UNIVERSIDADE FEDERAL DE SANTA CATARINA
DEPARTAMENTO DE ECONOMIA E RELAÇÕES INTERNACIONAIS
CURSO DE RELAÇÕES INTERNACIONAIS

TIAGO BERWANGER

O DISCURSO DE SECURITIZAÇÃO DA CIBERNÉTICA NOS ESTADOS UNIDOS DA AMÉRICA NO PERÍODO ENTRE 2007 E 2015

FLORIANÓPOLIS
2015

TIAGO BERWANGER

O DISCURSO DE SECURITIZAÇÃO DA CIBERNÉTICA NOS ESTADOS UNIDOS DA AMÉRICA NO PERÍODO ENTRE 2007 E 2015

Monografia submetida ao curso de Relações Internacionais da Universidade Federal de Santa Catarina, como requisito obrigatório para a obtenção do grau de Bacharelado.

Orientadora: Prof. Dra. Graciela De Conti Pagliari

FLORIANÓPOLIS
2015

TIAGO BERWANGER

O DISCURSO DE SECURITIZAÇÃO DA CIBERNÉTICA NOS ESTADOS UNIDOS DA AMÉRICA NO PERÍODO ENTRE 2007 E 2015

A Banca Examinadora resolveu atribuir a nota 10,0 ao aluno Tiago Berwanger na disciplina CNM 7280 – Monografia, pela apresentação deste trabalho.

Banca Examinadora:

Prof. Dra. Graciela De Conti Pagliari (RI/PPGRI/UFSC)

Me. Naiane Inêz Cossul (PPGEEI/UFRGS)

Me. Jonathan Vieira da Rosa (RI/UFSC)

AGRADECIMENTOS

Não foi fácil. Pensei que não conseguiria, que não teria a capacidade para tal feito, que isso só os outros conseguem… mas é com imenso orgulho que eu me uno aos meus colegas (remanescentes ou não) nesse momento tão importante. Por isso, gostaria de agradecer imensamente aos participantes dessa conquista. Em primeiro lugar, essencial e fundamental, minha família. Graças ao carinho e ao apoio de cada um dos seus membros, esse trabalho que começou lá em 2009 se tornou realidade. Ao meu pai, Paulo Berwanger, pelo apoio incondicional que tem prestado à minha educação, tanto financeiramente quanto com conselhos e palavras de conforto; à minha mãe, Eranice Maria Theisen Berwanger, pelo amor e dedicação com que me trata a cada dia, pelos abraços quentes e apertados que me proporcionaram força; e ao meu irmão, Daniel Berwanger, que mesmo sendo o mais novo da família, consegue me oferecer grandes lições de vida e de companheirismo; além de todos os avôs e avós, tios e tias, primos e primas pelo apoio.

Em segundo lugar, agradeço à família *ad hoc* (utilizando a terminologia do curso), Vilcon Pamplona Pereira, Marise do Nascimento Pereira; aos seus pais, que com alegria me lembravam meus avôs e avós que estão longe; e aos seus filhos Rafael e Cibele do Nascimento Pereira (muito obrigado Cibele, você foi uma peça muito importante na minha vida). Eles me ofereceram sua morada para que eu realizasse um "intercâmbio" de quase dois anos. Ao me acolherem em um momento difícil da minha vida, me proporcionaram carinho e segurança para que eu trilhasse esse caminho até o fim. Tenho imensa gratidão e respeito por vocês.

Agradeço imensamente a minha orientadora, Graciela de Conti Pagliari. Sua paciência, seu conhecimento e sua dedicação foram fundamentais. Tu não és somente boa, és excelente!

Aos companheiros do Rotaract Club de Florianópolis-Leste, agradeço pelo apoio incondicional em momentos de baixa autoestima quanto a minha capacidade. Desde 2014, vocês são mais que grandes amigos, são os melhores companheiros que um rotaractiano pode ter.

Por fim, a todos os amigos e amigas que participaram desse trajeto. Em especial a dois *brothers* fundamentais: Anderson Tacca e Eric Poffo. Desde o cursinho eu cativo admiração e respeito por vocês, e nossas conversas foram fundamentais para que eu clareasse minhas ideias nesse trajeto. Ao Eric, em especial, que os nossos domingos nos bares universitários - compartilhando experiências de vida pessoal e acadêmica - perdurem e ultrapassem nossas estadas na universidade.

A todos os que não me recordo no momento, em função da pressa ou da minha memória seletiva (clássica), meu muito obrigado!

We reject kings, presidents and voting.
We believe in rough consensus and running code.

David Clark, 1992.

RESUMO

A Internet global é parte integrante do nosso cotidiano. Não se vislumbra mais viver sem suas beneficies e as facilidades proporcionadas às nossas vidas. No entanto, muito maior que a nossa visão individual desse ambiente, há um ambiente macro que dá todo o suporte para que a rede mundial exista. São cabos de fibra óptica submarinos cruzando os cinco continentes, atravessando fronteiras e desafiando - em certos aspectos - a soberania dos Estados. Nesse contexto, torna-se importante o conhecimento sobre a ciência que abarca a Internet, além de estudar os mecanismos de comunicação e de controle nas máquinas e nos seres vivos, conhecida como cibernética. Esse trabalho tem por objetivo introduzir alguns dos seus conceitos fundamentais, além de localizar os principais eventos que ocorreram no sistema internacional entre 2007 e 2015, buscando checar a evolução dos discursos de securitização em torno do assunto nesse período. O foco são os Estados Unidos da América, o país com maior produção científica na área, além de ser uma grande potência mundial; logo, detentores dos discursos mais aclamados pela audiência, e que influenciam diariamente estadistas ao redor do mundo na elaboração de suas agendas de segurança nacional.

Palavras-chave: Cibernética, Cibersegurança, Securitização, Estados Unidos.

ABSTRACT

Global Internet is an integral part of our daily life. Living today without its advantages may be difficult to imagine. However, much larger than our individual notion of this environment is the macro environment that provides full support to the existence of the global network. Fiber optic submarine cables expand across the five continents, crossing borders and challenging - in some respects - the sovereignty of States. In this context, knowledge about the science that covers the Internet is of essence, in addition to the study of mechanisms that regulate communication and control in machines and living creatures, known as Cybernetics. This paper aims at introducing some of the key concepts, as well as locating the main events that occurred in the international system between 2007 and 2015, seeking to check the progress of securitization discourse around the subject during that period. Our focus is the United States, a major world power with the largest scientific production in the area, and, therefore, holders of the most acclaimed speeches that influence statesmen around the world in developing their national security agendas daily.

Keywords: Cybernetics, Cybersecurity, Securitization, United States.

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ARPA	*Advanced Research Projects Agency*
ARPANET	*Advanced Research Projects Agency Network*
ASEAN	*Association of Southeast Asian Nations*
CCDCOE	*Cooperative Cyber Defense Centre of Excellence*
CERT	*Computer emergency response team*
CFR	*Council on Foreign Relations*
CIA	*Central Intelligence Agency*
CJCS	*Chairman of the Joint Chiefs of Staff*
CMF	*Cyber Mission Force*
CNCI	*Comprehensive National Cybersecurity Initiative*
COPRI	*Copenhagen Peace Research Institute*
CSIS	*Canadian Security Intelligence Service*
CSNET	*Computer Science Network*
DARPA	*Defense Advanced Research Projects Agency*
DDoS	*Distribution Denial of Service*
DHS	*Department of Homeland Security*
DNI	*Director of National Intelligence*
DOD	*Department of Defense*
DoDCS	*Department of Defense Cyber Strategy*
EUA	Estados Unidos da América
FBI	*Federal Bureau of Investigation*
FIRST	*Forum of Incident Response and Security Teams*
FISAAA	*Foreign Intelligence Surveillance Act Amendments Act*
GSI-PR	Gabinete de Segurança Institucional - Presidência da República
ICCC	*International Conference of Computer Communication*
IEC	Infraestruturas Críticas
ISFC	*International Strategy for Cyberspace*
JWICS	*Joint Worldwide Intelligence Communications System*
MILNET	*Military Network*

MS	*Microsoft*
NIPRNET	*Non-classified Internet Protocol Router Network*
NMS	*National Military Strategy*
NSA	*National Security Agency*
NSF	*National Science Foundation*
OECD	*Organization for Economic Cooperation and Development*
ONU	Organização das Nações Unidas
OTAN	Organização do Tratado do Atlântico Norte
SCADA	*Supervisory Control and Data Acquisition*
SIPRNET	*Secret Internet Protocol Router Network*
TCP/IP	*Transfer Control Protocol / Internet Protocol*
TIC	Tecnologias da Informação e Comunicação
UPI	*United Press International*
URSS	União das Repúblicas Socialistas Soviéticas
USB	*Universal Serial Bus*
USCYBERCOM	*United States Cyber Command*
VOIP	Voz por IP

SUMÁRIO

1 INTRODUÇÃO

As tecnologias proporcionadas pelo avanço da cibernética no século XXI são parte integrante da vida do ser humano moderno. Desde redes compostas por cabos de fibra óptica submarinos e seu ambiente macro que conecta os 5 continentes, até o indivíduo *end user* (usuário final) que recebe a internet de qualidade responsável por tornar sua vida mais confortável e organizada. Mas como tudo o que é novo, adaptar-se é um processo que influencia tanto um cidadão comum quanto o Estado em que ele está inserido.

