesmo outros documentos mencionados em outros capítulos desta tese compartilham da mesma ideia e apontam para maiores advertências e atenção geral para a adoção de maiores cuidados e uma política constante voltada para a segurança cibernética. Por outras palavras, o primeiro-ministro elenca os mesmos objetos de referência e as associações com o contexto comum da sociedade da informação.

O discurso do primeiro-ministro estoniano vem com um elemento agravante, reforçado por um conhecimento de causa proporcionado pelo episódio dos ataques, ao trazer a certeza de que o problema da segurança cibernética é uma realidade compartilhada por todos e a questão não seria especular se algum ataque informático será possível, mas sim, quando irá acontecer, já que, repetindo a ideia do presidente Ilves, pondera que as ameaças também se aprimoram juntamente com o desenvolvimento tecnológico.

Esse espaço de tempo que separa os discursos dessas duas autoridades revela também que, apesar de todos os esforços e medidas tomadas para aprimorar a cibersegurança, este não constitui um problema nunca completamente resolvido. Pelo contrário, a constância dos discursos e a insistência na ideia das ameaças sugere que a cibersegurança é uma questão a ser debatida e enfrentada constantemente. À sua maneira, os interlocutores entendem esse aspecto e propagam essa ideia.

Nesse sentido, o discurso da securitização, incorporando vários elementos que vem sendo abordados repetidamente, acaba tornando o movimento de securitização uma constante na política de segurança cibernética, ainda que não resulte necessariamente na adoção de medidas especiais esporádicas ou formuladas em um sentido ad hoc.Pelo contrário, ao manter o tema politizado, esse discurso de securitização gera políticas incorporadas em instituições e documentos oficiais bastante discutidos nas instâncias regulares e pela opinião pública em geral.

Assim, de forma mais específica, a insistência dessas mensagens de securitização veio a somar-se a uma compreensão geral e se encontra refletida em vários documentos oficiais do governo estoniano em relação às políticas para o ciberespaço e também tem se traduzido na criação de instituições para cuidar da segurança do ciberespaço, inclusive com objetivos de atuar em situações excepcionais.

Neste sentido, essas ideias trazidas a público pelas maiores autoridades estonianas dão o tom inicial da Estratégia Nacional para a Cibersegurança (2008 – 2013) publicada pelo governo estoniano. O documento em questão começa ressaltando o episódio dos ataques de modo a embasar o discurso e, automaticamente, a necessidade de tratar a questão da cibersegurança entre as questões emergentes de segurança contemporâneas:

> The acknowledgment that such attacks pose a threat to international security reached new heights in 2007 owing to the first-ever co-ordinated cyber-attack against an entire country - Estonia – and also because of large-scale cyber-attacks against information systems in many other countries as well. The recurrence and growing incidence of cyber-attacks indicate the start of a new era in which the security of cyberspace acquires a global dimension and the protection of critical information systems must be elevated, in terms of national security, on a par with traditional defence interests. The co-ordinated cyber-attacks against Estonian government agencies, banks, and media and telecommunications companies demonstrated that the vulnerability of a society's information systems is an aspect of national security in urgent need of serious appreciation. We have clearly and unambiguously acknowledged the need to protect information systems in advanced information societies, but the measures we have taken have not always been sufficient for that purpose. The protection of a country's entire cyber assets calls for a comprehensive effort involving all sectors of national society, a clear and efficient allocation of responsibilities therein for the prevention of cyber-attacks, and increased general competence and awareness regarding threats in cyberspace. Our overall task rests on a prescient awareness of the need to balance, on the one hand, the risks associated with the use of information systems and, on the other hand, the indispensability of extensive and free use of information technology to the functioning of open and modern societies — and the understanding that this is a challenge confronting not only Estonia but also the rest of the world (Estônia, 2008).

Os ataques de 2007 são revisitados em vários momentos, de modo a justificar a adoção de alguma política ou posições a serem tomadas pelo governo estoniano. Em termos

gerais, o documento repete e reafirma os pontos levantados nos discursos anteriores no que concerne à proteção dos objetos de referência e à aproximação da cibersegurança com as questões e instituições de defesa e segurança nacional. Advoga ainda por uma extensa rede de colaboração para o desenvolvimento de um sistema eficiente, envolvendo não só várias instâncias da burocracia estatal, mas principalmente instituições privadas, apontadas, inclusive, como uma das partes mais interessadas na segurança do ciberespaço.

Dois pontos ainda merecem destaque. Em primeiro lugar, o documento aponta para uma grande necessidade de cooperação internacional, já que entende que o problema da segurança do ciberespaço é de interesse de outros Estados e organizações internacionais e por, por princípio, entender que

> "Cyber security is ensured via international cooperation with allies and partners. Through cooperation, Estonia promotes global cybersecurity and enhances its own competence" (Estonia, 2014: 7).

Essa opção dá-se primeiramente, pela colaboração com instituições das quais o país faz parte, como as Nações Unidas, União Europeia, NATO, Conselho Europeu, OECD. Para além desses, aponta-se a colaboração com redes de cooperação internacional especialistas em segurança cibernética, como é o caso dos CERTs, já mencionados anteriormente. O segundo ponto é justamente a adoção de um constante discurso de advertência para os riscos para a segurança no ciberespaço. A preocupação com a segurança do ciberespaço é constante assim como são e serão as ameaças nesse ambiente.

A estratégia faz referência a vários documentos no âmbito do Ministério dos Assuntos Econômicos e Comunicação, que tem assumido, mais recentemente, a dianteira no desenvolvimento de políticas para o ciberespaço. Entre os documentos mencionados nesta área estão a Estratégia para a Sociedade da Informação (Estonia, 2013)e a Lei sobre Comunicações Eletrónicas (Estonia, 2004), entre outros provenientes do Ministério da Justiça, principalmente concernentes aos crimes cibernéticos, e deliberações do Ministério da Educação, que adotou uma política de disseminação da segurança cibernética entre outras questões relacionadas às tecnologias da informação no sistema de ensino.

A estratégia de cibersegurança estoniana, programada para ser implementada até 2013 foi substituída por outro documento que a atualiza, funcionando como uma espécie de segunda fase, compreendendo o período entre 2014 e 2017. Nele, o discurso da securitização

continua a elencar os mesmos objetos de referência e a apontar o constante desenvolvimento das ferramentas como uma questão a ser permanentemente tratada. Contudo, a novidade é que há a percepção de que um número crescente de atores estatais tem atuado no ciberespaço como uma nova plataforma para a espionagem e atos considerados agressivos. Assim, há uma percepção e uma diferenciação de crimes cometidos no ciberespaço, como a atuação do crime organizado, entre outros, com uma atuação mais agressiva de Estados, que passam a atuar no ciberespaço como atuam em um ambiente anárquico internacional.

> The main threat is cybercrime and its growth is reflected by the significant development of cyber criminals' skills and their increased ability to carry out organized attacks. An integral part of the processing of crimes is the collection and handling of digital evidence, which poses new challenges to the procedural and digital forensics capabilities of the police. National cyber security is affected by the actors operating in cyberspace with their various skills, targets and motivations. It is often difficult to distinguish between the actors or determine their relationship to national or international organizations. The number of state actors in cyberspace that are involved in cyber espionage targeted at computers connected to the Internet as well as closed networks continues to grow, with their aim being to collect information on both national security as well as economic interests. The amount and activeness of states capable of cyber-attacks are increasing. In addition to the activation of state actors, the ability of politically motivated individuals and groups with limited means to organize their activities using social networks and carry out denial of service and other types of attacks is growing as well. (Estonia, 2013)

O contexto nacional e a opção por um estilo de vida baseado essencialmente no bom funcionamento das tecnologias da informação aparecem como um dos principais objetos de referência e também uma das principais fontes de preocupação em relação às ameaças cibernéticas. Este aspeto condiciona a formulação e a aplicação de medidas e políticas para o ciberespaço. Essa posição não é necessariamente nova em relação à versão anterior, no entanto, o texto é mais assertivo e preciso em relação a essa característica cibernética da sociedade estoniana, por isso, ao que parece, surge como condicionante das políticas de segurança do ciberespaço.

> The main cyber security risks arise from the extensive and growing dependence on ICT infrastructure and e-services by the Estonian state, the economy and the population. Therefore, the key fields on which the Cyber Security Strategy focuses are ensuring vital services, combating cybercrime more effectively and advancing national defence capabilities. (Estonia, 2014)

Contudo, entre os oito princípios elencados pela Estratégia, está a defesa e preservação de direitos individuais e das liberdades pessoais de informação e identidade. Esse aspecto aparece no mesmo conjunto em que se entende que a defesa do ciberespaço é uma parte integral da segurança nacional e na adoção de políticas para prever e lidar com

ameaças neste espaço. Para este efeito, a Estratégia atribui ao indivíduo, e não necessariamente ao Estado e outros organismos públicos, a primeira responsabilidade para a segurança do ciberespaço. Há também um grande destaque relacionado à cooperação internacional para a cibersegurança.

Em comum, essas ideias compartilham uma gestação que precede os ataques de 2007, mas que, como afirmaram os nossos diversos entrevistados, tiveram sua importância reforçada por este episódio que, por sua vez, foi decisivo ou teve um peso bastante significativo para a implementação dessas medidas. Vale destacar duas delas. No âmbito interno, tem-se a criação e efetivação da Estonian Defense League´s Cyber Unit, e, num âmbito mais multilateral tendo a Estônia como um importante agente, o já mencionado Centro de Excelência de Cibersegurança da NATO (CCDCoE).

Para o efeito daquele que é o objetivo deste estudo de caso – a concretização, no caso estoniano, dos elementos da Teoria da Securitização e da sua lógica de conjunto – impõe-se destacar que muito do que resultou das políticas adotadas neste primeiro período não foram necessariamente medidas de exceção, como é defendido por aquela teorização, sobretudo na versão da Escola de Copenhaga. No entanto, essas medidas devem ser compreendidas em um âmbito mais alargado.

As medidas adotadas pelos agentes funcionais colocaram a Estônia na vanguarda de uma tendência mundial de preocupação com a questão da segurança cibernética. A segunda estratégia, como declara o próprio documento, vem no sentido de reforçar as medidas adotadas no âmbito da primeira, mas também na intenção de manter e fortalecer a institucionalização dessas ditas conquistas. Esta será porventura uma situação que as elaborações da teoria da securitização da Escola de Paris ajudem a ler melhor. Essas elaborações vêm trazer o foco para o movimento de securitização em si e para a agenda política dos atores. Neste sentido, as medidas de exceção que caracterizariam a securitização perdem importância para os elementos iniciais. As questões de segurança são constituídas através de práticas frequentemente rotinizadas e não necessariamente através de um discurso de securitização pontual. (McDonald, 2008: 570). Ou seja, os discursos da securitização que enfatizam o rótulo da segurança sobre uma determinada questão têm de estar relacionados com uma determinada condição histórico-social. Daí, portanto, a importância de observar o contexto do qual surgem os discursos de securitização. Em suma, o processo de securitização do ciberespaço no caso estoniano parece ser melhor entendido sob o leque mais amplo

proposto pelos acadêmicos da Escola de Paris da securitização, cuja ideia central pode ser sumarizada pela concepção de Balzacq:

> an articulated assemblage of practices whereby heuristic artefacts (metaphors, policy tools, image, repertoires, analogies, stereotypes, emotions, etc.) are contextually mobilized by a securitizing actor, who works to prompt an audience to build a coherent network of implications (feelings, sensations, thoughts, and institutions), about the critical vulnerability of a referent object, that concurs with the securitizing actor´s reasons for choices and actions, by investing the referent subject with such an aura of unprecedent threatening complexion that a customized policy must be undertaken immediately to block its development. (Balzacq, 2011: 3)

A consideração de questões para além dos discursos de securitização pontualmente permite uma verificação inclusiva, observando o contexto político-social estoniano. É este o ponto inicial e para o qual convergem as medidas geradas pelo movimento de securitização. Antes dos discursos de securitização em si, é preciso, por exemplo, considerar questões geográficas, demografia e a opção pelo fomento de uma sociedade altamente informatizada, que constituem especificações do caso estoniano.

Para além de uma melhor percepção do caso Estoniano em si, a abordagem mais ampla proposta pela Escola de Paris permite focar mais no movimento de securitização e perceber melhor a construção do objeto de referência e do rótulo da segurança para além dos resultados da securitização, que podem ter mais de uma dimensão ou atender a outros objetivos subjacentes ao movimento, como se poderá perceber adiante.

Os ataques cibernéticos à Estônia fomentaram um discurso de securitização que se refletiu em documentos oficiais posteriormente e embasaram a criação de instituições e orientaram as posições da Estônia no que tange a segurança cibernética. A já citada Estratégia para a Cibersegurança de 2008, publicada pelo Ministério da Defesa, previa a aplicação gradual de sistemas de segurança cibernética na Estônia, baseando-se no desenvolvimento de especializações e excelência técnica em segurança cibernética. O documento também incentiva desenvolvimento de marcos legais adequados para o suporte de atividades de segurança para o ciberespaço e o incentivo à cooperação internacional para a cibersegurança. Há uma tendência ao preparo técnico pronto a fazer frente às ameaças, o que pode ser traduzido na consolidação da "Cyber League", contudo, há uma generalização da responsabilidade pela cibersegurança para além de uma "tecnificação":

> a general social awareness of threats in cyberspace and the state of readiness to meet them should be fostered; these are important prerequisites, since every member of the information society is responsible for the security of the network-based instruments or systems in his or her possession. (Estonia, 2008: 7).

A revisão da Estratégia para a Cibersegurança de 2014, que substituiu o documento de 2008, mantém o teor discursivo, atentando para a necessidade de prontidão para fazer frente às ameaças do ciberespaço. A segurança do ciberespaço é consolidada como uma prioridade das políticas de segurança e defesa do Estado, de responsabilidade compartilhada com o setor privado e pela sociedade em geral. Neste contexto, destaca-se o princípio 6:

> A top priority in ensuring cyber security is anticipating as well as preventing potential threats and responding effectively to threats that materialize (Estonia, 2014: 7).

Em dois dos princípios (7 e 8), destaca-se a necessidade da cibersegurança ser tratada a nível internacional, de modo a desenvolver e aprimorar as políticas de preparo para as ameaças para o ciberespaço. Percebe-se assim, que o discurso de securitização do ciberespaço é uma questão permanente nas políticas propostas pelo governo estoniano. A securitização latente continuou a ser refletida nos documentos, na criação de instituições e na atuação internacional da Estônia.

No caso estoniano, tal como foi mencionado por vários dos entrevistados, acabou por acelerar o processo de implantação do Centro de Excelência da NATO, em Tallinn, bem como proporcionou uma marca da política externa estoniana que vem sendo seguida em diversos âmbitos multilaterais (Crandall, 2014) e no fortalecimento de medidas internas para o aprimoramento das capacidades de fazer frente às ameaças do ciberespaço. O próximo tópico explora traz exemplos dos impactos do movimento de securitização do ciberespaço por conta dos ataques cibernéticos de 2007.

3.4. Do movimento de securitização à implementação de instituições

Diferente de ataques tradicionais, com armamentos bélicos que destroem infraestruturas, cidades, meios de produção, entre outros, os ataques cibernéticos dificilmente causam danos físicos. Ao menos por hora é esta a percepção e é o que se comprova pelas recentes experiências. Muitos autores, como alguns já mencionados, tendem

a minimizar o tema justamente por causa dessas consequências menores. De fato, se comparados a um bombardeio ou à tomada de uma cidade ou instalação estratégica, as consequências dos ciberataques tendem a provocar menor preocupação. Contudo, as consequências não são, na verdade, tão menores assim. Por exemplo, um relatório da companhia de seguros inglesa Lloyd´s of London, em um caráter generalista, estima que um ataque cibernético de grandes proporções naquele país pode acarretar uma perda de 53 mil milhões de dólares, o que equivale, segundo a citada empresa, à perda gerada por uma tragédia natural de grandes proporções, como o furacão Sandy, em 2012 (Lloyd´s of London, 2017). Assim, as consequências podem não ser exatamente visíveis, mas custam tanto quanto uma tragédia de grande apelo político e midiático.

A questão da segurança do ciberespaço era debatida na Estônia antes dos ataques cibernéticos de 2007, tal como era de certa forma comum em outros países. Contudo, a Estônia emerge após os ataques como uma referência internacional no tema da segurança e defesa cibernética. O movimento de securitização do ciberespaço na Estônia foi capaz de consolidar uma posição que já era latente naquele contexto sociopolítico. O resultado direto deste movimento foi criação de instituições de prevenção e resposta a ciberataques, tanto em questões práticas e operacionais, como a Cyber Unity da Estonian Defense League, e por um viés mais político ou de cooperação internacional, com a instalação do Centro de Excelência da NATO (CCDCoE) em Tallinn e as iniciativas de cooperação internacional, abordados a seguir.

3.4.1. Küberkaitse üksus: *Estonian Defense League's Cyber Unit*

A *Estonian Defense League´s Cyber Unit (EDL CU)*, que atrás referimos, foi fundada no âmbito da *Estonian Defense League* (***Eesti Kaitseliit),*** organização paramilitar, ligada às Forças Armadas Estonianas com o objetivo de "to enhance, by relying on free will and self-initiative, the nation's readiness to defend the independence of Estonia and its constitutional order" (Estonian Defense League, 2017: online). Em 2010, a Unidade Cibernética, uma rede formada por voluntários altamente capacitados em assuntos informáticos, sem histórico de delitos e obrigatoriamente ligados ao país, foi adicionada a este órgão, em decorrência dos ataques cibernéticos de 2007. A Segunda Estratégia de Cibersegurança estoniana, ao fazer um balanço dos avanços das políticas da primeira estratégia (2008-2013), reconhece que,

> The creation of the Estonian Defence League's Cyber Unit (hereinafter EDL CU), which took place as a result of collaboration between the public, private and third-sector, has been instrumental in ensuring national defence. The expertise of EDL CU volunteers is applied to improve the security of Estonian state agencies' and companies' information systems through coordinated exercises, testing of solutions, training, etc.. The EDL CU can also be engaged to support civilian institutions and protect critical infrastructure in a crisis situation. Domestic and international cyber security training exercises have also played an important role in the development and assessment of cyber security capabilities (Estonia, 2013)

A "Cyber League" tem funcionado como uma espécie de base organizacional para as atividades dos elementos e subdivisões institucionais que dão suporte à segurança do ciberespaço. No caso da mencionada instituição, a sua marca característica é que a "Cyber League" carrega um sentido de urgência, ou seja, continuamente sua constituição não é fixa, embora tenha como base uma equipe previamente selecionada, sendo os seus membros em concreto convocados em determinadas situações quando se identifica uma ameaça ao correto funcionamento da infraestrutura de informação digital na Estónia. De fato, sendo uma componente de uma instituição essencialmente militar, a "Cyber League" é o que mais se assemelha a um exército digital institucionalizado.

Apesar de ter sido institucionalizada após os ataques cibernéticos de 2007 terem sido resolvidos, a lógica da sua criação está intimamente ligada aos discursos posteriores que ligavam a questão cibernética à segurança nacional, tendo como principal orador o então Ministro da Defesa, Jaak Aavikso (Markoff & Landler, 2007). De fato, para lá de todo o discurso atrás analisado, na prática o problema só foi realmente resolvido quando os especialistas técnicos se juntaram, compartilharam informações, inclusive com especialistas estrangeiros, conceberam uma arquitetura de reposta a estes ataques como se fosse um problema interno de uma empresa, não necessariamente de um país. O que significa que decisões essencialmente técnicas envolvendo questões de segurança foram priorizadas em detrimento de uma abordagem eminentemente política. De algum modo – e ainda que correndo o risco de algum exagero – o que veio a prevalecer foi uma lógica de ação direta ao mesmo tempo institucionalizada e flexível. É esse o sentido da "Cyber League".

Contudo, a "Cyber League" não é um órgão autónomo, pelo contrário, responde hierarquicamente, perante a "Defense League" e, em última instância, perante ao Ministério da Defesa. Há porém, uma coordenação em conjunto com o CERT Estoniano que, por sua vez, responde ao Ministério de Assuntos Econômicos e Comunicação. Esta ligação e interação são importantes porque permitem uma observação em rede, ou seja, há na verdade

uma ponte institucional, aparentemente sólida, entre as questões essencialmente técnicas e os representantes políticos designados pelo poder executivo[44].

Por fim, cumpre ressaltar que este modelo, que envolve um relacionamento híbrido entre corpo militar e voluntários civis, tem sido considerado um modelo para outros países e tem sido adotados com adaptações, como fez o estado de Michigan, nos Estados Unidos, ao criar, em 2017 o Cyber Civilian Corps (J. Williams, 2017).

3.4.2. O NATO Cooperative Cyber Defense Center of Excellence (CCDCoE)

Superadas as tensões políticas geradas pelos ciberataques, e tendo sido implementadas e consolidadas instituições no âmbito nacional e internacional ligadas à segurança cibernética, em agosto de 2008, a capital estoniana passou a ser a sede do NATO Cooperative Cyber Defense Centre of Excellence (CCD-COE).

Como descrito no Bilateral Brief on Relations Between NATO and Estonia,

> The coordinated cyber-attacks against Estonia in 2007 focused more of NATO's attention than ever before on the need to ensure the security of this vital infrastructure. Comprehensive and coordinated attacks on communication infrastructure can seriously affect communication among NATO allies or national institutions and cause significant damage by disrupting civil life or allowing information leaks. Cyber-attacks could prove to be a serious threat to the effective implementation of NATO's collective defense in a crisis situation, thus ensuring cyber security is a justified priority for NATO. (Nato, 2013)

Há dois aspectos que interessa ressaltar a respeito do CCDCoE em relação aos ataques de 2007. Primeiramente, a ideia de estabelecer um centro de excelência com este caráter em Tallinn não deriva dos ataques, mas sim da vocação do país para tais assuntos e certa articulação política envolvendo o governo, especialistas e o setor privado, junto à NATO. Os ataques, como confirmaram diversos entrevistados, vieram consolidar essa ideia e, automaticamente, acelerar o processo de implantação. Em segundo lugar, é comum entender o CCDCoE como uma instituição semelhante a Cyber League, ou seja, uma plataforma que concentra especialistas em uma espécie de exército eletrônico. Mas, na realidade, o CCDCoE é mais próximo de um *think tank* centrado na questão cibernética, mas focado sobretudo no campo jurídico e assessoria não só aos países membros da NATO, mas eventualmente a outros.

[44] Entrevistas com representantes do CERT-Estonia, representantes envolvidos com a fundação da "Cyber League".

3.4.3. Cooperação Internacional

Esta reposta institucional no quadro da NATO é uma expressão particular do que se pode considerar um movimento de securitização mais vasto e que consistiu em mobilizar uma audiência de alcance internacional para a necessidade de medidas de exceção, ao mesmo tempo que, numa operação de capitalização típica de política externa, com o relativo sucesso do país na resposta aos ataques, a Estônia conseguiu ser vista internacionalmente como um país de excelência em segurança cibernética.

Segundo afirma o ex-primeiro-ministro Andrus Ansip, a princípio, a ideia original era chamar a atenção mundial para um problema emergente e não necessariamente fazer da questão da cibersegurança um trampolim para alçar a Estônia enquanto referência:

> We didn't push to become the spokespeople for cyber security in the world, but we were placed in this position. Estonia experienced pretty strong denial of service attacks for three weeks, and we managed pretty well responding to those attacks, most of all thanks to the fact that different institutions, but also people in the private sector worked together very fruitfully outside their job descriptions. Thanks to cooperation with the corresponding authorities of other countries most of these attacks that were directed at Estonia couldn't even cross the border. (Ansip, 2017b).

Contudo, apesar de aparentemente não ter sido uma medida calculada, os responsáveis pela política externa estoniana souberam capitalizar a situação e apresentar o país como um importante ator global. De fato, como mostram os dados da tabela, atrás analisada, que ordena os países em um Índice Geral de Cibersegurança, a Estônia aparece entre os dez primeiros mais eficientes no mundo. Mais do que isso, o país figura entre potências econômicas como a Alemanha, os Estados Unidos e o Canadá, também conhecidos como expoentes nesse setor. No que se refere à Estônia, no entanto, a particularidade que torna este lugar cimeiro possível é que o país justifica abertamente sua experiência com os ciberataques para sua promoção. Essa posição se faz presente em discursos das mesmas autoridades que tiveram de tratar dos ataques em 2007, por exemplo, o já mencionado presidente Toomas Ilves, ao comparar a situação da cibersegurança e o risco de novos ataques, salienta que

> The tools used for cyber attacks have changed a lot since then, but Estonia's experience of resolving the situation at that time is still useful to countries that lack such experience. Another thing I worked on as president for ten years was to raise awareness of Estonia as an IT-savvy country. (Ilves, 2017)

Assim, após os ataques de 2007 e de toda a atenção conseguida com os discursos, a Estônia, a nível diplomático e técnico, passou a auxiliar países que tiveram o mesmo tipo de dificuldades. Nesse âmbito, destacam-se outros países que anteriormente pertenceram à esfera de influência da União Soviética, como a Ucrânia (2015) e a Geórgia (2008), que tiveram seus sistemas digitais atacados, algo que foi igualmente atribuído a origem russa.

3.5. Considerações finais

A dinâmica do processo de securitização, no caso da Estônia especificamente, faz com que o ator funcional assuma também o papel de agente da securitização, em função da agenda política e da audiência. Isso fica evidente no papel do presidente estoniano, que, embora figurasse entre os atores funcionais, por vezes assume uma posição mais identificada aos próprios agentes da securitização em seus discursos e pronunciamentos.

Neste sentido, entendemos que há lugar a um alargamento da teoria, designadamente com uma consideração mais fina de elementos de análises na definição dos atores funcionais e agentes da securitização. O que o caso estoniano mostra é que é preciso considerar características intrínsecas aos atores, tais como suas posições hierárquicas, o contexto político em que estão envolvidos, as suas proximidades e responsabilidades em relação ao objeto de referência e, também, a audiência à qual se dirigem, quando assumem o papel de agente da securitização.

Um segundo aprofundamento relaciona-se com a dinâmica do processo em si. Foi possível perceber que o movimento de securitização não é necessariamente linear e tampouco leva obrigatoriamente ao estabelecimento de medidas de exceção concretas. Há, no caso estoniano, um movimento de securitização que utiliza todos os elementos para identificar um objeto de referência. Contudo, não há necessariamente um estado de exceção propriamente dito ao fim do processo, como parecem pressupor os preceitos da Escola de Copenhague. Pelo contrário, há uma canalização do discurso para o fomento de medidas que já estavam sendo concebidas na vigência normal da ordem política, ainda que com uma intensificação e com um quadro institucional especial. O exemplo mais característico deste aspecto é o estabelecimento do Centro de Excelência da NATO, tal como foi apontado nas entrevistas por praticamente todos os inqueridos.

Esse segundo aspecto vem, então, reforçar a necessidade de ampliar a investigação sobre o papel dos atores funcionais e dos agentes da securitização. Aparentemente, e

independentemente do papel que desenvolvem nos diferentes momentos do processo de securitização, suas ações obedecem a uma agenda ou uma intenção política, ligada necessariamente ao seu contexto político. Há uma capitalização dos esforços para uma eventual securitização para a aprovação de uma agenda política. No caso da Estônia, no âmbito interno, houve uma aceleração de uma agenda baseada na segurança do ciberespaço com a criação de instituições e, no âmbito internacional, a consolidação de uma postura política que enfatizou a necessidade de implementação de instrumentos nesta mesma área.

CAPÍTULO 4. A dessecuritização como resposta: da espionagem cibernética ao Marco Civil da Internet

"If you spend more on coffee than on
IT security, you will be hacked.
What's more, you deserve to be hacked"

Richard Clarke, 2002
(Coordenador Nacional de Segurança,
Proteção de Infraestrutura e
Contra-Terrorismo dos
Estados Unidos)

O processo de aprovação do Marco Civil da Internet (MCI) no Brasil, em 2014, serve aqui como estudo de caso para verificar um processo de dessecuritização que tem o ciberespaço como objeto de referência. Parte-se do entendimento de que a aprovação da lei mencionada resultou, em grande medida, de um movimento de "dessecuritização antecipada ou preventiva" que, ao invés de medidas de exceção, visou assegurar garantias civis no ciberespaço.

Visto que o processo de securitização do ciberespaço no Brasil é derivado de um processo mais amplo, envolvendo os Estados Unidos e suas agências de segurança, considera-se importante verificar os aspectos do processo de securitização do ciberespaço naquele outro país, de modo a introduzir o contexto e suas repercussões no Brasil. Desde já, convém afirmar que o entendimento das ações brasileiras como uma resposta dessecuritizadora não vem de algo estritamente defendido ou sequer mencionado pelos atores envolvidos no processo, mas sim de uma interpretação fruto de uma avaliação teleológica do processo.

Deste modo, o argumento central deste capítulo repete a intenção já mencionada de que os processos de dessecuritização não obedecem necessariamente a uma estrutura teoricamente formulada, assim como os movimentos de securitização, mas dão-se a partir das configurações contextuais e das dinâmicas particulares dos atores envolvidos. No caso brasileiro, a dessecuritização de um objeto de referência que apresentava todos os elementos para um movimento de securitização, resultou em grande parte do interesse governamental

em aspectos que não tinham envolvimento direto com a questão relacionada com a segurança nacional ou a ameaças identificadas neste sentido. O que ocorreu foi, então, um discurso baseado em questões inerentes à segurança nacional, aproveitado por agentes do Governo para impulsionar uma agenda com implicações internas e externas que, ao menos até a atual conjuntura, significaram o que se pode entender como um desmonte do movimento de securitização.

4.1. Os Estados Unidos e a informação ao serviço da segurança

4.1.1. Os EUA e o ciberespaço: direito à conexão, securitização e *surveillance*

A própria história da concepção do ciberespaço tem relações bastante próximas com a questão militar, de segurança e defesa. Com efeito, como foi abordado no capítulo 1, foi em um ambiente compartilhado entre acadêmicos e militares que a Internet se constituiu, para anos mais tarde disseminar-se com o aprimoramento, desenvolvimento e abertura das redes para a exploração comercial, apoiadas ou não por incentivos estatais (Naughton, 2016). Com esta abertura, a face da Internet hoje mundialmente reconhecida é a que está ligada às possibilidades de interações, facilitação de negócios, difusão de conhecimentos e partilha de ideias, entretenimento, entre outros. Contudo, a componente militar ligada à defesa e à segurança não está, de todo, ausente, somente menos evidente aos olhos do grande público.

A exploração da Internet sobretudo pelo setor privado fomentou o surgimento de um novo segmento industrial que acabou por impulsionar a capacidade competitiva dos setores comerciais e de serviços por todo o mundo. Ao examinar este contexto, nota-se que tinha razão o então vice-presidente americano, Al Gore, quando afirmava que o maior impacto da ascensão da Internet tal como concebida pelos militares e ampliada pelo setor privado teria grande impacto para as relações sobretudo comerciais e industriais:

> The biggest impact may be in other industrial sector where those technologies will help American companies compete better and smarter in the global economy. Today, more than ever, business run information. A fast, flexible information network is as essential to manufacturing as steel and plastic. (Al Gore, 1994)

As posições assumidas pelo Governo norte-americano relativamente à disseminação da Internet não obedecem, contudo, necessariamente a uma lógica linear. Desde o início da década de 2000 as decisões políticas norte-americanas para a Internet têm sido muito diversas e até contraditórias em certos aspectos, com uma multiplicidade de direcionamentos, dependendo da instância que propõe as medidas em causa. Por um lado, há um grande incentivo à liberdade de expressão na Internet, como defende a ex-Secretária de Estado Hillary Clinton:

> […] I'm proud that the State Department is already working in more than 40 countries to help individuals silenced by oppressive governments. We are making this issue a priority at the United Nations as well, and we're including Internet freedom as a component in the first resolution we introduced after returning to the United Nations Human Rights Council. We are also supporting the development of new tools that enable citizens to exercise their rights of free expression by circumventing politically motivated censorship. We are providing funds to groups around the world to make sure that those tools get to the people who need them in local languages, and with the training they need to access the Internet safely. The United States has been assisting in these efforts for some time, with a focus on implementing these programs as efficiently and effectively as possible. Both the American people and nations that censor the Internet should understand that our government is committed to helping promote Internet freedom. We want to put these tools in the hands of people who will use them to advance democracy and human rights, to fight climate change and epidemics, to build global support for President Obama's goal of a world without nuclear weapons, to encourage sustainable economic development that lifts the people at the bottom up. (Department of State, 2010)

Este discurso da então Secretária de Estado tinha como objetivo promover apenas um segmento da política norte-americana. O seu foco era uma ação de política exterior que encontrasse apoios em atores privados em busca de expandir seus negócios e impulsionasse também a expansão do próprio modelo americano de Internet, aumentando ou consolidando sua influência através da comercialização de produtos e serviços e pelo estabelecimento de medidas de governança da rede (DeNardis, 2015; Powers & Jablonski, 2015).