Os Estados Unidos da América, nas palavras de seus governantes, são considerados um *wired country* (país altamente conectado). Ao mesmo tempo que usufruem dessa tecnologia responsável por impulsionar sua economia, integrar seus cidadãos, e permitir o avanço do país; também sofrem com dilemas de como garantir a sua segurança tanto para o indivíduo (privacidade, qualidade de serviço, imparcialidade), quanto para a segurança nacional do país (invasões, ciberataques, ciber-espionagem).

Em razão do conteúdo dessa monografia ser em função da cibernética, é importante que seja introduzido um pequeno histórico da sua evolução, e como surgiram os conceitos hoje amplamente difundidos internacionalmente sobre o assunto na área acadêmica. O ponto de partida será em 2007, com os ataques realizados contra a Estônia, popularmente conhecidos como "primeiro grande ciberataque" ou "primeiro ato de ciberguerra", mesmo que o uso desses conceitos tenha sentido ainda limitado nos dias atuais. Percorrerá os últimos oito anos, até os dias atuais, com a exposição dos eventos internacionais que influenciaram no equilíbrio de poder no sistema internacional, derivados dessa nova forma assimétrica de combate, e geraram preocupação dos atores estatais. Focar-se-á, após a exposição desses eventos, na institucionalização proposta e nos discursos relativos a cibernética - delineados nos cargos de poder dos Estados Unidos, por atores securitizadores relevantes que integram o governo norte-americano.

Logo, o trabalho tem por objetivo geral introduzir alguns dos conceitos fundamentais da cibernética, além de localizar os principais eventos que ocorreram no sistema internacional entre 2007 e 2015, buscando checar a evolução dos discursos de

securitização em torno do assunto nesse período. Assim sendo, é de grande relevância entender nessa pesquisa: Como os discursos de securitização da cibernética nos Estados Unidos influenciaram o *status quo* do modo de pensar a segurança nacional? Afinal, tendo em vista as instituições que foram criadas com o intuito de defender e combater os ciberataques - cada vez mais comuns - é visível que há uma preparação e um planejamento sendo almejados pelos Estados. E essa é consequência de eventos ciber-relacionados – cada vez mais sofisticados - que foram delineando e moldando o cenário internacional da segurança cibernética, bem como os discursos proferidos pelos atores que sentiram um nível de temor em torno do tema.

Assim, será desenvolvida uma pesquisa baseada em um estudo exploratório, que será realizada através de revisões bibliográficas de autores especializados que debatam o tema em pauta. Como o modo em que a segurança internacional se relaciona com a cibernética é algo bastante novo no cenário acadêmico, o objetivo não é resolver ou explicar questões, muito menos chegar a conclusões exatas, e sim revisar conteúdos e expor o que está sendo produzido no cenário atual. Tendo ciência que no momento não existe base teórica consolidada em forma de uma doutrina sobre o assunto, as fontes de suporte ao conteúdo produzido provirão de teses e dissertações, muitas delas bem recentes quando consideradas do ponto de vista da história das teorias acadêmicas das Relações Internacionais.

Além dessas fontes, artigos de mídias eletrônica de sites renomados como o *The New York Times, The Guardian, BBC News, Reuters, Agence France-Press e Associated Press* serão úteis a fim de apresentar o histórico de acontecimentos durante esses anos de atividades cibernéticas. Por fim, serão utilizadas revistas científicas, sites governamentais dos Estados Unidos – *US Homeland Security, US Department of Defense, White House,Defense Advanced Research Projects Agency*-, além de canais de vídeo (*Youtube, Dailymotion, Vimeo*) que contenham discursos e entrevistas relevantes a pesquisa. Possivelmente serão propostas interações entre os discursos analisados, a fim de que sejam categorizados e apresentem possíveis respostas ao problema.

Para dar suporte as análises sobre esses eventos internacionais, o foco no discurso de securitização da cibernética nos Estados Unidos da América terá por base teórica o paradigma da securitização, trabalhada por autores como Barry Buzan, Ole Wæver e Jaap de Wilde. Segundo autores e pesquisadores da Escola de Copenhague, "as

ameaças à segurança são socialmente construídas […] e os critérios de securitização são práticas intersubjetivas, por meio das quais um agente securitizador procura estabelecer socialmente a existência de uma ameaça à sobrevivência de uma unidade" (BUZAN *et al*., 1998, p. 29-31, tradução própria). A securitização, segundo os autores, é realizada através de um "ato de fala". Ela só é efetivada quando o público/audiência considera legítima a demanda do agente securitizador, e a ameaça é estabelecida com saliência suficiente para que se justifique a quebra das regras normais da política com vistas a contrabalançar essa ameaça (Ibidem, p. 25). Quando um tema é securitizado, ele sai da esfera da política normal e passa para a esfera da política emergencial, caracterizada pela confidencialidade e pela desconsideração dos mecanismos institucionais normais - o que costuma legitimar, por exemplo, o uso da força. (Ibidem, p. 26).

O motivo por trás da realização dessa pesquisa se justifica de um crescimento em torno desses *speech acts* (atos de fala) que envolvem palavras como "*cybernetics*", "*cybersecurity*", "*cyberdefense",* "*cyberspace*", "*cyberattacks*", "*cyberwar*", "*cyberterrorism", "cyberdissuasion",* "*Electronic Pearl Harbor*", "*Third World War*", "*fifth dimension of combat*", *"asymetric warfare",* sendo essas proferidas por atores importantes como chefes e representantes de alto escalão do governo dos Estados Unidos.

Como consequência, sabe-se que esses discursos têm o potencial de moldar políticas públicas e modos de agir dos Estados e demais atores no tocante à segurança internacional. Ademais, a escolha dos Estados Unidos se justifica em função da sua proeminência no pensamento da segurança cibernética no cenário acadêmico e de poder internacionais. Discursos por partes dos chefes de Estados dos EUA tendem a influenciar de maneira sobrevalorizada outros atores de poder no cenário internacional. Assim, "segurança é uma palavra que empodera […] justificando o uso da força, a intensificação dos poderes executivos, a reivindicação de direitos de sigilo, e outras medidas extremas. A maneira como a segurança é compreendida e usada afeta profundamente o modo como a vida política é conduzida" (BUZAN *et al.*, 1998, p. 208, tradução própria).

2 REVISÃO TEÓRICA E CONCEITUAL

Esse capítulo tem por objetivo abordar preceitos teóricos e conceituais que são definidores da área e os quais serão trabalhados nesse estudo, e será dividido em duas partes. Na primeira, desenvolver-se-á uma abordagem do paradigma da Securitização e seu surgimento na Escola de Copenhague, que irá embasar teoricamente as análises dos discursos nos próximos capítulos. Na segunda, será feita uma apresentação dos principais conceitos que permeiam a Cibernética, e cuja compreensão se faz necessária para entender as palavras-chaves presentes nos discursos que serão analisados mais à frente. Inicia-se com a revisão teórica, apresentada a seguir.

2.1 A ESCOLA DE COPENHAGUE

Em função do tema escolhido e tendo em vista o que proporciona o campo teórico de Relações Internacionais, optou-se por identificar e compreender o paradigma da "Securitização", proposto por autores como Barry Buzan, Jaap de Wilde e Ole Wæver. De maneira a se fazer compreensível esse paradigma, é necessária a apresentação do histórico do seu surgimento.

Criado em 1985 com a finalidade de promover estudos para a paz o *Copenhagen Peace Research Institute* (COPRI) constitui, nos dias de hoje, referência na área de estudos em segurança internacional. Ele surgiu como resposta à ausência de justificativa por parte dos teóricos realistas em prever o fim da Guerra Fria. Apesar da credibilidade que a teoria realista possui até hoje para explicar certos fenômenos, ela foi incapaz de prever o término do fenômeno de balanço de poder entre os EUA e a URSS colapsado no início da década de 90. Assim, ficou claro que as análises de cunho tradicional não davam mais conta de analisar os fenômenos chaves da segurança internacional naquele momento. Esse fato proporcionou credibilidade aos críticos, e ofereceu espaço à corrente que desenvolvia seus estudos na Escola de Copenhague, a chamada Corrente Ampliada (do inglês "*widener*").

> O movimento de renovação teórica surgiu por meio do debate sobre a redefinição do conceito de segurança utilizado em relações internacionais. A análise aprofundada sobre o conceito de segurança demonstrava que sua utilização e significado encontravam-se imbuídos pelas premissas realistas, que associavam segurança exclusivamente ao Estado e aos aspectos militares

> e estratégicos. É necessário salientar que o debate então iniciado na área de segurança é contemporâneo daquele sobre teoria de relações internacionais (TANNO, 2003, p. 50).

A Corrente Ampliada proporcionou um novo escopo entre as vertentes teóricas, incorporando tanto ameaças militares quanto aquelas advindas das áreas política, econômica, ambiental e societal (BUZAN, 1991). Nela o autor assegura que cada um desses setores tem diferentes tipos de interações, com diferentes unidades de análise de segurança.

O decorrer de um novo campo de pesquisa foi um ponto de inflexão para a teoria das Relações Internacionais, pois começaram a ser adotadas novas perspectivas teóricas. Nessas perspectivas o mundo social não exibe leis imutáveis, e quaisquer regularidades podem ser alteradas ou quebradas, mesmo quando se refere a qualidade de um assunto de segurança.

> Processos de construção de questões de segurança ocorrem, primordialmente, por meio de discursos proferidos pelos autores mais interessados em estabelecer as agendas de segurança. Questões políticas podem, portanto, sofrer processos ou movimentos de "securitização" e "desecuritização" (TANNO, 2003, p. 57).

Utilizando como alicerce o livro "*Security: A New Framework for Analysis"* de Barry Buzan, Jaap de Wilde e Ole Wæver - concebido em 1998 durante os estudos na Escola de Copenhague - foi possível identificar que o conceito de segurança foi remodelado; e, além disso, tornou-se tanto mais amplo, quanto mais integrado do que o então proposto pela vertente tradicionalista.

Sua amplitude se explica pela escolha dos autores por expandir o leque de setores em que a segurança pode ser analisada. São eles o setor militar, dominado pelas relações de força (sendo até então o único a ser considerado pela corrente tradicional); o setor político, pelas relações de autoridade e reconhecimento externo; o setor econômico, pelas relações de comércio, produção e finanças; o setor societal, pelas relações entre identidades coletivas; e, por fim, o setor ambiental caracterizado pelas relações entre as atividades humanas e a biosfera. Para efeitos de análise, esse trabalho se concentrará no setor militar, mas com possíveis efeitos em outros setores como o econômico e político.

Uma ressalva do paradigma é que os Estados abordam a segurança como um agregado, e não como cinco setores em separado. Sendo assim, sua integração decorre

do fato de nenhum setor examinado isoladamente ser capaz de fornecer uma análise completa da segurança internacional; ou seja, cada setor poderá possuir objetos referentes[1] de segurança próprios que não necessariamente incluirão os Estados (TANNO, 2003, p. 59)

Possuindo como base essa nova referência, a segurança é assim descrita:

> "Segurança" é o movimento que trata a política para além das regras do jogo estabelecidas e enquadra a questão, ou como um tipo particular de política, ou como algo que a transcende. Securitização pode então ser vista como uma versão extrema da politização. [...] Segurança é, assim, uma prática auto referida porque é no contexto desta prática que se torna uma questão de segurança – não necessariamente porque haja uma ameaça existencial real mas porque é apresentada como ameaça (WÆVER et al, 1998, p. 23-24, tradução própria).[2]

Partindo desse princípio, os autores consideram que as ameaças à segurança são socialmente construídas, enquanto os tradicionalistas vinculam o estudo da segurança a existência apenas de ameaças objetivas (armas de fogo, nucleares, biológicas, química). A securitização e os critérios de securitização são práticas intersubjetivas, por meio das quais um agente securitizador – uma pessoa ou um grupo de pessoas em posição de autoridade que realizam um "ato de fala"[3] (AUSTIN, 1962) – procura estabelecer socialmente a existência de uma ameaça à sobrevivência de uma unidade. A securitização, conforme os autores, é apresentada por meio desses atos de fala. No entanto, ela só é efetivada quando o público considera legítima a demanda do agente securitizador, e a ameaça é estabelecida com saliência suficiente para que se justifique a quebra das regras normais da política com vistas a contrabalançar essa ameaça. Senão, não passa de um "movimento de securitização", que pode ser bem-sucedido ou não.

No movimento de securitização de determinados assuntos - seja no setor militar em que esses processos tendem a ser mais institucionalizados, seja em um dos outros setores propostos pelos autores como novos campos a serem considerados - há uma

---

[1] Objeto referente é qualquer objeto visto como existencialmente ameaçado e que têm uma reivindicação legítima para a sobrevivência.

[2] *"Security" is the move that takes politics beyond the established rules of the game and frames the issue either as a special kind of politics. Securitization can thus be seen as a more extreme version of politization [...] "Security" is thus a self-referential practice, because it is in this practice that the issue becomes a security issue - not necessarily because a real existential threat exists but because the issue is presented as such a threat.*

[3] Ato de fala (*speech act*) é um conceito criado pelo filósofo J.L. Austin que representa um modo de expressão intencional de um locutor que causa um certo efeito sobre seu ouvinte.

travessia por níveis, os quais os atores chamam de "espectros", até atingir a securitização plena.

> Na teoria, qualquer assunto público pode ser localizado entre um espectro de não politizado (ou seja, o Estado não lida com isso e não é de qualquer outra forma feita uma questão de debate público e de decisão), para politizado (ou seja, a questão é parte de uma política pública, exigindo decisão governamental e alocações de recursos ou, mais raramente, alguma outra forma de governança popular), até securitizada (ou seja, a questão é apresentada como uma ameaça existencial, necessitando de medidas de emergência e justificando ações fora dos limites normais do processo político) (BUZAN; WEAVER, WILDE, 1998, p. 23).

Ainda, a securitização pode ser *ah hoc* ou institucionalizada. Se um determinado tipo de ameaça é persistente ou recorrente é provável que a resposta e o senso de urgência a tornará institucionalizada. Ademais, tanto a politização quanto a securitização podem ser considerados "processos intersubjetivos". Ou seja, quando não há uma ameaça iminente e objetiva, compreender esse processo não é um trabalho fácil.

Para os autores, além disso, há um conjunto de níveis de análise que deve ser considerado em todos os tipos de análises de segurança. Por meio de cada um deles podem ser visualizados tanto objetos referentes quanto atores securitizadores. São: (1) Sistemas Internacionais, o nível mais alto de análise que engloba grandes conglomerados de interação ou unidades interdependentes que não possuem nenhum sistema acima deste; (2) Subsistemas Internacionais, que podem ser grupos de unidades com uma natureza particular e com algum nível de interdependência entre eles (grandes blocos como a ASEAN, a União Europeia ou o Mercosul podem entrar nessa categoria); (3) Unidades, organizações, comunidades ou mesmo um grupo de indivíduos com coesão suficiente e independente para se diferenciar de outros níveis (são esses Estados, nações, companhias transnacionais); (4) Subunidades, grupos organizados de indivíduos dentro de unidades que podem afetar o comportamento das mesmas (como burocracias, lobbies); (5) Indivíduos, o nível mais baixo de análise nas ciências sociais (BUZAN; WEAVER, WILDE, 1998). Para efeitos de análise, esse trabalho se concentrará no nível estatal.

Por fim, mas não esgotando os preceitos teóricos, os autores propõem o que seria uma "securitização bem-sucedida". Primeiramente, quem decide se o assunto será ou

não securitizado é a audiência[4] e não o ator securitizador. Depois, de que maneira foi proferido esse "ato de fala" a fim de tentar criar o impacto desejado. Um ato de fala deve seguir duas categorias:

> (1) o interno, linguístico-gramatical deve seguir as regras do ato (ou, como Austin argumenta, devem existir procedimentos convencionais aceitos, e o ato tem que ser executado de acordo com estes procedimentos); e (2) o externo, contextual e social - a deter uma posição a partir da qual o ato pode ser feito ("as pessoas e circunstâncias particulares de um determinado caso devem ser apropriadas para a invocação do procedimento especial evocado"). [...] Um ato de fala bem-sucedido é uma combinação de linguagem e sociedade, ambos com características intrínsecas de expressão e um grupo que autoriza e reconhece aquela fala. [...] O mais importante é seguir o método de segurança, a gramática de segurança, e construir uma trama que inclui ameaça existencial, ponto de não retorno, e uma possível saída. [...] o capital social do enunciador, o ator securitizador, que deve estar em uma posição de autoridade. [...] Por si só, esses objetos não significam necessariamente uma securitização bem sucedida, mas definitivamente facilitam as condições para tal (BUZAN *et al.*, 1998, p. 32-33, tradução própria).[5]

Com efeito, esse ator securitizador deve ser alguém como por exemplo um chefe de Estado, um ministro de defesa, um diretor nacional de inteligência, um comandante militar ou algum cientista social ou político respeitado. Além disso, esse ator deve estar em uma posição que, quando profere determinada fala, é capaz de gerar consequências nas decisões de estadistas dentro de suas respectivas nações.