Em sentido oposto está um discurso que enfatiza a prioridade da segurança:

> In the year since my speech, people worldwide have continued to use the Internet to solve shared problems and expose public corruption, from the people in Russia who tracked wildfires online and organized a volunteer firefighting squad, to the children in Syria who used Facebook to reveal abuse by their teachers, to the Internet campaign in China that helps parents find their missing children. […] For the United States, the choice is clear. On the spectrum of Internet freedom, we place ourselves on the side of openness. Now, we recognize that an open Internet comes with challenges. It calls for ground rules to protect against wrongdoing and harm. And Internet freedom raises tensions, like all freedoms do. But we believe the benefits far exceed the costs. […] The first challenge is achieving both liberty and security. Liberty and security are often presented as equal and opposite; the more you have of one, the less you have of the other. In fact, I believe they make it each other possible. Without security, liberty is fragile. Without liberty, security

> is oppressive. The challenge is finding the proper measure: enough security to enable our freedoms, but not so much or so little as to endanger them. |…| Finding this proper measure for the Internet is critical because the qualities that make the Internet a force for unprecedented progress – its openness, its leveling effect, its reach and speed – also enable wrongdoing on an unprecedented scale. Terrorists and extremist groups use the Internet to recruit members, and plot and carry out attacks. Human traffickers use the Internet to find and lure new victims into modern-day slavery. Child pornographers use the Internet to exploit children. Hackers break into financial institutions, cell phone networks, and personal email accounts. So we need successful strategies for combating these threats and more without constricting the openness that is the Internet's greatest attribute. The United States is aggressively tracking and deterring criminals and terrorists online. We are investing in our nation's cyber-security, both to prevent cyber-incidents and to lessen their impact. We are cooperating with other countries to fight transnational crime in cyber-space. The United States Government invests in helping other nations build their own law enforcement capacity. We have also ratified the Budapest Cybercrime Convention, which sets out the steps countries must take to ensure that the Internet is not misused by criminals and terrorists while still protecting the liberties of our own citizens. […] we are leading the push to strengthen cyber security and online innovation, building capacity in developing countries, championing open and interoperable standards and enhancing international cooperation to respond to cyber threats. […] This is a foreign policy priority for us, one that will only increase in importance in the coming years. That's why I've created the Office of the Coordinator for Cyber Issues, to enhance our work on cyber security and other issues and facilitate cooperation across the State Department and with other government agencies. (Department of State, 2011: online)

Do cruzamento destas duas óticas resulta uma linha de complementaridade: é preciso estabelecer políticas de segurança que por vezes restrinjam o acesso ou signifiquem uma violação de princípios como o da privacidade e neutralidade para que o sistema como um todo continue a funcionar de maneira confiável e livre. Embora tenha dado um peso relevante a esses pontos, Clinton não deixou claro como ou quem seria responsável por dosar as medidas para que essas ações referentes à segurança não se tornassem opressivas, justamente o cenário que se pretendia evitar[45].

A preocupação com a questão da segurança no ciberespaço não é uma medida iniciada por Clinton e mesmo a dualidade das políticas não constitui uma característica exclusiva da sua gestão enquanto Secretária de Estado, tampouco da Administração Obama da qual fazia parte. Naturalmente essa preocupação vem desde a criação da Internet, mas a

[45] Um exemplo bastante emblemático desta tensão entre duas lógicas diversas é o uso do Navegador Tor. Sendo uma ferramenta que permite o envio de dados de maneira anônima e relativamente segura, o que ajuda repórteres, investigadores, ativistas a ultrapassarem a barreiras eletrônicas de regimes que securitizam a informação ou os conteúdos das mensagem, o Governo norte-.mericano incentiva seu uso. No entanto, por ser uma ferramenta que também permite o uso por grupos terroristas e criminosos em geral, a National Security Agency (NSA) tem coletado e armazenado o número de I.P. de quem o usa ou simplesmente acessa a página do Navegador (BBC, 2014; Koch et al., 2016; Zetter, 2014).

formalização política da securitização do ciberespaço nos Estados Unidos pode ser identificada em documentos e iniciativas no governo de Bill Clinton, na década de 1990.

Em dezembro de 1999, o presidente Bill Clinton apresentou oficialmente uma nova concepção para a segurança tendo em vista os desafios para o século vindouro. O documento "*A New Strategy for a New Century*" (White House, 1999) buscava identificar tais desafios e colocou entre eles a cibersegurança face à ascensão do terrorismo:

> […] We also face threats to critical national infrastructures, which increasingly could take the form of a cyber-attack in addition to physical attack or sabotage, and could originate from terrorist or criminal groups as well as hostile states" (White House, 1999: 2). "We know that other governments and terrorist groups are creating sophisticated, well organized capabilities to launch cyber-attacks against critical American information networks and the infrastructures that depend on them (White House, 1999: 17).

De fato, já desde o início da década de 1990 alguns relatórios de agências especializadas apontavam uma preocupação em relação ao risco do uso das tecnologias de informação para fins terroristas. Foram, nessa altura, produzidos importantes discursos que se poderiam considerar elementos de um movimento de securitização, apontando a iminência de um risco, identificando objetos de referência e levantando um sentido de urgência na adoção de medidas de exceção. Um dos mais emblemáticos desses discursos foi o elaborado pela Academia Nacional das Ciências:

> We are at risk. Increasingly, America depends on computers. They control power delivery, communications, aviation, and financial services. They are used to store vital information, from medical records to business plans to criminal records. Although we trust them, they are vulnerable to the effects of poor design and insufficient quality control, to accident, and perhaps most alarmingly, to deliberate attack. The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb. (National Research Council, 1991)

A grande mudança, portanto, não foi a noção do advento das ameaças do ciberespaço. Os atentados de 11 de setembro puseram a questão em evidência, principalmente após a promulgação do *Patriot Act* (Congress of United States of America, 2001) que reforçava medidas de segurança para fazer frente à ameaça terrorista[46]. A

[46] No que concerne à segurança da informação, o Patriot Act apresentava algumas definições sobre o que seriam transgressões eletrônicas e as classificou como atos terroristas, dependendo das circunstâncias. Mais do que isso, permitiu a intercetação de comunicações por agentes oficiais, aprimorando suas capacidades de rastreio. Reforçou e regulamentou alguns elementos referentes à proteção das infraestruturas críticas já mencionadas nas administrações anteriores (Smith, Seifert, Mcloughlin, & Moteff, 2002).

segurança do ciberespaço, então, deixou de ser um assunto discutido essencialmente por um pequeno grupo de técnicos percebida como uma exigência fundamental, sobretudo no quadro de uma sociedade cada vez mais interdependente, assumindo aspectos de uma hiperpolitização (Lichtenbaum & Schneck, 2002; Lobato & Kenkel, 2015). Nesse sentido, o presidente Bush criou, após os referidos atentados, o Office of Cyberspace Security, na casa Branca e nomeou como chefe o seu então chefe da divisão contraterrorismo, Richard Clarke (Weimann, 2005). A partir da década de 2000 o teor desses discursos de securitização passou a figurar como textos em documentos oficiais.

4.1.2. A segurança do ciberespaço como política

A década de 2000 pode ser entendida como o período em que a preocupação com a segurança do ciberespaço se tornou um objeto concreto de ação política. Para isso muito contribuiu a exploração do tema pela mídia e pela indústria de entretenimento em geral, superestimando, por vezes, efeitos supostamente catastróficos ou conspiratórios, como em alguns documentários que por vezes exacerbavam a percepção de ameaças iminentes e muitas produções de Hollywood, que se multiplicaram nesta década[47].

A partir da década de 2000, alguns países formulavam e publicavam suas respectivas estratégias de cibersegurança e ciberdefesa e marcavam presença em fóruns multilaterais para discutir, juntamente com representantes de setores privados, organizações não-governamentais e instituições internacionais, princípios e medidas para implementar a governança do ciberespaço (Hofmann, 2016; Mathiason, 2009; von Bernstorff, 2003).

Esse movimento está ligado a uma percepção mais nítida das ameaças provenientes do ciberespaço. Contudo, diferente de outros elementos que dizem respeito à segurança, tanto interna como internacional, as políticas do ciberespaço foram sendo concebidas em função de duas singularidades. Primeiro, não há um ciberataque que tenha causado grande dano físico ou humano, grandes perdas financeiras e mesmo questões alarmantes de

O think tank *Cybersecurity Ventures* elencou as produções de Hollywood relacionadas à cibersegurança desde 1969. Naturalmente, à medida em que a realidade virtual se tornava mais comum ao longo dos anos, mais frequentes eram as produções. Contudo, a partir da década de 2000 há um aumento substancial na produção de filmes com a temática do ciberespaço ou que contenham elementos que se relacionam com temas como hacking, ativismo digital, investigações envolvendo meios eletrônicos, entre outros. A lista completa e uma breve descrição de cada título pode ser conferida em: https://cybersecurityventures.com/movies-about-cybersecurity-and-hacking/

segurança. Segundo, a continuidade do funcionamento do ciberespaço éser essencial ao funcionamento da sociedade contemporânea, já que há uma interdependência de funções e atividades essenciais propiciadas pelas conexões em rede. Assim, as políticas de segurança e de defesa que envolvem o ciberespaço não foram desenhadas de modo a restringir o seu uso. Pelo contrário, as estratégias de cibersegurança e de ciberdefesa publicadas nos EUA a partir da década de 2000 advogam a criação de políticas e instituições para o gerenciamento de mecanismos de contenção de ameaças no ciberespaço e, simultaneamente, incentivam a disseminação do uso[48]. Aliás, esta orientação norte-americana foi comum a outros países, considerando nautralmente as suas particularidades internas. Essas orientações comuns foram no sentido de estabelecer incentivos para o uso, ao mesmo tempo que se estabeleceram mecanismos de vigilância, ligados às forças armadas, aos serviços de inteligência ou mesmo autônomos para tratar da segurança no ciberespaço.

No caso dos Estados Unidos, essas políticas foram sendo refletidas nos discursos oficiais. Em fevereiro de 2000, o presidente Bill Clinton proclamava:

> "We know that we have to keep cyberspace open and free. We have to make, at the same time, computer networks more secure and resilient, and we have to do more to protect privacy and civil liberties. And we're here to work together." (The White House, 2000: online).

O discurso de securitização, no entanto, ganhou contornos muito mais definidos no mandato seguinte, do presidente George W. Bush, que já no preâmbulo da Estratégia Nacional para a Segurança do Ciberespaço, publicada em 2003, afirmava:

> In the past few years, threats in cyberspace have risen dramatically. The policy of the United States is to protect against the debilitating disruption of the operation of information systems for critical infrastructures and, thereby, help to protect the people, economy, and national security of the United States. We must act to reduce our vulnerabilities to these threats before they can be exploited to damage the cyber systems supporting our Nation's critical infrastructures and ensure that such disruptions of cyberspace are infrequent, of minimal duration, manageable, and cause the least damage possible. Securing cyberspace is an extraordinarily difficult strategic challenge that requires a coordinated and focused effort from our

[48] Os diversos documentos relativos às estratégias de ação para a promoção da segurança do ciberespaço têm elementos padrões. No geral os governos começam pelo reconhecimento da importância do ciberespaço e das tecnologias da informação para o desenvolvimento do país, passam para apontar os setores ameaçados seja por ciberataques ou pelo mal funcionamento das redes. Elencam setores governamentais responsáveis por criar bases para a proteção do ciberespaço e geralmente se dispõem a cooperar internacionalmente, seja através de parcerias bilaterais, ou através de ações multilaterais junto as instituições das quais são membros. O CCDCoE da NATO disponibiliza um banco de dados com as estratégias tanto de estados-membro quanto de terceiros (https://ccdcoe.org/cyber-security-strategy-documents.html). As bases das ações dos países para o ciberespaço estão lançadas em suas respetivas estratégias, contudo, a análise de outros documentos domésticos e internacionais é necessária para uma visão mais completa de cada caso.

> entire society—the federal government, state and local governments, the private sector, and the American people. (White House, 2003: iii)

A ideia expressa nesas palavras do presidente Bush foi acentuada por uma lógica de urgência das políticas a serem desenvolvidas para a segurança e defesa cibernética. Esse documento de 2003 não previa ações concretas, mas uma série de recomendações e princípios aplicáveis tanto em tempos de paz como em situações de guerra. Em tempos de paz, as preocupações de segurança focam-se sobretudo em atos de espionagem, enquanto em tempos de guerra as atenções priorizam a defesa das infraestruturas críticas. A Estratégia Nacional para a Segurança do Ciberespaço de 2003 contribuiu para um movimento de securitização do ciberespaço nos Estados Unidos porque previu uma política de vigilância constante, no pressuposto de que os objetos de referência (economia, liberdades civis, infraestruturas críticas e o próprio ciberespaço) estariam sob permanente ameaça.

Durante o governo Bush essa preocupação com a segurança e a defesa cibernética foram traduzidas na implementação de instituições militares e civis incumbidas de garantir e monitorar as ameaças no ciberespaço. Um dos resultados práticos dessas políticas deu-se em 2008, com a criação do Centro Nacional de Cibersegurança (White House, 2008). Com o foco na proteção das comunicações da Administração contra ameaças internas e externas, a criação desse sentro, juntamente com as recomendações do Cyberspace Policy Review, de 2009 (já no governo de Barack Obama) trouxe para o centro do poder norte-americano a proteção contra ameaças no ciberespaço (Homeland Security, 2009). Outras instituições, como o Centro de Segurança e Contraespionagem, a Secção de Cibersegurança e Comunicações , o Departmento de Defesa, o US CyberComm e a Agê3ncia Nacional de Segurança vêm compor a grade de instituições criadas para garantir a cibersegurança e a proteção contra ameaças cibernéticas à Administração norte-americana (Helms, 2015).

Em 2011, a Administração finalmente institucionalizou os critérios para a prevenção e redução de riscos provenientes do ciberespaço através da já mencionada Estratégia Internacional para o Ciberespaço (White House, 2011). O documento reforça os conceitos dos documentos anteriormente citados, mas três aspectos merecem ser destacados: a indispensabilidade do ciberespaço para as atividades diárias, a transnacionalização das ameaças e a noção de que a segurança do ciberespaço é um desafio multinível, de responsabilidade simultaneamente individual, do setor privado e do Estado. Assim, aparentemente, com base num discurso da securitização, as políticas de segurança – e em algumas mesmo de defesa – foram ampliadas e aprofundadas durante a Administração

Obama. O governo Obama recolheu, naturalmente, os resultados das políticas iniciadas nos mandatos anteriores e por isso foi-lhe possível conceber uma noção maior das ameaças provenientes do ciberespaço:

> It's the great irony of our Information Age -- the very technologies that empower us to create and to build also empower those who would disrupt and destroy. And this paradox […] is something that we experience every day. It's about the privacy and the economic security of American families. We rely on the Internet to pay our bills, to bank, to shop, to file our taxes. But we've had to learn a whole new vocabulary just to stay ahead of the cyber criminals who would do us harm -- spyware and malware and spoofing and phishing and botnets. Millions of Americans have been victimized, their privacy violated, their identities stolen, their lives upended, and their wallets emptied. According to one survey, in the past two years alone cyber crime has cost Americans more than $8 billion. (White House, 2009: online).

O presidente Obama elencou cinco áreas-chave[49], pelas quais reforçou as políticas de segurança e defesa do ciberespaço. Simbólico da abordagem da Administração Obama à segurança do ciberespaço é a sua intenção de alargar a agência em cibersegurança a estudantes através da promoção da literacia digital:

> we will begin a national campaign to promote cybersecurity awareness and digital literacy from our boardrooms to our classrooms, and to build a digital workforce for the 21st century. And that's why we're making a new commitment to education in math and science, and historic investments in science and research and development. Because it's not enough for our children and students to master today's technologies […] we need them to pioneer the technologies that will allow us to work effectively through these new media and allow us to prosper in the future. So these are the things we will do.(White House, 2009)

Essa conscientização para a responsabilidade social alargada pela cibersegurança vai a par com uma clara identificação das instâncias do Estado responsáveis pela aprovação das medidas tidas como necessárias. Por exemplo, em 2012 o presidente veio a público, através de um artigo de imprensa, pressionar o Senado para aprovar a Lei sobre Cibersegurança nestes termos:

> Today we can see the cyber threat to the networks upon which so much of our modern American lives depend. We have the opportunity—and the responsibility—to take action now and stay a step ahead of our adversaries. For the sake of our national and economic security, I urge the Senate to pass the Cybersecurity Act of 2012 and Congress to send me comprehensive legislation so I can sign it into law. (Obama, 2012).

[49] São elas: Parecerias do governo com organizações não-governamentais; trabalho em conjunto com todos os setores chave (incluindo governos locais e setor privado); estabelecer parcerias entre o setor público e setor privado; investimento em investigação e desenvolvimento, campanhas de conscientização para a cibersegurança e promoção da literacia digital.

Ainda que o Legislativo não tenha aprovado o projeto de lei como queria o presidente, prevaleceu uma tendência bastante marcada de hipersecuritização do ciberespaço na Administração Obama.

Com Donald Trump, a questão a segurança e da defesa cibernética parece assumir na verdade, a compreensão de Trump será a de que as capacidades de defesa e segurança cibernética dos Estados Unidos deve sobretudo ser um instrumento da expansão da influência americana:

> Protecting America's national security and promoting the prosperity of the American people are my top priorities. Ensuring the security of cyberspace is fundamental to both endeavors. Cyberspace is an integral component of all facets of American life, including our economy and defense. Yet, our private and public entities still struggle to secure their systems, and adversaries have increased the frequency and sophistication of their malicious cyber activities. America created the Internet and shared it with the world. Now, we must make sure to secure and preserve cyberspace for future generations. (White House, 2018: I)

Donald Trump declara que a revisão das políticas de cibersegurança feita na sua gestão devem não só dar continuidade ao conteúdo das políticas precedentes, mas também, "expand American influence abroad to extend the key tenets of an open, interoperable, reliable, and secure Internet".(White House, 2018: II). Apesar de aparentemente menos focado na securitização, o presidente Trump assume a necessidade de reforçar os instrumentos existentes em relação à segurança cibernética. Assim, em 2019, o presidente adotou uma Ordem Executiva que fortalecia os instrumentos existentes com financiamento e recursos humanos (White House, 2019). Mas, dado que o mandato em questão acontece depois do recorte temporal analisado neste trabalho, limitar-nos-emos aqui a aprofundar as questões das instituições de segurança da informação nos mandatos de Obama. Ora, tendo em conta os desdobramentos do movimento de securitização do ciberespaço no contexto brasileiro que estudaremos a seguir, importa aprofundar o papel da National Security

Agency (NSA)[50] neste domínio, pois tornou-se uma peça-chave para uma política mais agressiva e invasiva relacionada à segurança do ciberespaço[51].

Em 2013, o ex-colaborador da agência, Edward Snowden, denunciou que a NSA estava a coletar e a armazenar dados massivamente, incluindo cidadãos americanos (Harding, 2014; Richards, 2017; Zetter, 2014). Mais do que isso, as denúncias deram conta de que a comunicação de muitos líderes mundiais e autoridades de importantes organizações nacionais e internacionais também estavam sendo monitoradas. As denúncias causaram firme reprovação mundo afora e reações diplomáticas negativas por parte dos líderes visados (Abdenur, 2014; Guitton, 2013; Local, 2017). Houve também repercussões internas, já que provocou questionamentos acerca da violação da Quarta Emenda da Constituição (Atkins, 2013).

Esta situação foi, de algum modo, o culminar de uma evolução marcada por uma fundamental tensão de princípios. Desde os primeiros impulsos oficiais, tendo como marco os atentados de 11 de setembro e o Patriot Act, a questão da segurança e defesa do ciberespaço se consolidou na lei e na ação política, incluindo a admissão de práticas invasivas, ao longo das administrações Bush e Obama, em que o foco deixou de ser um indivíduo ou determinados grupos em concreto e passou a ser o monitoramento coletivo de cidadãos, facilitado pelo aprimoramento da capacidade tecnológica de processamento. Todavia, ao mesmo tempo que se promoveram tais ações para a garantia da segurança, foi seriamente questionada a necessidade e a legalidade da vigilância promovida pela NSA, sobretudo por sua capacidade de processamento de dados e abrangência do seu campo de ação[52].

[50] A National Security Agency é atualmente responsável pelo monitoramento e processamento de dados, interceptação de comunicações e criptografia com o propósito de contribuir para a garantia da segurança dos Estados Unidos. É responsável ainda pela segurança das comunicações da Administração norte-americana. Importa ressaltar que a NSA foca sua ação principalmente na coordenação e no processamento de dados coletados através de uma ferramenta chamada SINGINT50, baseada em sinais eletrônicos e metadados. Suas atividades não implicam, necessariamente, no emprego de recursos humanos para a coleta de dados, mas sim o processamento de dados coletados eletronicamente e de forma massiva (NSA, 2012).Essa coleta de dadosapesar de alvo de acusações crescentes de violação em larga escala da privacidade dos usuários das ferramentas de comunicação tanto internacionais quanto domésticas, tem base no Patriot Act, editado em 2001, por conta dos atentados terroristas daquele ano (Congress of United States of America, 2001: SEC 215, p. 17)

[51] Há estudos aprofundados sobre a análise do processo de securitização do ciberespaço nos Estados Unidos que focam desde o governo de Bill Clinton até o governo Obama: (Boys, 2018, 2018; "From Cyberterrorism to Cyberwar, Back and Forth : How the United States Securitized Cyberspace | Scinapse," n.d.; Georgieva, 2015; Hansen & Nissenbaum, 2009a; Hersee, 2019; Kasper, 2014; Schmoldt, 2019; Stojaković, 2018; Lobato, 2015).

[52] Vale ressaltar que, segundo as revelações, a prática da vigilância massiva foi replicada em outros países: "The surveillance practices revealed by Snowden show clearly if not completely that governments – especially

O resultado foi uma espécie de movimento de securitização "spill over" securitizador em dois sentidos. Em primeiro lugar, a securitização não visou originariamente o ciberespaço: apesar de haver registros da percepção das ameaças envolvendo o ciberespaço anteriores aos ataques terroristas de 11 de setembro, somente depois deste evento é que a questão da segurança do ciberespaço e "através" do ciberespaço ganhou peso e se tornou mais concreta. Assim, verificou-se um processo de securitização que transbordou para outro. Em síntese, nos Estados Unidos, o movimento de securitização do ciberespaço radicou, em grande parte, nas ações contra o terrorismo internacional.

Esse movimento de securitização em spill over está patente na justificativa do presidente Obama, quando questionado sobre denúncias de espionagem da NSA:

> It is hard to overstate the transformation America's intelligence community had to go through after 9/11. Our agencies suddenly needed to do far more than the traditional mission of monitoring hostile powers and gathering information for policymakers. Instead, they were now asked to identify and target plotters in some of the most remote parts of the world, and to anticipate the actions of networks that, by their very nature, cannot be easily penetrated with spies or informants.
>
> […] Today, new capabilities allow intelligence agencies to track who a terrorist is in contact with, and follow the trail of his travel or his funding. New laws allow information to be collected and shared more quickly and effectively between federal agencies, and state and local law enforcement. Relationships with foreign intelligence services have expanded, and our capacity to repel cyber-attacks have been strengthened. And taken together, these efforts have prevented multiple attacks and saved innocent lives -- not just here in the United States, but around the globe.
>
> […]Laboring in obscurity, often unable to discuss their work even with family and friends, the men and women at the NSA know that if another 9/11 or massive cyber-attack occurs, they will be asked, by Congress and the media, why they failed to connect the dots. What sustains those who work at NSA and our other intelligence agencies through all these pressures is the knowledge that their professionalism and dedication play a central role in the defense of our nation. (White House, 2011)

A consolidação da NSA como uma das principais ferramentas de combate ao terrorismo deu suporte a um segundo transbordamento. Com a assunção do terrorismo como preocupação de natureza e alcance internacionais, muitas das práticas adotadas nos Estados Unidos foram replicadas mundo afora, não só nos países desenvolvidos, mas de forma geral. Uma vertente dessas posturas foi precisamente a securitização da comunicação através do

American, British, Canadian, and possibly other agencies – engage in astonishingly large scale monitoring of populations, and also how they do it" (Lyon, 2014: 2).

ciberespaço. A hegemonia dos EUA no continente americano mais acentuou esse efeito de imitação das soluções norte-amercianas para o ciberespaço. É neste contexto que, por um lado, se explica a evolução da abordagem da segurança do ciberespaço pelas autoridades brasileiras e, por outro, ganha relevo a especificidade dessa abordagem, materializada no Marco Civil para a Internet.

4.2. Uma dessecuritização não intencional? A atuação brasileira nas políticas para o ciberespaço

Avaliando as políticas brasileiras para o ciberespaço, percebe-se um reflexo do que ocorre em outros contextos e, desde logo, nos Estados Unidos. Também no Brasil o poder público vê no ciberespaço um sinônimo de desenvolvimento social e necessário para o desenvolvimento tecnológico do país, mas que traz consigo novas ameaças e necessidades ainda não vislumbradas em termos jurídicos ou estratégicos. Há, no entanto, no caso brasileiro, algo de singular: apesar de ser determinante um discurso que, ainda que não dirigido explicitamente a uma securitização, advoga um endurecimento das leis e uma regulamentação reforçada (inclusive criminal) das atividades no ciberespaço, ele deu lugar a uma resposta que pode ser classificada como dessecuritizadora em um momento de tensão definidora envolvendo este meio,.

Para desenvolver este raciocínio, este capítulo passa por três momentos principais. O primeiro é uma breve avaliação de como as políticas para o ciberespaço se foram desenvolvendo no Brasil, quer em termos de segurança e defesa quer em termos mais gerais. Para tanto, aborda-se primeiramente a evolução das leis referentes a segurança digital dos usuários, proteção de privacidade, entre outros aspectos envolvendo a Internet e o ciberespaço. A segunda parte analisa o referido momento de tensão definidora, situado entre a denúncia de espionagem por Edward Snowden e a aprovação do MCI pela Câmara dos Deputados no Brasil. Por fim, a terceira parte analisa as respostas a esse momento. Naturalmente, a matéria-prima para a investigação veio, como já mencionado, de discursos oficiais, entrevistas a autoridades e representantes da sociedade civil participantes ativamente das discussões sobre a questão digital no Brasil, colhidas pessoalmente ou através de terceiros. Não obstante e não menos importante, documentos oficiais e relatórios produzidos pelos governos brasileiro, norte-americano e por organizações internacionais também são usadas na construção do argumento central.

4.2.1. O Brasil e o ciberespaço: utilização, expansão e organização.

Assim como outras potências emergentes, o Brasil tem experimentado um constante crescimento do uso das tecnologias de comunicação. Atualmente, o país conta com pouco mais de 123 milhões de usuários, ou seja, aproximadamente 60% da população, com uma tendência e potencial de crescimento através do próprio avanço dessas tecnologias e com programas de expansão propostos pelo governo federal, como o Internet Para todos (Ministério da Ciência, Tecnologia, 2018), entres outros programas de inclusão digital, com alcance local ou estadual. Estima-se que em 2022 o número de usuários aumente para cerca de 65% da população (Statista, 2018). Esse montante, no entanto, não é distribuído igualitariamente. Há desigualdades entre as regiões, classes econômicas e zonas de habitação. Enquanto 98% das pessoas da classe A utilizam a Internet, esse índice é de 49% nas classes mais baixas (CETIC, 2017c). A região sudeste é a que mais conta com usuários da Internet. Utilizam-na através de mais de um ponto de acesso (CETIC, 2017b, 2017d, 2017e, 2017a).

A comunicação pessoal é a principal atividade realizada pelos usuários que tem nos celulares o seu principal instrumento de acesso. Não obstante, atividades como *Internet Banking*, tratamento de assuntos administrativos, comércio virtual e serviços de *streaming* são atividades largamente utilizadas. A expectativa apontava para 120 milhões de compras virtuais, movimentando aproximadamente 75 bilhões de reais em 2019 (EcommerceBrasil, 2020)[53].

Seguindo a tendência mundial, o Brasil reconheceu a questão da segurança da informação como um dos três setores de importância estratégica para a segurança nacional, ao lado dos setores espacial e nuclear. A Estratégia de Defesa Nacional, de 2008, apresenta um forte componente em direção ao fortalecimento desses setores não somente em face as ameaças, mas também à independência brasileira em relação às tecnologias estrangeiras:

> "Projeto forte de defesa favorece projeto forte de desenvolvimento. Forte é o projeto de desenvolvimento que, sejam quais forem suas demais orientações, se guie pelos seguintes princípios",
>
> […] Independência nacional, alcançada pela capacitação tecnológica autônoma, inclusive nos estratégicos setores espacial, cibernético e nuclear. Não é

[53] Há várias instituições que tratam das estatísticas da Internet brasileira. Dados mais completos podem ser conferidos na página do Instituto Brasileiro de Geografia estatística (ibge.gov.br) e do Comitê Gestor da Internet (cgi.br) e EcommerceBrasil (ecommercebrasil.com.br).

> independente quem não tem o domínio das tecnologias sensíveis, tanto para a defesa como para o desenvolvimento. (Presidência da República, 2008: online)

De fato, como afirmam Geraldo & Cossul (2017), o desenvolvimento tecnológico assim como a busca pela autonomia tecnológica são elementos centrais para o desenvolvimento das políticas de defesa em qualquer cenário. No Brasil, a busca por desenvolvimento esbarra em problemas como deficiências na capacidade de produção da própria tecnologia. Assim, a ascensão do setor da cibersegurança entre os pilares da defesa nacional também implica em uma adequação da indústria militar brasileira, que deve incorporar a questão cibernética, mas também integrar a comunicação das Forças Armadas e os recursos existente a este setor.

Este desafio brasileiro, por sua vez, sublinha a carência de recursos humanos devidamente capacitados:

> A primeira prioridade do Estado na política dos três setores estratégicos será a formação de recursos humanos nas ciências relevantes. Para tanto, ajudará a financiar os programas de pesquisa e de formação nas universidades brasileiras e nos centros nacionais de pesquisa e aumentará a oferta de bolsas de doutoramento e de pós-doutoramento nas instituições internacionais pertinentes. (Presidência da República, 2008, online)

A questão do desenvolvimento tecnológico e a falta de recursos humanos capacitados para promovê-los no âmbito nacional impõe a necessidade de cooperação internacional. Essa necessidade está identificada em outro documento-guia da cibersegurança brasileira. O Livro Verde da Cibersegurança no Brasil, entende que a

> segurança cibernética caracteriza-se cada vez mais como condição *sine qua non* de desenvolvimento, requerendo para tanto, dentre outras ações, a promoção de diálogos e de intercâmbios de ideias, de iniciativas, de dados e informações, de melhores práticas, para a cooperação no tema, no país e entre países. (Presidência da República, 2010)

Deste modo, ao mesmo tempo em que o país busca autonomia tecnológica, tem em consideração que necessita buscar esse desenvolvimento através da cooperação e da formação de recursos humanos em academias exteriores. Os documentos

Diferente das estratégias de cibersegurança de outros países, o Livro Verde da Cibersegurança no Brasil não só sugere as direções que as políticas de cibersegurança deveriam seguir, mas pondera, tema a tema, as oportunidades e os desafios da segurança da informação no Brasil, entre eles, as questões tradicionais desse assunto (como a proteção a infraestruturas críticas, o próprio desenvolvimento das tecnologias da informação, os

desafios jurídicos e as possibilidades de cooperação internacional), como também temas que não são necessariamente apontados nas demais estratégias, como a relação da cibersegurança com a educação e com as questões de meio ambiente.

É importante enfatizar que o Estado Brasileiro distingue conceitualmente a defesa cibernética das questões de segurança cibernética. Assim:

> [a defesa cibernética é] conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planeamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente. (Ministério da Defesa, 2014: 18).