De maneira a contextualizar adequadamente esse paradigma à pesquisa em desenvolvimento, buscar-se-á a seguir relacionar alguns desses conceitos com o tema proposto nesse trabalho.

---

[4] Audiência pode ser entendida como os receptores/ouvintes de um assunto (apresentado através de um "ato de fala") que está no movimento de ser securitizado.

[5] *(1) the internal, linguistic-grammatical - to follow the rules of the act (or, as Austin argues, accepted conventional procedures must exist, and the act has to be executed according to these procedures), and (2) the external, contextual and social - to hold a position from which the act can be made ("the particular persons and circumstances in a given case must be appropriate for the invocation of the particular procedure invoked") [...] A successful speech act is a combination of language and society, of both intrinsic features of speech and the group that authorizes and recognizes that speech. [...] The most important is to follow the security form, the grammar of security, and construct a plot that includes existential threat, point of no return, and a possible way out. [...] the social capital of the enunciator, the securitizing actor, who must be in a position of authority. [...] In themselves, these objects never make for necessary securitization, but they are definitely facilitating conditions.*

2.1.1 O paradigma da securitização empregado aos EUA

Para efeitos dessa pesquisa, optou-se por centrar a análise no setor militar. Muito embora os setores se inter-relacionem na análise de segurança para a Escola de Copenhague, dados os limites deste trabalho e o material disponível, será enfatizado as consequências e resultados mais específicos ao setor militar - também é apresentado pelo nome de "agenda militar de segurança". Especialmente porque o mesmo pode ser caracterizado com as consequências do ponto de vista da cibernética mais bem estudadas e mapeadas até agora. Afinal, mesmo que os EUA comandem o maior poderio militar do mundo, o sentimento de autopreservação - inerente à natureza dos Estados -, poderá ser posto à prova uma vez que o país adquire consciência de sua vulnerabilidade no setor cibernético.

Nesse novo campo da cibernética[6] que surgiu no final do século XX, e ganhou força durante o século XXI, as ameaças se tornaram mais difíceis de se prever e de localizar os autores passíveis de punição. É uma nova forma de assimetria entre o poder bélico e as ameaças. Isso não significa ou justifica necessariamente o uso de ações ofensivas contra outros atores (estatais ou não), mas a preparação de um conjunto de ações defensivas contra ameaças advindas dos recentes usos dessa nova tecnologia.

Ainda sobre o setor militar, na visão dos autores, o Estado é o objeto referente mais importante (mesmo que não o único), e as elites governantes são os mais importantes (mesmo que não os únicos) atores securitizadores. Para efeito dessa pesquisa, considerar-se-á os Estados Unidos da América como o objeto referente; pois o país possui - como já comentado - a maior força militar do planeta, além de deter os maiores quantias investidas na proteção e defesa de sua soberania.[7] Além do mais, como atores securitizadores, serão examinados seus governantes de mais alto escalão - chefe de Estado, secretário de defesa, diretores de agências de inteligência e comandantes militares de alta patente – pois, além de limitarem o escopo da pesquisa, são atores com maior probabilidade de, em seus atos de fala, influenciarem a audiência (estadistas de outros países, por exemplo).

---

[6] O prefixo "ciber-", que é derivado da palavra "cibernética" possui um significado geral de "através do uso do computador" (CAVELTY, 2008).

[7] Os EUA possuem mais de 40% dos gastos militares entre os 15 países com maiores orçamentos, sendo cerca de 3x maior que o segundo colocado, a China. O terceiro colocado é a Rússia, com um investimento equivalente a menos da 1/2 do chinês, ou aproximadamente 1/7 do estadunidense (SIPRI, 2015).

> Na prática, a agenda militar de segurança gira principalmente em torno da capacidade dos governos de se manterem contra ameaças militares internas e externas, mas também pode envolver o uso da força militar para defender Estados ou governos contra ameaças à sua existência […] quando a ameaça é percebida como interna, a segurança militar é principalmente sobre a capacidade da elite dominante de manter a paz civil, a integridade territorial e, de maneira controversa, a máquina governamental em face dos desafios dos seus cidadãos […] quando a securitização é focada em ameaças externas, a segurança militar é principalmente focada na interação entre dois níveis: capacidades ofensivas e defensivas do estado por um lado, e suas percepções das capacidades e intenções dos outros por outro (BUZAN *et al*., 1998, p. 50-51, tradução própria).[8]

Finalmente, a presença dos Estados Unidos como objeto referente também se deve ao fato de que, desde os princípios fundacionais da internet, o país é um dos mais interessados tanto na defesa de sua segurança interna como na propagação de um sentimento de segurança global. Colocando-se como líder no sistema internacional no que pese à cibernética, há diversos pontos que demonstram parte de uma construção de preceitos, identificados na sua Estratégia Nacional Militar de 2015 (*2015 Military National Strategy*)[9]. Ainda, o país é também um dos mais ativos na elaboração e nos debates em torno dos conceitos que envolvem o desenvolvimento tecnológico da cibernética (os quais serão exemplificados à frente); e, a preocupação com um emergente campo da cibernética (quando visto de um ponto histórico), condicionou potências como os EUA a responderem de forma mais ativa a qualquer sinal de mudança no sistema internacional, ampliando suas capacidades ofensivas e defensivas.

> Capacidades militares, sejam absolutas ou relativas, não determinam o processo de securitização por si mesmo […] um número de variáveis além de capacidades militares pode desempenhar um papel significativo no estabelecimento (ou não) e manutenção da securitização militar […] a geografia molda a percepção e operação de ameaças militares e vulnerabilidades de duas maneiras: através da distância e do terreno. A distância funciona sob o princípio tradicional em que ameaças militares são mais difíceis de serem escaladas e mais fáceis de serem defendidas contra quando é necessário percorrer grandes distâncias em relação a curtas […] e especulações sobre a ciberguerra apontam para modos de conflito em que a distância não importa muito […] a história afeta fortemente as ameaças

[8] *In practice, the military security agenda revolves largely around the ability of governments to maintain themselves against internal and external military threats, but it can also involve the use of military power to defend states or governments against nonmilitary threats to their existence [...] when the perceived threat is internal, military security is primarily about the ability of the ruling elite to maintain civil peace, territorial integrity, and, more controversially, the machinery of government in the face of challenges from its citizens [...] when securitization is focused on external threats, military security is primarily about the two-level interplay between the actual armed offensive and defensive capabilities of states on the one hand an their perceptions of each other's capabilities and intentions on the other.*

[9] *"The U.S. military's purpose is to protect our Nation and win our wars. We do this through military operations to defend the homeland, build security globally, and project power and win decisively"* (p. 5)

> militares no sentido de impactos sofridos no passado e na percepção do presente. A existência de inimizade histórica e guerras contínuas tenderão a amplificar as percepções sobre ameaças (BUZAN *et al.,* 1998, p. 58-59, tradução própria).[10]

Em consequência das altas capacidades militares dos EUA, apesar de mantê-los em uma posição de liderança militar nos dias atuais, podem não ser suficientes frente à novas ameaças que estão surgindo como decorrência da evolução tecnológica do século XXI. Essas capacidades só serão postas à prova caso algum evento maior nos sistemas interconectados do ciberespaço se realize; no entanto, desde os acontecimentos ocorridos na Estônia[11] em 2007 – e outros durante esses últimos oito anos – há o temor por parte de qualquer grande potência, não somente dos EUA, de que um evento ocorrido naquele país possa se repetir em proporções maiores em outros. Ainda, as interações de capacidades militares entre os Estados estão profundamente condicionadas por relações políticas. No nível interestatal, a agenda militar de segurança é principalmente sob o modo em que os Estados se preparam ao usar a força, e como seu comportamento a este respeito é interpretado e respondido por outros Estados (BUZAN *et al*., 1998).

Por fim, para que esses movimentos militares no ciberespaço fiquem mais claros e, a fim de compreender melhor o que representa a cibernética e quais os valores que ela possui, será apresentado um histórico do surgimento da internet (do ponto de vista militar), e descritos alguns dos conceitos essenciais em torno da criação da mesma e seu desenvolvimento, responsáveis por moldar os discursos no sistema internacional e redefinir a segurança nos últimos anos.

---

[10] *Military capabilities, whether absolute or relative, do not determine the process of securitization itself […] a number of variables other than military capabilities can play a significant role in the establishment (or not) and maintenance of military securitization [...] Geography shapes the perception and operation of military threats and vulnerabilities in two ways: through distance and terrain. Distance works on the traditional principle that military threats are more difficult to mount and easier to defend against when they have to travel over longer distances than over shorter ones [...] speculation about cyberwar points toward modes of conflict in which distance may not matter much [...] History affects military threats largely in terms of the impact of past experience on present perception. The existence of historical enmity and repeated war will tend to amplify present perceptions of threat.*

[11] Referência a um grande ciberataque direcionado ao governo estoniano que marcou sistema internacional e foi considerado como o "primeiro ato de ciberguerra". Haverá mais explicação e análise do ocorrido no decorrer desse trabalho.

2.2 REVISÃO CONCEITUAL

2.2.1 Histórico da Internet

"A revolução na capacidade de interações – incluindo mísseis balísticos intercontinentais, aviões a jato, satélites, e o desenvolvimento do ciberespaço – têm erodido o significado de distância"[12] (BUZAN *et al*., 1998, p. 163, tradução própria). Se o ciberespaço já foi uma preocupação para os teóricos da segurança internacional nos anos 90 do século XX, é possível que as consequências de sua evolução nos últimos anos do século XXI continuem a impactar o Sistema Internacional de forma mais contundente. Por essa razão, inicia-se com um breve histórico desse processo de evolução, que foca, no entanto, nos aspectos militares que interessam a essa pesquisa.

A concepção do que se conhece como internet iniciou durante a década de 60 do século XX em torno de um projeto da ARPA (*Advanced Research Projects Agency*), uma agência do Departamento de Defesa norte-americano responsável pelo desenvolvimento de tecnologias para uso militar. O motivo que gerou sua criação foi basicamente a disputa ideológica que permeava os EUA e a URSS em uma corrida tecnológica que caracterizou o período da Guerra Fria. Após o lançamento bem-sucedido do satélite soviético *Sputnik,* em 1957, e do fracasso da tentativa estadunidense de lançar seu primeiro satélite ao espaço no mesmo ano, a solução para o problema de pesquisa em defesa foi a criação de uma nova agência civil no Pentágono que combinou os melhores talentos científicos do Exército, Marinha e Força Aérea, evitando duplicações e limitando a rivalidade interserviços sobre o espaço e da pesquisa de mísseis. No momento em que a ARPA começou os seus trabalhos, seu Escritório de Técnicas de Processamento de Informações tinha apenas dois membros, Bob Taylor e seu secretário, que juntos administravam um orçamento de US$16 milhões de dólares[13] (RYAN, 2010).

> O Departamento de Defesa [dos EUA] era o maior comprador de equipamentos de informática do mundo. Somente a ARPA financiava a

[12] "*The revolution in interaction capacity – including intercontinental ballistic missiles (ICBMs) and jumbo jets, satellites, and the development of cyberspace – has eroded the significance of distance."*

[13] "*...the solution to the defence research problem was a new civilian agency within the Pentagon that combined the top scientific talent of the Army, Navy and Air Force, avoiding duplication and limiting inter-service rivalry over space and missile research… At the time that arpabegan to work on networking, its Information Processing Techniques Office had only two staff members, Bob Taylor and his secretary, who together administered a $16million budget."*

> instalação de grandes computadores em centros de pesquisa em todo o país. No entanto, as incompatibilidades entre as grandes variedades de computadores adquiridos impediam uns de se comunicarem com os outros, e uma duplicação desnecessária de equipamentos foi acrescentando ao centro grandes despesas. No próprio escritório de Taylor havia três terminais de computadores separados e incompatíveis ligados a computadores em diferentes centros financiados pela ARPA. Em um discurso de vinte minutos Taylor propôs ao diretor da ARPA, Charlie Herzfeld, que a ARPA poderia resolver o problema de duplicação e isolamento. Sua proposta era simples: a ARPA deveria financiar um projeto para tentar conectar um pequeno número de computadores em conjunto e estabelecer uma rede por meio da qual os pesquisadores que a utilizam poderiam cooperar entre si. Se bem-sucedida, a rede não só permitiria que diversos computadores se comunicassem, mas também permitiria aos investigadores de um centro usar programas remotamente em computadores de outros centros, desse modo permitindo a ARPA cortar custos. A rede descrita por Taylor ficou conhecida mais tarde como "ARPANET" (RYAN, 2010, p. 26, tradução própria).[14]

No entanto, somente em outubro de 1972, foi organizada uma grande demonstração dessa nova tecnologia de rede para o público - muito bem-sucedida - da ARPANET na *International Conference of Computer Communication* (ICCC). A ARPANET (*Advanced Research Projects Agency Network*) foi a precursora do que hoje é a internet global, desenvolvida em conjunto por cientistas americanos e britânicos.

No início dos anos 80, a ARPANET era amplamente usada por um grande número de redes militares, e estava começando a ser também expandida ao uso civil. A iniciativa pioneira partiu de um professor da Universidade de Wisconsin, Lawrence Landweber, que propôs a Fundação Nacional da Ciência (*National Science Foundation - NSF*) do EUA a criar uma rede científica de computadores (*Computer Science Network – CSNET*). Essa proposta contou com a cooperação da ARPA, e foi aprovada pela NSF em 1981[15]. Nela a NSF se comprometeria em apoiar o projeto pelo período de cinco anos, sendo que após esse período a rede teria que ser sustentável por si só. A

---

[14] *The Department of Defense was the largest purchaser of computer equipment in the world. ARPA itself was funding the installation of large computers at research centers across the country. Yet incompatibilities between the wide varieties of computers purchased prevented them from talking to each other, and unnecessary duplication of equipment was adding to this enormous expense. In Taylor's own office there were three separate and incompatible computer terminals linked to computers at different arpa-funded centres. In a twenty-minute pitch Taylor proposed to the arpa Director, Charlie Herzfeld, that arpa could resolve the problem of duplication and isolation.16 His proposal was simple: arpa should fund a project to attempt to tie a small number of computers together and establish a network over which researchers using them could cooperate. If successful the network would not only allow different computers to communicate but it would enable researchers at one facility to remotely use programs on computers at others, thereby allowing arpa to cut costs.17 The network Taylor was describing would later be known as the 'ARPANET'.*

[15] Informações disponíveis no documento "*History and Overview of CSNET (1982)"*, dos autores Peter J. Denning, Anthony Hearn e William Kern.

nova CSNET foi conectada a já existente ARPANET usando o moderno TCP/IP[16], e adquirindo novos papéis diferenciados. Em primeiro lugar, o papel central desempenhado pela NSF marcou o início de uma transição da governança militar da internet para a civil. Em segundo lugar, a rede foi aberta a todos os investigadores da área nos EUA e posteriormente para fora do país.

Em razão desse fato, em 1984, buscou-se desvencilhar certas atividades da ARPANET e transformar em MILNET (*Military Network*) a parte designada aos fins operacionais e militares, deixando a ARPANET para as necessidades de investigação e pesquisa acadêmicas. Durante os anos 1980, a MILNET expandiu para se tornar a Rede de Informação de Defesa (*Defense Information Network*), um conjunto mundial de redes militares que funcionam em diferentes níveis de segurança. Na década de 1990, a MILNET se desdobrou em NIPRNET (*Non-classified Internet Protocol Router Network*) e SIPRNET (*Secret Internet Protocol Router Network*). Tanto a NIPRNET quanto a SIPRNET usam a mesma tecnologia da internet global, mas possuem linhas dedicadas que as separam dos outros sistemas de comunicação. Há ainda uma terceira rede pouco conhecida, a JWICS (*Joint Worldwide Intelligence Communications System*) utilizada para informações ultrassecretas (classificação "*TOPSECRET"*).

> Para simplificar, vamos dizer que existem basicamente três redes do Departamento de Defesa [dos EUA]. A primeira é a NIPRNET é a intranet de assuntos não confidenciais. Sistemas nessa rede usam endereços ".mil". A NIPRNET se conecta à internet pública em dezesseis nós. Embora os dados sejam não-confidenciais que se movimentam sobre a rede, não significam que não são importantes. Boa parte das informações logísticas, como o fornecimento para unidades do exército dos EUA de alimentos é feita através da NIPRNET. Boa parte das unidades militares não conseguem se sustentar por longos períodos sem o suporte de companhias privadas, e essas comunicações são realizadas através da NIPRNET. A segunda rede do Departamento de Defesa é chamada SIPRNET e é usada para passagem de informações confidenciais. Muitas ordens militares são transmitidas através da SIPRNET. Deveria haver um *air gap* entre as redes não confidenciais e secretas. Usuários das redes confidenciais baixam coisas da internet global e carregam elas na SIPRNET, assim por vezes passando *malwares* nesse processo de modo inconsciente. Especialistas em segurança do pentágono chamam esse problema de *"sneakernet threat"*. […] A terceira maior rede do Departamento de Defesa é a rede de informações sensíveis, consideradas ultrassecretas, chamada de JWICS. Essa rede mais limitada é projetada para repassar informações de inteligência para os militares. Seus terminais estão em salas altamente seguras e especiais conhecidas como "Instalações de

[16] TCP/IP (*Transfer Control Protocol/Internet Protocol*) é um tipo de protocolo usado na internet atualmente, e se destaca por ser uma linguagem responsável por conectar e governar a comunicação entre todos os computadores conectados à rede.