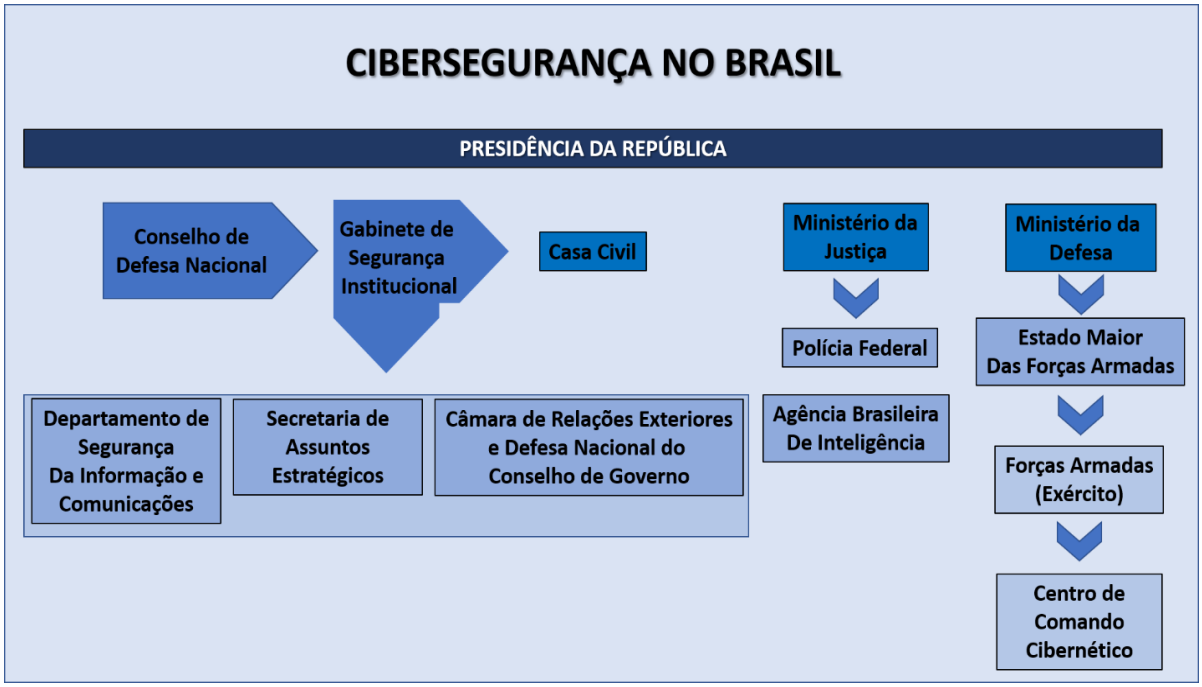
Por outro lado, a segurança cibernética é um conceito mais genérico, capaz de agregar não só a defesa cibernética, mas a garantia do bom funcionamento do ciberespaço para fins civis, por exemplo:

> [a segurança cibernética é] arte de assegurar a existência e a continuidade da sociedade da informação de uma nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas". (Ministério da Defesa, 2014: 19).

Em termos de quadro legal e institucional, o Brasil adotou algumas leis específicas de proteção contra crimes cibernéticos, como em matéria de privacidade dos usuários ou de exposição de informações sensíveis de usuários. Por ora, o Brasil ainda não tem guias definitivos que apontem direções para a governança da Internet, embora este seja um assunto bastante presente em organismos como o Comitê Gestor da Internet. Contudo, o MCI, aprovado em 2014, fixa princípios a serem seguidos em uma futura iniciativa de governança. Por fim, o país não conta com uma lei definitiva de proteção de dados na Internet. Esses marcos legais serão revisitados de uma maneira mais profunda mais adiante por trazerem importantes elementos úteis para o entendimento do processo e, sobretudo, dos discursos de securitização do ciberespaço no Brasil.

Em termos de responsabilidade técnicas, a Agência de Inteligência Brasileira (Abin), o Ministério da Defesa, a Polícia Federal, o Centro de Treinamento de Incidentes de redes do Governo (CTIR), o Centro de Estudos, Respostas e Treinamentos de Incidentes de Segurança (CERT), e setores das Forças Armadas, sobretudo do Exército com o Centro de Defesa Cibernética, são os responsáveis pelo monitoramento e proteção das informações.

Figura 1. Organização da Cibersegurança no Brasil



Fonte: Adaptado de Diniz et al. (2014); Ministério da Defesa, Ministério da Justiça, Conselho de Defesa Nacional.

No topo da hierarquia da estrutura institucional da segurança cibernética no Brasil está a Presidência da República. Diretamente subordinados à Presidência da República, estão o Conselho der Defesa Nacional (CDN), a Câmara de Relações Exteriores e defesa Nacional do Conselho de Governo (CREDEN) e o Gabinete de Segurança Institucional. Este último tem status de ministério ao qual está subordinado a Agência Brasileira de Inteligência (ABIN). Esses órgãos têm como função o planejamento político-estratégico e eventualmente elaboram normativas em relação às políticas de segurança e defesa cibernética. Sob um aspecto civil, o tema também é parte das atribuições do Ministério da Justiça e da Casa Civil.

O Ministério da Defesa, também subordinado à Presidência da República, se ocupa do segmento operacional da segurança e defesa cibernética através do Estado Maior das Forças Armadas, que coordena o Comando de Defesa Cibernética das Forças Armadas (CDCFA). Através das Forças Armadas, especificamente do Exército Brasileiro, o CDCFA coordena temas mais específicos como, por exemplo, guerra cibernética. Neste aspecto, o Comando de Defesa Cibernética tem tido oportunidades de se especializar no campo da defesa cibernética em grandes eventos (Conferência Rio+20, Copa das Confederações, visita do Papa Francisco, Copa do Mundo e Olimpíadas).

Figura 2. Organização da Defesa Cibernética no Brasil

Fonte: Adaptado de Ministério da Defesa (2014)

4.2.2. A securitização induzida pelo contexto: das leis e discussões sobre crimes cibernéticos ao Marco Civil da Internet

Os debates sobre as questões jurídicas aplicadas ao ciberespaço tiveram um importante precedente em 1999, com o Projeto de Lei da Câmara dos Deputados (PL. 84/1999[54]), apresentado ao Senado Federal como substitutivo de outras leis discutidas ainda na década de 1990. O Projeto de Lei (PL) propunha medidas preventivas relativas à identificação e possíveis punições de crimes cibernéticos (Câmara dos Deputados, 1999a). Diante do contexto de crescente uso dos meios digitaisl, a necessidade de criar novos mecanismos legais de modo a atualizar aspectos da Lei Penal vigente desde 1940, o projeto de lei versava sobre uma diversidade de situações que passariam a ser configuradas propriamente como crimes cibernéticos, sendo desde questões relacionadas com abusos a

[54] O projeto de lei PL Nº 84/1999 não foi o primeiro a ser proposto com o intuito de estabelecer e regular os crimes eventualmente cometidos através do uso das tecnologias da informação. Outros projetos (PLS 152/91; PL 4102/93; PL 2644/96; PL1713/96; PL3258/97; PLS 76/00 e PLS 137/00) com propostas semelhantes ou que tratavam de temas que depois foram agregados ao PL 84/1999 já abordavam o tema no início da década de 1990. Contudo, como a Internet no Brasil só veio a se disseminar para fora dos meios acadêmicos ou governamentais nos anos seguintes, a questão ganhou mais substância e contornos mais concretos a partir do momento em que a Internet estava em vias de consolidação como meio de comunicação amplamente utilizado.

crianças[55], o acesso indevido ou sem o consentimento a dados de terceiros e respectiva divulgação ou as fraudes financeiras.

Ao passar da Câmara dos Deputados para o Senado Federal, a Lei ficou conhecida como Lei Azeredo em alusão ao seu relator (o então senador Eduardo Azeredo) e ganhou notoriedade através de polêmicas discussões que envolviam a falta de garantias a direitos individuais e a imputação da fiscalização das ações a agentes não investidos dessa capacidade jurídica. Deste modo, a lei foi bastante criticada por entidades ligadas à defesa da liberdade de expressão e de liberdades no ambiente virtual até que foi aprovada em fevereiro de 2012 com modificações substanciais, mais de uma década depois da proposta inicial. Neste sentido, a organização-não governamental Article19 apontava que:

> O Projeto de Lei prevê uma série de medidas que transformariam as empresas privadas responsáveis pelo fornecimento de serviços de Internet em uma força policial online. É possível que o Projeto de Lei exija que essas empresas denunciem à polícia supostas violações do código penal e imponha responsabilidade penal às partes que não cumprirem esses deveres. As mesmas medidas exigem a fiscalização maciça e a retenção de dados de todas as comunicações online por essas mesmas empresas privadas, que não possuem responsabilidade jurídica necessária para tais atos, por um período de três anos, com poucas restrições nas circunstâncias sob as quais um tribunal poderia ordenar a divulgação dos dados. Medidas semelhantes já foram consideradas inconstitucionais em alguns países europeus, e o governo brasileiro se mostra ávido a enfrentar semelhante disputa em seus próprios tribunais. (Article19, 2012) .

Por ter um caráter que lembrava um regime de exceção e também pelas suas definições vagas, o PL ganhou uma alcunha abertamente pejorativa, passando a ser conhecido como AI-5 Digital[56]. Na altura, o Deputado Lincoln Portela levantava o teor excepcional do PL e se posicionava contra à aprovação do projeto:

> Esse PL aborda um tema pulsante, porém polêmico, e tem sido amplamente criticado, especialmente por ameaçar o direito à privacidade, uma vez que determina que os provedores de acesso à rede mundial de computadores mantenham, pelo prazo de 3 anos, os dados de conexão do usuário. O enfoque dado pela proposta em curso privilegia a criminalização em detrimento da liberdade de acesso e aos direitos democráticos dos usuários. É preciso, porém, Sr. Presidente, que, antes de propormos punições por crimes cometidos na Internet, sejam estipulados os direitos e deveres dos usuários e provedores. Para tanto, é

[55] Uma das questões mais sensíveis nas discussões jurídicas sobre o ciberespaço no Brasil é justamente a questão da proteção infantil em ambiente digital. Questões como pedofilia e a divulgação de pornografia infantil são recorrentes e, em outras situações, foram alvo de inquéritos parlamentares. Assim, temas envolvendo ameaças a usuários menores de idade ou crianças tendem a estar presentes nas discussões não só no Brasil, mas a nível internacional.

[56] O Ato Institucional Número 5 (AI-5) foi um decreto presidencial emitido em 1968 pelo então presidente Artur da Costa e Silva. No contexto da ditadura militar, o AI-5 suspendia as garantias constitucionais e cassava os mandatos de parlamentares como também instituía interferências do Governo Federal nas esferas municipais e Estaduais.

> fundamental a aprovação do anteprojeto do marco regulatório da Internet, elaborado pelo Poder Executivo com base em consulta popular. O PL 84/99, que recebeu dos ativistas da Internet livre a alcunha de "AI-5 Digital", tem sido alvo de duras críticas da população, que apresentou petição contrária à proposta, com quase 350 mil assinaturas. A aprovação desse projeto poderia significar imenso atraso para o País, pois a Internet é hoje instrumento essencial ao desenvolvimento da cidadania. Sr. Presidente, não vamos colocar em risco a democracia e a liberdade de nossos cidadãos! Aguardemos, portanto, a análise da proposta de marco civil da Internet, pois não podemos pensar em punição sem cuidarmos, primeiro, dos direitos dos usuários da rede. […] (Portela, 2011: online).

É interessante ressaltar como o deputado enfatiza sua crítica ao projeto destacando uma ameaça à democracia e à liberdade. O PL passa a ser também uma ameaça, ao viabilizar uma medida de exceção. Mesmo assim, apesar de rejeitar a proposta, não rejeita o projeto, mas o posterga para um contexto em que já se tenham estabelecido os papeis dos atores e direitos dos usuários da Internet no Brasil.

Do mesmo modo, a Deputada Manuela D´Ávila, menos enfática, tinha uma visão semelhante. Segundo ela, o PL

> […] cria um estado de exceção permanente na Internet, que controla e pune os usuários. O projeto, além da censura e vigilância, também apresenta problemas jurídicos. Estes vão desde a ignorância de princípios fundamentais do Direito Penal e chegam a graves ofensas à Constituição.

De fato, o texto inicial do PL era bastante amplo e ambíguo e previa punições a ações comuns, como por exemplo, o artigo 8.º, que previa punição a quem "Apagar, destruir, modificar ou de qualquer forma inutilizar total ou parcialmente dado ou programa de computador de forma indevida ou não autorizada". Ou o artigo 9.º, que punia quem obtivesse "acesso indevido ou não autorizado, a computador ou rede de computadores". Ou ainda o artigo 10.º: " Apagar, destruir. alterar, ou de qualquer forma inutilizar, senha ou qualquer outro mecanismo de acesso a computador, programa de computador ou dados. de forma indevida ou não autorizada". Ainda havia a discussão sobre a questão da vigilância e a fiscalização das supostos delitos, responsabilidade que seria compartilhada com os provedores de acesso (Câmara dos Deputados, 1999b)

A versão final aprovada e sancionada pela então presidente Dilma Rousseff resumiu-se em prever penas a quem:

> Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita. (Presidência da República, 2012: online)

Quase concomitantemente, outro projeto de lei de conteúdo correlato ganhava repercussão nacional e foi discutido em regime de urgência no Congresso Nacional. O projeto de Lei 2793/2011 ganhou notoriedade por fazer referência ao roubo eletrônico de informações, nomeadamente fotos, através de *phishing* de uma famosa atriz, que acabou involuntariamente emprestando seu nome à lei que, ficou conhecida como Lei Carolina Dieckman. A lei tipificou como crime a "invasão de dispositivo informático alheio […], mediante violação […] de mecanismo de segurança (a) fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita" (Câmara dos Deputados, 2012: online), para além da interrupção do serviço de comunicação e a falsificação de documentos.

Nota-se que, apesar de não resultarem em uma situação de securitização propriamente dita, estas elaborações legislativas e os debates em torno delas compuseram um contexto de enfrentamento ao que os poderes públicos consideraram como ameaças. Estas iniciativas acabaram assim por politizar as questões relativas ao ciberespaço, mobilizando reações não só de parlamentares, mas de importantes setores da sociedade.

De fato, alguns dos entrevistados para este trabalho, principalmente os que estavam ligados ao terceiro setor, mencionaram receio em relação às tentativas de criação de uma lei de proteção de dados no Brasil. De acordo com sua percepção, o ambiente político no país não favorecia necessariamente uma lei de proteção de dados que tivesse em conta as garantias individuais. Embora reconhecessem a necessidade de se implementar uma diretiva para as políticas de proteção de dados, mencionaram um certo alívio ao constatar que esse tema ainda permanecia aguardando melhores definições, mesmo depois da aprovação do MCI.

Ainda que tenham, a princípio, descartado os elementos mais controversos que poderiam ser entendidos como propícios a medidas de exceção, as duas leis referidas se aproximam de temas bastante sensíveis à segurança cibernética pois tratam de estabelecer medidas de dissuasão contra os crimes cibernéticos, uma questão bastante relevante nas políticas de cibersegurança, já que engloba um vasto leque de atividades (roubo de dados, falsificação de identidades, fraudes econômicas). Essas questões, devido ao ambiente em que se propiciam, estão intimamente ligadas à questão da segurança cibernética, neste sentido, a União Internacional das Telecomunicações tem considerado os crimes cibernéticos e a questão da cibersegurança como elementos indissociáveis (ITU, 2012: 2).

O tema dos crimes cibernéticos ganhou destaque em 2015 quando foi instalada na Câmara dos Deputados uma Comissão Parlamentar de Inquérito (CPI) destinada, como resumia o então presidente da Câmara, Eduardo Cunha, "a investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país" (Prado, 2016: online). Os principais motivos foram uma investigação da Polícia Federal que sondava desvios de dinheiro via *Internet banking* através de *phishing* (Polícia Federal, 2014), um aumento de quase 200% nas denúncias envolvendo páginas na Internet ligadas ao tráfico de pessoas e um relatório produzido pela empresa de segurança cibernética Symantec apontando uma soma de 15 bilhões de dólares de gastos relacionados a crimes cibernéticos no Brasil. A CPI ouviu diversos profissionais e representantes de diversos setores da sociedade, entre eles diretores de grandes empresas de Internet como Yahoo!, Google, Twitter, Facebook, responsáveis de órgãos governamentais, como o Instituto Nacional de Tecnologia da Informação e Serviço Nacional de Processamento de Dados, representantes de entidades de proteção aos Direitos da Criança e do Adolescente e procuradores estaduais e federais (Câmara dos Deputados, 2016)[57].

4.2.3. Objeto e conteúdo do Marco Civil da Internet e seu caráter dessecuritizador.

A elaboração de leis e iniciativas governamentais para a promoção do acesso à Internet e os debates sobre questões de segurança e, principalmente, sobre a privacidade dos usuários e a neutralidade das redes, convergiram para o MCI. Mesmo na urgência da

[57] Entre os resultados da CPI estão a proposição de projetos de leis que incrementam a capacidade dos órgãos e instituições existentes para combater o mau uso e a páticas de crimes na internet. É possível destacar a possibilidade de confisco de bens ligados a crimes cibernéticos, ainda que tenham sido adquiridos de forma legal. A ampliação da abrangência do crime de invasão de equipamentos eletrônicos, passando a compreender, por exemplo, a obtenção e exposição de dados pessoais privados. A disposição de fundos provenientes do Fundo de Fiscalização das Telecomunicações (FISTEL) para a investigação de crimes cibernéticos. A ampliação da responsabilidade pelas investigações dos crimes cibernéticos, passando a ser reconhecidos como assunto de repercussão interestadual e internacional. Propôs o bloqueio de aplicações mediante ordem judicial. Propõe a ampliação da fiscalização e controle através do Tribunal de Contas da União (TCU), Agência Nacional de Telecomunicações (Anatel) e pela Comissão de Ciência, Tecnologia, Comunicação e Informática. Sugere ainda que o Poder Executivo adote uma série de medidas que melhore a segurança da infraestrutura de TIs, tais como a implementação de processos de gestão de risco, a adoção de tecnologias padrões de formato aberto, a realização de auditorias de forma a complementar as políticas já previstas pelo próprio governo. Sugere a integração institucional no combate ao crime cibernético, envolvendo o Banco Central, a Polícia Federal, a Presidência da República e o Ministério da Justiça (que atualmente também integra a pasta da Segurança Pública). Sugere também a criação de uma vara judicial específica dedicada aos crimes em ambiente virtual. O relatório final da CPI dos Crimes Cibernéticos pode ser encontrado em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=214D61B364D3F74027CAB7F56C3E0C39.proposicoesWeb2?codteor=1455189&filename=REL+4/2016+CPICIBER+%3D%3E+RCP+10/2015 (Camara dos Deputados, 2016)

elaboração de medidas que tipificassem e coibissem práticas criminosas em ambiente virtual, muito foi manifestado no sentido de estabelecer direitos dos usuários e o papel dos provedores de acesso como também dos atores públicos. Ainda durante as discussões das leis mencionadas no tópico anterior, argumentou-se no sentido de que a aprovação do MCI precedesse a formulação de novas leis referentes ao tema do ciberespaço. Assim, o Marco Civil passou a ser a referência que estabelece princípios para a agenda brasileira sobre a Internet, tanto no âmbito interno quanto nas sugestões de pautas em âmbito multilateral.

Segundo entrevistados que estiveram presentes nas primeiras discussões preparatórias do MCI, as primeiras ideias que vieram a constituir o texto inicial do MCI foram concebidas entre 2009 e 2011 no âmbito do Ministério da Justiça em parceria com a Escola de Direito da Fundação Getúlio Vargas, do Rio de Janeiro tendo em vista o que é resumido por Tomasevicius (2016: 273) como "uma lei sobre comportamento na esfera virtual". O projeto da Lei 12.965/12 foi aprovado em 2014, após várias rodadas de consultas públicas, votações em uma Comissão Especial na Câmara dos Deputados (CGI, 2013; Goulart & Silva, 2015; Pilati & Olivo, 2017), sendo uma das últimas medidas regulamentadas no mandado da presidente Dilma Rousseff, em maio de 2016 (G1, 2016). O MCI tem três focos principais: a privacidade dos usuários, a liberdade de expressão e a neutralidade da rede. Com base nessa tripla grade, desenvolve-se um quadro normativo que visa estabelecer direitos dos usuários, garantir a proteção dos dados que fornecem, regular o uso jurídico desses dados, bem como densificar a função social da Internet, principalmente através da garantia da liberdade de expressão e da construção em conjunto de conhecimento. Nos mesmo termos, o MCI ainda estabelece responsabilidades civis dos usuários e provedores de acesso à Internet (Presidência da República, 2014; Tomasevicius Filho, 2016).

A relevância do MCI evidencia-se em ao menos em dois aspectos. Juridicamente, apesar do Brasil não estar inserido em grandes marcos internacionais referentes ao ciberespaço ou mesmo internamente não contar com uma lei de proteção de dados, a aprovação do MCI colocou o país na vanguarda, pois foi a primeira lei do seu tipo no mundo, ou seja, a primeira iniciativa a favor da garantia de direitos individuais no ciberespaço. Para além disso, o Marco Civil pretende funcionar também como uma diretriz para a aprovação de outras medidas de governança da Internet através do estabelecimento de princípios orientadores para o efeito.

Por outro lado, no plano político propriamente dito, não obstante ter sofrido mudanças substanciais no texto original, o MCI é considerado uma das iniciativas mais exitosas do Governo Dilma Rousseff, ou como a própria presidente pontuava no Twitter:

> A aprovação do #MarcoCivil da Internet pela Câmara dos Deputados é uma vitória de toda a sociedade brasileira. O projeto mostra o protagonismo do Brasil em um tema q o mundo debate, a segurança, a privacidade e a pluralidade na rede #MarcoCivil. (Braga, 2014).

E, nesse sentido, o MCI somado a outras iniciativas do Governo acabou por pavimentar o caminho da Política Externa brasileira na tentativa de assumir um protagonismo internacional no campo da governança da Internet (Guerrini, 2014; Santoro & Borges, 2017). Foi assim que o MCI recebeu elogios do presidente do ICANN, Fadi Chehadé, bem como de Sir Tim Berners-Lee[58], que destacou a natureza inspiradora do MCI para muitos outros países: "Esta abordagem visionária já teve impactos globais. Da Itália até a Nigéria, outros países estão tentando imitar o Brasil. E por isso, a Internet ama o Brasil" (Berners-Lee, 2016: online).

O texto final trata, em resumo, das relações entre usuários e provedores de acesso. Há, no entanto, elementos-chave que determinam o teor e o objetivo do documento. Esses temas não surgem necessariamente como uma novidade nas discussões sobre a governança e a promoção dos Direitos Humanos na Internet. Temas como a inclusão digital (art. 27), proteção e a inviolabilidade da privacidade (art. 8) e a liberdade de expressão (art. 2) entre outros não são necessariamente inéditos na regulação desta matéria. Contudo, o MCI os coloca como princípios que, num total de 8, determinam as diretrizes para a ação do poder público sobre a matéria (Presidência da República, 2014b). E essa foi a sua novidade no plano comparado.

A lei nº 12.965 (Marco Civil da Internet) é composta por 32 artigos, divididos em 5 capítulos que estabelecem como marcos regulatórios o respeito à liberdade de expressão, a busca da universalização do acesso à informação para os brasileiros, a intenção de promover inserção internacional através da tecnologia e proteção de direitos fundamentais tanto de quem produz conteúdos quanto de quem os consome, a proteção de dados e a privacidade dos usuários e garantia da neutralidade das redes. O primeiro capítulo estabelece os princípios, tais como a proteção da liberdade de expressão, da livre iniciativa, da defesa

[58] Cientista da computação britânico, professor do Massachusetts Institute of Technology, conhecido por formular o sistema WWW (World Wide Web), no qual se baseia a Internet contemporânea.

do consumidor, das garantias de neutralidade da rede, entre outros que norteiam não só o documento, mas as políticas a serem implementadas tendo o Internet como tema. O segundo capítulo trata exclusivamente da garantia dos direitos dos usuários. Começa por reconhecer que o acesso à Internet é essencial para o exercício da cidadania, coloca condições para a coleta de dados e reforça a garantia da privacidade e a inviolabilidade dos dados pessoais, do sigilo do fluxo de informações. O capítulo terceiro é dedicado às responsabilidades dos provedores de serviços de Internet. Destaca-se a garantia da neutralidade das redes, que não deve ser passível de interferências que alterem a prestação do serviço em termos de qualidade e continuidade. O MCI atribui aos provedores de acesso como responsáveis pela custódia dos dados dos usuários, mas os exime de culpa em caso de danos a terceiros. Por fim, o capítulo condiciona a requisição de dados aos processos judiciais, cíveis ou penais, sempre sob o impulso de um juiz.

O papel do poder público é definido no capítulo quarto. O MCI reconhece outros atores que não o Estado como partícipes da gestão e expansão da Internet no Brasil. O poder público se coloca como um fomentador do desenvolvimento e expansão da Internet através de uma gestão compartilhada

Por fim, no capítulo quinto, o MCI reforça a garantia da liberdade de escolha do usuário em relação aos terminais de acesso e ao conteúdo acessado, tendo em conta, por exemplo, disposições do Estatuto da Criança e do Adolescente (Lei Nº 8069, de 1990) e enfatiza o papel do poder público, compartilhado com os setores-chaves acima citados, na promoção da educação e inclusão digital.

Cabe ainda destacar dois aspectos que agregam considerável valor ao MCI. O primeiro deles é o princípio da neutralidade da rede. Para além dos protocolos técnicos, a neutralidade da rede, tal como disposta no MCI, prevê que os dados sejam tratados de modo isonômico pelos provedores de acesso. Isso implica que os provedores de acesso não poderão, por exemplo, diminuir a velocidade de transmissão dos dados dependendo da sua proveniência, do tipo de aparelho que os processa ou, principalmente, de seu conteúdo. O segundo aspecto é a questão da privacidade dos dados. O MCI prevê que os provedores de acesso não podem divulgar os dados fornecidos pelos usuários. Tampouco podem monitorá-los, a não ser sob ordem judicial. Também para fins judiciais, os provedores têm de guardar, por tempo determinado, os dados de acesso a aplicações sem que sejam revelados os conteúdos acessados. Os usuários, por sua vez, devem ser informados sobre qualquer coleta de dados que os provedores ou qualquer outro interessado vier a requisitar. Esses dois

aspectos colocam o usuário da Internet no centro, objeto direto da proteção legal. Apesar de algumas críticas a este aspecto do MCI alertando para possíveis práticas de vigilância, o MCI tem servido como referência para a elaboração de medidas mais específicas em relação à proteção de dados.

Esses destaques, tal como enfatizaram os entrevistados que participaram da elaboração do projeto de lei, embora estivessem presentes desde o início da tramitação do projeto, ganharam força a partir das denúncias de espionagem por Edward Snowden, ex-colaborador da Agência Nacional de Segurança dos Estados Unidos (NSA). Assim, não só por ser um projeto de lei pioneiro em seu campo, mas também por ter sido transformado em uma resposta às denúncias de Snowden, o MCI também funciona como um *case study* para esta dissertação. Com efeito, no preciso momento em que se desenhava o advento de um movimento de securitização do ciberespaço no Brasil, com leis restritivas ou portadoras de uma vigilância alegadamente excessiva (como a Lei Azeredo discutida anteriormente) a que acresceram as denúncias de Snowden, a resposta a esse movimento não foi no sentido da criação de medidas de exceção. Pelo contrário, o que veio a ser elaborado foi um sistema legal de garantias de direitos das pessoas e de estabelecimento de papeis das instituições. O MCI é o elemento nuclear desse sistema.

É importante ressaltar o caráter civil desta lei ao marcar necessariamente um distanciamento de eventuais medidas de exceção, sendo, portanto, um elemento de dessecuritização. Os entrevistados para esta tese espontaneamente enfatizavam a iniciativa civil na formulação do projeto de lei, gestado inicialmente em grupos de trabalho temáticos sob o Ministério da Justiça. A intenção primária do projeto era formular um sistema legal que garantisse os direitos dos usuários bem como o tratamento de situações específicas através da condução normal das normas estabelecidas.

De fato, o texto do MCI enfatiza em vários momentos a obrigação de determinações jurídicas quando alguma situação venha a contrariar os direitos garantidos como, por exemplo, quando trata da requisição dos registros de conexão, dados pessoais e comunicações privadas:

> § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no **caput,** de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º . (Capítulo 2, Seção II, Art. 10, Parágrafo 1º). (Presidência da República, 2014: online)

A necessidade de análise e fundamentação jurídica também aparece nas disposições sobre a guarda de registros de acessos a aplicações de internet:

> § 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no **caput.** (Capítulo 3, Seção II, Art. 15, Parágrafo 2º). (Presidência da República, 2014: online.

Para além de reafirmar a vigência da condução de situações pela normalidade jurídica, o MCI enfatiza em seus princípios elementos que enfatizam o seu caráter civil para além de temas específicos do ciberespaço abarcando temas caros à democracia. Esses aspectos ficam bastante evidentes em várias passagens do texto. Logo no primeiro capítulo se destaca o respeito à liberdade de expressão, os direitos humanos, reconhece o caráter plural, livre, social e colaborativo da rede como fundamentos (Capítulo 1, Art. 2º). Esses mesmos fundamentos são reafirmados no Art. 3º acrescentando a proteção da privacidade dos usuários, dos dados pessoais e a neutralidade da rede. (Presidência da República, 2014, online).

Não há um apelo a uma tecnificação, que seriam um elemento comum da securitização do ciberespaço segundo os termos de Hansen & Nissenbaum (2009), abordado anteriormente. Pelo contrário, o documento reafirma o objetivo de disseminar "padrões tecnológicos abertos que permitam a comunicação, acessibilidade e a interoperabilidade entre aplicações e bases de dados" (Art. 4º, IV). Ainda trata como objetivo o fomento do direito do acesso à internet, bem como a participação dos usuários na condução dos assuntos públicos, ainda que não ofereça detalhes ou maiores definições neste subtema. (Presidência da República, 2014). O capítulo IV também enfatiza elementos que afastam da tecnificação da condução do ciberespaço ao conceber sua gestão de modo multiparticipativo, incluindo o poder público e organizações da sociedade civil, como o Comitê Gestor da Internet:

> I - estabelecimento de mecanismos de governança multiparticipativa, transparente, colaborativa e democrática, com a participação do governo, do setor empresarial, da sociedade civil e da comunidade acadêmica;
>
> II - promoção da racionalização da gestão, expansão e uso da internet, com participação do Comitê Gestor da internet no Brasil; (Capítulo IV, Art. 24, I e II) (Presidência da República, 2014).

Para além desses elementos, vale ressaltar a ênfase na questão da garantia do direito à privacidade e à liberdade de expressão: "A garantia do direito à privacidade e à liberdade

de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.” (Art 8º), (Presidência da República, 2014: online), temas securitizados em outras situações que envolvem não só a atuação de usuários da Internet mas também questões de liberdade religiosa ou conflitos étnicos.

Questionados sobre a existência de discursos de securitização na formulação e articulação do MCI, alguns entrevistados reconheceram que houve discussões marginais que nunca tiveram grande repercussão no texto do projeto. Enfatizaram, no entanto, que o tema da segurança do ciberespaço ganhou repercussão após as denúncias de espionagem trazidas a público por Edward Snowden. Segundo os entrevistados, a questão da segurança foi útil por ter sido possível usá-la para justificar a aprovação e a urgência na tramitação do projeto de lei.

Em resumo, desde a sua concepção o MCI tem um caráter popular, enfatiza garantias de direitos, trata de temas que consolidam a utilização democrática das redes e reafirma a necessidade de tratar de eventuais conflitos de interesses sob a égide do ordenamento jurídico. É, portanto, um tema politizado, sem dar espaço a movimentos de securitização, ainda que tenha sido aprovado sob discursos de securitização, como se verá adiante.

4.2.4. Direitos justificados pela ameaça: da securitização à aprovação do Marco Civil da Internet

Como referimos no início deste capítulo, a atuação da NSA no domínio da cibersegurança colocou a agência no centro de um controverso escândalo diplomático em 2013, quando um dos seus quadros, Edward Snowden, denunciou através de uma entrevista, as práticas de vigilância massiva realizadas pela NSA (Harding, 2014; Lefébure, 2015). Essa denúncia evidenciou que, para além dos milhares de cidadãos, tanto nacionais como estrangeiros, a NSA também tinha como alvo líderes mundiais, como François Hollande (Rubin & Shane, 2015), Angela Merkel (Furgang, 2018: 72), e Dilma Rousseff(Abdenur, 2014; Atkins, 2013; Bessa, 2014; Lyon, 2014). Naturalmente, as denúncias de Snowden desencadearam uma verdadeira tempestade diplomática.

O presidente Barack Obama tentou, sem sucesso, desqualificar o denunciante e diminuir a importância das denúncias. Em defesa da sua administração, Obama alegou ter modificado as operações de vigilância antes mesmo das denúncias de Snowden, o que não suavizou a crise diplomática em que se viu envolvido (Wolf, 2013).

As denúncias de espionagem americana através da NSA, trazidas a público por Edward Snowden em junho de 2013 envolveram assim diretamente o centro do poder brasileiro, tendo a presidente Dilma Rousseff como um dos principais alvos, já que as denúncias davam conta de que suas comunicações e contas de e-mails haviam sido monitoradas e que a Administração norte-americana estaria espionando de forma massiva cidadãos brasileiros (Nascimento, 2013).

Naturalmente, na necessidade de dar uma resposta ainda que simbólica e imediata às denúncias, o governo brasileiro, através do Ministério das Relações Exteriores (Itamaraty), cobrou explicações do governo norte-americano. Segundo nota oficial publicada um dia após a veiculação das denúncias pela imprensa, o então Ministro das Relações Exteriores, Antônio Patriota, veio a público afirmando que

> O Governo brasileiro recebeu com grave preocupação a notícia de que as comunicações eletrônicas e telefônicas de cidadãos brasileiros estariam sendo objeto de espionagem por órgãos de inteligência norte-americanos. O Governo brasileiro solicitou esclarecimentos ao governo norte-americano por intermédio da Embaixada do Brasil em Washington, assim como ao Embaixador dos Estados Unidos no Brasil. (Minisério das Relações Exteriores, 2013: online).