> Informações Secretas Compartimentadas". As pessoas também se referem a esses quartos como "o cofre". O acesso a esses terminais é mais restrito por causa de sua localização, mas o fluxo de informações na rede ainda tem que ir através de cabos de fibra óptica e através de roteadores e servidores, assim como qualquer outra rede. Os roteadores podem ser atacados a fim de cortar comunicações. O *hardware* utilizado nos computadores, servidores, roteadores e *switches* podem ser todos comprometidos na própria fabricação ou posteriormente. Portanto, não podemos assumir que mesmo essa rede seja segura. Sobre o plano do CNCI[17] [*Comprehensive National Cybersecurity Initiative*], o Departamento de Defesa está coordenando um extensivo programa para atualizar a segurança em todos esses três níveis de redes. Parte do que está sendo feito é confidencial, boa parte é de um custo elevado, e provavelmente levará um longo tempo[18] (CLARKE; KNAKE, 2010, p. 83-84, tradução própria).

Essas três redes são o alicerce virtual das comunicações do Departamento de Defesa dos EUA, e continuam sendo utilizadas atualmente para coordenar suas operações. Em detrimento da segurança dessas redes o país necessita hoje um esforço muito superior ao despendido no passado para controlar e comandar as atividades militares no ciberespaço.

---

[17] Esse plano será melhor delineado no terceiro capítulo.

[18] *For simplicity, let's say that there are basically three DoD networks. The first, NIPRNET, is the unclassified intranet. Systems on that network use the dot-mil addresses. The NIPRNET connects to the public Internet at sixteen nodes. While it is unclassified data that moves on NIPRNET, unclassified does not mean unimportant. Most logistical information, like supplying Army units with food, is on the NIPRNET. Most U.S. military units cannot sustain themselves for long without support from private-sector companies, and most of that communication goes through the NIPRNET. The second DoD network is called SIPRNET and is used to pass secret-level classified information. Many military orders are transmitted over the SIPRNET. There is supposed to be an "air gap" between the unclassified and secret-level networks. Users of the classified network download things from the Internet and upload them to the SIPRNET, thus sometimes passing malware along unknowingly. Pentagon information security specialists call this problem the "sneakernet threat." [...] The third major DoD network is the Top Secret/Sensitive Compartmented Information (TS/SCI) network called JWICS. This more limited network is designed to pass along intelligence information to the military. Its terminals are in special highly secured rooms known as Secret Compartmentalized Information Facilities, or SCIFs. People also refer to those rooms as "the vault." Access to these terminals is more restricted because of their location, but the information flowing on the network still has to go across fiber-optic cables and through routers and servers, just as with any other network. Routers can be attacked to cut communications. The hardware used in computers, servers, routers, and switches can all be compromised at the point of manufacture or later on. Therefore, we cannot assume that even this network Under the CNCI plan, DoD is embarked on an extensive program to upgrade security on all three kinds of networks. Some of what is being done is classified, much of it is expensive, and some of it will take a long time. A real possibility is the use of high-bandwidth lasers to carry communications to and from satellites. Assuming the satellites were secure from hacking, such a system would reduce the vulnerabilities associated with fiber-optic cable and routers strung out around the world.is reliable.*

2.2.2 À luz dos conceitos

É natural que todo Estado se preocupe com seu bem-estar e o de sua população no plano físico, protegendo seus ativos contra quaisquer ameaças à sua soberania, seja por meio de uma violação à sua infraestrutura ou de uma tentativa de invasão ao seu território. No plano virtual é possível também trabalhar com ideias semelhantes.

Segundo o mestre em estudos estratégicos Walfredo Bento Ferreira Neto (2014), o território do domínio cibernético é artificial, produto do homem e fruto do nível tecnológico atual; e é, originariamente, um "território rede", ou melhor, uma "rede-território". No ambiente cibernético do globo, os Estados definem seus territórios "nitidamente", isto é, apropriam-se de um espaço comum (*global common*) por meio do poder. Como exemplos imediatos, mas não únicos, tem-se os domínios dos sítios ".br"; ".us"; ".uk"; ".it"; que indicam perfeitamente os respectivos territórios. A fronteira cibernética, por conseguinte, obedece à forma de "pontos" ("nós") ou "pacotes" de informações eleitos pelos Estados devido ao seu grau de interesse – sistemas de defesa, infraestruturas críticas ou estruturas estratégicas e a informação em si são alguns dos exemplos.

É nesse interim que entra a definição de Ciberespaço. Em 2008 houve uma tentativa por parte do Pentágono, reunindo um time de especialistas, que levaram cerca de um ano para chegar em um consenso de uma definição de ciberespaço. Eles decidiram que o termo seria condizente com "o domínio global dentro do ambiente de informação que consiste na rede interdependente de infraestruturas de tecnologia da informação, incluindo a Internet, redes de telecomunicações, sistemas computacionais e quaisquer processadores e controladores incorporados" (SINGER; FRIEDMAN, 2014). Na visão dos autores Peter Singer e Allan Friedman, a essência do ciberespaço é o domínio das redes de computadores (e os usuários por trás dela) em que a informação é armazenada, compartilhada e comunicada online. Apesar de funcionar no meio online, não significa que o ciberespaço é puramente virtual. Ele também compreende os computadores que armazenam dados e sistemas com infraestruturas que permitem que esses dados possam fluir. Incluem-se nesse meio a internet global, as intranets privadas, tecnologias de celulares, cabos de fibra óptica, e quaisquer tipos de comunicações baseadas no espaço (satélites, por exemplo).

> Isso leva a um ponto importante muitas vezes incompreendido. Ciberespaço pode ser global, mas não é "apátrida" ou um "bem comum global", dois termos frequentemente utilizados no governo e mídia. Assim como nós, seres humanos, temos dividido artificialmente nosso globo em territórios que chamamos de "nações" e, por sua vez, nossa espécie humana em vários grupos como "nacionalidades", o mesmo pode ser feito com o ciberespaço. Ele se baseia em infraestrutura física e os usuários humanos ligados à geografia e, portanto, também está sujeito a noções humanas como a soberania, a nacionalidade e a propriedade. Ou, dito de outra maneira, as divisões do ciberespaço são tão reais quanto a significativa, no entanto imaginária, fronteira que divide os Estados Unidos do Canadá ou a Carolina do Norte da Carolina do Sul. Mas o ciberespaço, como a vida, está em constante evolução. A combinação da tecnologia híbrida e dos seres humanos que a usam está sempre mudando, inexoravelmente alterando tudo desde o tamanho e da escala do ciberespaço até as regras técnicas e políticas que servem para guiá-lo. Como disse um especialista, "A geografia do ciberespaço é muito mais mutável do que outros ambientes. Montanhas e oceanos são difíceis de se mover, mas partes do ciberespaço podem ser ligadas e desligadas com o clique de um botão". As características essenciais permanecem as mesmas, mas a topografia está em constante fluxo. O ciberespaço de hoje é ao mesmo tempo igual, mas também totalmente diferente, do ciberespaço criado em 1982[19] (SINGER; FRIEDMAN, 2014, p. 14, tradução própria).

Por meio dessa visão de ciberespaço, vêm à tona uma pergunta de suma importância: quais são as reais ameaças em torno desse fluxo virtual e dessas fronteiras imaginárias que afetam direta ou indiretamente a soberania de um Estado?

Myriam Dunn Cavelty (2008), chefe da Unidade de Pesquisa em Novos Riscos (*New Risks Research Unit - Center for Security Studies)* da Universidade de Zurique, desenvolveu uma lista de palavras-chave que indicam movimentos de securitização na cibernética. É com base nessa lista que se identifica as palavras que serão definidas a seguir.

---

[19] *This leads to an important point often misunderstood. Cyberspace may be global, but it is not "stateless" or a "global commons," both terms frequently used in government and media. Just as we humans have artifi cially divided our globe into territories that we call "nations" and, in turn, our human species into various groups like "nationalities," the same can be done with cyberspace. It relies on physical infrastructure and human users who are tied to geography, and thus is also subject to our human notions like sovereignty, nationality, and property. Or, to put it another way, cyberspace's divisions are as real as the meaningful, but also imaginary, lines that divide the United States from Canada or North from South Carolina. But cyberspace, like life, is constantly evolving. The hybrid combination of technology and the humans that use it is always changing, inexorably altering everything from cyberspace's size and scale to the technical and political rules that seek to guide it. As one expert put it, "The geography of cyberspace is much more mutable than other environments. Mountains and oceans are hard to move, but portions of cyberspace can be turned on and off with the click of a switch." The essential features remain the same, but the topography is in constant fl ux. The cyberspace of today is both the same as but also utterly different from the cyberspace of 1982.*

Tabela 1 – Palavras-chave para ciberameaças

Threat framing keywords (for cyber-threats)
• Computer (-based) attack
• Computer intrusion
• Critical information infrastructures
• Critical infrastructures
• Cyber-attack
• Cyber-security
• Cyber-terrorism
• Cyber-threat
• Cyber-vulnerability
• Cyber-war(fare)
• Electronic Pearl Harbor
• Information operations
• Information warfare
• National security (in connection with information security, etc.)
• Vulnerabilities of information infrastructure

Fonte: Cyber-Security and Threat Politics - CAVELTY (2008)

Em razão do escopo dessa pesquisa, optou-se pelo foco mais limitado em palavras que abrangem suficientemente o discurso de securitização. Serão delimitadas a seguir cinco desses conceitos: "cibersegurança ou segurança cibernética", "ciberameaça", "cibervulnerabilidade", "infraestruturas críticas da informação", "segurança nacional".