Mais do que pedir esclarecimentos, o Ministro indicava ações a serem tomadas via organismos internacionais com vista a pôr cobro ao que chamou de abusos contra os cidadãos e a garantir a proteção da soberania dos países:

> […] o Brasil lançará nas Nações Unidas iniciativas com o objetivo de proibir abusos e impedir a invasão da privacidade dos usuários das redes virtuais de comunicação, estabelecendo normas claras de comportamento dos Estados na área de informação e telecomunicações para garantir segurança cibernética que proteja os direitos dos cidadãos e preserve a soberania de todos os países. (idem, 2013: online)

Esta nota tem grande importância, não só por ser uma reação natural e imediata às denúncias. Há ao menos dois fatos relevantes a serem considerados que permeiam a reação brasileira. O primeiro deles é de que a nota acaba por mencionar, ainda que de forma bastante resumida e genérica, as posturas a serem tomadas pelo país nos desdobramentos da questão.

O Brasil, com um certo grau de sucesso, diante do contexto em que foi colocado, adotou medidas correlatas às que o Ministro mencionava, sendo a mais relevante e popular o MCI, e trabalhou para expor, em âmbito multilateral e multissetorial, tais medidas como exemplos a serem adaptados em um eventual sistema internacional de governança da Internet. Antes disso, no entanto, de maneira mais emergencial, o Itamaraty convocou o embaixador norte-americano no Brasil para exigir esclarecimentos. Além disso, a presidente Dilma Rousseff empenhou-se em uma reunião de emergência e criou um grupo Interministerial formado por representantes da Defesa, Relações Exteriores, das Comunicações, Justiça, pelo Gabinete de Segurança Institucional e Assessorias da Presidência da República para avaliar a situação e, segundo a nota oficial, tomar medidas cabíveis (Mendes, 2013). Ainda, abriu-se um inquérito junto à Polícia Federal e à Agência Nacional de Telecomunicações para apurar os fatos (Ministério das Relações Exteriores, 2013: online).

O segundo aspecto que merece especial atenção demonstra uma fragilidade do Governo em relação aos sistemas de segurança vigentes para os sistemas de comunicação eletrônica no país. O encadeamento dos fatos demonstra que o Governo soube das interferências denunciadas por Snowden através da imprensa. Isso fica evidente nas declarações da própria presidente Dilma Rousseff em um encontro com o presidente Obama, alguns dias depois, por ocasião do encontro do G-20, em São Petersburgo:

> O que eu pedi é o seguinte: eu acho muito complicado ficar sabendo dessas coisas pelo jornal. Num dia eu sei uma coisa, passam dois dias eu sei outra coisa, e a gente vai sabendo aos poucos. Eu gostaria de saber o que tem (sobre espionagem). Eu quero saber o que há. Se tem ou não tem, eu quero saber. Tem ou não tem? Além do que foi publicado pela imprensa, eu quero saber tudo que há em relação ao Brasil. Tudo. […] (Presidente Dilma Rousseff, transcrito por Rocha, 2013: online)

Segundo a presidente, o seu homólogo norte-americano se comprometeu a dar explicações sobre o episódio:

> O presidente Obama declarou para mim que assumia a responsabilidade direta e pessoal pelo integral esclarecimento dos fatos, e que proporia para exame do Brasil, medidas para sanar o problema" (Presidente Dilma Rousseff, transcrito em reportagem de Jornal Nacional, 2013: online).

Na sequência do que afirmou a presidente Rousseff, o então ministro da Justiça, José Eduardo Cardozo, se posicionou de um modo mais assertivo:

> Não se pode aceitar violação de soberania e que cabe a um governo cuidar para que sua soberania seja respeitada. Vamos aguardar a posição dos Estados Unidos da América, as informações, as declarações que eles têm que fazer, e partir daí evidentemente medidas que devam ser tomadas, além dessas que já anunciamos,

> serão reveladas, ditas e anunciadas pelo governo. (Ministro José Eduardo Cardozo, transcrito por Serra, 2013: online).

O que interessa no pronunciamento do ministro é o fato de que ele classifica as ações norte-americanas como um ato ofensivo à soberania do país. Este entendimento do ministro, classificando a situação como uma violação da soberania do Brasil e, portanto, algo diretamente ligado à segurança nacional, abre claramente espaço para uma dinâmica de securitização.

Os passos seguintes dessa dinâmica foram, na verdade, típicos de uma lógica de securitização. O primeiro foi a decisão de adiamento de uma viagem que a presidente Rousseff faria aos Estados Unidos, a convite do presidente Obama. Segundo o Palácio do Planalto, as respostas oferecidas pelo governo norte-americano sobre as denúncias de espionagem não haviam sido satisfatórias, justificando esta decisão (T. Monteiro, 2013). Na nota emitida pelo governo brasileiro o tema da violação da soberania nacional voltou a ser repetido e enfatizado:

> As práticas ilegais de interceptação das comunicações e dados de cidadãos, empresas e membros do governo brasileiro constituem fato grave, atentatório à soberania nacional e aos direitos individuais, e incompatível com a convivência democrática entre países amigos. (Presidência da República, 2013: online).

Em segundo lugar, como medida técnica, mas sempre com alcance político, o Ministério das Comunicações decidiu, em parceria com a Empresa Brasileira de Correios e Telégrafos, desenvolver um sistema de e-mails inteiramente nacional como uma medida contraespionagem. Terceiro passo: a presidente Dilma Rousseff retomou o assunto na 68ª Reunião da Assembleia Geral das Nações Unidas, ainda no mesmo mês de setembro. Desta vez, direcionada a uma audiência bastante diversificada e global, incluindo outros líderes que também haviam sido vítimas das mesmas práticas norte-americanas, Rousseff expôs novamente sua indignação, repúdio e preocupações em relação às revelações de Snowden. Conceitos como ‘soberania nacional’, ‘Direito Internacional’, ‘direitos fundamentais do cidadão’, foram elencados de modo a ilustrar a gravidade das denúncias, já que a própria presidente classificou os atos como uma violação a esses:

> Quero trazer à consideração das delegações uma questão a 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. No Brasil, a situação foi ainda mais grave, pois aparecemos como alvo dessa intrusão. Dados pessoais de cidadãos foram indiscriminadamente objeto de interceptação. […] Também representações diplomáticas brasileiras, entre elas a Missão Permanente junto às Nações Unidas

> e a própria Presidência da República tiveram suas comunicações interceptadas. Imiscuir-se dessa forma na vida de outros países fere o Direito Internacional e afronta os princípios que devem reger as relações entre eles, sobretudo, entre nações amigas. Jamais pode uma soberania firmar-se em detrimento de outra soberania. Jamais pode o direito à segurança dos cidadãos de um país ser garantido mediante a violação de direitos humanos e civis fundamentais dos cidadãos de outro país. […] Estamos, senhor presidente, diante de um caso grave de violação dos direitos humanos e das liberdades civis; da invasão e captura de informações sigilosas relativas as atividades empresariais e, sobretudo, de desrespeito à soberania nacional do meu país. […] (Presidência da República, 2013b: online).

Rousseff, ao apontar elementos atingidos pela ação de espionagem acaba por identificar espécies de objetos de referência. Entre esses, cabe ressaltar dois elementos. Em primeiro lugar, a presidente não indica uma oposição entre a questão da segurança e as liberdades civis. Ao contrário de outras situações, como no seguimento dos atentados terroristas de Setembro de 2001 nos Estados Unidos (Baker, 2003), em que as liberdades civis foram tomadas como conceito a ser relativizado em favor da segurança nacional, a presidente Dilma Rousseff, ao chamar a atenção para o que classificou como ameaças à segurança e à soberania, colocou as liberdade civis e os direitos humanos no mesmo grupo dos objetos de referência. Sugeriu, portanto, uma outra lógica em que a segurança das instituições e da soberania do país não é posta em campo oposto às garantias de direitos.

É precisamente a questão da soberania o segundo aspecto a ser enfatizado. Parece bastante acertada a ideia da defesa da soberania para uma audiência formada por representantes de países soberanos. Como referimos noutro momento deste trabalho, a escolha de elementos significativos para audiências específicas é de grande importância para os movimentos de securitização e também de dessecuritização. Como afirmam autores já mencionados, como Williams (2003) e Balzacq (2005), a escolha de utilização de elementos que fazem sentido à audiência na intenção de oferecer uma lógica ao discurso direcionada ao convencimento e eventual tomada de decisão é fundamental para que o movimento de securitização se desenvolva. Ora, neste caso, o mesmo parece aplicar-se também à dessecuritização. Também para esse movimento de sentido oposto a escolha de elementos significativos que permitam mobilizar a audiência para uma abordagem de politização comum e não para uma abordagem de exceção se revela fundamental. Essa postura, adotada pela presidente Rousseff, fica bastante evidente ao prosseguir com seu discurso:

> O Brasil, senhor presidente, redobrará os esforços para dotar-se de legislação, tecnologias e mecanismos que nos protejam da interceptação ilegal de comunicações e dados. […] Meu governo fará tudo que estiver a seu alcance para defender os direitos humanos de todos os brasileiros e de todos os cidadãos do

> mundo e proteger os frutos da engenhosidade de nossos trabalhadores e de nossas empresas. (Presidência da República, 2013b: online).

A presidente não especifica quais as medidas que o seu Governo tomaria para defender seus objetos de referência ali apontados. Dado o lapso de tempo desde a veiculação das denúncias de espionagem (menos de um mês), é provável que o Governo nem sequer tenha tido tempo para conceber ações mais elaboradas. Tampouco era a Assembleia Geral das Nações Unidas o lugar ideal para esmiuçar políticas nacionais. Contudo, o que interessa neste segmento do discurso é precisamente a sinalização das medidas a serem tomadas e a natureza das mesmas.

O Brasil, através da sua Presidente da República, se compromete a tomar providências em relação aos atos de interceção. O país assume, então, o papel do que a teoria da securitização denomina de ator funcional. Vale lembrar que a lógica do discurso não aponta para medidas de exceção. Ainda que até então não esteja claro no posicionamento da presidente, começava a se delinear um processo que teria um desfecho na garantia de direitos, e não na restrição de liberdades e adoção de medidas especiais. Ao seguir, o discurso compartilha o problema com seus pares na audiência:

> O problema, porém, transcende o relacionamento bilateral de dois países. Afeta a própria comunidade internacional e dela exige resposta. As tecnologias de telecomunicação e informação não podem ser o novo campo de batalha entre os Estados. Este é o momento de criarmos 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, ao tratar da questão do uso das tecnologias da informação como armas de guerra não traz nenhuma novidade à sua audiência. Pelo contrário, reforça a percepção de ameaças do ciberespaço como um problema comum. O trecho do discurso, no entanto, chama a atenção para o fato de que a presidente não defende uma espécie de preparação técnica e política para futuros conflitos que eventualmente teriam espaço no ciberespaço. Pelo contrário, identifica o episódio como um momento-chave para evitar uma belicização das tecnologias da informação.

O discurso da presidente Dilma Rousseff na Assembleia Geral das Nações Unidas era, de certa forma, esperado, no que diz respeito às críticas que faria às denúncias de espionagem dos Estados Unidos. Apesar de conversas amigáveis entre os mandatários dos dois países, ficou evidente e explicitado que Rousseff não se deu por satisfeita com as explicações e as medidas adotadas por Obama. Contudo, Rousseff escolheu não direcionar

uma crítica mais contundente aos Estados Unidos, mas sim trazer o problema das ameaças do ciberespaço a um parâmetro comum para o qual as opiniões tendem a convergir, inclusive a dos Estados Unidos. Assim, mais do que sinalizar caminhos para uma certa posição comum em meio aos diferentes interesses dos países, Rousseff coloca o Brasil à frente de um movimento que busca o estabelecimento de princípios internacionais para a governança da Internet. Posteriormente, essa postura passaria por modificações, mas ganharia ações mais concretas, tanto no âmbito doméstico quanto nas movimentações internacionais do Brasil.

4.2.5. A securitização que dessecuritiza

As denúncias de Snowden e a confirmação de que os Estados Unidos, através da NSA, interceptavam as comunicações de importantes autoridades do Governo brasileiro encontrou um executivo aparentemente sem um plano de ação para situações deste tipo. Contudo, à medida que o assunto foi se desenvolvendo, as medidas não foram no sentido de criar políticas "anormais" que dessem resposta específica às denúncias. De imediato, como mencionado anteriormente, o Governo requisitou a criação de um sistema de e-mails e comunicações eletrônicas baseado exclusivamente em infraestrutura nacional através da Empresa Brasileira de Correios (Armato, 2013). Por outro lado, há um papel bastante interessante de atores nacionais ligados à gestão e governança da Internet que viram nas denúncias uma oportunidade de darem impulso político e legislativo ao até então pouco abordado MCI entre outras agendas referentes à governança. Na verdade, como sublinham Trinkunas & Wallace (2015), organizações como o Comitê Gestor da Internet, assim como diversos grupos e organizações não-governamentais (Coletivo Digital, Artigo19, Coletivo Intervozes, entre outras), souberam capitalizar o cenário de denúncias e de sentido de urgência de ações e para direcionar as iniciativas do Governo para a aprovação do que veio a ser o MCI.

As entrevistas que realizámos a representantes desses coletivos deram conta de que as denúncias de Snowden serviram essencialmente para que o Governo brasileiro voltasse suas atenções para projetos que já estavam com alguma articulação nas Câmaras Legislativas. Vários dos entrevistados, principalmente os que representavam organizações da sociedade civil envolvidos com um ativismo em favor da aprovação do Marco Civil, confirmaram esse movimento, ou seja, embora o Marco Civil não fosse uma resposta

específica e direta ao contexto exposto por Snowden, as denúncias criaram um sentido de urgência para o qual o governo teria de apresentar alguma resposta. Este contexto, o MCI, que embora estivesse em segundo plano em relação a outras pautas, foi ganhando força. Esse crescimento nas atenções culminou em um pedido de urgência na tramitação do processo (Câmara dos Deputados, 2013b)[59][60].

A génese deste movimento talvez se possa situar no já mencionado discurso da presidente na ONU, que encontrou eco na defesa da aprovação do que veio a ser o MCI nas Câmaras Legislativas. A começar pelo então líder do partido do Governo, deputado José Guimarães, a defesa do MCI está diretamente ligada às denúncias de Snowden:

> As recentes denúncias de espionagem contra o Brasil pelos Estados Unidos, conforme documentos mostrados pelo ex-analista da Agência Nacional de Segurança (NSA) Edward Snowden, tornaram ainda mais urgente a aprovação de um marco regulatório para a Internet no Brasil. Sua aprovação não resolverá o problema da espionagem, mas é um passo importante para proteger a privacidade da sociedade da ciberespionagem, bem como para promover a inovação e o desenvolvimento social e econômico do Brasil, e impulsionar uma Internet mais igualitária e justa. (Guimarães, 2013: online).

O deputado deixou assim claro que a aprovação do MCI não seria uma contramedida que serviria para rebater as investidas americanas em relação à espionagem de cidadãos brasileiros e da própria presidente. No entanto, em um sistema legal em que ações como a da espionagem estrangeira por meios eletrônicos e massivos não estava devidamente contemplada, a prioridade deveria ser um marco regulatório aplicável não só à atuação do Estado Brasileiro em relação a atores externos (outros Estados ou mesmo empresas), mas

[59] Esse pedido, sendo um ato oficial próprio da Presidência da República, implica no trancamento da pauta da Câmara por 45 dias, sendo este o prazo máximo que os deputados tem para votar o objeto em questão que, por sua vez, segue para o Senado Federal, que tem outros 45 dias para discutir e votar o projeto de lei.

[60] Há questões metodológicas a serem consideradas. Os discursos dos próprios parlamentares funcionam aqui como principal fonte primária. Esses discursos estão transcritos e disponíveis no portal da Câmara dos Deputados. Como recorte temporal, escolheu-se o período que compreende o período entre pedido de urgência da presidente Dilma Rousseff para a votação pelo Congresso do MCI, em setembro de 2013, a sua aprovação pelo Senado Federal, em abril de 2014. O foco principal desta dinâmica foi a Câmara dos Deputados, em detrimento do Senado. Primeiramente, porque o pedido de urgência da presidente se dirigiu à Câmara dos Deputados que, então, absorveu e assimilou a condição de urgência para com o projeto de lei. Apesar do pedido de urgência envolver também o Senado, já que os processos de aprovação das leis obedecem a um ritual que passa necessariamente pela aprovação das duas Câmaras Legislativas, foi na Câmara dos Deputados que as discussões sobre o projeto tomaram dimensões mais concretas. Ao Senado caberia aprovar ou modificar o texto da Câmara dos Deputados. Em caso de modificações pelo Senado, o texto teria que retornar à Câmara reiniciando todo o processo, o que não aconteceu, já que o Senado aprovou o texto. Essa opção por priorizar os discursos dos deputados não vem em detrimento dos senadores. Pelo contrário, sendo também parte dos atores funcionais em relação a tomada de decisões, os discursos dos senadores não só importam, como também são utilizados mas, ao invés de servirem como fontes primárias para a percepção do sentimento de urgência e direcionamento das políticas, vêm no sentido de ilustrar ou dar suporte às percepções que se extraem dos seus pares deputados.

também à atuação interna do Estado, enquanto seu limite jurídico, impedindo que, em situações críticas envolvendo a segurança da informação, adotasse medidas que ferissem princípios básicos e direitos fundamentais.

Neste sentido, esse marco regulatório foi pensado, desde o primeiro momento, como uma espécie de ferramenta de dessecuritização de um contexto crítico ou, mais precisamente, como mecanismo preventivo de eventuais movimentos de securitização.

O tema da proteção da soberania foi igualmente central nas discussões sobre esse marco regulatório. Nas audiências públicas que discutiram o MCI foram proferidos diversos discursos que entendiam que o Marco Civil funcionaria como um dispositivo de defesa da soberania nacional, na medida em que possibilitaria que o Brasil se tornasse menos dependente da tecnologia e do armazenamento de dados produzidos no Brasil em infraestrutura estrangeira. O melhor exemplo, talvez, tenha vindo do deputado social-democrata Jefferson Campos:

> […] hoje trago a esta tribuna um tema muito relevante. Quero me expressar sobre uma questão de segurança. Trago à pauta o combate à espionagem. Antes de ser uma pessoa pública, sou um cidadão brasileiro e, como tal, reservo-me o direito de ter minha privacidade preservada. Creio que a Nação brasileira pode e deve garantir este direito a todos nós, os brasileiros. Da mesma forma, num Estado há questões sigilosas que realmente só competem aos regentes daquele Estado. Confesso que encontrei-me chocado ao saber que o Brasil, na figura de nossa Presidente, foi vítima de espionagem por parte da National Security Agency (NSA), agência americana de segurança. Fiquei imaginando sob que pretexto o Sr. Presidente Barack Obama permitiu tal investida. Buscando que tipo de informação, ou melhor, procurando nos acusar do quê? Posteriormente soube que buscava por informações sobre terrorismo. No Brasil, um lugar onde definitivamente nunca tivemos registros de tais práticas! Por isso, juntamente com as Comissões de Constituição e Justiça e de Cidadania (CCJC), de Relações Exteriores e de Defesa Nacional (CREDN) e de Ciência e Tecnologia, Comunicação e Informática (CCTCI), participei de uma discussão a respeito de tais notícias, visando solucionarmos esta fragilidade em nossa segurança. Buscamos com isso aprimorar nossas leis nacionais, para que possamos usá-las como ferramentas na defesa da privacidade dos cidadãos e também do Estado. Propomos um novo MCI, ou seja, o Projeto de Lei 2.126/11, apensado ao Projeto de Lei 5.403/01, intencionando garantir publicamente o combate à espionagem, de forma a nos tornarmos um exemplo para todas as nações que desejam ter os seus direitos e a sua soberania garantidos. Apesar não termos sido o único país espionado - até a Alemanha passou por tal constrangimento -, concordo com a Presidente em seu pronunciamento na 68ª Assembleia Geral da ONU, em Nova York, declarando o programa de inteligência dos Estados Unidos como "uma grave violação dos direitos humanos" e "desrespeito à soberania nacional". (Câmara dos Deputados, 2013j)

Nesta intervenção há como que uma síntese de todo o percurso do movimento. O deputado afirma que há uma ameaça grave à segurança nacional, identifica elementos que deveriam ser protegidos, tais como a privacidade dos brasileiros e a própria questão da

soberania nacional, reconhece a fragilidade dos sistemas da segurança nacional, conclama a adoção de medidas mais eficazes, inclusive no âmbito legal, contextualiza seus posicionamentos agregando outros exemplos de países que teriam sido vítimas da mesma ação norte-americana e ilustra seus argumentos referenciando o pronunciamento da presidente na Assembleia Geral da ONU, do qual retira dois objetos de referência: a soberania nacional e os direitos e liberdades fundamentais.

Os deputados Newton Lima e Leonardo Medeiros, igualmente do Partido dos Trabalhadores, discursam num tom parecido. Em comparação, seguem os dois trechos:

> Minha segunda observação, muito breve, é sobre o meu orgulho de ser brasileiro e de ter uma Presidenta da República que com altivez, no dia de ontem, na Assembleia das Nações Unidas, deu ao mundo o recado de que é inaceitável que os Estados Unidos continue espionando todas as nações, com objetivos políticos e econômicos, como fez com o Brasil, como já amplamente denunciado pela imprensa. Mais do que isso, tal fato enseja a todos nós a responsabilidade de aprovarmos o marco civil da Internet, sob a relatora do Deputado Alessandro Molon, para que nós tenhamos estabelecidos na legislação brasileira os limites, o regulamento, a regulação necessária para que esse instrumento moderno e tão importante não sirva também de instrumento contra a privacidade das pessoas. A Presidenta fez bem ao solicitar que o mundo discuta esse monopólio da governança americana sobre a Internet, propondo um marco civil internacional. Façamos a nossa parte. Quero lembrar, para encerrar, a fala da Presidenta, que me tocou muito e que trago ao conhecimento da população, pedindo inclusive o registro deste pronunciamento nos Anais da Casa e em *A Voz do Brasil*: *"Lutei contra o arbítrio e a censura e não posso deixar de defender de modo intransigente o direito à privacidade dos indivíduos e a soberania do meu País. Sem ele - o direito à privacidade - não há verdadeira liberdade de expressão e opinião e, portanto, não há efetiva democracia. Sem respeito à soberania, não há base para o relacionamento entre as nações."* Por isso, a Presidenta fez bem ao cancelar sua ida aos Estados Unidos, aguardando que os Estados Unidos deem explicações, peçam desculpas e estabeleçam uma parceria, um acordo com o nosso País, para que essa bisbilhotagem só aconteça em casos efetivos de terrorismo que possam vir a abalar todas as nações. (Deputado Newton Lima, in Câmara dos Deputados, 2013o)

> Quero ainda registrar, Sr. Presidente, que ao se fortalecer perante o nosso País, a Presidenta Dilma tem-se destacado também como uma grande líder. Nesse sentido, a Presidenta Dilma Rousseff está resgatando a dignidade do povo brasileiro. É necessário ressaltar a posição da nossa Presidenta como uma estadista, uma líder que tem a capacidade de nos liderar e, sobretudo, de mostrar a importância do Brasil para o mundo inteiro. Prova disso foi seu discurso na abertura da Assembleia Geral da Organização das Nações Unidas, agora em setembro, em que a nossa Presidenta criticou a espionagem que o governo norte-americano faz, inclusive contra nações aliadas como o Brasil. Dilma foi muito feliz ao defender o estabelecimento de um marco civil multilateral para a governança e o uso da Internet, com medidas que garantam a efetiva proteção dos dados. É fundamental aprovarmos o projeto de lei do marco civil da Internet que a nossa Presidenta encaminhou a este Congresso, a fim de ampliarmos a proteção da privacidade dos brasileiros que utilizam a rede de computadores. A espionagem contra o povo brasileiro foi denunciada à ONU, porque a nossa Presidenta não admite, nem nós podemos admitir, as atividades de uma rede global de espionagem eletrônica. Mais recentemente tomamos conhecimento também de que o Ministério de Minas e Energia foi alvo de espionagem canadense, com

> motivações econômicas. Repudiamos a guerra cibernética e aplaudimos a Presidenta Dilma por exigir que os Estados Unidos e seus aliados encerrem as atividades de espionagem. É inaceitável que dados pessoais de cidadãos e cidadãs e da própria Presidenta da República sejam objeto de interceptação, ainda mais por parte de países que pretendem ser parceiros do Brasil. Assim que aprovarmos o Marco Civil da Internet, o nosso Governo vai propor à ONU a adoção de um marco civil internacional. Será, Sr. Presidente, a implementação de mecanismos multilaterais capazes de garantir os seguintes princípios: liberdade de expressão, privacidade do indivíduo e respeito aos direitos humanos; governança democrática, multilateral e aberta; universalidade que assegure o desenvolvimento social e humano e a construção de sociedades inclusivas e não discriminatórias; diversidade cultural, sem imposição de crenças, costumes e valores; e neutralidade da rede, ao respeitar apenas critérios técnicos e éticos, tornando inadmissível qualquer restrição por motivos políticos, comerciais e religiosos. Devemos evitar que o espaço cibernético seja instrumentalizado como arma de guerra, pois, como bem defendeu a Presidenta Dilma, a espionagem atenta contra a soberania das Nações e a privacidade das pessoas e das empresas. (Deputado Leonardo Medeiros, in Câmara dos Deputados, 2013m)

Ao abrir a Sessão da Assembleia Geral das Nações Unidas, a presidente representa uma voz ativa para a adoção de medidas a favor de uma causa que ganha força a partir de um acontecimento marcante, assemelhando-se em papel ao do presidente estoniano abordado no capítulo anterior. Outro especto em relação à figura da presidente é a sua relação bastante próxima do contexto por ela exposto. Sendo ela própria vítima de espionagem e sendo chefe de Estado, a presidente ganha protagonismo e oferece, pela sua posição, elementos com que sua audiência naquele público se identifica. Assim, a figura da presidente é central para o desenvolvimento deste processo. A invocação de Dilma pelos deputados funciona, assim, como uma estratégia de legitimação dos seus discursos para os apresentar como uma espécie de "interpretação autêntica" do pensamento da presidente sobre a resposta a dar aos atos de espionagem

Por outro lado, tão importante quanto exaltar a figura da presidente dando-lhe legitimidade enquanto ator da dessecuritização, é a ligação entre as denúncias da espionagem e a necessidade de aprovar um marco regulatório como veio a ser o MCI. Naturalmente, os deputados percebem que o MCI não é uma resposta direta às denúncias ou uma contramedida, como já foi mencionado anteriormente. Contudo, fica evidente que, diante das denúncias, o MCI aparece como uma resposta diferente de uma represália, afastando-se de uma espiral de agravamento das tensões que pudesse resultar numa pauta assumidamente securitária:

> Ao discursar na abertura da 68ª Assembleia-Geral das Nações Unidas, em Nova York, a Presidente Dilma Rousseff defendeu a criação de um marco civil multilateral para governança internacional e uso da Internet. É crescente a preocupação dos governos e da sociedade sobre as fragilidades de segurança na transmissão das informações e na privacidade dos nossos cidadãos. A Presidenta

destacou que os recentes acontecimentos de denúncias de espionagem ferem o direito internacional e afrontam os princípios que regem a relação entre os países. Ela também disse que o processo envolve os marcos civis locais da Internet e que esse esforço exige uma engenharia da Internet internacional que permita que a gente garanta esse espaço democrático para todos os cidadãos do mundo. […] É chegada a hora de um marco civil construído com a preocupação de preservar a liberdade de expressão, a privacidade e a segurança. O texto que foi produzido e relatado com extrema sensibilidade teve a participação da sociedade, durante um processo democrático e transparente de consulta e audiências públicas, propondo à sociedade eixos de discussão abrangendo as condições de uso da Internet em relação aos direitos e deveres de seus usuários, prestadores de serviços e provedores de conexão, e também o papel do poder público com relação à Internet. […] O Marco Civil assegura o papel do cidadão e favorece o exercício da cidadania digital. (Deputada Benedita da Silva, in Câmara dos Deputados, 2013a)

No mundo de hoje, em que questões como liberdade de expressão, privacidade e espionagem estão na pauta do dia, o Brasil larga na frente e ocupa posição de vanguarda nas discussões sobre uma legislação para a Internet. O Marco Civil, construído de maneira colaborativa por vários setores da sociedade, é a proposta mais avançada já feita desde o surgimento da Rede Mundial de Computadores. Ela estabelece princípios, direitos e deveres aos usuários, ou seja, cria uma espécie de Constituição da Internet. O Brasil tem a chance de se tornar o primeiro país do mundo a estabelecer diretrizes claras para proteger os direitos de seus cidadãos na rede, e sabemos que hoje esses direitos estão ameaçados por uma série de práticas do mercado. O mundo precisa de uma legislação como esta que estamos pretendendo aprovar agora. Por isso, muito me espanta a postura de alguns Deputados desta Casa, que querem modificar o atual texto do Marco Civil, permitindo assim a quebra da neutralidade da rede. […] No mundo de hoje, em que questões como liberdade de expressão, privacidade e espionagem estão na pauta do dia, o Brasil larga na frente e ocupa posição de vanguarda nas discussões sobre uma legislação para a Internet. O Marco Civil, construído de maneira colaborativa por vários setores da sociedade, é a proposta mais avançada já feita desde o surgimento da Rede Mundial de Computadores. Ela estabelece princípios, direitos e deveres aos usuários, ou seja, cria uma espécie de Constituição da Internet. O Brasil tem a chance de se tornar o primeiro país do mundo a estabelecer diretrizes claras para proteger os direitos de seus cidadãos na rede, e sabemos que hoje esses direitos estão ameaçados por uma série de práticas do mercado. O mundo precisa de uma legislação como esta que estamos pretendendo aprovar agora. (Deputado Gustavo Petta, in Câmara dos Deputados, 2013h)

[…] depois de várias audiências públicas, quando nós, inclusive, em função das denúncias do Snowden, chamamos algumas operadoras que vieram aqui, tanto das teles (empresas de telecomunicações no país), quanto o Google, quanto Facebook, Twitter […] e ouvimos, de maneira, assim pra todos nós, dramática o fato de que, como todos os data centers estão nos Estados Unidos, as empresas que estão aqui, sobre os dados, elas prestam contas, exclusivamente à justiça americana. É exatamente por conta disso que a presidenta Dilma fez o discurso que fez na ONU que o (deputado relator do Projeto de Lei do Marco Civil da Internet, Alessandro) Molon muito bem retratou aqui. E nós ao aprovarmos o Marco Civil da Internet, nós vamos não só dar para os brasileiros e brasileiras a condição de direitos e deveres sobre a banda larga e a Internet, como também garantir a soberania ou, pelo menos, trabalharmos sem nenhuma ingenuidade para diminuir espaços de invasão da nossa privacidade que é um dos temas centrais que o Molon bem colocou nesse brilhante relatório que fez. O outro lado da democracia, nem se fale, porque não adiante, sem neutralidade, não haverá acesso democrático das pessoas mais humildes aos conteúdos da rede. E o meu argumento é o maior que eu tenho usado, como educador, alguém que trabalha com a educação, ciência e tecnologia, é impensável nós exilarmos brasileiros e brasileiras da Internet que hoje é um instrumento fundamental do aprendizado, fundamental pra educação, formação e

> construção da cidadania, por isso Marco Civil da Internet já! […] (Deputado Milton Lima, in Câmara dos Deputados, 2013a)

> […] passo à Mesa o meu pronunciamento, que trata da questão da espionagem norte-americana no Brasil, no qual faço a proposta de seis pontos a serem encaminhados a esta Casa, à Presidência da República, aos Ministros da Defesa e da Ciência e Tecnologia. O primeiro ponto, depois que esta Casa e o nosso Governo condenaram as ações de espionagem, e como o assunto diz respeito à nossa soberania e aos direitos humanos, é fortalecer os recursos para a área de defesa […] O segundo é para que o Congresso aprove com celeridade o PL nº 2.126, de 2011, que estabelece princípios e garantias, direitos e deveres do uso da Internet no Brasil, como um marco civil da Internet […] (Deputado Francisco Chagas, in Câmara dos Deputados, 2013q).

> A decisão do Brasil de fazer um Marco Civil da Internet não é recente. Como 2º Presidente do Conselho de Altos Estudos e Avaliação Tecnológica, que foi criado quando eu fui Presidente da Câmara, gostaria de dizer que este assunto foi tratado naquele Conselho com o projeto do Deputado Luiz Piauhylino. Nesse tempo, dizia-se que eram crimes da Internet ou crimes cibernéticos. Muito mais do que isso, quero dizer que, com essa espionagem agora feita pela agência nacional americana, tornou-se mais evidente ainda a decisão para que a gente possa cada vez mais colocar um marco civil, para que a gente possa cada vez mais evitar... Não vamos ter a ilusão de que vamos corrigir de maneira total, mas pelo menos vamos corrigir algumas coisas que estão sendo espionadas pelos Estados Unidos. Os Estados Unidos, através da sua agência de inteligência, espionaram todos os países do mundo e continuam espionando! Continuam espionando! […] Tenho certeza absoluta de que depois desta sessão tão importante e da Relatoria do Deputado Alessandro Molon haveremos de fazer um Marco Civil da Internet que possa prevenir o País contra a espionagem, não só dos Estados Unidos. Não pensem que só os Estados Unidos estão espionando o Brasil, muitos países fazem a mesma coisa. (Deputado Inocêncio Oliveira, in Câmara dos Deputados, 2013i).