2.2.2.1 Cibersegurança ou Segurança Cibernética

Segurança cibernética ou cibersegurança é muitas vezes um termo incompreendido ou utilizado de maneira errônea, e sua compreensão é um desafio complexo que exige raciocínio interdisciplinar, pois qualquer definição deve atrair interessados divergentes em uma área ao invés de ser imparcial, significativa e

fundamentalmente útil. Ou seja, pode possuir (e de fato possui) vários conceitos diferenciados que focam mais em um ou outro aspecto do termo.

Se analisados os conceitos chaves da literatura é possível chegar à conclusão que segurança cibernética é "a organização e coleta de recursos, processos e estruturas usadas para proteger o ciberespaço e os sistemas habilitados para o ciberespaço de ocorrências que desalinhem direitos de propriedade "de direito" (*de jure*) de direitos de propriedade "de fato" (*de facto*)" (CRAIGEN *et al*., 2014). Para que fique mais claro, os autores desse conceito desconstruíram a essência dessa definição.

> *a)* *A organização e recolha de recursos, processos e estruturas* [...]: Este aspecto capta as múltiplas dimensões entrelaçadas e a complexidade inerente à segurança cibernética, que ostensivamente envolvem as interações entre os seres humanos, entre sistemas, e entre seres humanos e sistemas. Ao evitar a discussão de quais recursos, processos ou estruturas, a definição torna-se não-prescritiva e reconhece a natureza dinâmica da segurança cibernética.
>
> *b)* [...] *usados para proteger ciberespaço e sistemas habilitados para o ciberespaço* [...]: Este aspecto inclui a proteção, no sentido mais amplo, de todas as ameaças, incluindo perigos intencionais, acidentais e naturais. Este aspecto também incorpora a visão tradicional do ciberespaço, mas inclui aqueles sistemas que não são tradicionalmente vistos como parte do ciberespaço, tais como sistemas de controle de computadores e sistemas ciber-físicos. Por extensão, a proteção aplica-se a bens e informações de preocupação dentro do ciberespaço e a sistemas conectados.
>
> *c)* [...] *de ocorrências* [...]: Este aspecto reconhece que "proteções" são destinadas a abordar toda a gama de eventos intencionais, acidentais, eventos e riscos naturais. Além disso, sugere que algumas das ocorrências são imprevisíveis.
>
> *d)* [...] *que desalinhem direitos de propriedade "de direto" dos diretos de propriedade "de fato"* [...]: Este aspecto incorpora as duas noções distintas de propriedade e controle que dominam a discussão da segurança cibernética e ativos digitais introduzidas no quadro dos direitos de propriedade que incluem o acesso, extração, a contribuição, a remoção, a gestão, a exclusão e a alienação. Qualquer evento ou atividade que desalinha os reais (de fato) direitos de propriedade dos perceptivos (de direto) direitos de propriedade, seja por intenção ou acidente, conhecidos ou não, é um incidente de segurança cibernética[20] (Craigen *et al*., 2014, tradução própria).

[20] • *...the organization and collection of resources, processes, and structures*…: This aspect captures the multiple, interwoven dimensions and inherent complexity of cybersecurity, which ostensibly involve interactions between humans, between systems, and between humans and systems. By avoiding discussion of which resources, processes, or structures, the definition becomes non-prescriptive and recognizes the dynamic nature of cybersecurity.
• …*used to protect cyberspace and cyberspace-enabled systems*…: This aspect includes protection, in the broadest sense, from all threats, including intentional, accidental, and natural hazards. This aspect also incorporates the traditional view of cyberspace but includes those systems that are not traditionally viewed as part of cyberspace, such as computer control systems and cyber-physical systems. By

É claro que essa definição é ampla. Segundo a Casa Branca dos Estados Unidos da América, uma definição foi imputada no *Cyberspace Policy Review* (2009), e faz parte de uma ação do país chamada de Iniciativa Abrangente de Cibersegurança Nacional (*Comprehensive National Cybersecurity Initiative* - CNCI). Para o órgão, cibersegurança é a atividade, processo, habilidade, capacidade ou estado em que a informação e os sistemas de comunicação e suas informações contidas dentro são protegidas de e/ou defendidas contra danos, uso não autorizado, modificação ou exploração. Se estendida, a definição pode incluir estratégias, políticas e normas relativas à segurança das operações no ciberespaço, e que englobam uma gama de redução de ameaças e vulnerabilidades, a dissuasão, engajamento internacional, resposta a incidentes, resiliência e políticas de recuperação; além de atividades, incluindo as operações de rede de computadores, garantia à informação, aplicação da lei, missões de inteligência, diplomáticas, ou militares, e como elas se relacionam com a segurança e a estabilidade da infraestrutura de informação e comunicação global. Desse modo, o Estado terá a perspectiva de que estará se protegendo de certas ameaças que vêm surgindo no decorrer dos últimos anos no ciberespaço. Mas o que são ciberameaças e quais são os seus principais perigos?

2.2.2.2 Ciberameaças ou Ameaças Cibernéticas

Ameaça, segundo a Associação Brasileira de Normas Técnicas, é nada mais que a "causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização" (ABNT, 2005). Ao adicionarmos o prefixo "ciber" podemos concluir que uma ciberameaça de maneira literal é uma tentativa de ataque (bem ou malsucedida) utilizando-se de uma rede (intranet ou internet) a fim de danificar um

---

extension, the protection applies to assets and information of concern within cyberspace and connected systems.

• …*from occurrences*…: This aspect recognizes that "protections" are intended to address the full range of intentional events, accidental events, and natural hazards. It also suggests that some of the occurrences are unpredictable.

• …*that misalign de jure from de facto property rights*…: This aspect incorporates the two separate notions of ownership and control that dominate discussion of cybersecurity and digital assets introduced in the property rights which include access, extraction, contribution, removal, management, exclusion, and alienation. Any event or activity that misaligns actual (de facto) property rights from perceived (de jure) property rights, whether by intention or accident, whether known or unknown, is a cybersecurity incident.

sistema ou organização. No entanto, mesmo que o conceito pareça simples, são várias as possibilidades de ameaças que podem ser categorizadas dentro do mesmo.

Tabela 2 - Lista de Ciberameaças

Operadores de *Botnet*[21]	São hackers; no entanto, em vez de invadir sistemas como desafio ou para se gabar, eles assumem múltiplos sistemas, a fim de coordenar os ataques e distribuir esquemas de *phishing*[22], *spam*[23] e ataques de *malware*[24]. Os serviços dessas redes são por vezes distribuídos nos mercados clandestinos. (ex: a compra de um ataque a um sistema)
Grupos de criminosos	Procuram atacar sistemas para ganho monetário. Especificamente os grupos de crime organizado usam *spam, phishing, spyware*[25]*/malware* para cometer roubo de identidade e fraude online. Espiões corporativos internacionais e organizações do crime organizado também representam uma ameaça aos EUA por meio de sua capacidade de espionagem industrial, roubo monetário de grande escala e para contratar ou desenvolver hackers de talento.
Serviço de Inteligência Estrangeiros	Utilizam ferramentas virtuais como parte das suas coletas de informações e atividades de espionagem. Além disso, vários países estão trabalhando agressivamente para desenvolver doutrinas de guerra da informação, programas e capacidades. Esses recursos permitem que uma única entidade tenha um impacto significativo e sério por interrupção da distribuição, comunicações e infraestruturas econômicas que suportam o poder militar - impactos que podem afetar a vida quotidiana dos cidadãos norte-americanos em todo o país.

[21] Um *botnet* (também conhecido como um "exército de zumbis") é uma série de computadores na Internet que, apesar de seus proprietários não estarem conscientes disso, foram configurados para encaminhar transmissões (incluindo spam ou vírus) para outros computadores na Internet. Qualquer computador é referido como um zumbi - na verdade, um computador "robô" ou "bot" - serve a vontade de algum criador de spam ou vírus que o comada a distância.

[22] Essa prática, como o nome sugere ("*phishing*" em inglês corresponde a "pescaria"), tem o objetivo de "pescar" informações e dados pessoais importantes através de mensagens falsas. Com isso, os criminosos podem conseguir nomes de usuários e senhas de um site qualquer, como também são capazes obter dados de contas bancárias e cartões de crédito.