> Respeito todos aqueles que querem combater crimes na Internet, que querem impedir influências que sejam nefastas na Internet. Mas nós temos que tomar certo cuidado com o chamado "vigilantismo". Ou seja, se você estabelece a lógica de que o cidadão que usa a Internet primeiro é culpado, e depois é que se vai verificar, você passa a censurar. Não tem lógica essa questão. Eu acho que até o modelo de espionagem internacional feita pelos Estados Unidos está aí. Em nome do combate ao terrorismo, estabeleceu-se vigilância total e o desrespeito à soberania nacional, inclusive à posse de dados, e assim por diante. Nós entendemos que esse sentido de privacidade é um direito de cidadania e assim deve ser visto. Por isso, é um grande avanço na forma como está colocada aqui no projeto. Particularmente, uma das questões mais polêmicas, sem dúvida, é a questão da neutralidade da rede, que eu entendo que nós não podemos ter. […] defendemos, sim, o projeto da forma como está, o relatório, que é, sem dúvida, um avanço. Não podemos mais protelar essa decisão. Precisamos votar imediatamente o Marco Civil da Internet, como um grande ganho, um grande avanço legislativo brasileiro sobre questão tão abrangente, tão importante para a sociedade brasileira. Espero que façamos o mais rápido possível, na semana que vem, a votação do Marco Civil do relatório (Alessandro) Molon. (Deputado Ivan Valente, in Câmara dos Deputados, 2013j)

Embora os deputados apontassem para uma justificativa indireta para a aprovação do Marco Civil houve vozes, não obstante, que destacavam especificamente a relação entre a aprovação do MCI e a proteção dos usuários contra os atos de espionagem e a favor da proteção da privacidade. Neste sentido, o professor Pablo Ortellado, especialista em Políticas

Públicas da Universidade de São Paulo, convidado pela Comissão Especial para o MCI chamava a atenção da audiência nas reuniões da Comissão para:

> [...] alguns dos dispositivos relativos à proteção da privacidade que estão presentes no Marco Civil da Internet. Esse é um assunto que ganhou grande relevância em face das denúncias recentes de espionagem dos Estados Unidos, tendo por objeto o Brasil. O que a publicitação da espionagem americana de governos, empresas e cidadãos brasileiros nos ensinou, nesse caso recente, é que nós temos bancos de dados amplos demais e desregulados demais, que estão à disposição para uso político e comercial indevido. Esses bancos de dados, com informações privadas, se constituíram para atender um modelo de negócio principal, que vigora hoje na Internet, que é a publicidade dirigida. A publicidade dirigida consiste em apresentar anúncios publicitários para um público muito específico, que está interessado num determinado produto. Para saber qual anúncio apresentar para qual usuário, as empresas de serviços têm reunido uma quantidade enorme de informações dos usuários: o histórico da sua localização geográfica pelos dados do GPS dos smartphones, as palavras-chave colocadas em ferramentas de busca, o padrão de relacionamento nas redes sociais e mesmo o conteúdo de *e-mails*. É essa grande massa de informação, recolhida pelas empresas, que foi mobilizada para a espionagem política e comercial. Para enfrentar esse problema, o Marco Civil, nos arts. 7º e 8º, disciplina a coleta de dados, estabelecendo que as empresas precisam informar aos usuários quais dados elas vão coletar e para qual fim; e essas empresas devem se restringir a esse uso que foi informado ao usuário. (Pablo Ortellado Câmara dos Deputados, 2013t)

Diante desses pronunciamentos, vale ressaltar, no entanto, que o alinhamento do discurso não foi automático e tampouco unânime. Embora houvesse uma diversidade de deputados de várias formações políticas que adotaram a mesma linha de discurso, houve vozes dissonantes que apresentaram questionamentos em ao menos duas direções. Primeiro, apontaram a óbvia falta de ligação da proposta com a causa. Afinal, o Marco Civil não serviria necessariamente para responder, ao mesmo nível, às espionagens americanas que lhe conferiram caráter de urgência. Segundo, questionaram justamente esse aspecto de urgência imposto pela Presidência da República. Contudo, a crítica mais relevante voltava-se para uma modificação no texto do projeto que obrigava que empresas de Internet mantivessem seus dados em *datacenters* no Brasil, de modo que esses dados ficassem sob a jurisdição brasileira[61].

> O remédio para a espionagem é outro, o tratamento é outro, completamente diferente. São outras garantias de Intranet e de redes de segurança de dados que

[61] Especialistas e participantes das discussões em entrevistas para este trabalho afirmaram que uma das mais relevantes mudanças no texto do Marco Civil da Internet por influência direta das denúncias de Snowden foi justamente a ideia de manter os dados de usuários no Brasil, ao menos parcialmente. Essa medida vem da ideia de que, como os datacenters que servem o Brasil, assim como outros países, estão localizados no exterior, as leis brasileiras não atingiam essas empresas em caso de possíveis requisições judiciais. A crítica dos deputados argumentavam que os preços da manutenção de informação no Brasil não traria nenhum benefício prático para os usuários. Pelo contrário, poderia haver um acréscimo nos custos dos serviços e prejudicar inovações próprias das tecnologias da informação, como por exemplo, a Cloud Computing, em ascensão. A medida foi excluída do texto final.

> devem ser providenciadas pelo Governo e pelas autoridades governamentais. Agora, impor ao consumidor brasileiro um *data center* local para encarecer a operação de Internet no Brasil, pura e simplesmente, por questão de vaidade, por questão de estratégia eleitoral da Presidente Dilma Rousseff, é um tremendo e absurdo erro. (Deputado Mendonça Filho, Câmara dos Deputados, 2013n).

> [...] esse projeto, que tomou o nome de Marco Civil da Internet, perdeu esse DNA popular para se tornar o marco legal no momento em que a ação monocrática da Presidente da República acrescentou o dispositivo que obriga o armazenamento de dados de brasileiros em *data centers* localizados em território nacional, além de impor tramitação em regime de urgência constitucional. A causa alegada para essa proposta, absolutamente na contramão dos atributos da Internet, foi a identificação de espionagem em comunicações de autoridades brasileiras. Repudiamos essa invasão da privacidade e da soberania nacional. Mas, daí a imaginar que o armazenamento de dados dos internautas brasileiros no Brasil vai acabar com a espionagem é um grande equívoco, para dizer o mínimo. A Internet foi o instrumento usado dessa vez, mas não é o único existente. O processamento de informações internas e externas é fundamental para as políticas de segurança de qualquer país. Infelizmente, os métodos de tempos de paz são os mesmos métodos de tempos de guerra. Segundo os especialistas no assunto, o melhor instrumento de defesa é a criptografia. A Agência Brasileira de Inteligência - ABIN, que por certo não faz espionagem, poderá ratificar essa afirmativa. Trata-se, portanto, de uma justificativa vazia para a urgência constitucional e para a introdução do art. 10-A no projeto do Relator. A exigência de armazenamento local dos dados dos brasileiros transforma nossos internautas em categoria inferior ao limitar a liberdade do uso pleno da Rede Mundial, por exemplo, na computação em nuvem, no fluxo livre de informações transfronteiras, na redundância de guarda de dados etc. A contradição é reforçada quando lembramos que tramita nesta Casa, com aceitação unânime, proposta de emenda à Constituição que inclui o acesso à Internet em banda larga como direito individual fundamental. (Deputado Arolde de Oliveira, in Câmara dos Deputados, 2013f)

> [...] se a Presidente Dilma e seu Governo consideram que espionagem é um argumento para se votar o Marco Civil da Internet - e será, se Deus quiser, a partir da semana que vem, a melhor legislação do mundo voltada à Internet -, que nós votemos o Marco Civil. Mas não é só isso. Os *data centers*, as unidades de processamento de dados, aqui no Brasil, não vão ajudar em nada a acabar com a espionagem no Brasil, com os dados que pertencem ao Executivo ou ao Governo Federal. A resposta que a Presidente Dilma está buscando se chama SERPRO, chama-se Serviço Federal de Processamento de Dados. Os investimentos têm que acontecer lá. Não é a localização dos *data centers*. (Deputado João Arruda , in Câmara dos Deputados, 2013l)

Ainda que houvesse discordância, não houve movimentos ou campanhas contra a aprovação do MCI. Pelo contrário, sendo o MCI marcado por uma grande participação popular em sua formulação, havia uma percepção de que a população teria, por isso, interesse na sua aprovação. As entrevistas realizadas para este trabalho deram conta de que, para além do Governo, as denúncias de Snowden acabaram impactando na opinião pública. A politização gerada pela veiculação das denúncias em rede nacional acabou fazendo com que a população se tenha mobilizado para o tema, não só discutindo, mas cobrando alguma atitude do Governo e dos parlamentares. Nesse sentido, a aprovação do MCI ganhouum significado e um alcance político maiores do que aqueles que a estrutura governamental

prefigurou, deixando de ser uma simples questão de governo e passando a ser verdadeiramente uma questão de Estado. Isso mesmo é resumido no pronunciamento do deputado Vicentinho:

> Em tempos de espionagem industrial e a líderes de Estado, como foi com a Presidenta Dilma, não podemos, como Parlamentares, nos furtar de votar o Marco Civil da Internet. É nosso dever votá-lo, sem delongas. Acima de tudo, o Marco Civil da Internet não é um projeto de governo; é um projeto de Estado, para o povo brasileiro. Aqui não há partido, pessoal, aqui há a soberania nacional e democracia participativa, nesse meio tão importante que, inclusive, suplanta o controle das grandes mídias neste País. O povo brasileiro aguarda e exige nosso posicionamento. A comunidade internacional acompanha atenta nosso pioneirismo nesse campo. Senhoras e senhores, é nosso ofício votar o Marco Civil da Internet. (Deputado Vicentinho, in Câmara dos Deputados, 2013p)

Por fim, cabe ressaltar que, embora estivesse intimamente ligada às denuncias de espionagem e ao discurso da presidente Rousseff na ONU, havia a consciência de que o MCI serviria ao país mais como um qudro estratégico para postulações futuras no âmbito doméstico e internacional, que como espécie de resposta direta aos atos de espionagem. Essa noção não deixou de ser exposta no parlamento e também pautou as argumentações para os votos em favor do PL:

> [...] sem dúvida esta Comissão Geral por si só já reflete a importância estratégica de debatermos um assunto em que nós vamos ser, sem dúvida nenhuma, vanguarda no mundo, na medida em que nós estamos exatamente elaborando um marco civil de uso da Internet que garante os direitos e os deveres dos usuários e de todo o sistema de Internet - dos provedores, daqueles que garantem a infraestrutura, que é a nossa rede de telecomunicações, do pacote de *softwares* usados para fazer as informações transitarem no mundo todo. Acho que nós estamos também diante de um assunto que é mais do que urgente e contemporâneo, pelo grau de vulnerabilidade em que nós estamos com esse instrumento de comunicação e de informação, que é uma das ferramentas, sem dúvida nenhuma, que revela sua eficácia, sua pujança, sua força, seu valor de informação e de formação de opinião, num país em que nós temos uma questão muito grave, que é o monopólio das comunicações, em que há pouca liberdade de expressão. Por isso, há a necessidade de a gente poder garantir e fazer valer uma Internet que hoje já funciona, com um modelo que funciona, mas com as suas restrições. Sem dúvida, qualquer ameaça a esse movimento, que já tem as suas limitações, levará ao perigo de termos a nossa liberdade de expressão comprometida. […] Podemos também, nesse bojo, levantar a discussão da questão da segurança nacional, porque o que está em jogo, é evidente, são as espionagens por parte do governo norte-americano, que deixa nosso País vulnerável, à mercê dos interesses econômicos das empresas de outros países e dos interesses estratégicos de outros Estados, como é o caso dos interesses estratégicos dos Estados Unidos, deixando-nos, portanto, em uma situação em que é preciso reagir à altura, porque isso também diz respeito ao debate da soberania e da segurança nacional. (Deputada Luciana Santos, in Câmara dos Deputados, 2013b).

O relator do projeto, o deputado Alessandro Molon, tem essa consciência da dimensão estratégica do Marco Civil. É nesse sentido que ele sublinha a articulação entre a

resposta à pressão popular interna e a capitalização desse passo em favor de um gesto significativo da política externa brasileira:

> Mas eu venho, Presidenta, a esta tribuna para tocar em outro tema também tratado pela Presidenta da República na Organização das Nações Unidas. Eu refiro-me à proposta dela de um marco civil internacional para a Internet. A Presidenta da República […] fez cinco propostas em relação à Internet mundial: primeiro, uma Internet que garanta liberdade de expressão, privacidade do indivíduo e respeito aos direitos humanos; segundo, uma Internet com governança democrática, multilateral e aberta, exercida com transparência, estimulando a criação coletiva e a participação da sociedade, dos governos e do setor privado; terceiro, uma Internet em que se tenha uma universalidade que assegure o desenvolvimento social e humano e a construção de sociedades inclusivas e não discriminatórias; quarto, a garantia do respeito à diversidade cultural, sem imposição de crenças, costumes e valores; e, por fim, como quinto ponto, uma Internet com neutralidade da rede, que respeite apenas critérios técnicos e éticos, tornando inadmissíveis restrições por motivos políticos, comerciais, religiosos ou de qualquer outra natureza. Senhoras e senhores, a Presidenta da República teve autoridade para fazer esse pronunciamento na ONU porque ela está propondo para o mundo o que ela propôs para o Brasil: a criação de um marco civil da Internet […]. (Deputado Alessandro Molon, in Câmara dos Deputados, 2013d)

Deste modo, fica claro um grande movimento capitalizado pelo Governo com apoio de sua base para a aprovação do Marco Civil. Nasce de um discurso preocupado com a escalada de ameaças, ilustrado com bastante clareza pelas denúncias de Snowden e sua publicização em meios de comunicação com repercussões mundiais. Passa, então, por uma articulação entre a base governista da Câmara dos Deputados com entidades de interesse, principalmente no que se refere a questões de governança da Internet. Culmina, então, por fim, na aprovação do projeto, primeiramente na Câmara em 25 de março de 2014 e depois no Senado, em 23 de abril do mesmo ano.

Contudo, esse movimento não teve na aprovação do MCI o seu fim. A aprovação do MCI funcionou como um suporte para o Governo traçar planos mais ambiciosos em âmbito multilateral. O próximo tópico trata desse aspecto.

4.2.6. Os princípios do Marco Civil da Internet e a agenda de política externa do governo Rousseff

O movimento que impulsionou as discussões sobre a questão da regulamentação da Internet através da pauta do MCI não se encerrou com sua aprovação pelas duas casas legislativas, em 2014. Pelo contrário, os desdobramentos que se seguiram não permitem colocar um encerramento definitivo da questão, principalmente porque a Política Externa brasileira e a própria atuação da presidente vieram a reforçar em âmbito multilateral a ideia

de adotar princípios que norteassem as discussões sobre a governança e regulamentação do ciberespaço em âmbito internacional. Ou seja, o caráter estratégico mencionado por alguns deputados no tópico anterior foi realmente colocado à frente e veio a somar-se a iniciativas de outros nomes e instituições de relevância nas discussões sobre a governança da Internet, como o ICANN (Internet Corporation for Assigned Names and Numbers) e a própria ONU, através dos fóruns de governança da Internet.

Essa agenda internacional começa a se delinear antes mesmo da aprovação do MCI. Em um movimento articulado com a primeira-ministra alemã, Angela Merkel, Brasil e Alemanha, apoiados nomeadamente pelos governos da Áustria, Liechtenstein, México, Noruega e Suíça, apresentaram uma resolução à Assembleia Geral das Nações Unidas tentando convencer a comunidade internacional a estender às suas respetivas agendas internacionais a garantia de direitos contra espionagem (Reuters, 2013). A resolução (A/RES/68/167), depois de justificar-se nas então recentes denúncias de espionagem, vinha a requerer ao

> United Nations High Commissioner for Human Rights to submit a report on the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or the interception of digital communications and the collection of personal data, including on a mass scale, to the Human Rights Council at its twenty-seventh session and to the General Assembly at its sixty-ninth session, with views and recommendations, to be considered by Member States.

Essa resolução, apesar de não prever nenhuma medida a ser implementada de imediato, é relevante por institucionalizar parâmetros e alguns princípios para a gestão da Internet em um âmbito internacional bastante específico. Mais do que isso, a forma de endereçamento da mensagem foi eficiente de modo que não encontrou grandes resistências.

A questão da governança da Internet não é um assunto alheio à Política Externa brasileira, nem mesmo surgiu por conta das denúncias de Snowden. É verdade que esses fatos serviram para reforçar a agenda internacional brasileira que já vinha acompanhando de perto os Internet Governance Foruns (IGF), inclusive sediando as reuniões em duas ocasiões: em 2007, no Rio de Janeiro e depois em 2015, em João Pessoa (IGF, 2014, 2015). Essas reuniões, apesar de serem um importante fórum de discussões com várias edições tratando de diferentes temas, não configuram o maior destaque do Brasil no campo da governança da Internet.

Por conta das discussões sobre o MCI, a presidente Dilma foi pessoalmente procurada pelo diretor do ICANN. Deste encontro e de procedentes negociações, nasceu, então a ideia de promover um encontro a nível mundial a fim de fomentar diálogos focados na governança do ciberespaço. Deste modo, a iniciativa NetMundial surgiu com o objetivo de abordar as questões importantes da governança da Internet sob o sistema de múltiplas partes interessadas (*multistakeholder governance*), com o objetivo de fornecer uma plataforma que ajudasse a organizar a cooperação prática entre as partes interessadas para abordar questões da Internet e avançar na implementação dos Princípios e Roteiros do NETmundial (NETmundial, 2014; Pilati & Vieira Cancelier de Olivo, 2017).

É importante ressaltar, porém, uma mudança significativa de posicionamento do Brasil em relação ao seu entendimento de modelo ideal para a governança da Internet. Como explicam Trinkunas & Wallace (2015), as posições sobre modelos de governança da Internet dividem-se, resumidamente, em dois grupos. O primeiro, cuja ideia Europa e Estados Unidos compartilham, defende que a governança da Internet deve passar por decisões tomadas por concertação de atores provenientes de diversos setores da sociedade, incluindo setor privado, organizações não-governamentais, instituições internacionais, acadêmicos e os próprios governos, um modelo multissetorial (*multistakeholder governance)*. O segundo, do qual países como Rússia, China e Brasil tendiam a concordar por motivos não necessariamente idênticos, defende que a governança do ciberespaço deve ser objeto de políticas multilaterais, submetidas aos interesses dos Estados que atuariam através de organizações internacionais, como a União Internacional para as Telecomunicações. Esse debate ainda está em andamento, apesar do que se entende pela governança do ciberespaço atual dar-se principalmente no primeiro modelo, com relevante influência dos Estados Unidos (G. Austin, 2017; Fritz, 2012; Internet Society, 2017; Kurbalija, 2010; Mueller, 2012). Ora, inicialmente, o Brasil partilhava do entendimento de que a governança da Internet deveria ser promovida através de instituições e organizações internacionais em uma concertação multilateral. No entanto, no contexto de negociações com entidades internacionais e da própria organização da governança da Internet no âmbito interno brasileiro, o Brasil foi se aproximando de uma visão mais voltada para o modelo multissetorial. Essa posição ficou bastante evidente durante os encontros da NETMundial que assume este modelo como ideal[62].

[62] Mais do que una reunião de impacto regional, o NETMundial foi reconhecido a nível global através da resolução A/RES/166, pela Assembleia Geral, em 2015:

A presidente Dilma Rousseff, escolheu o NETMundial para sancionar o MCI, aprovado dias antes pelo Senado Federal (Roncolato, 2014). Na ocasião, acompanhada pelo deputado, Alessandro Molon, e pelo senador Walter Pinheiro, relatores do MCI em suas respectivas Casas Legislativas, entre outras autoridades, Rousseff enfatizou:

> A internet que queremos, ela só é possível num cenário de respeito aos direitos humanos, em particular a privacidade e a liberdade de expressão. Daí porque no meu discurso na 68ª Assembleia da ONU, fiz uma proposta de combate a essas práticas, e propus uma discussão a respeito do estabelecimento de um marco civil global para governança e uso da internet, e de medidas que garantissem a efetiva proteção dos dados que por ela trafegam. Também, junto com a chanceler Ângela Merkel, nós levamos à ONU um projeto de resolução sobre o "Direito à Privacidade na Era Digital". Aprovamos por consenso esse projeto e aprovamos também o chamado aos Estados para que cessassem a coleta arbitrária ou ilegal de dados pessoais e fizessem valer o direito à privacidade. Aliás, e importante reiterar que os direitos que as pessoas têm *offline* também devem ser protegidos *online*.
>
> A NET Mundial ela vem impulsionar esse esforço. E esta reunião responde a um anseio global por mudanças na situação vigente e pelo fortalecimento sistemático da liberdade de expressão na Internet e da proteção à direitos humanos básicos como é o caso do direito à privacidade e sem, sem sombra de dúvidas, também o direito ao tratamento das discussões na internet de forma respeitosa, garantindo o seu caráter democrático e aberto. (Presidência da República, 2014a)

Eis, pois, em síntese, o que quisemos demonstrar neste capítulo. O ponto de partida foi um processo que começa com um movimento robusto de securitização da ascensão do terrorismo internacional. Por arrastamento, registou-se uma crescente politização da regulação das tecnologias da informação, criando, concomitantemente, um alerta importante sobre as ameaças provenientes deste meio, sobretudo por se entender que podem potenciar ou facilitar a atuação terrorista.

Nesta conjuntura, alegando o combate ao terrorismo, as respostas, principalmente norte-americanas, acabaram se transformando em vigilância em massa que se tornou crítica quando incluiu altas autoridades de governos, inclusive de países considerados parceiros. No desenrolar dos acontecimentos, a atuação brasileira conseguiu canalizar os esforços político-diplomáticos em favor do estabelecimento de princípios e garantias a nível internacional, ao invés do recrudescimento das tensões bilaterais e da restrição do acesso à

> Noting the holding of the Global Multi-stakeholder Meeting on the Future of Internet Governance, “NETmundial”, in São Paulo, Brazil, in April 2014, and recognizing that effectively addressing the challenges relating to the right to privacy in the context of modern communications technology will require an ongoing, concerted multi-stakeholder engagement.

Internet e à liberdade de expressão. Deste modo, partindo de um fator externo e terminando em uma proposta também endereçada a um palco internacional, passando por importantes configurações internas no caso brasileiro, esse processo pode ser entendido como um processo de securitização sui generis que resulta em medidas que garantem um ambiente dessecuritizado ao centrar-se nas garantias dos usuários da Internet e seus direitos à privacidade e livre expressão.

Vale ressaltar, no entanto, que esta é uma interpretação que incide sobre um processo em aberto. A atuação brasileira, apesar do reconhecimento da sua liderança no assunto pelas instituições internacionais, está fortemente concentrada no desempenho de um governo específico e da presidente Dilma Rousseff. Embora disponha de uma organização interna estruturada e consolidada, a manutenção do MCI como quadro de referência da atuação brasileira no debate internacional sobre a governança da Internet depende muito da diplomacia presidencial dos mandatários pós-Rousseff. De acordo com entrevista dada por assessores da presidente, a conjuntura política interna que sucedeu nos meses seguintes não favoreceu a consolidação deste assunto como uma posição efetiva do Estado brasileiro em relações internacionais, identificando-se mais com o governo Rousseff do que como uma política estatal. Ainda assim, embora não tenham dado as mesmas ênfases, os governos sucessores não têm adotado posições que contrariam o que foi construído no governo Rousseff em relação as políticas de governança da internet. É prudente, portanto, entender esse contexto como algo aberto, passível de mudanças inclusive radicais.

4.3. Considerações finais sobre a análise dos casos

O caso brasileiro apresenta algumas similaridades com o caso estoniano abordado no capítulo anterior, em termos de análise dos processos de securitização e dessecuritização. Nos dois casos há um movimento de securitização iniciado a partir de um evento significativo, de grande impacto midiático. No caso brasileiro, especificamente, fica bastante evidente, tanto pelas entrevistas colhidas quanto pelos discursos dos parlamentares, que a denúncia de espionagem norte americana tem crucial importância para o andamento e aprovação do MCI. Assim, tanto no caso brasileiro, com os Estados Unidos, quanto no estoniano, com a Rússia, há um elemento externo que pode ser identificado como um ponto inicial no movimento de securitização.

Há também uma mobilização de ambos os governos para capitalizar politicamente o evento em favor de suas agendas políticas externas. Ambos os países foram hábeis em politizar a situação a ponto de conseguirem implementar algumas de suas políticas a nível internacional com implicações internas em maior ou menor grau. O Governo brasileiro conseguiu, derivando da aprovação do MCI, trazer as discussões de forma objetiva a nível internacional ao patrocinar a NetMundial, com o apoio do ICANN. O governo estoniano, por sua vez, conseguiu de maneira bastante eficiente, consolidar o país a nível internacional como uma referência em segurança cibernética.

O movimento de securitização, no entanto, teve caminhos diferentes nos dois casos. Enquanto o Governo estoniano respondeu aos ataques cibernéticos com a implementação de políticas de segurança direcionadas à defesa cibernética, o Brasil, ao invés de responder às denúncias com medidas de exceção, direcionou a politização do discurso sobre a segurança para a aprovação de um documento que visa basicamente definir, estabelecer e delimitar as funções e direitos dos usuários da Internet no país. O movimento de securitização, bastante evidente nos discursos dos deputados e outras autoridades brasileiras acabou por gerar um resultado dessecuritizador.

Conclusões e Considerações Finais

Este trabalho visou analisar a especificidade do ciberespaço enquanto domínio no qual as ameaças desencadeiam processos político-discursivos inteligíveis à luz do arsenal conceitual das escolas da securitização e dessecuritização (designadamente a de Copenhague e a de Paris). Para esse efeito, identificámos, em primeiro lugar, a dimensão e a relevância para o sistema internacional contemporâneo da ascensão e disseminação das TIs e as interações virtuais no ciberespaço. Como vimos, tais ferramentas tornaram-se, ao longo das décadas de 1990 e 2000, um elemento que permeia e reflete as relações sociais e políticas no mundo. É possível perceber que esta tendência tende a se solidificar e se sofisticar de então para cá, desde o nível individual, considerando uma simples comunicação interpessoal, até ao nível internacional, onde são implementadas políticas específicas para atuações de Estados no ciberespaço, a nível nacional e multilateral.

O debate sobre o ciberespaço inclui, naturalmente, muitos dos temas tradicionalmente discutidos no plano internacional, como as questões de segurança vertidas em termos e conceitos específicos, como segurança da informação ou defesa cibernética.

1. Há dois momentos cruciais para a definição de uma agenda internacional da segurança da informação. Primeiramente, alguns episódios de ataques a estruturas cibernéticas demonstraram a sua fragilidade e ineficácia de suas proteções. Posteriormente, em resposta a esses ataques ou à percepção de futuras ameaças, os governos foram tomando medidas de segurança, firmando acordos internacionais ou desenvolvendo leis e regulamentos internos para o papel do Estado, dos usuários e demais atores no ciberespaço.

Nessa formulação de regulamentações, bem como na atuação por meio das instituições responsáveis pela gestão do acesso ao ciberespaço – como a União Internacional pelas Telecomunicações e os diversos fóruns de governança da Internet (IGF, WSIS) – os Estados sinalizaram que questões como soberania e o próprio papel do Estado não são, de todo, alheisa às novas dinâmicas do ciberespaço. Pelo contrário, embora de maneira reativa aos fenômenos e episódios experimentados recentemente envolvendo o ciberespaço, os Estados têm se demonstrado presentes, afirmativos e propositivos em suas posições. Mais do que isso, os Estados têm conseguido, de maneira bastante efetiva, incorporar o ciberespaço como objeto e instrumento de suas políticas internas e externas, inclusive

através de movimentos de securitização que acabam por fomentar e impulsionar agendas políticas tanto no âmbito doméstico como em nível multilateral.

Em suma, a ascensão das TIs e suas implicações sociais são elementos de grande relevância nos sistema internacional contemporâneo, mobilizando a ação de atores de diferentes níveis. Essa nova configuração social – a que alguns chamam, porventura equivocamente, Sociedade da Informação – não tem significado uma diminuição ou erosão da soberania estatal. O Estado tem mantido a sua capacidade de ação e é chamado a intervir em situações práticas de modo a promover a defesa e a segurança. Ainda que haja outros atores que ganharam espaço com voz relativamente ativa, como em muitos fóruns de discussão sobre a governança da Internet, o Estado permanece como ator fundamental no ciberespaço.

2. As Teorias da Securitização e Dessecuritização constituem uma das expressões conceituais da abertura e evolução do pensamento internacional sobre a segurança, que abandona seus limites tradicionalistas, centrados exclusivamente na instituição Estado, e gradualmente incorpora outros aspectos, como questões internas dos próprios Estados, assuntos discutidos a nível global, questões econômicas e uma infinidade de objetos de referência. A escola de Copenhague foi capaz de propor um enquadramento teórico que organizou a interpretação de assuntos ou objetos de referência que passaram a ser incluídos no pensamento e na ação política de segurança e com este rótulo discutidas tanto no debate teórico como nas esferas dos decisores. Apesar do enquadramento proposto ser sofisticado o suficiente para tecer uma interpretação teórica que explica realidades emergentes na segurança, a própria Teoria da Securitização mostra-se aberta a sofisticações que reforçaram suas já definidas estruturas e ferramentas de análise. Cabe destacar que a questão do contexto que envolve os movimentos de securitização e de dessecuritização, tal como enfatizado por Williams (2003) e Balzacq (2005), tem grande importância para a interpretação dos movimentos de securitização do ciberespaço.

3. Os casos da Estônia e do Brasil apresentam elementos contextuais relevantes para o estudo dos movimentos de securitização. O fator geopolítico que situa a Estônia em uma esfera de influência da Rússia e a grande penetração das TI naquela sociedade são elementos contextuais imprescindíveis para a compreensão do movimento de securitização

do ciberespaço ali registado. Tais elementos influenciaram a condução do movimento de securitização, que resultou, em grande medida, na afirmação de uma agenda política confrontacional, em que o perfil de uma securitização declarada atingiu patamares de alta intensidade, materializada na aproximação a instituições como a NATO, posteriormente consolidada com a instalação do CCDCoE em Tallinn.

No caso brasileiro, o que pesa sobre o contexto do movimento de securitização foram as denúncias de espionagem da NSA trazidas a público pelo ex-funcionário da agência, Edward Snowden. Pela sua extrema delicadeza diplomática e pela sua gravidade, os fatos facilmente teriam justificado um movimento de securitização "típico", de algum modo idêntico ao registado na Estônia. E, se é certo que houve claramente um discurso de securitização nos debates parlamentares que se seguiram às denúncias de Snowden, e se é também certo que a presidente Rousseff foi a primeira a politizar, interna e internacionalmente, a questão, a verdade é que o perfil de securitização atingido no Brasil foi totalmente diferente do da Estônia, com um resultado principal – o MCI – centrado numa governança da Internet orientada para a defesa dos direitos dos usuários e da liberdade de expressão, e com um resultado derivado – a veiculação desta filosofia regulatória nos debates sobre a governança internacional da Internet – através de um protagonismo brasileiro em fóruns sobre esta questão. Ou seja, no caso brasileiro ainda mais que no caso estoniano, a intensidade da excecionalidade das respostas às ameaças no ciberespaço foi baixa ou mesmo nula, o que nos leva a sugerir como hipótese interpretativa a de uma verdadeira "dessecuritização preventiva".

4. A precisão com que a concepção da securitização formulada pela Escola de Copenhague trata seus elementos, como os atores funcionais e os atores da securitização, pode limitar a análise dos concretos movimentos de securitização envolvendo o ciberespaço. Os atores, seus respectivos papéis, e os setores de análise devem estar abertos a influências mútuas, o que já é comportado pelas visões teóricas da securitização. A análise dos movimentos de securitização do ciberespaço presentes nos dois casos estudados mostra que as interpretações desses fenômenos devem estar abertas para incorporar uma influência de um setor de análise em outro e, mais interessante, ser capaz de compreender que os papéis desempenhados pelos atores envolvidos não estão necessariamente restritos ao seu principal meio de atuação. É perceptível, por exemplo, que o ator funcional também pode ser um

agente da securitização. Os mesmos atores podem assumir papeis diferentes em momentos distintos de um mesmo movimento de securitização ou dessecuritização.

Embora haja algum trânsito dos atores entre os papeis, os discursos empregados no movimento de securitização parecem ser constantes e não mudam significativamente de acordo com as audiências. No caso estoniano foi possível observar essa constância nos discursos proferidos pelo presidente Thomas Ilves na Assembleia das Nações Unidas ao falar para seus pares representantes de seus respectivos países e nas entrevistas dadas à imprensa pelo primeiro-ministro estoniano, Andrus Ansip. Os discursos basicamente repetem a necessidade de proteção do ciberespaço com medidas excecionais, de modo a manter o seu bom funcionamento e, automaticamente, a manutenção correta das atividades cotidianas que dependem do ciberespaço.

Por outro lado, os discursos de securitização do ciberespaço refletem e são refletidos, em grande medida nos documentos oficiais que estendem a necessidade de proteção do ciberespaço às atividades mais cotidianas e a fatores de relevância coletiva, como as infraestruturas críticas. Isso ilustra que as audiências na Era da Informação estão de tal modo ligadas ao contexto do ciberespaço que diminui a necessidade de adaptações significativas no discurso de securitização. Naturalmente, há particularidades, como por exemplo, a questão da proximidade com a Rússia na questão dos ciberataques estonianos, o que vem contribuir, como foi visto, para a consolidação do ciberespaço enquanto objeto de referência. Mas são elementos contextuais e não mais que isso.

No caso brasileiro, essa padronização dos discursos também é perceptível. Ao defenderem a aprovação do MCI, parlamentares basicamente reforçaram as ideias presentes no discurso da presidente Rousseff na Assembleia Geral das Nações Unidas e nas notas do Ministério das Relações Exteriores. A questão da soberania e da proteção da privacidade e das comunicações internas do governo brasileiro foram as questões que deram substância às defesas do projeto, ainda que o texto do PL não refletisse esses aspectos diretamente. De todo modo, essas preocupações já constavam em documentos do Ministério da Defesa e em outros documentos oficiais que tratam da questão da segurança e defesa cibernética no Brasil.

Nos casos analisados, foi possível constatar que o trânsito entre papeis dos atores, que ora são atores funcionais, ora assumem como fomentadores da securitização, diminui a relevância da especificidade da audiência, já que não se revela necessário um grande investimento na adaptação dos discursos.

5. No que se refere especificamente à dessecuritização, a nossa ideia inicial era tentar aplicar a concepção da securitização de modo inverso, ou seja, tentando encontrar num movimento de dessecuritização os agentes da dessecuritização e os atores funcionais, tal como nos movimentos de securitização. Intencionava-se, assim, examinar a dessecuritização como um movimento espelhado, buscando identificar os mesmos elementos da securitização, mas que desempenhassem o movimento contrário, rumo à dessecuritização do objeto de referência. Contudo, as primeiras leituras da ainda escassa literatura sobre a dessecuritização já mostravam que essa interpretação não teria contornos devidamente definidos, ou sólidos o suficiente para propor uma formulação teórica neste sentido. E o estudo de caso sobre o Brasil confirmou que os movimentos de dessecuritização podem não tem um padrão tão definido quanto os movimentos de securitização.

Essa falta de padrão ou de elementos teóricos definidos com precisão para a dessecuritização não é, necessariamente, uma falha na formulação de ferramentas teóricas ou metodologias de análise, mas sim o resultado de esses movimentos serem de tal modo singulares que têm que ser examinados com a ressalva de que seus elementos possam não ser replicados em outros casos.

Neste sentido as considerações da Escola de Paris acabam por servir melhor como instrumentos de análise e de explicação do que a própria formulação de Copenhague, já que priorizam o contexto e as intenções dos atores envolvidos nos processos de securitização. Permitem assim estender a análise para além das questões de segurança e entender como esta se relaciona a outros aspectos da agenda política. Nos dois casos estudados esses aspectos ficam bastante evidentes e têm grande influência no curso dos acontecimentos. No caso da Estônia, os ataques cibernéticos acabaram por impulsionar uma agenda de política exterior de forma exitosa. No caso brasileiro, houve até mais frutos com os resultados já que o Governo conseguiu aprovar o projeto do MCI e ao mesmo tempo em que conseguia visibilidade internacional.

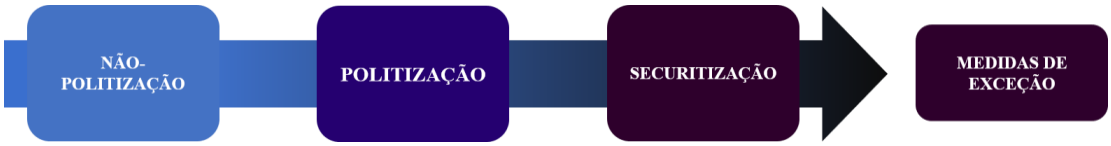
De algum modo, seria possível identificar a presidente Dilma Rousseff e os deputados brasileiros como agentes da dessecuritização ao aprovarem o MCI. Do mesmo modo, considerando que esses atores têm autoridade para implementar medidas, também poderiam ser classificados como atores funcionais da dessecuritização. Contudo, embora os resultados de suas ações tenham promovido a dessecuritização de um objeto de referência, os discursos não tinham um teor que vocalizasse a desmobilização do discurso de

securitização. A estratégia tanto do Governo quanto dos deputados estava completamente em função da aprovação do projeto de lei que gerou, como um resultado indireto, uma dessecuritização.

O que quisemos demonstrar foi que a dessecuritização não depende necessariamente da desmobilização de um processo de securitização consumado. Weaver (2005) sugere que dessecuritização poderia partir de um processo de securitização em andamento através do emprego de discursos que desmobilizam o movimento de securitização. No entanto, no caso brasileiro, os discursos não apresentaram esse viés. Novamente, a análise da intenção política dos atores se impõe sobre a dinâmica da evolução do processo. Dependendo da sua articulação, a agenda do ator funcional, quando se apresenta também como ator da securitização e da dessecuritização, são determinantes para o resultado do processo. No caso do MCI, o Governo brasileiro, ao articular sua base no Congresso para capitalizar politicamente o episódio protagonizado por Snowden, acabou utilizando de um movimento de securitização para promover uma agenda política, simbolizada pela aprovação do projeto de lei dessecuritizador.

A título de ilustração, é possível representar os casos abordados em uma espécie de linha do tempo teórica em função da evolução do movimento de securitização formulado pela escola de Copenhague. Tal como se abordou no capítulo 2, o movimento de securitização evolui tal como na figura abaixo:

Figura 3. Evolução do movimento de securitização:



Fonte: Adaptado de Buzan et al. (1998).

O caso estoniano (Figura 2) apresenta uma linha que conduz a um cenário não necessariamente securitizado, mas cujo discurso de securitização permanece. Por isso, a linha teórico-cronológica desvia-se levando o movimento a um cenário dominado pela agenda política em detrimento das medidas de exceção ostensivas.

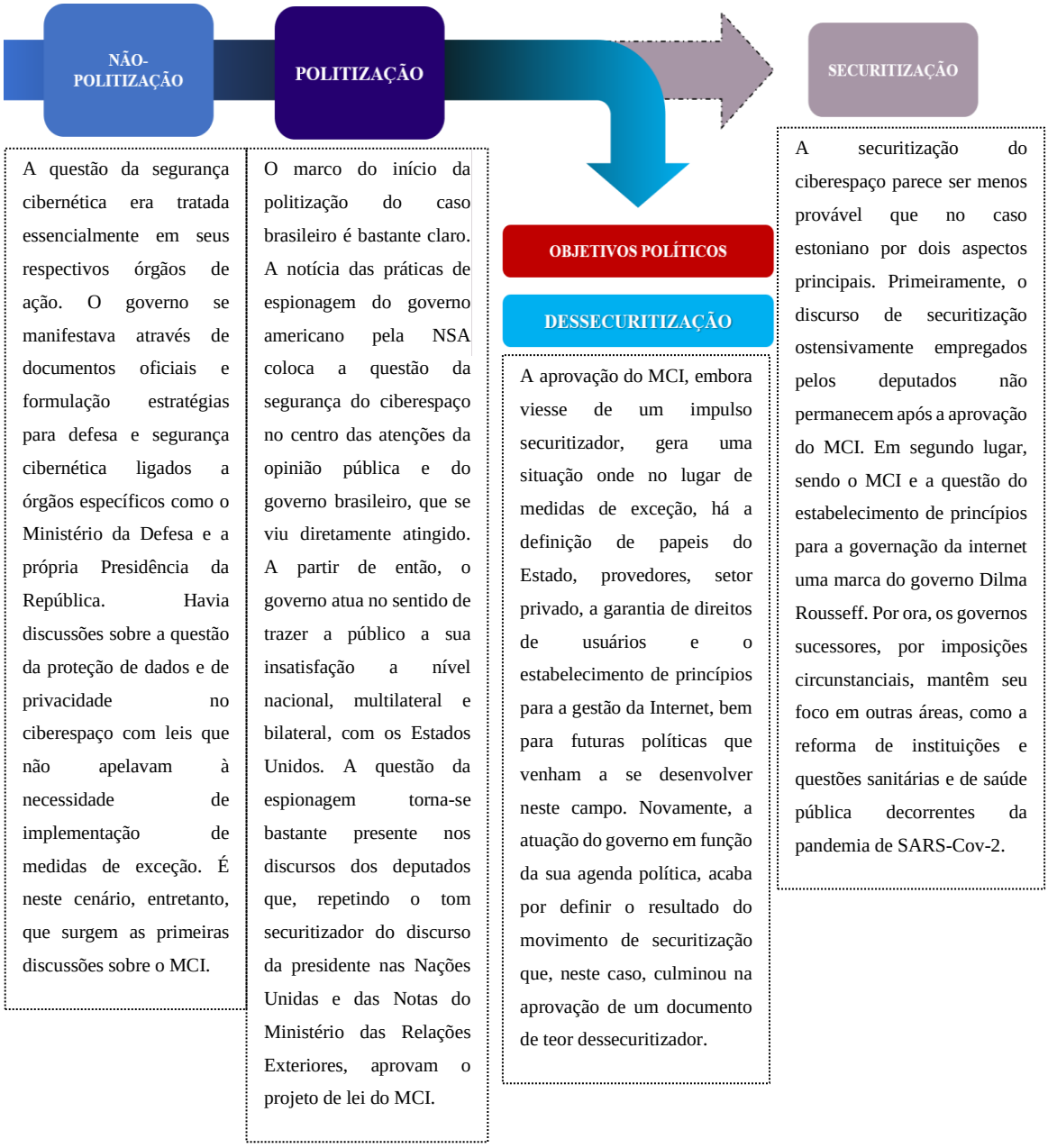
Figura 4. Evolução do movimento de securitização no caso estoniano

Cenário em que as questões de segurança e defesa do ciberespaço são regidas pela normalidade política. Há avanços e implementações de medidas de segurança do ciberespaço em todos os aspectos principalmente em função da informatização da sociedade estoniana, que desde a década de 1990 promovia uma digitalização dos serviços gerais e práticas de e-governance. O assunto, embora debatido com as devidas menções à questão de segurança era tratado dentro da normalidade política.	A politização das questões de segurança do ciberespaço começa quando as autoridades estonianas decidem ir a público e chamar a atenção internacional não só para os ataques cibernéticos dos quais a Estônia era alvo, mas também para a criação de mecanismos ou de práticas internacionais para fazer frente a ameaças do ciberespaço. Esse discurso se mantém até os dias atuais, não dependendo necessariamente das mudanças de governo.	O discurso de securitização permanece justificando as políticas e posições adotadas pelo governo estoniano tanto no âmbito nacional, quanto internacional. Embora tenha superado a crise gerada pelos ataques de maneira eficiente, as medidas de exceção permanecem como opções a serem invocadas eventualmente. Há, portanto, uma politização permanente do tema que serve aos interesses políticos do governo estoniano e se refletem nas políticas internas e externas do país.

Fonte: Elaborado pelo autor.

O caso brasileiro, diferentemente do estoniano, não termina em um cenário em que o discurso de securitização corre em paralelo. Naturalmente, há sempre uma securitização quando se trata da segurança do Estado. Ainda assim, analisando os discursos dos parlamentares, observa-se que as alegações da necessidade de securitização cessaram com a aprovação do MCI, levando a um cenário dessecuritizado.

Figura 5. Evolução do movimento de securitização e dessecuritização do ciberespaço no Brasil.



Fonte: Elaborado pelo autor.

6. A securitização do ciberespaço não pode ser vista como um processo completamente universal, apesar de o ciberespaço ser apresentado como um problema

comum a todos e de os discursos de securitização apresentarem características similares. A razão é que os processos levam a resultados e interpretações diferentes.

Em termos de conceitualização, especificamente no que se refere à diferenciação da defesa e segurança cibernética, apesar de ambas serem originadas por um discurso de securitização comum, generalizações nestes conceitos podem levar a uma análise pouco clara dos agentes e suas funções e alcance. Uma das primeiras dificuldades encontradas reside na própria definição dos conceitos de defesa e segurança no ciberespaço. Os conceitos de segurança cibernética e defesa cibernética têm sido usados pelos diversos atores em função dos seus objetivos, variando conforme o escopo das políticas ou práticas que querem atingir. Embora a contribuição para melhores definições dos conceitos também tenha sido um dos elementos a serem observados neste trabalho, optámos por tomar as definições existentes e adaptá-las ao foco central do trabalho, que são as contribuições do ciberespaço para a sofisticação das teorias da securitização. Há ainda a necessidade de explorar e melhor definir os conceitos relacionados à segurança e à defesa cibernética. É esta, portanto, uma das lacunas científicas a serem exploradas em futuros trabalhos com este intuito.

7. A questão da governança da Internet parece ser o maior desafio para a segurança do ciberespaço análise isso desafia um estudo mais aprofundado das relações de poder entre os *stakeholders* nos fóruns multilaterais para a governança da Internet. Ainda neste aspecto, as relações de poder entre Estados nas organizações internacionais como a ITU, NATO e na própria ONU precisam ser analisadas com mais profundidade. É no âmbito das Organizações Internacionais que melhor se podem verificar os reflexos das dinâmicas de poder entre os Estados.

Sobre os estudos de caso aqui abordados, seria relevante abordar as eventuais iniciativas de cooperação internacional da Estônia com os outros países que tiveram incidentes de segurança cibernética atribuídos à Rússia, como a Geórgia, Ucrânia entre outros mencionados no capítulo 3. O governo estoniano foi bastante eficiente em direcionar a imagem do país em nível multilateral enquanto especialista ou potência em segurança cibernética. Um importante desafio de pesquisa é o de saber se essa postura depende de uma constância do discurso de securitização e como este é recebido pelos países com os quais existe aquela cooperação.

Já no caso brasileiro a particularidade da figura do presidente Dilma Rousseff coloca uma questão importante: considerando que houve um relevante rompimento na condução da política brasileira com o impedimento da presidente Rousseff, é relevante entender como essa questão será abordada pelos governos seguintes, quer (como acontece presentemente) venham de um parâmetro ideológico radicalmente diferente do que defendia a presidente, quer venham hipoteticamente a regressar a esse parâmetro no futuro.

Fontes e Referências Bibliográficas

Aaviksoo, J. (2010). Cyberattacks Against Estonia Raised Awareness of Cyberthreats. *Defence Against Terrorism Review*, *3*(2), 13–22. Retrieved from http://www.coedat.nato.int/publication/datr/volume6/02-Cyberattacks_Against_Estonia_Raised_Awareness_of_Cyberthreats.pdf

Abdenur, A. (2014). *Brazil and Cybersecurity in the Aftermath of the Snowden Revelations". En International Security: a European-South American Dialogue*. Rio de Janeiro.

Academi. (2018). Academi - About Us - Industries. Retrieved October 1, 2018, from https://www.academi.com/pages/about-us/industries

Adamides, C. (2012). *Institutionalized, horizontal and bottom-up securitization in ethnic conflict environments: the case of Cyprus*. University of Birmingham. Retrieved from http://etheses.bham.ac.uk/3791/

AFP. (2017, May 6). Macron says hacked documents have been mixed with false ones to "sow doubt and disinformation." *The Journal*. Retrieved from https://www.thejournal.ie/macron-emmanuel-hacking-documents-french-election-3376197-May2017/

Albert, M., & Buzan, B. (2011). Securitization, sectors and functional differentiation. *Security Dialogue*, *42*(4–5), 413–425. https://doi.org/10.1177/0967010611418710

Alles, D., Guilbaud, A., & Lagrange, D. (2018). Interviews in International Relations. In G. Devin (Ed.), *Resources and Applied Methods in International Relations* (pp. 109–122). New York: Springer International Publishing. https://doi.org/10.1007/978-3-319-61979-8_8

Alsayyad, N. (2012). The Virtual Square: Urban Space, Media and the Egyptian Uprising. *Harvard International Review*, *34*(Summer 2012).

Ansip, A. (2017a). *Speech by Vice-President Ansip at the Munich Cybersecurity Conference | European Commission*. Munich: European Commision. Retrieved from https://ec.europa.eu/commission/commissioners/2014-2019/ansip/announcements/speech-vice-president-ansip-munich-cybersecurity-conference_en

Ansip, A. (2017b, April). Andrus Ansip: 'We decided to solve the problem before it got out of hand. *ERR*.

Apps, P. (2014). DDoS attacks get bigger, smarter, more damaging. *Reuters*. Retrieved from http://www.reuters.com/article/2014/03/05/us-cyber-ddos-idUSBREA240XZ20140305

Arora, R. K., & Kaura, V. (2017). *India-US Homeland Security Cooperation in the Time of Modi and Trump*. Delhi. Retrieved from https://www.orfonline.org/wp-content/uploads/2017/08/ORF_Issue_Brief_India-US_Homeland.pdf

Arquilla, J. (2013). Twenty Years of Cyberwar. *Journal of Military Ethics*, *12*(1). https://doi.org/10.1080/15027570.2013.782632

Article19. (2012). *Brasil: Projeto de Lei de Cibercrimes*. Brasília. Retrieved from www.article19.org

Ashmore, W. C. (2009). Impact of Alleged Russian Cyber Attacks. *Baltic Securityt &*

Defense Review, *11*(2009), 4–40. Retrieved from http://www.bdcol.ee/files/files/documents/Research/BSDR2009/1_ Ashmore - Impact of Alleged Russian Cyber Attacks .pdf

Atkins, E. (2013). Spying on Americans: At What Point Does The NSA's Collection and Searching of Metadata Violate The Fourth Amendment? *Washington Journal of Law, Technology & Arts*, *10*(1). Retrieved from http://digital.lib.washington.edu/dspace-law/handle/1773.1/1390

Attia, A. M., Aziz, N., Friedman, B., & Elhusseiny, M. F. (2011). Commentary: The impact of social networking tools on political change in Egypt's "Revolution 2.0." *Electronic Commerce Research and Applications*. https://doi.org/10.1016/j.elerap.2011.05.003

Austin, G. (2017). Restraint and Governance in Cyberspace. In *Global Insecurity* (pp. 215–233). London: Palgrave Macmillan UK. https://doi.org/10.1057/978-1-349-95145-1_12

Austin, J. (1962). *How to do things with words*. Oxford: Oxford University Press. Retrieved from http://pubman.mpdl.mpg.de/pubman/item/escidoc:2271128:3/component/escidoc:2271430/austin_1962_how-to-do-things-with-words.pdf

Baker, N. V. (2003). National Security versus Civil Liberties. *Presidential Studies Quarterly*, *33*(3). Retrieved from http://ieas.unideb.hu/admin/file_3879.pdf

Baldwin, D. A. (1997). The concept of security*. *Review of International Studies*, *23*, 5–26. Retrieved from https://www.princeton.edu/~dbaldwin/selected articles/Baldwin (1997) The Concept of Security.pdf

Balzacq, T. (2005a). The three faces of securititization: political agncy, audience and context. *European Journal of International Relations*, *11*(2), 171–201.

Balzacq, T. (2005b). The Three Faces of Securitization: Political Agency, Audience and Context. *European Journal of International Relations* , *11*(2), 171–201. Retrieved from http://www.guillaumenicaise.com/wp-content/uploads/2014/08/Balzacq_three-faces-of-securitization.pdf

Balzacq, T. (2011). *Securitization Theory: how security problems emerge and dissolve*. London: Routledge.

Bargh, J. A., & McKenna, K. Y. A. (2004). The Internet and Social Life. *Annual Review of Psychology*, *55*(1), 573–590. https://doi.org/10.1146/annurev.psych.55.090902.141922

Barker, T. (2017). Germany Strengthens Its Cyber Defense. *Foreign Affairs*. Retrieved from https://www.foreignaffairs.com/articles/germany/2017-05-26/germany-strengthens-its-cyber-defense?cid=int-lea&pgtype=hpg

Barney, D. D. (2004). *The network society*. Polity.

Baylis, J., Smith, S., & Owens, P. (2016). *The globalization of world politics : an introduction to international relations*. Oxford: Oxford University Press. Retrieved from https://global.oup.com/ukhe/product/the-globalization-of-world-politics-9780198739852?cc=be&lang=en&

BBC. (2014). NSA "targets" Tor web servers and users. *BBC News*. Retrieved from http://www.bbc.com/news/technology-28162273

Beatrix Toth. (n.d.). *Estonia under cyber attack*. Budapest. Retrieved from http://www.cert.hu/sites/default/files/Estonia_attack2.pdf

Bell, Daniel. (1999). *The coming of post-industrial society : a venture in social forecasting*. Basic Books.

Bell, David. (2001). *An introduction to cybercultures*. London: Routledge.

Benedikt, M. (2000). Cyberspace: first steps. In *The Cybercultures Reader* (pp. 29–44). New York: Psychology Press.

Bennett, A., & Elman, C. (2007). Case Study Methods in the International Relations Subfield. *Comparative Political Studies*, *40*(2), 170–195. https://doi.org/10.1177/0010414006296346

Berners-Lee, S. T. (2016). Uma Carta Aberta Aos Legisladores Brasileiros / An Open Letter to Brazilian Lawmakers – World Wide Web Foundation. Retrieved November 9, 2018, from https://webfoundation.org/2016/04/uma-carta-aberta-aos-legisladores-brasileiros-an-open-letter-to-brazilian-lawmakers/

Berners-Lee, T. (1998). The World Wide Web and the "Web of Life" The World Wide Web Consortium. Retrieved from https://www.w3.org/People/Berners-Lee/UU.html

Bessa, J. (2014). *O Escândalo da espionagem no Brasil* (1st ed.). Brasília: Thesaurus.

Blank, S. (2017). Cyber War and Information War à la Russe. In *Understanding Cyber Conflict: Fourteen Analogies*. Washington, D.C.: Georgetown University Press.

Borger, J. (2017). US official says France warned about Russian hacking before Macron leak. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2017/may/09/us-russians-hacking-france-election-macron-leak

Boulanin, V. (2013). Cybersecurity and the arms industry. In *SIPRI Yearbook 2013: Armaments, disarmaments and international security.* (pp. 210–226). Oxford: Oxford University Press.

Boys, J. D. (2018). The Clinton administration's development and implementation of cybersecurity strategy (1993–2001). *Intelligence and National Security*, *33*(5), 755–770. https://doi.org/10.1080/02684527.2018.1449369

Braga, J. (2014, March 26). Para Dilma, aprovação do Marco Civil da Internet é "vitória" da sociedade. *G1 - Política*. Retrieved from http://g1.globo.com/politica/noticia/2014/03/dilma-diz-que-aprovacao-do-marco-da-internet-e-vitoria-da-sociedade.html

Brauch, H. G. (2008). Conceptualising the environmental dimension of human security in the UN. *International Social Science Journal*, *59*, 19–48. https://doi.org/10.1111/j.1468-2451.2008.00631.x

Brenner, S. (2007). At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare. *Journal of Criminal Law and Criminology*, *97*(2), 379–475. Retrieved from https://www.jstor.org/stable/40042831?seq=1#page_scan_tab_contents

Bronk, C. (2016). *Cyber threat : the rise of information geopolitics in U.S. national security*. Retrieved from http://publisher.abc-clio.com/9781440834998

Buzan, B. (2008). People, States and Fear. In *People, States asd Fear* (2nd ed., p. 310). Essex: ECPR PRESS.

Buzan, B., Wilde, J. de., & Weaver, O. (1998). *Security : a new framework for analysis*.

London: Lynne Rienner Pub.

Calhoun, C. (2013). Occupy Wall Street in perspective. *The British Journal of Sociology*, *64*(1), 26–38. https://doi.org/10.1111/1468-4446.12002

Câmara dos Deputados. Projeto de Lei No. 84/1999 (1999). Brasília: Câmara dos Deputados. Retrieved from http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=588033&filename=Tramitacao-EMS+84/1999+%3D%3E+PL+84/1999

Câmara dos Deputados. Projeto de Lei Original Nº 84, DE 1999 (1999). Brasília: Câmara dos Deputados.

Câmara dos Deputados. Lei Nº 12.737, de 30 DE Novembro de 2012. (2012). Brasília: Câmara Federal. Retrieved from http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm

Câmara dos Deputados. (2013a). *Frente Parlamentar em Defesa dos Direitos Humanos e Movimento Marco Civil da Internet Já*. Brasília: Câmara dos Deputados. Retrieved from http://imagem.camara.gov.br/internet/audio/Resultado.asp?txtCodigo=46699

Câmara dos Deputados. (2013b). Marco civil da internet ganha urgência constitucional na tramitação. Brasília: Câmara dos Deputados. Retrieved from http://www2.camara.leg.br/camaranoticias/noticias/COMUNICACAO/451694-MARCO-CIVIL-DA-INTERNET-GANHA-URGENCIA-CONSTITUCIONAL-NA-TRAMITACAO.html

Câmara dos Deputados. Pronunciamento da deputada Benedita da Silva em 19/11/2013 (2013). Brasília: Câmara dos Deputados. Retrieved from http://www.camara.leg.br/internet/sitaqweb/TextoHTML.asp?etapa=5&nuSessao=377.3.54.O

Câmara dos Deputados. (2013d). Pronunciamento da deputada Luciana Santos em 06/11/2013. Brasília: Câmara dos Deputados. Retrieved from http://www.camara.leg.br/internet/sitaqweb/TextoHTML.asp?etapa=5&nuSessao=359.3.54.O

Câmara dos Deputados. (2013e). Pronunciamento do deputado Alessandro Molon em 26/09/2013. Brasília: Câmara dos Deputados. Retrieved from http://www.camara.leg.br/internet/sitaqweb/TextoHTML.asp?etapa=5&nuSessao=293.3.54.O

Câmara dos Deputados. (2013f). Pronunciamento do deputado Arolde de Oliveira em 06/11/2013. Brasília: Câmara dos Deputados. Retrieved from http://www.camara.leg.br/internet/sitaqweb/TextoHTML.asp?etapa=5&nuSessao=359.3.54.O

Câmara dos Deputados. (2013g). Pronunciamento do deputado Gustavo Petta em 19/03/2014. Brasília: Câmara dos Deputados. Retrieved from http://www.camara.leg.br/internet/sitaqweb/TextoHTML.asp?etapa=5&nuSessao=052.4.54.O

Câmara dos Deputados. (2013h). Pronunciamento do deputado Inocêncio Oliveira em 06/11/2013. Retrieved November 23, 2018, from http://www.camara.leg.br/internet/sitaqweb/TextoHTML.asp?etapa=5&nuSessao=359.3.54.O

Câmara dos Deputados. (2013i). Pronunciamento do deputado Ivan Valente em 06/11/2013. Brasília: Câmara dos Deputados. Retrieved from

http://www.camara.leg.br/internet/sitaqweb/TextoHTML.asp?etapa=5 &nuSessao=359.3.54.O

Câmara dos Deputados. (2013j). Pronunciamento do deputado Jefferson Campos em 08/10/2013. Brasília: Câmara dos Deputados. Retrieved from http://www.camara.leg.br/internet/sitaqweb/TextoHTML.asp?etapa=5 &nuSessao=308.3.54.O

Câmara dos Deputados. (2013k). Pronunciamento do deputado João Arruda em 06/11/2013. Brasília: Câmara dos Deputados. Retrieved from http://www.camara.leg.br/internet/sitaqweb/TextoHTML.asp?etapa=5 &nuSessao=359.3.54.O

Câmara dos Deputados. (2013l). Pronunciamento do deputado Leonardo Monteiro em 08/10/2013. Brasília: Câmara dos Deputados. Retrieved from http://www.camara.leg.br/internet/sitaqweb/TextoHTML.asp?etapa=5 &nuSessao=308.3.54.O

Câmara dos Deputados. (2013m). Pronunciamento do deputado Mendonça Filho em 06/11/2013. Brasília: Câmara dos Deputados. Retrieved from http://www.camara.leg.br/internet/sitaqweb/TextoHTML.asp?etapa=5 &nuSessao=359.3.54.O

Câmara dos Deputados. (2013n). Pronunciamento do deputado Newton Lima em 25/09/2013. Brasília: Câmara dos Deputados. Retrieved from http://www.camara.leg.br/internet/sitaqweb/TextoHTML.asp?etapa=5 &nuSessao=291.3.54.O

Câmara dos Deputados. (2013o). Pronunciamento do deputado Vicentinho 19/03/2014. Brasília: Câmara dos Deputados. Retrieved from http://www.camara.leg.br/internet/sitaqweb/TextoHTML.asp?etapa=5 &nuSessao=052.4.54.O

Câmara dos Deputados. (2013p). Pronunciamento do sr. Francisco Chagas em 16/07/2013. Brasília: Câmara dos Deputados. Retrieved from http://www.camara.leg.br/internet/sitaqweb/TextoHTML.asp?etapa=3&nuSessao=212.3.54.O &nuQuarto=25&nuOrador=3&nuInsercao=0&dtHorarioQuarto=14:48&sgFaseSessao=PE &Data=16/07/2013&txApelido=FRANCISCO CHAGAS&txFaseSessao

Câmara dos Deputados. (2013q). Pronunciamento do sr. Pablo Ortellado em 06/11/2013. Brasília: Câmara dos Deputados. Retrieved from http://www.camara.leg.br/internet/sitaqweb/TextoHTML.asp?etapa=5 &nuSessao=359.3.54.O

Câmara dos Deputados. (2016). *Relatório Final da Comissão Parlamentar de Inquérito destinada a Investigar a pr+atica de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país.* Brasília. Retrieved from http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra;jsessionid=214D61B364D3F74027CAB7F56C3E0C39.proposicoesWeb2?codteor=1455189&filename=REL+4/2016+CPICIBER+%3D%3E+RCP+10/2015

Campbell, K. M. (2008). *Climatic cataclysm : the foreign policy and national security implications of climate change*. Washington: Brookings Institution Press. Retrieved from https://www.jstor.org/stable/10.7864/j.ctt1262fp

Cardoso, G. (1998). *Comunidades virtuais em português* (2nd ed.). Oeiras: Celta Editora.

Carr, J. (2012). *Inside cyber warfare*. O'Reilly.

Carreiro, M. (2012). A guerra cibernética: cyberwarfare e a securitização da Internet. *Revista Cantareira*, *17*(Jul-Dez), 123–138. Retrieved from http://www.boxofficemojo.com/

Castells, M. (2004). *The network society : a cross-cultural perspective*. Barcelona: Edward Elgar Pub.

Castells, M., & Borges, M. L. X. de A. (2003). *A galáxia da internet : reflexões sobre a internet, os negócos e a sociedade*. Jorge Zahar.

Casula, P. (2014). The Road to Crimea: Putin's Foreign Policy Between Reason of State, Sovereignty and Bio-Politics The Ups and Downs in Russia's Foreign Policy Relationship With the West, *148*(2). Retrieved from http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/RAD-148-2-6.pdf

Casula, P. (2017). Russia's Foreign Policy from the Crimean Crisis to the Middle East: Great Power Gamble or Biopolitics? *Rising Powers Quarterly*, *2*(1), 27–51. Retrieved from http://risingpowersproject.com/wp-content/uploads/2017/02/vol2.1-Philipp-Casula.pdf

Cavelty, M. D., & Brunner, E. (2007). Introduction: Information, Power, and Security: An Outline of Debates and Implications. In *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace* (pp. 1–18). Aldershot: Ashgate.

CETIC. (2017a). *Indicadores*. São Paulo. Retrieved from https://www.cetic.br/tics/domicilios/2017/individuos/C5/

CETIC. (2017b). *Usuários de Interner por frequeência de uso*. São Paulo. Retrieved from https://www.cetic.br/tics/domicilios/2017/individuos/C3/

CETIC. (2017c). *Usuários de Internet - Indicador Ampliado*. São Paulo. Retrieved from https://www.cetic.br/tics/domicilios/2017/individuos/C2A/

CETIC. (2017d). *Usuários de Internet por dispositivo utilizado*. São Paulo. Retrieved from https://www.cetic.br/tics/domicilios/2017/individuos/C16/

CETIC. (2017e). *Usuários de Internet por frequência de uso*. São Paulo. Retrieved from https://www.cetic.br/tics/domicilios/2017/individuos/C3/

CGI. (2013). *O CGI.br e o Marco Civil da Internet*. São Paulo. Retrieved from https://cgi.br/media/docs/publicacoes/4/CGI-e-o-Marco-Civil.pdf

Chamorro, E., Lopez, J. R., & Fernandez, S. (2012). *Establishing a National Cybersecurity System in the Context of National Security and Defence Sector Reform*. *Spanish Cyber Security Institute*. https://doi.org/10.11610/isij.3104

Chan, S. (2017). Fearful of Hacking, Dutch Will Count Ballots by Hand. *New York Times*. Retrieved from https://www.nytimes.com/2017/02/01/world/europe/netherlands-hacking-concerns-hand-count-ballots.html

Choucri, N. (2012). *Cyberpolitics in international relations*. Cambridge: MIT Press.

Choucri, N., Madnick, S., & Ferwerda, J. (2014). Institutions for Cyber Security: International Responses and Global Imperatives. *Information Technology for Development*, *20*(2). https://doi.org/10.1080/02681102.2013.836699

Choucri, N., & Ridgeway Center, M. B. (2012). *Emerging Trends in Cyberspace: Dimensions & Dilemmas Prepared for Conference on Cyberspace: Malevolent Actors, Criminal Opportunities and Strategic Competition*. Pittsburgh. Retrieved from

https://nchoucri.mit.edu/sites/default/files/documents/%5BChoucri%5D 2012 Emerging Trends in Cyberspace-Dimensions %26 Dilemmas.pdf

Christensen, K. K., & Liebetrau, T. (n.d.). *Security Meets Cyberspace: The Politics of Cyber Security*. Retrieved from http://dpsa.dk/papers/Security Meets Cyberspace - The Politics of Cyber Security DRAFT.pdf

Clark, D. (2010). *Characterizing Cyberspace: Past, Present, and Future*. Retrieved from http://ecir.mit.edu/index.php/research/working-papers/112-characterizing-cyberspace-past-present-and-future

Clark, E., & Johansson, S. (2012). *Social Movement & Social Media: A qualitative study of Occupy Wall Street*. Södertörn University . Retrieved from http://www.diva-portal.org/smash/get/diva2:539573/FULLTEXT01.p

Clarke, R. A. (Richard A., & Knake, R. K. (2012). *Cyber war : the next threat to national security and what to do about it*. Ecco.

Clemente, D. (2013). *Cyber Security and Global Interdependence: What Is Critical? Charity Registration Number: 208223 Cyber Security and Global Interdependence: What Is Critical?* London. Retrieved from https://www.chathamhouse.org/sites/default/files/public/Research/International Security/0213pr_cyber.pdf

Cohen-Almagor, R. (2011). Internet History. *International Journal of Technoethics*, *2*(2), 45–64. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1871866

Congress of United States of America. Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA Patriot Act) act of 2001, 26 Congress of the United States § (2001). Washington. Retrieved from https://www.sec.gov/about/offices/ocie/aml/patriotact2001.pdf

Cook, J. (2014). Sony Hackers Have Over 100 Terabytes of Documents. Only Released 200 Gigabytes so far. *Business Insider*. Retrieved from http://www.businessinsider.com/the-sony-hackers-still-have-a-massive-amount-of-data-that-hasnt-been-leaked-yet-2014-12

Council of Foreign Relations. (2018). Mission Statement - Council on Foreign Relations. Retrieved October 1, 2018, from https://www.cfr.org/about/mission-statement

Craig, A. (2015). *Arms Racing in Cyberspace*. University of Glasgow. Retrieved from http://endeavour.gla.ac.uk/117/1/2015CraigMResdissertation.pdf

Craig, A., & Valeriano, B. (2016a). Conceptualising cyber arms races. In *2016 8th International Conference on Cyber Conflict (CyCon)* (pp. 141–158). IEEE. https://doi.org/10.1109/CYCON.2016.7529432

Craig, A., & Valeriano, B. (2016b). Reacting to Cyber Threats: Protection and Security in the Digital Age. *Global Security and Intelligence Studies*, *1*(2). Retrieved from https://www.researchgate.net/profile/Brandon_Valeriano/publication/305037963_Reacting_to_Cyber_Threats_Protection_and_Security_in_the_Digital_Age/links/57f2931b08ae280dd0b56421.pdf

Damiris, N., & Wild, H. (1997). The Internet: A new agora? In J. Berleur & D. Whitehouse (Eds.), *An Ethical Global Information Society* (pp. 307–317). Boston: Springer US. https://doi.org/10.1007/978-0-387-35327-2_27

David, M., & Spargo, C. (2014). Premiere of Kim assassination film CANCELED after hacker terror threat: Thousands of movie theaters refuse to show Seth Rogen's The

Interview - and crisis-hit Sony says it “won’t object.” *Daily Mail*. Retrieved from http://www.dailymail.co.uk/news/article-2876942/Movie-theaters-warned-cancel-showings-Kim-Jong-assassination-film-Interview-hacker-terror-threats-Sony-says-pull-film-want.html

Davis, J. (2007). Hackers Take Down the Most Wired Country in Europe. *Wired*. Retrieved from https://www.wired.com/2007/08/ff-estonia/

Deibert, R. (2011). Ronald Deibert: Tracking the emerging arms race in cyberspace. *Bulletin of the Atomic Scientists*, *67*(1), 1–8. https://doi.org/10.1177/0096340210393703

Demchak, C. C., & Dombrowski, P. (2011). Rise of a Cybered Westphalian Age. *Strategic Studies Quarterly*, (Spring), 32–62. Retrieved from https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-05_Issue-1/Demchak-Dombrowski.pdf

DeNardis, L. (2015). *The global war for Internet governance*. New Haven: Yale University Press.

Denning, P. J., Hearn, A., Kern, C. W., Denning, P. J., Hearn, A., & Kern, C. W. (1983). History and overview of CSNET. In *Proceedings of the symposium on Communications Architectures & Protocols - COMM ’83* (Vol. 13, p. 138). New York, New York, USA: ACM Press. https://doi.org/10.1145/1035237.1035267

Department of Homeland Security. (2013). *Executive Order 13636: Improving Critical Infrastructure Cybersecurity Department of Homeland Security Integrated Task Force Incentives Study Analytic Report*. Washington. Retrieved from https://www.dhs.gov/sites/default/files/publications/dhs-eo13636-analytic-report-cybersecurity-incentives-study.pdf

Department of State. (2010). *Remarks on Internet Freedom*. Washington: Department of State. Retrieved from https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm

Dijck, D. (2006). ‘Is EU policy on illegal immigration securitized? Yes Of Course! A study into the dynamics of institutionalized securitization. In *Pan-European Conference on EU Politics*. Istanbul.

Dougherty, J., & Kaljurand, R. (2015). *Estonia´s Virtual Russian World": The influence of Russian Media on Estonia´s Russian Speakers* (No. October 2015). Tallinn. Retrieved from https://www.icds.ee/fileadmin/media/icds.ee/failid/Jill_Dougherty__Riina_Kaljurand_-_Estonia_s__Virtual_Russian_World_.pdf

Drent, M., Hendriks, R., & Zandee, D. (2015). *New Threats, New EU and NATO Responses*. Amsterdam.

Dubroff, M. D. (2009). Russia’s Innovative Cyber-War on Estonia. *Inventor Spot*. Retrieved from http://inventorspot.com/articles/russias_innovative_cyberwar_estonia_25100

Dunn Cavelty, M. (2013). From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review*, *15*(1), 105–122. https://doi.org/10.1111/misr.12023

Duque, M. G. (2009). O papel de síntese da escola de Copenhague nos estudos de segurança internacional. *Contexto Internacional*, *31*(3), 459–501. https://doi.org/10.1590/S0102-85292009000300003

Economic Times. (2012, November 6). Global cooperation must for cyber security: Kapil

Sibal - The Economic Times. *The Economic Times*. Retrieved from https://economictimes.indiatimes.com/tech/internet/global-cooperation-must-for-cyber-security-kapil-sibal/articleshow/17114025.cms

Estonia. (1998). Principles of Estonian Information Policy. Tallinn. Retrieved from http://intosaiitaudit.org/pas/010402estoniacpapp.pdf

Estonia. Electronic Communications Act (2004). Tallinn: Estonian Pairliament. Retrieved from https://www.riigiteataja.ee/en/eli/501042015003/consolide

Estonia. (2007). *Discurso do Presidente Mr. Toomas Hendrik Ilves à 62nd session of the United Nations General Assembly*. New York: United Nations. Retrieved from http://www.un.org/webcast/ga/62/2007/pdfs/estonia-eng.pdf

Estonia. Information Society Strategy 2013 (2013). Tallinn: Ministry of Communication and Economy. Retrieved from http://unpan1.un.org/intradoc/groups/public/documents/unpan/unpan033997.pdf

Estonia hit by "Moscow cyber war." (2007). *BBC News*.

Estonian Defense League. (2017). Estonian Defence League. Tallinn: Estonian Defense League. Retrieved from http://www.kaitseliit.ee/en/edl

EURACTIV. (2004). Full interview with Jaak Aaviksoo, former education minister of Estonia. *Euractiv*, online. Retrieved from http://www.euractiv.com/section/enlargement/interview/full-interview-with-jaak-aaviksoo-former-education-minister-of-estonia/

European Comission. (2015). *eGovernment in Estonia Country Profile History Strategy Legal Framework Actors Who's Who Infrastructure Services for Citizens Services for Businesses*. Brussels. Retrieved from https://joinup.ec.europa.eu/sites/default/files/egov_in_estonia_-_january_2015_-_v_17_final.pdf

Export.gov. (2018). Brazil - eCommerce. Retrieved October 12, 2018, from https://www.export.gov/article?id=Brazil-e-Commerce

Exteriores, M. das R. (2013). Denúncias de espionagem de cidadãos e instituições brasileiras por órgãos de inteligência norteamericanos. Brasília: Ministério das Relações Exteriores. Retrieved from http://www2.planalto.gov.br/acompanheoplanalto/%0Anotasoficiais/%0Anotasoficiais/%0Anotaoficialdenunciasdeespionagemnorteamericanas

Exteriores, M. das relações. (2013). Declaração à imprensa do Ministro Antonio Patriota sobre denúncia de espionagem contra cidadãos brasileiros. Brasília: Ministério das Relações Exteriores. Retrieved from http://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/3516-declaracao-a-imprensa-do-ministro-antonio-patriota-sobre-denuncia-de-espionagem-contra-cidadaos-brasileiros

Fernandes, J. P. T. (2014). *Ciberguerra: Quando a utopia se transforma em realidade*. Vila do Conde: Quindinovi.

Ferreira, R. B. (2010). *A ONU e a OMS no divã: O movimento de securitização do trauma em processos de reconsrução em estados pós-conflito.* Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, Brazil. https://doi.org/10.17771/PUCRio.acad.17458

Fisher, M. (2017). Canada's forces deployed in Latvia to include 'cyber warriors' to counter Russians. *National Post*. Retrieved from http://news.nationalpost.com/news/world/matthew-fisher-canadas-forces-deployed-in-

latvia-to-include-cyber-warriors-to-counter-russian-attacks

Fleck, D. (2013). Searching for international rules applicable to cyber warfare-a critical first assessment of the new tallinn manual. *Journal of Conflict and Security Law*. https://doi.org/10.1093/jcsl/krt011

Floyd, R. (2007). Human Security and the Copenhagen School´s Securituzation Approach: Conceptualizing Human Security. *Human Security Journal*, *5*(37), 38–49.

Freire, M. R. (2009). A política externa em transição: o caso da Federação Russa. *Relações Internacionais (R:I)*, *23*, 75–89. Retrieved from http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S1645-91992009000300005

Freire, M. R. (2015). *A Rússia de Putin: Vectores Estruturantes de Política Externa eBook: Freire, Maria Raquel: Amazon.com.br: Loja Kindle*. (Almedina, Ed.). Coimbra: Almedina. Retrieved from https://www.amazon.com.br/Rússia-Vectores-Estruturantes-Política-Externa-ebook/dp/B014GGC9TI

Freire, M. R., & Kanet, R. E. (2012). *Russia and its Near Neighbors. Identity, Interests and Foreign Policy*. New York: Palgrave. https://doi.org/10.1057/9780230390164

Fritz, J. (2012). Book Review: International Relations: Networks and States: The Global Politics of Internet Governance Networks and States: The Global Politics of Internet Governance by MuellerMilton L.. London: MIT Press, 2010. 313pp., £25.95, ISBN 978 0 262 01459 5. *Political Studies Review*, *10*(1), 115–115. https://doi.org/10.1111/j.1478-9302.2011.00251_19.x

From Cyberterrorism to Cyberwar, Back and Forth : How the United States Securitized Cyberspace | Scinapse. (n.d.). Retrieved April 6, 2020, from https://scinapse.io/papers/1724642280

Furgang, A. (2018). *Edward Snowden*. Berkeley: Enslow Pub Inc.

G1. (2016, May 12). Dilma Rousseff regulamenta o Marco Civil da Internet - notícias em Tecnologia e Games. *G1*. Retrieved from http://g1.globo.com/tecnologia/noticia/2016/05/dilma-rousseff-regulamenta-o-marco-civil-da-internet.html

Galinec, D., Možnik, D., & Guberina, B. (2017). Cybersecurity and cyber defence: national level strategic approach. *Automatika Journal for Control, Measurement, Electronics, Computing and Communications*, *58*(3), 273–286. Retrieved from https://doi.org/10.1080/00051144.2017.1407022

Geers, K., Kindlund, D., Moran, N., & Rachwald, R. (2013). *Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks*. Milpitas. Retrieved from www.fireeye.com

Georgieva, M. (2015). *Contesting the State Securitization of Cyberspace: The Impact of Alternative Securitizing Actors*. Central European University, Budapest.

Geraldo, M. S., & Cossul, N. I. (2017). *Tecnologia como fator estratégico para o Brasil e para a segurança da América do Sul*. *Revista Política Hoje* (Vol. 26). Retrieved from https://periodicos.ufpe.br/revistas/politicahoje/article/viewFile/9596/17861

Giacomello, G. (2005). *National governments and control of the Internet : a digital challenge*. Routledge.

Giacomello, G., & Eriksson, J. (2006). The Information Revolution, Security, and International Relations: (IR)relevant Theory? *International Political Science Review*,

27(3), 221–244. Retrieved from https://myweb.rollins.edu/tlairson/pek/inforevintrela.pdf

Giacomello, G., & Eriksson, J. (2007). *International Relations and Security in the Digital Age* (1st ed.). Routledge.

Gibson, W. (1992). *Neuromancer*. São Paulo: Aleph.

Goulart, G. M., & Silva, R. L. da. (2015). Construção colaborativa e multissetorial: o Marco Civil da Internet e a inédita experiência de regulação no Brasil / Colaborative and multi-sectoral construction: the civil rights framework for internet and the unprecedented experience of regulation in Brazil. *Revista de Direitos e Garantias Fundamentais*, *16*(2), 201. https://doi.org/10.18759/rdgf.v16i2.684

Green, J. A. (2015). *Cyber warfare : a multidisciplinary analysis*. London: Routledge

Guerrini, F. (2014). Il Brasile vara il Marco Civil, la sua costituzione per internet libera e inclusiva. *La Stampa*. Retrieved from https://www.lastampa.it/2014/04/24/tecnologia/il-brasile-vara-il-marco-civil-la-sua-costituzione-per-internet-libera-e-inclusiva-6REnJndwPLFrxUGXw0fUUJ/pagina.html

Guimarães, J. (2013). A urgência do Marco Civil da Internet. Brasília: Conversa Afiada. Retrieved from https://www.conversaafiada.com.br/brasil/2013/10/25/a-urgencia-do-marco-civil-da-internet

Guitton, C. (2013). Cyber Insecurity as a National Threat: Overreaction from Germany, France and UK? *European Security*, *22*(1). https://doi.org/http://dx.doi.org/10.1080/09662839.2012.749864

Hales, P. (2008a). Russian desperadoes launch cyber attack on Lithuania. *The Inquirer*. Retrieved from https://www.theinquirer.net/inquirer/news/1028719/russian-desperadoes-launch

Hales, P. (2008b). Russians launch cyber attack on Lithuania: media reports. *ItNews*. Retrieved from https://www.itnews.com.au/news/russians-launch-cyber-attack-on-lithuania-media-reports-115647

Halpin, E., Trevorrow, P., Webb, D., & Wright, S. (2006). *Cyberwar, Netwar and the Revolution in Military Affairs*. New York: Springer. Retrieved from https://books.google.pt/books?id=3uuHDAAAQBAJ&pg=PA35&lpg=PA35&dq=%22a+framework+of+interdependent+networks+and+systems,+generally+interlinked+at+many+different+levels,+including+industries,+institutions+and+distribution+capabilities+that+provide+a+flow+o

Hansen, L., & Nissenbaum, H. (2009a). Digital disaster, cyber security, and the copenhagen school. *International Studies Quarterly*, *53*(4), 1155–1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x

Hansen, L., & Nissenbaum, H. (2009b). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, *53*(4), 1155–1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x

Harding, L. (2014). *Os Ficheiros Snowden*. Porto: Porto Editora.

Hare, F. (2010). The Cyber Threat to National Security: Why can´t we agree. In *Conference on Cyber Conflict*. Tallinn. Retrieved from https://ccdcoe.org/sites/default/files/multimedia/pdf/Hare - The Cyber Threat to National Security Why Cant We Agree.pdf

Harris, S. (2014). *@War* (1st ed.). London: Headline Publishing.

Hart, C. (2011). Mobilizing the CyberspaceMobilizing the Cyberspace race: the Securitization of the Internet and its Implications for Civil Liberties. *Cyber-Surveillance in Everyday Life*, *Maio*(2011), 1–12.

Hassan, J., & Saleem, M. (2009). *"Cyber warfare", the truth in a real case*. Linköping.

Healey, J. (2013). *A fierce domain : conflict in cyberspace, 1986 to 2012*. Lanham: Cyber Conflict Studies Association.

Helms, C. (2015). *The Digital GCC: USCybercom as combatant command*. Maxwell Airforce Base. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/1012758.pdf

Hersee, S. (2019). *The cyber security dilemma and the securitisation of cyberspace*. Royal Holloway, University of London, London.

Hjalmarsson, O. (2013a). *The Securitization of Cyberspace How the Web Was Won*. Lund University, Lund. Retrieved from http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=3357990&fileOId=3357996

Hjalmarsson, O. (2013b). *The Securitization of Cyberspace How the Web Was Won*. Lund University, Uppsala.

Hofmann, J. (2016). Multi-stakeholderism in Internet governance: putting a fiction into practice. *Journal of Cyber Policy*, *1*(1), 29–49. https://doi.org/10.1080/23738871.2016.1158303

Holloway, H. (2002). *Evolution of Cyberspace as a Landscape in Cyberpunk Novels*. Georgia Southern University. Retrieved from http://digitalcommons.georgiasouthern.edu/etd

Homland Security. (2009). *Cyberspace Policy Review*. Washington. Retrieved from https://web.archive.org/web/20110424173823/http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

Howard, P. N., Duffy, A., Freelon, D., Hussain, M. M., Mari, W., & Mazaid, M. (2011). Opening Closed Regimes: What Was the Role of Social Media During the Arab Spring? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2595096

Hughes, D., & Colarik, A. (2017). The Hierarchy of Cyber War Definitions (pp. 15–33). Springer, Cham. https://doi.org/10.1007/978-3-319-57463-9_2

Hughes, H. (2007). *Climate Change and Securitization*. Cambridge University. Retrieved from http://www.academia.edu/4591407/Climate_Change_and_Securitization

Hungary. Government Decision No. 1139/2013 (21 March) on the National Cyber Security Strategy of Hungary (2013). Retrieved from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/HU_NCSS.pdf

Huysmans, J. (1998, December 24). Revisiting Copenhagen: Or, on the creative development of a security studies agenda in Europe. *European Journal of International Relations*. https://doi.org/10.1177/1354066198004004004

Huysmans, J. (2000). The European Union and the Securitization of Migration. *JCMS: Journal of Common Market Studies*, *38*(5), 751–777. https://doi.org/10.1111/1468-5965.00263

IGF. (2014). *IGF 2014: Connecting Continents for Enhanced Multistakeholder Internet*

Governance DESA Mission Statement. Istanbul. Retrieved from http://www.intgovforum.org/cms/documents/publications/613-igf-2014-istanbul-evolution-of-internet-governance-empowering-sustainable-development/file

IGF. (2015). *The 10th Internet Governance Forum*. João Pessoa. Retrieved from http://www.intgovforum.org/cms/10th IGF Chairs Summary_Finalv2.pdf

Ilves, T. H. (2017). The Consequences of Cyber Attacks. *Journal of International Affais, online*. Retrieved from https://jia.sipa.columbia.edu/consequences-cyber-attacks

India Times. (2013, December 12). Some nations are indulging in cybercrime: Kapil Sibal, IT News, ET CIO. *India Times*. Retrieved from https://cio.economictimes.indiatimes.com/news/digital-security/some-nations-are-indulging-in-cybercrime-kapil-sibal/27237087?redirect=1

Information System Authority. (2017). Information System Authority - Estonian Information System Authority. Retrieved April 24, 2017, from https://www.ria.ee/en/about-estonian-information-system-authority.html

Institute of International and Social Studies. (2008). *Integration of Second Generation Russians in Estonia Country report on TIES survey in Estonia*. Tallinn. Retrieved from http://www.tiesproject.eu/component/option,com_docman/task%2Cdoc_download/gid%2C351/Itemid%2C142/index.html.pdf

Internet Society. (2016). *Why use the multistakeholder approach?* Retrieved from https://www.internetsociety.org/sites/default/files/IG-MultiStakeholderApproach.pdf

Internet Society. (2017). History of Internet Governance. Retrieved August 8, 2017, from https://www.internetsociety.org/history-internet-governance

Itamaraty. (2013). *Ministério das Relações Exteriores*. Brasília: Ministério das Relações Exteriores. Retrieved from http://www.itamaraty.gov.br/index.php?option=com_content&view=article&id=4684

ITU. (2007). *Global Cybersecurity Agenda (GCA) High-Level Experts Group (HLEG)*. Geneve. Retrieved from https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf

ITU. (2012). *Understanding cybercrime: Phenomena, challenges and legal response*. Retrieved from www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

Jajodia, S., Cybenko, G., Liu, P., Wang, C., & Wellman, M. (2019). *Adversarial and uncertain reasoning for adaptive cyber defense : control- and game-theoretic approaches to cyber security*. London.

Jari Rantapelkonen, E., & Salminen, M. (2013). *THE FOG OF CYBER DEFENCE* (1st ed.). Helsinki: National Defense University. Retrieved from http://www.doria.fi/bitstream/handle/10024/88689/The Fog of Cyber Defence NDU 2013.pdf

Jasper, S. (2017). *Strategic cyber deterrence : the active cyber defense option*. London: Rowman & Littlefield Publishers .

Jenik, A. (2009). Cyberwar in Estonia and the Middle East. *Network Security*, *2009*(4), 4–6. https://doi.org/10.1016/S1353-4858(09)70037-6

Johnson, T. A. (n.d.). *Cybersecurity : protecting critical infrastructures from cyber attack and cyber warfare*.

Joubert, V. (2012). *Five years after Estonia's cyber attacks: lessons learned for NATO?*

(May 2012 No. 76). Rome. Retrieved from https://www.files.ethz.ch/isn/143191/rp_76.pdf

Kaiser, R. (2015). The birth of cyberwar. *Political Geography*, *46*, 11–20. https://doi.org/10.1016/j.polgeo.2014.10.001

Karabacak, B., Ozkan Yildirim, S., & Baykal, N. (2016). Regulatory approaches for cyber security of critical infrastructures: The case of Turkey. *Computer Law and Security Review*, *32*(3). https://doi.org/10.1016/j.clsr.2016.02.005

Karampelas, P., & Bourlai, T. (2017). *Surveillance in action : technologies for civilian, military and cyber surveillance*. London: Springer.

Karatzogianni, a. (2008). *The Politics of Cyberconflict.* London: Routledge.

Karatzogianni, A. (2009). *Cyber-conflict and global politics*. London: Routledge.

Karatzogianni, A. (2010). Blame it on the Russians: Tracking the Portrayal of Russians During Cyber conflict Incidents. *Digital Icons: Studies in Russian, Eurasian and Central European New Media*, *4*(2010), 128–150.

Kasper, A. (2014). The fragmented securitization of cyber threats. In *Regulating Etechnologies in the European Union: Normative Realities and Trends* (pp. 157–188). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-08117-5_9

Keyes, R. W. (2006). The Impact of Moore's Law. *IEEE Solid-State Circuits Newsletter*, *20*(3), 25–27. https://doi.org/10.1109/N-SSC.2006.4785857

Khamel, A. (2013). Dilma cobra de Obama explicações sobre denúncias de espionagem. Brasil: Rede Globo. Retrieved from http://g1.globo.com/jornal-nacional/noticia/2013/09/dilma-cobra-de-obama-explicacoes-sobre-denuncias-de-espionagem.html

Kivirähk, J., & Jermalavicius, T. (2014). Integrating Estonia's RussianSpeaking Population: Findings of National Defense Opinion Surveys. Tallinn. Retrieved from https://www.icds.ee/fileadmin/media/icds.ee/failid/Juhan_Kivirahk_-_Integrating_Estonias_Russian-Speaking_Population.pdf

Kleinrock, L. (2010). An early history of the internet [History of Communications. *IEEE Communications Magazine*, *48*(8), 26–36. https://doi.org/10.1109/MCOM.2010.5534584

Koch, R., Golling, M., Rodosek, G. D., Koch, R., Golling, M., & Rodosek, G. D. (2016). How Anonymous is the Tor Network? A Long-Term Black-Box Investigation. *Computer*, *49*(3), 42–49. https://doi.org/10.1109/MC

Kozlowski, A. (2014). Comparative analysis of cyberattacks on estonia, georgia and kyrgyzstan. *European Scientific Journal*, *3*, 1857–7881. Retrieved from http://www.eujournal.org/index.php/esj/article/viewFile/2941/2770

Kurbalija, J. (2010). *An introduction to internet governance.* Diplo Foundation: Geneve

Lacy, M., & Prince, D. (2018). Securitization and the global politics of cybersecurity. *Global Discourse*, *8*(1), 100–115. https://doi.org/10.1080/23269995.2017.1415082

Laenen, R. (2012). Russia's 'Vital and Exclusive' National Interests in the Near Abroad. In *Russia and its Near Neighbours* (pp. 17–38). Palgrave Macmillan UK. https://doi.org/10.1057/9780230390164_2

Landau, S. E. (2010). *Surveillance or security? : the risks posed by new wiretapping*

technologies. Cambridge: MIT Press.

Lee, T. (2019). The global rise of "fake news" and the threat to democratic elections in the USA. *Public Administration and Policy*, *22*(1), 15–24. https://doi.org/10.1108/pap-04-2019-0008

Lefébure, A. (2015). *O caso Snowden*. Lisboa: Antígona.

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., … Wolff, S. S. (1997). The past and future history of the Internet. *Communications of the ACM*, *40*(2), 102–108. https://doi.org/10.1145/253671.253741

Lévy, P. (1999). *Cibercultura*. Lisboa: Instituto Piaget.

Lewis, J. (2014). National Perceptions of Cyber Threats. *Strategic Analysis*, *38*(4). https://doi.org/10.1080/09700161.2014.918445

Lewis, J. A. (2013, October). On the offense in the cyberspace arms race. *The Washington Post*. Retrieved from http://eds.b.ebscohost.com/eds/detail/detail?sid=cde4cdb3-a97d-41b6-9fb9-ddfc26be8c9d%40sessionmgr120&vid=0&hid=111&bdata=JkF1dGhUeXBlPWlwLGNvb2tpZSxzaGliLHVpZCZsYW5nPXB0LWJyJnNpdGU9ZWRzLWxpdmUmc2NvcGU9c2l0ZQ%3D%3D#AN=edsgcl.345516563&db=edsgao

Lichtenbaum, P., & Schneck, M. (2002). The Response to Cyberattacks: Balancing Security and Cost. *The International Lawyer*, *36*(1), 39–48. https://doi.org/10.2307/40707641

Licklider, J. C. R., & Clark, W. E. (1962). On-line man-computer communication. In *Proceedings of the May 1-3, 1962, spring joint computer conference on - AIEE-IRE '62 (Spring)* (p. 113). New York, New York, USA: ACM Press. https://doi.org/10.1145/1460833.1460847

Lin, H. (2013). Cyber Conflict and National Security. In *International Politics: Enduring Concepts and Contemporary Issues*,. New York: Pearson.

Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies*, *22*(3), 365–404. https://doi.org/10.1080/09636412.2013.816122

Lithuania cyber attacks: Round two. (2008). *The Baltic Times*. Retrieved from http://www.baltictimes.com/news/articles/20897/

Lobato, L. C., Kenkel, K. M., Lobato, L. C., & Kenkel, K. M. (2015). Discourses of cyberspace securitization in Brazil and in the United States. *Revista Brasileira de Política Internacional*, *58*(2), 23–43. https://doi.org/10.1590/0034-7329201500202

Local, T. (2017). "No spying among friends": How Merkel's NSA criticism came to haunt her. *The Local*.

Loftus, S., & Kanet, R. E. (2015). Whose Playground Is It, Anyway? Power Rivalries in Post-Soviet Space. In *Power, Politics and Confrontation in Eurasia* (pp. 15–41). Palgrave Macmillan UK. https://doi.org/10.1007/978-1-137-52367-9_2

London, L. of. (2017). *Counting the cost Cyber exposure decoded*. London.

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society*, *1*(July-December), 1–14.

Lytle, N. (2017). *Climate Change as a Contributor to Terrorism: A Case Study in Nigeria and Pakistan*. University of South Carolina. Retrieved from https://scholarcommons.sc.edu/senior_theses/207

Macedo, de F. C. M. R. (2016). *Cyber Warfare in the context of International Criminal*

Law. Universidade Católica Portuguesa. Retrieved from https://repositorio.ucp.pt/bitstream/10400.14/22001/1/Rafaela Miranda.pdf

MackeyRobert. (2010). Updates on Leak of U.S. Cables. *New York Times*. Retrieved from https://thelede.blogs.nytimes.com/2010/12/06/latest-updates-on-leak-of-u-s-cables-day-9/?_r=1#operation-payback-plans-attacks-on-paypal

Mancini, F. (2013). *New Technology and the Prevention of Violence and Conflict*. New York: International Peace Institute.

Mansfield-Devine, S. (2012). Estonia: what doesn't kill you makes you stronger. *Network Security*, *2012*(7), 12–20. https://doi.org/10.1016/S1353-4858(12)70065-X

Markoff, J., & Landler, M. (2007, May). In Estonia, what may be the first war in cyberspace. *New York Times*. Retrieved from http://www.nytimes.com/2007/05/28/business/worldbusiness/28iht-cyberwar.4.5901141.html

Markov, S. (2009). Behind The Estonia Cyberattacks. Retrieved from http://www.rferl.org/a/Behind_The_Estonia_Cyberattacks/1505613.html

Martin, J. E. (2013). *Paradigm Change: Cyberspace of Critical Infrastructure*. Joint Advanced Warfighting School. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a581225.pdf

Mathiason, J. (2009). *Internet governance : the new frontier of global institutions*. Routledge.

Mazanec, B. M. (2015). *The evolution of cyber war : international norms for emerging-technology weapons*. Sterling: Potomac Books.

McDonald, M. (2008). Securitization and the Construction of Security. *European Journal of International Relations*, *14*(4), 563–587. https://doi.org/10.1177/1354066108097553

McGraw, G. (2013). Cyber War is Inevitable (Unless We Build Security In). *Journal of Strategic Studies*, *36*(1), 109–119. https://doi.org/10.1080/01402390.2012.742013

McLaughlin, D. (2008). Lithuania accuses Russian hackers of cyber assault after collapse of over 300 websites. *The Irish Times*. Retrieved from http://www.irishtimes.com/news/lithuania-accuses-russian-hackers-of-cyber-assault-after-collapse-of-over-300-websites-1.942155

Medeiros, B. P., & Goldoni, L. R. F. (2020). The fundamental conceptual trinity of cyberspace. *Contexto Internacional*, *4*(1), 31–54.

Mendes, P. (2013, September 2). Dilma faz reunião de emergência com ministros sobre espionagem. *G1 - Política*. Retrieved from http://g1.globo.com/politica/noticia/2013/09/dilma-faz-reuniao-de-emergencia-com-ministros-sobre-espionagem.html

Ministério da Ciência, Tecnologia, I. e C. (2018). Internet Para Todos. Retrieved October 12, 2018, from http://internetparatodos.mctic.gov.br/portal_ipt/opencms

Ministério da Defesa. (2014). Doutrina Militar de Defesa Cibernética. Brasília: Ministério da Defesa. Retrieved from https://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_2014.pdf

Monteiro, S. D. (2007). O Ciberespaço: o termo, a definição e o conceito The Cyberspace:

the term, the definition and the concept. *DataGramaZero - Revista de Ciência Da Informação*, *8*(3), 1–20.

Monteiro, T. (2013, September 17). Dilma cancela viagem aos EUA. *O Estado de S. Paulo*. Retrieved from https://politica.estadao.com.br/noticias/geral,dilma-cancela-viagem-aos-eua,1075730

Mozur, P. (2013). Chinese Internet Hit by Attack over weekend. *The Wall Street Journal*. Retrieved from http://blogs.wsj.com/chinarealtime

Mueller, M. L. (2012). From telecommunications policy to Internet governance. *Telecommunications Policy*. https://doi.org/10.1016/j.telpol.2012.04.005

Müller, L. (2014). Ataque hacker rendeu US$ 200 milhões em prejuízo para a Sony Pictures. *TecMundo*. Retrieved from https://www.tecmundo.com.br/ataque-hacker/69727-ataque-hacker-rendeu-us-200-milhoes-prejuizo-sony-pictures.htm

Muqsith, M. A., & Muzykant, V. L. (2019). Effect Fake News for Democracy. *Jurnal Cita Hukum*, *7*(3), 307–318. https://doi.org/10.15408/jch.v7i3.12956

Myriam Dunn, C., & Elgin, B. (2007). Introduction: information, power, and security - an outline of debates abd implications.

Naim, M. (2014). *O fim do poder*. Lisboa: Gradiva.

Nakashima, E. (2016). Is there a Russian master plan to install Trump in the White House? Some intelligence officials are skeptical. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/is-there-a-russian-master-plan-to-install-trump-in-the-white-house-some-intelligence-officials-are-skeptical/2016/07/27/788accf8-5428-11e6-bbf5-957ad17b4385_story.html?utm_term=.87c54c5e1d68

Nascimento, L. (2013). “Brasil é um grande alvo”, diz jornalista sobre vigilância dos EUA. Brasil: Rede Globo. Retrieved from http://g1.globo.com/fantastico/noticia/2013/07/brasil-e-um-grande-alvo-diz-jornalista-que-divulgou-denuncias-de-espionagem-americana.html

Nasu, H. (2011). The Expanded Conception of Security and International Law: Challenges to the UN Collective Security System. *Amsterdam Law Forum*, *3*(3), 15–33. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1922928

National Research Council (U.S.). Computer Science and Telecommunications Board. System Security Study Committee., N. R., & CORPORATE. (1991). *Computers at risk : safe computing in the information age*. Washington: National Academy Press. Retrieved from https://dl.acm.org/citation.cfm?id=102690

NATO. (2012). *National Cyber Security*. (A. Klimburg, Ed.). Brussels: NATO. Retrieved from www.ccdcoe.org

NATO. (2017). Warsaw Summit Key Decisions. Warsaw: NATO. Retrieved from www.nato.int

Naughton, J. (2016). The evolution of the Internet: from military experiment to General Purpose Technology. *Journal of Cyber Policy*, *1*(1), 5–28. https://doi.org/10.1080/23738871.2016.1157619

Nazario, Jose. (2007). *Estonian DDoS Attacks – A summary to date*. Retrieved from https://www.arbornetworks.com/blog/asert/estonian-ddos-attacks-a-summary-to-date/

Nazario, Jose. (2009). Politically Motivated Denial of Service Attacks. In C. Czosseck & K.

Geers (Eds.), *The Virtual Battlefield: Perspectives on Cyber Warfare* (pp. 163–181). Amsterdam: OIS Press. Retrieved from https://ccdcoe.org/sites/default/files/multimedia/pdf/12_NAZARIO Politically Motivated DDoS.pdf

Nazario, José. (2009). Politically Motivated Denial of Service Attacks. In C. Czossek & K. Geers (Eds.), *The virtual battlefield : perspectives on cyber warfare* (pp. 163–181). Melbourne.

NetMundial. (2014). *NETmundial Multistakeholder Statement*. São Paulo. Retrieved from http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf

Neuendorf, K.A; Kumar, A. (2015). Content Analysis. In H. Mazzoleni, Gianpietro; Barnhurst, Kevin; Ikeda, Ken'Ichi; Wessler (Ed.), *The International Encyclopedia of Political Communication*. London: Wiley-Blackwell.

NSA. (2012). *National Security Agency: Defending our Nation, Securying the future*. Washington: NSA.

Nye, J. (2011). *O futuro do poder*. Lisboa: Temas & Debates.

Obama, B. (2012, July 19). Taking the Cyberattack Threat Seriously - WSJ. *The Wall Street Journal*. Retrieved from https://www.wsj.com/articles/SB10000872396390444330904577535492693044650

Olive, N. L. G. (2013). *Cybersecurity: The Nation´s Greatest Threat to Critical Infrastructure*. United States Army War College. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a589328.pdf

Özcan, S. (2013). Securitization of Energy through the lenses of Copenhagen School. In *The 2013 WEI International Academic Conference Proceedings* . Orlando. Retrieved from http://www.nato.int/docu/basictxt/b911108a.htm

Paletta, D., Yadron, D., & Valentino-Devries, J. (2015). Cyberwar Ignites a New Arms Race. *Wall Street Journal*. Retrieved from https://www.wsj.com/articles/cyberwar-ignites-a-new-arms-race-1444611128

Pilati, J. I., & Vieira Cancelier de Olivo, M. (2017). Privacidade, Pós-modernidade jurídica e Governança digital: o exemplo do Marco Civil da Internet na direção de um novo direito. *Espaço Jurídico Journal of Law [EJJL] - Qualis A2*, *18*(1), 65. https://doi.org/10.18593/ejjl.v18i1.7252

Podesta, J., & Ogden, P. (2007). The Security Implications of Climate Change. *The Washington Quarterly*, *31*(1), 1–115. Retrieved from http://www2.dsi.gov.tr/iklim/dokumanlar/the_security_implications_of_climatechange.pdf

Poleshchuck, V. (2009). *Minority Rights in Estonia*. Tallinn. Retrieved from http://www.lichr.ee

Polícia Federal. (2014). Operação IB2K desarticula quadrilha que lesava clientes via internet — Agência de Notícias - Polícia Federal. Retrieved October 24, 2018, from http://www.pf.gov.br/agencia/noticias/2014/09/operacao-ib2k-desarticula-quadrilha-que-lesava-clientes-via-internet

Portela, L. (2011). Posicionamento do orador contrário à aprovação do Projeto de Lei nº 84, de 1999, a respeito da tipificação de crimes cometidos na área da informática. Imediata aprovação do marco regulatório do setor. Discurso em 30/08/2011 às 18:08. Brasília:

Câmara dos Deputados. Retrieved from http://www.camara.leg.br/internet/sitaqweb/TextoHTML.asp?etapa=5&nuSessao=225.1.54.O &nuQuarto=35&nuOrador=1&nuInsercao=0&dtHorarioQuarto=18:08&sgFaseSessao=PE &data=30/08/2011&txApelido=LINCOLN+PORTELA+PR-MG&txFaseSes

Poulsen, K. (2007). 'Cyberwar' and Estonia's Panic Attack. *Wired*. Retrieved from https://www.wired.com/2007/08/cyber-war-and-e/

Powers, S. M., & Jablonski, M. (2015). *The real cyber war : the political economy of Internet freedom*. Chicago: University of Illinois Press.

Prado, J. (2016, March). O que o polêmico relatório da CPI de Crimes Cibernéticos muda na sua vida. *Terra Tecnologia*. Retrieved from https://tecnoblog.net/194875/cpi-crimes-ciberneticos-relatorio/

Presidência da República. Estratégia de Defesa Nacional, Decreto nº 6703 (2008). Brasília: Presidência da República. Retrieved from http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/Decreto/D6703.htm

Presidência da República. (2010). *Livro Verde da Cibersegurança no Brasil*. Brasília. Retrieved from http://dsic.planalto.gov.br/legislacao/1_Livro_Verde_SEG_CIBER.pdf

Presidência da República. LEI Nº 12.737, De 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. (2012). Brasília: Congresso Nacional. Retrieved from http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm

Presidência da República. (2013a). Adiamento da visita de Estado da presidenta Dilma Rousseff aos EUA em virtude da falta de explicações do governo norte-americano às denúncias de espionagem ao governo e a empresas brasileiras. Brasília: Presidência da República. Retrieved from http://www.biblioteca.presidencia.gov.br/notas-oficiais/notas-oficiais/comunicado-oficial

Presidência da República. (2013b). Discurso da Presidenta da República, Dilma Rousseff, na abertura do Debate Geral da 68ª Assembleia-Geral das Nações Unidas - Nova Iorque/EUA. New York: Presidência da República. Retrieved from http://www.biblioteca.presidencia.gov.br/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

Presidência da República. (2014a). *Discurso da Presidente Dilma Rousseff na abertura da NetMundial*. São Paulo. Retrieved from https://www.defesanet.com.br/cyberwar/noticia/15102/NET-MUNDIAL---Discurso-Dilma-Rousseff/

Presidência da República. LEI Nº 12.965, DE 23 DE ABRIL DE 2014. Marco Civil da Internet (2014). Brasília: Congresso Nacional. Retrieved from http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

Press, A. (2013). US-funded Radio Free Europe hit by cyberattack. *CNSNews*. Retrieved from http://www.cnsnews.com/news/article/us-funded-radio-free-europe-hit-cyberattack

Radu, R. (2013). Negotiating meanings for security in the cyberspace. *Info : The Journal of Policy, Regulation and Strategy for Telecommunications, Information and Media*.

https://doi.org/http://dx.doi.org.ezproxy.ulb.ac.be/10.1108/info-04-2013-0018

Reigas, A. (2008). Estonia convicts first “cyber-war” hacker: prosecutors. *The Sydney Morning Herald*. Retrieved from http://www.smh.com.au/technology/estonia-convicts-first-cyberwar-hacker-prosecutors-20080123-1nro.html

Reuters. (2013). Germany, Brazil introduce anti-spying resolution at UN General Assembly. *Deutche Welle*. Retrieved from https://www.dw.com/en/germany-brazil-introduce-anti-spying-resolution-at-un-general-assembly/a-17213179

Richards, R. J. (2017). *NSA Civil Liberties and Privacy Office Review of U.S. Person Privacy Protections in the Production and Dissemination of Serialized Intelligence Reports Derived from Signals Intelligence Acquired Pursuant to Title I and Section 702 of the Foreign Intelligence Surveillance Act*. Retrieved from https://www.dni.gov/files/documents/icotr/Annex-1-NSA-CLPO-Dissemination-Report-20171027.pdf

Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies*, *35*(1), 5–32. https://doi.org/10.1080/01402390.2011.608939

Rid, T. (2013). *Ciberwar will not take place*. London: Hurst & Company.

Rid, T., & Buchanan, B. E. N. (2014). Attributing Cyber Attacks. *The Journal of Strategic Studies*, *00*(00). https://doi.org/10.1080/01402390.2014.977382

Riley, M., & Vance, A. (2011). Cyber Weapons: The New Arms Race. *Bloomberg Business Week*.

Robinson, M., Jones, K., & Janicke, H. (2015). Cyber warfare: Issues and challenges. *Computers & Security*, *49*, 70–94. https://doi.org/10.1016/j.cose.2014.11.007

Rocha, L. (2013, September 7). Dilma ‘quer tudo’ de Obama: brasileira pede explicações sobre caso e resposta deve vir quarta. *Correio 24 Horas*, p. Mundo. Retrieved from https://www.correio24horas.com.br/noticia/nid/dilma-quer-tudo-de-obama-brasileira-pede-explicacoes-sobre-caso-e-resposta-deve-vir-quarta/

Roe, P. (2008). Actor, Audience(s) and Emergency Measures: Securitization and the UK’s Decision to Invade Iraq. *Security Dialogue*, *39*(6), 615–635. https://doi.org/10.1177/0967010608098212

Ron Keys, G., Solutions, R., Winstead, C., & Simmons, K. (2010). *Cyberspace Security and Attribution*. Smithfield. Retrieved from http://www.nsci-va.org/WhitePapers/2010-07-20-Cybersecurity Attribution-Keys-Winstead-Simmons.pdf

Roncolato, M. (2014, April 23). Dilma Rousseff sanciona Marco Civil durante NETmundial. *O Estado de S. Paulo*. Retrieved from https://link.estadao.com.br/noticias/geral,dilma-rousseff-sanciona-marco-civil-durante-netmundial,10000031498

Rosenau, J. N. (2006). *The study of world politics. Vol. 1, Theoretical and methodological challenges*. New York: Routledge.

Rosenau, J., & Singh, J. (2002). *Information Technologies and Global Politics*. Albany: State University of New York. Retrieved from https://www.bookdepository.com/Information-Technologies-Global-Politics-James-N-Rosenau/9780791452042

Rosenfield, D. K. (2009). Rethinking Cyber War. *Critical Review*, *21*(1), 77–90. https://doi.org/10.1080/08913810902812156

Rosenzweig, P. (2013). *Cyber warfare : how conflicts in cyberspace are challenging*

America and changing the world. Praeger.

Rubin, A., & Shane, S. (2015). Hollande Condemns Spying by U.S., but Not Too Harshly. *New York Times*.

Rudner, M. (2013). Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge. *International Journal of Intelligence and CounterIntelligence*, *26*(3). https://doi.org/10.1080/08850607.2013.780552

Ruus, K. (2008). Cyber War I: Estonia Attacked from Russia. *European Affairs*, *9*(1–2). Retrieved from http://www.europeaninstitute.org/index.php/component/content/article?id=67:cyber-war-i-estonia-attacked-from-russia

Sanchez, R. (2015). US spy agency hacked North Korea before the Sony attack. *The Telegraph*. Retrieved from http://www.telegraph.co.uk/news/worldnews/asia/northkorea/11355146/US-spy-agency-failed-to-warn-Sony-Pictures-of-North-Korea-hacking-plans.html.

Santoro, M., & Borges, B. (2017). Brazilian Foreign Policy Towards Internet Governance. *Revista Brasileira de Política Internacional*, *60*(1), 1–16. Retrieved from http://www.scielo.br/pdf/rbpi/v60n1/1983-3121-rbpi-60-01-e003.pdf

Satter, R. (2017). French election: Russian hackers 'targeted Emmanuel Macron camp.' *The Independent*. Retrieved from http://www.independent.co.uk/news/world/europe/french-election-russian-hackers-emmanuel-macron-target-japan-trend-micro-france-president-a7700721.html

Schimidt, M. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Tallinn: Cambridge University Press.

Schmidt, E., & Cohen, J. (2013). *The New Digital Age: Reshaping the Future of People, Nations and Business*. London: John Murray. Retrieved from https://www.amazon.com/New-Digital-Age-Reshaping-Business-ebook/dp/B00A7YYYE2/ref=tmm_kin_swatch_0?_encoding=UTF8&qid=&sr=

Schmidt, E., & Sanger, D. (2016). Spy Agency Consensus Grows That Russia Hacked D.N.C. *New York Times*. Retrieved from https://www.nytimes.com/2016/07/27/us/politics/spy-agency-consensus-grows-that-russia-hacked-dnc.html?_r=0

Schmoldt, J. (2019). ICCWS 2019 14th International Conference on Cyber Warfare and Security ... - Google Livros. In *ICCWS 2019 14th International Conference on Cyber Warfare and Security* (pp. 261–268). Stellenbosch, South Africa.

Schreier, M. (2012). *Qualitative Content Analysis in Practice*. London: SAGE Publications Ltd.

Scott, S. V. (2012). The Securitization of Climate Change in World Politics: How Close have We Come and would Full Securitization Enhance the Efficacy of Global Climate Change Policy? *Review of European Community & International Environmental Law*, *21*(3), 220–230. https://doi.org/10.1111/reel.12008

Searle, J. R. (1976). A classification of illocutionary acts'. *Language in Society*, *5*(1), 1–23. Retrieved from https://sites.duke.edu/conversions/files/2014/09/Searle_Illocutionary-Acts.pdf

Serra, C. (2013, September 3). Dilma encontrará Obama pela 1ª vez depois de denúncias de espionagem. *Bom Dia Brasil*. Retrieved from http://g1.globo.com/bom-dia-

brasil/noticia/2013/09/dilma-encontrara-obama-pela-1-vez-depois-de-denuncias-de-espionagem.html

Shelley, M., & Krippendorff, K. (2004). *Content Analysis: An Introduction to its Methodology. Journal of the American Statistical Association* (Vol. 79). London: Sage Publications. https://doi.org/10.2307/2288384

Silva, M. F. da. (2016). Cyber security vs. cyberdefense - a Portuguese view on the disticntion. *Cyberlaw*, *1*(Junho 2016), online. Retrieved from https://www.academia.edu/23986861/CYBER_SECURITY_VS._CYBER_DEFENSE_A_PORTUGUESE_VIEW_ON_THE_DISTINCTION

Simao, L. (2011). Discursive differences and policy outcomes: EU-Russia relations and security in Europe. *Eastern journal of european studieS*, *2*(1), 81–96. Retrieved from https://www.academia.edu/961023/Discursive_differences_and_policy_outcomes_EU_Russia_relations_and_security_in_Europe

Simão, L. (2012, July). Do leaders still decide the role of leadership in Russian foreign policymaking. *International Politics*. https://doi.org/10.1057/ip.2012.12

Singer, D., & Perloth, N. (2014). U.S. said to find North Korea Ordered Cyberattack on Sony" The New York Times. *New York Times*. Retrieved from http://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html?_r=1

Singh, J. (2002). Information Technologies and the changing scope of global power and governance. In J. Rosenau & J. P. Singh (Eds.), *Information Technologies and Global Politics: The Changing Scope of Power and Governance*. Albany: State University of New York.

SISR. (2013). *La cyber security in Italia - Sistema di informazione per la sicurezza della Repubblica*. Roma. Retrieved from https://www.sicurezzanazionale.gov.it/sisr.nsf/sicurezza-in-formazione/la-cyber-security-in-italia.html

Smith, M. S., Seifert, J. W., Mcloughlin, G. J., & Moteff, J. D. (2002). *CRS Report for Congress The Internet and the USA PATRIOT Act: Potential Implications for Electronic Privacy, Security, Commerce, and Government*. Washington. Retrieved from https://nsarchive2.gwu.edu/NSAEBB/NSAEBB436/docs/EBB-004.pdf

Sofaer, A. (2010). Cyber Security and International Agreement. In *Proceedings of a Workshop on Deterring Cyberattacks*. Washington, D.C.: National Academies Press. https://doi.org/10.17226/12997

Soldatov, A., & Borogan, I. (2015). *The red web : the struggle between Russia's digital dictators and the new online revolutionaries*.

Souza, C. H. M., & Costa, M. A. B. (2006). Abordagens Antropológicas e Sociais no (não) Lugar. *Revista Espaço Acadêmico*, *Julho 2006*(62). Retrieved from http://www.espacoacademico.com.br/062/62souzacosta.htm

Srikanth, D. (2014). Non-traditional security threats in the 21st century. *International Journal of Development and Conflict*, *4*(2014), 60–68.

St. Jean, E. (2007). The changing nature of International Security. The need for an integrated definition. *Paterson Review - Graduate Journal of International Affairs*, *8*, 22–33. Retrieved from http://www.diplomatonline.com/pdf_files/npsia/2007-08/2_Int_Security_C_Elisabeth_St_Jean_FINAL.pdf

Statista. (2018). Brazil: number of internet users 2022. Retrieved October 12, 2018, from https://www.statista.com/statistics/255208/number-of-internet-users-in-brazil/

Stepanova, E. (2011). The Role of Information Communication Technologies in the "Arab Spring"*; Implications beyond the region*, 159 (1),. *PONARS Eurasia Policy Memo*. Retrieved from https://www2.gwu.edu/~ieresgwu/assets/docs/ponars/pepm_159.pdf

Stephens, H. (2008). Belarusian Cyber Attack. *World Politics Review*. Retrieved from http://www.worldpoliticsreview.com/trend-lines/2012/belarusian-cyber-attack

Stoddart, K. (2016). UK cyber security and critical national infrastructure protection. *International Affairs*, *92*(5). https://doi.org/10.1111/1468-2346.12706

Stojaković, F. (2018). *Eu cybersecurity strategy: securitization of cyberspace through a rhetorical lens*. Central European University: Budapest.

Sulovic, V. (2010). Meaning of Security and the Theory of Securitization. Belgrade: Belgrade Center of Security Policy.

Sungwon, B. (2014). North Korea denies involvement in cyber-attacks on Sony Pictures. *Voice of America*. Retrieved from http://www.voanews.com/content/exclusive-north-korea-denies-involvement-in-cyber-attack-sony-pictures/2545372.html

Sutter, J. (2011). Could the U.S. shut down the internet? *CNN Tech.* Retrieved from http://edition.cnn.com/2011/TECH/web/02/03/internet.shut.down/.

Sytas, A. (2016). Lithuania said found Russian spyware on its government computers. *Reuters*. Retrieved from http://www.reuters.com/article/us-lithuania-cyber-idUSKBN14B1PC

Thorne, S. (2017). Expecting cyber-attacks in Latvia. *Legion Magazine*. Retrieved from https://legionmagazine.com/en/2017/03/expecting-cyber-attacks-in-latvia/

Tikk, E., Kaska, K., & Vihul, L. (2010). *International Cyber Incidents*. Tallinn: CCDCOE. Retrieved from www.ccdcoe.org

Times, T. B. (2017). Former President Ilves: Estonia's cyber security experience is trusted. *The Baltic Times*. Retrieved from http://www.baltictimes.com/former_president_ilves__estonia_s_cyber_security_experience_is_trusted/

Tomasevicius Filho, E. (2016). Marco Civil da Internet: uma lei sem conteúdo normativo. *Estudos Avançados*, *30*(86), 269–285. https://doi.org/10.1590/S0103-40142016.00100017

Trachtman, J. P. (1998). Cyberspace, Sovereignty, Jurisdiction, and Modernism. *Indiana Journal of Global Legal Studies*, *5*(2), 561–581. https://doi.org/10.2307/25691120

Trachtman, J., & Trachtman, J. P. (1998). Cyberspace, Sovereignty, Jurisdiction, and Modernism. *Indiana Journal of Global Legal Studies Joel Indiana Journal of Global Legal Studies*, *5*(2). Retrieved from http://www.repository.law.indiana.edu/ijgls

Trinkunas, H., & Wallace, I. (2015). *Converging on the Future of Global Internet Governance The United States and Brazil*. Washington. Retrieved from https://www.brookings.edu/wp-content/uploads/2016/06/USBrazil-Global-Internet-Governance-web-final.pdf

Turner, F. (2006). *From counterculture to cyberculture : Stewart Brand, the Whole Earth Network, and the rise of digital utopianism*. University of Chicago Press.

Turner, L. (2013). Anonymous hackers jailed for DDoS attacks on Visa, Mastercard and

Paypal. *The Independent*.

United Nations. Carta das Nações Unidas (1945). San Francisco: United Nations. Retrieved from http://nacoesunidas.org/docs/carta_da_onu.pdf

U.S.A Department of Homeland Security. (2016). Cyber hygiene & cyber security recommendations. Washington: United States Secret Service. Retrieved from https://www.secretservice.gov/forms/Cyber-Hygiene.pdf

USA. The White House. (2018). National Cyber Strategy of the United States of America. Washington: The White House. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

USA. The White House. (2000). President Clinton: Working to Strengthen Cybersecurity. Washington, D.C.: The White House. Retrieved from https://clintonwhitehouse4.archives.gov/WH/Work/021600.html

Valeriano, B., & Mannes, R. (2015). *Cyberwar versus cyber realities*. Oxford: Oxford University Press.

Vallée, R. (2003). History of cybernetics. In L. Parra (Ed.), *Cybernetics : Cybernetics and the theory of Knowledge, systems science and cybernetics*. Oxford: Eloss Publishers. Retrieved from http://www.eolss.net/sample-chapters/c02/E6-46-03-01.pdf

Vassil, K., Solvak, M., Vinkel, P., Trechsel, A. H., & Alvarez, R. M. (2016). The diffusion of internet voting. Usage patterns of internet voting in Estonia between 2005 and 2015. *Government Information Quarterly*, *33*(3), 453–459. https://doi.org/10.1016/j.giq.2016.06.007

Vaughn, K., Gold, P., & Khamis, S. (2012). Beyond Egypt's "Facebook Revolution" and Syria's "YouTube Uprising:" Comparing Political Contexts, Actors and Communication Strategies. *Arab Media & Society*, *12*, 1–30. Retrieved from https://scholar.google.com.br/citations?view_op=view_citation&hl=en&user=sDNJp-IAAAAJ&citation_for_view=sDNJp-IAAAAJ:LkGwnXOMwfcC

Ventre, D. (2011). Cyberconflict: Stakes of Power. In *Cyberwar and Information Warfare* (pp. 113–240). London: ISTE.

Viegas, P., Carlos, N., Mendes, P., Ralo, J., Santos Luís Camelo, L., Santos, D., … Casimiro, V. (2018). *Instituto da Defesa Nacional Contributos para uma Estratégia naCional dE CibErdEfEsa Instituto da Defesa Nacional nº 28 nº 28*. Lisboa. Retrieved from https://www.idn.gov.pt/publicacoes/cadernos/idncadernos_28.pdf

Villa, R. (1999). A Segurança Global Multidimensional. *Lua Nova*, *46*(1), 99–118.

Vincent, J. (2013). Chinese domains downed by ´largest ever´ cyber attack. *The Independent*. Retrieved from http://www.independent.co.uk/life-style/gadgets-and-tech/news/chinese-domains-downed-by-largest-ever-cyber-attack-8786091.html

von Bernstorff, J. (2003). Democratic Global Internet Regulation? Governance Networks, International Law and the Shadow of Hegemony. *European Law Journal*, *9*(4), 511–526. https://doi.org/10.1111/1468-0386.00189

von Heinegg, W. (2012). Legal Implications of Territorial Sovereignty in Cyberspace. In *2012 4th International Conference on Cyber Confl ict*. Tallinn: NATO CCD COE Publications. Retrieved from https://ccdcoe.org/publications/2012proceedings/1_1_von_Heinegg_LegalImplicationsOfTerritorialSovereigntyInCyberspace.pdf

Walt, S. M. (1991). The Renaissance of Security Studies. *International Studies Quarterly*,

35(2), 211–239. Retrieved from http://users.metu.edu.tr/utuba/Walt Renais.pdf

Waltz, N. K. (1978). *Theory of International Politics*. *International Journal* (Vol. 35). Long Gross: Waveland Press. https://doi.org/10.2307/40201892

Watson, S. (2011). The "human" as referent object? Humanitarianism as securitization. *Security Dialogue*. Sage Publications, Ltd. https://doi.org/10.2307/26301782

Weaver, O. (2012). Aberystwith, Paris, Copenhagen: the Europeanness of new "schools" of security theory in an American field. In *Thinking International Relations Differently* (1st ed., pp. 48–71). New York: Routledge.

Weimann, G. (2005). Cyberterrorism: The Sum of All Fears? *Studies in Conflict & Terrorism*, *28*, 129–149. https://doi.org/10.1080/10576100590905110

Weingartl, H., Czub, S., Copps, J., Berhane, Y., Middleton, D., Marszal, P., … Czub, M. (2005). Invasion of the Central Nervous System in a Porcine Host by Nipah Virus. *Journal of Virology*, *79*(12), 7528–7534. https://doi.org/10.1128/JVI.79.12.7528-7534.2005

White House. (1999). *A National Security Strategy for a New Century*. Washington. Retrieved from https://clintonwhitehouse4.archives.gov/media/pdf/nssr-1299.pdf

White House. (2003). The National Strategy to Secure the Cyberspace. Washington, D.C.: The White House. Retrieved from https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

White House. (2008). *NSPD 54: Cybersecurity Policy*. Deparment of Homeland Security. Retrieved from http://www.lloydthomas.org/5-SpecialStudies/nspd-54Jan08.pdf

White House. (2009). *Remarks by the President on Securing Our Nation's Cyber Infrastructure | whitehouse.gov*. Washington: Office of rhe Press Secretary. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure

White House. (2011). International Strategy for Cyberspace. Washington, D.C. Retrieved from https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

White House. National Cyber security Strategy of the united States of America (2018). Washington D.C. Retrieved from whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

White House. Strengthening America's Cybersecurity Workforce to Secure Our Nation and Promote Prosperity | The White House (2019). Washington, D.C.: White House. Retrieved from https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-strengthening-americas-cybersecurity-workforce-secure-nation-promote-prosperity/

Whittaker, J. (2004). *The cyberspace handbook*. London: Routledge.

Wijk, R. de. (2015). *Power Politics*. Amsterdam: Amsterdam University Press.

Williams, J. (2017, March 7). Could a corps of civilian cybersecurity volunteers save state networks? *StatesCoop*. Retrieved from http://statescoop.com/could-a-corps-of-cyber-civilian-volunteers-save-state-networks#.WL8q4vmy6Vo.twitter

Williams, M. C. (2003). Words, Images, Enemies: Securitization and International Politics. *International Studies Quarterly*, *47*(4), 511–531. https://doi.org/10.1046/j.0020-

8833.2003.00277.x

Wirtz, J. J. (2015). Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy. In K. Geers (Ed.), *Cyberwar in Perspective: Russia Aggression against Ukraine* (1st ed., p. 11). Tallinn: CCDCOE Publications. Retrieved from https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Wirtz_03.pdf

Włodarska-Frykowska, A. (2016). Ethnic Russian Minority in Estonia. *International Studies. Interdisciplinary Political and Cultural Journal*, *18*(2), 153–164. https://doi.org/10.1515/ipcj-2016-0015

Wolf, B. (2013). Fact-checking Obama's claims about Snowden. *CNN Politics*. Retrieved from https://edition.cnn.com/2013/08/12/politics/obama-snowden-whistleblower

Wolff, J. (2014). NATO's Empty Cybersecurity Gesture. *Slate.Com*. Retrieved from https://slate.com/technology/2014/09/natos-statement-on-cyberattacks-misses-some-fundamental-points.html

WSIS. Declaration of Principles Building the Information Society: a global challenge in the new Millennium (2003). Geneva. Retrieved from http://www.itu.int/net/wsis/docs/geneva/official/dop.html

Yannakogeorgos, P. A., & Lowther, A. (2013). *Conflict and cooperation in cyberspace : the challenge to national security*. Taylor & Francis.

Zakem, V., Saunders, P., & Antoun, D. (2015). *Mobilizing Compatriots: Russia's Strategy, Tactics, and Influence in the Former Soviet Union* (No. November 2015). Retrieved from https://www.cna.org/cna_files/pdf/DOP-2015-U-011689-1Rev.pdf

Zetter, K. (2014). The NSA is targeting users of privacy services, leaked code shows. *Wired*. Retrieved from https://www.wired.com/2014/07/nsa-targets-users-of-privacy-services/

Zetter, K. (2016). Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. *Wired*. Retrieved from https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/

Lista de entrevistas

Entrevistado 1. (2016). International Center for Defense and Security. Tallinn. 11 de abril.

Entrevistado 2. (2016). Cooperative Cyber Defence Centre of Excellence. Tallinn, 12 de abril.

Entrevistado 3. (2016). Ministério dos Assuntos Estrangeiros. Tallinn, 13 de abril.

Entrevistado 4. (2016). Estonia Information System Authority. Tallinn, 14 de abril.

Entrevistado 5. (2016). Universiade de Tallinn. Tallinn, 18 de abril.

Entrevistado 6. (2016). Ministério da Defesa. Tallinn, 18 de abril.

Entrevistado 7. (2016). e-governance Academy. Tallinn, 20 de abril.

Entrevistado 8. (2016). Ministério do Interior. Tallinn, 27 de abril.

Entrevistado 9. (2016). Universidade Técnica de Tallinn, 4 de maio.

Entrevistado 10. (2016). Ex-assessor da presidência da Estonia. Tallinn, 5 de maio.

Entrevistado 11. (2016). Ativista. São Paulo, 29 de novembro.

Entrevistado 12. (2016). Ativista. São Paulo, 29 de novembro.

Entrevistado 13. (2016). Ativista. São Paulo, 29 de novembro.

Entrevistado 14. (2017). Assessor parlamentar e ativista. São Paulo, 5 de janeiro.

Entrevistado 15. (2017). Assessor parlamentar. São Paulo, 11 de janeiro.

Entrevistado 16. (2017). Investigador Universidade de Brasília. Brasília, 13 de janeiro.

Entrevistado 17. (2017). Consultor do Ministério da Defesa brasileiro. Rio de Janeiro, 14 de fevereiro.

Entrevistado 18. (2017). Parlamentar. (Porto Alegre, online) Rio de Janeiro, 14 de fevereiro.

Entrevistado 19. (2017). Investigador, consultor da Presidência da República. (Belo Horizonte, online) Rio de Janeiro, 14 de fevereiro.

Entrevistado 20. (2017). Investigador da Escola de Guerra Naval. Rio de Janeiro, 16 de fevereiro.

Entrevistado 21. (2017). Investigador Universidade Técnica de Tallinn / Membro da Estonian Defense League – Cyber Unit. Tallinn, 12 de agosto.

Entrevistado 22. (2018). Diplomata belga. Bruxelas, 28 de novembro.

Entrevistado 23. (2018). Investigador Universidade Livre de Bruxelas. International Telecommunication Union. Bruxelas, 3 de dezembro.