[23] É o termo usado para se referir às mensagens eletrônicas que são enviadas para você sem o seu consentimento - e que, geralmente, são despachadas para um grande número de pessoas. Esse tipo de "email indesejável" contém, em sua grande maioria, propagandas.

[24] Os *malwares*, conhecidos pelo termo *malicious software* (do inglês software malicioso), são programas desenvolvidos para executarem ações danosas e ilícitas em um sistema. Entre os danos mais conhecidos, podem ser destacados a perda de dados e o roubo de informações sigilosas.

[25] Os *spywares* são programas espiões que, uma vez instalados no sistema do usuário, realizam o monitoramento de suas atividades e enviam as informações coletadas para terceiros, por meio da internet. Originariamente, eles tinham um enfoque mais publicitário. Ou seja, investigavam os hábitos dos usuários com o objetivo de direcionar propagandas. Com o passar do tempo, ganharam características de cunho ilegítimo como, por exemplo, o roubo de dados confidenciais.

Hackers	Invadem redes pela emoção do desafio ou para exigir suas demandas em uma comunidade hacker. Enquanto craquear[26] remotamente requer uma quantidade razoável de habilidades ou conhecimentos de computadores, os hackers podem agora fazer o download de scripts e protocolos de ataque a partir da Internet e lançá-los contra sites vítimas. Enquanto ferramentas de ataque se tornaram mais sofisticados, eles também se tornaram mais fáceis de usar. De acordo com a Agência Central de Inteligência (CIA), a grande maioria dos hackers não têm os conhecimentos necessários para ameaçar alvos difíceis, tais como redes críticas norte-americanas. No entanto, a população mundial de *hackers* representa uma ameaça relativamente elevada de uma perturbação isolada ou breve causando sérios danos.
Insiders	A organização *insider*[27] descontente é a principal fonte de criminalidade informática. *Insiders* podem não precisar de uma grande quantidade de conhecimento sobre invasões a computadores, porque seu conhecimento de um sistema de destino muitas vezes lhes permite ter acesso irrestrito para causar danos ao sistema ou roubar seus dados. A ameaça interna também inclui fornecedores de *outsourcing*, bem como os funcionários que acidentalmente introduzem *malwares* em sistemas.
Phishers	Indivíduos ou grupos pequenos, que executam esquemas de *phishing* em uma tentativa de roubar identidades ou informações para ganho monetário. Os *phishers* também podem usar spam e *spyware / malware* para realizar seus objetivos.
Spammers	Indivíduos ou organizações que distribuem mensagens eletrônicas não solicitadas com informações escondidas ou falsas a fim de vender produtos, realizar esquemas de *phishing*, distribuir *spyware / malware*, ou de atacar organizações.
Autores de *spyware/ malware*	Indivíduos ou organizações com intenções maliciosas ao realizar ataques contra os usuários ao produzirem e distribuírem *spyware* e *malware*. Vários vírus de computador destrutivos têm prejudicado arquivos e discos rígidos, incluindo o vírus Melissa Macro, o vírus Explore.Zip, o vírus CIH (Chernobyl), Nimda, Code Red, Slammer, e Blaster.
Terroristas[28]	Procuram destruir, incapacitar, ou explorar infraestruturas críticas a fim de ameaçar a segurança nacional, causar mortes em massa, enfraquecer a economia dos EUA, e danificar a moral pública e a confiança. Os terroristas podem usar esquemas de *phishing* ou *spyware / malware* a fim de gerar fundos ou reunir informações sensíveis.

Fonte: Análise baseada em dados do *Federal Bureau of Investigation* (FBI), *Central Intelligence Agency* (CIA), e do Instituto de Engenharia de Software (CERT *Coordination Center*) (Adaptado pelo autor).

Como se pode notar, há uma variada amplitude em termos de ciberameaças passíveis de serem empregadas, e que já são preocupação de alguns Estados no presente, por ameaçarem sistemas que comandam suas infraestruturas críticas ou causarem severo dano econômico, vulnerabilidades essas que tendem a aumentar no decorrer do século XXI. Algumas das ameaças ilustradas na tabela 2 vão ser exemplificadas no próximo capítulo, pois são claramente verificáveis nos eventos

[26] *Crackers* são pessoas aficionadas por informática que utilizam seu grande conhecimento na área para quebrar códigos de segurança, senhas de acesso a redes e códigos de programas com fins criminosos.

[27] Pessoas que trabalham dentro de uma entidade pública ou privada. Como exemplo temos o caso recente de *Edward Snowden*, contratado pela Agência Nacional de Segurança (NSA) dos EUA para prestar serviços como terceirizado, e sendo o responsável pelo vazamento de inúmeros dados sensíveis do governo norte-americano.

[28] Segundo o código dos EUA (*U.S. Code (U.S.C.),* epígrafe 22, capítulo 38), o termo "terrorismo" significa: violência premeditada, politicamente motivada, perpetrada contra alvos não-combatentes por grupos subnacionais ou agentes clandestinos (Não será feita nessa pesquisa uma discussão política, teórica ou jurídica do uso do termo, pois esse trabalho tem a intenção de considerar as fontes de ameaças cibernéticas ao setor militar dos EUA).

internacionais que marcaram a cibernética dos EUA nos últimos oito anos. São ações como essas que tornam os Estados vulneráveis, como será exposto a seguir.

2.2.2.3 Cibervulnerabilidade ou Vulnerabilidade Cibernética

Tomando o termo "vulnerabilidade" como um conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação (GSI-PR, 2009); e, ao pensar o termo como parte de um complexo tecnológico da cibernética atual, é possível a construção de parâmetros mais difíceis de controlar; e, portanto, mais perigosos aos Estados.

No caso da cibernética, as vulnerabilidades de um Estado em manter suas tecnologias de informação e comunicação (TICs) são muitas vezes assimétricas. Ou seja, ao mesmo tempo que trazem inúmeras vantagens, também podem levar Estados que não possuem um grande domínio em conflitos convencionais a se utilizar dessas redes para atacar – a um custo muito inferior – nações como os EUA.

> Isso cria a estranha ironia da guerra cibernética. Quanto mais conectada é uma nação, mais ela pode tirar proveito da Internet. Mas, quanto mais conectada é uma nação, mais ela potencialmente pode ser prejudicada por aqueles que utilizam a Internet de forma maliciosa. [...] Como Diretor Nacional de Inteligência 2007-2009, Mike McConnell supervisionou uma onda de capacidades de guerra cibernética norte-americana, financiadas por dezenas de bilhões de dólares, que culminou com o desenvolvimento de armas como *Stuxnet*[29]. Mas, em vez de se sentir mais confiante sobre em que posição os Estados Unidos ficaram situados na cibersegurança após este esforço, McConnell declarou ao Senado: "Se o país entrasse em guerra hoje, em uma guerra cibernética, perderíamos. Nós somos os mais vulneráveis. Nós somos os mais conectados. Nós temos mais a perder. " [...] Ao contrário de muitos de seus potenciais adversários neste espaço, os Estados Unidos e, especialmente, os militares dos EUA são altamente dependentes de redes de computadores para tudo, desde comunicações até eletricidade (a grande maioria da energia elétrica usada por bases militares dos EUA, por exemplo, vêm de locais comerciais utilizando redes de energia bastante vulneráveis). Sendo assim, ciberataques de resistência equivalente teriam consequências muito mais devastadoras sobre os Estados Unidos do que em potenciais adversários como a China, cuja rede militar ainda é menos conectada, e muito menos um "pigmeu" cibernético como a Coréia do Norte, cuja economia nunca entrou na era da informação. Como o ex-oficial da NSA Charlie Miller

[29] O Stuxnet foi um vírus de alta complexidade criado em 2006, e aperfeiçoado ao longo dos anos, que tem a capacidade para invadir, espionar e modificar sistemas SCADA (um sistema operacional com sinais codificados que proporciona o controle de equipamentos industriais remotamente). Nesse sistema, o vírus coletou informações industriais e causou um movimento de rotação acelerado nas centrífugas iranianas, comprometendo seu funcionamento. Haverá uma seção dedicada a análise desse fenômeno no segundo capítulo (fonte própria).

> explica: "Uma das maiores vantagens da Coréia do Norte é que ela tem quase nenhuma infraestrutura conectada à Internet para atacar. Por outro lado, os Estados Unidos têm de toneladas de vulnerabilidades que um país como a Coréia do Norte poderia explorar" [30](SINGER; FRIEDMAN 2014, p. 152-153, tradução própria).

Essas vulnerabilidades têm relação direta com as infraestruturas críticas dos EUA, que em sua grande maioria estão ligadas às Tecnologias da Informação e Comunicação, como será exposto a seguir.

2.2.2.4 Infraestruturas Críticas da Informação ou Infraestruturas Digitais

Por infraestruturas críticas (IEC) entendem-se as instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provocará sério impacto social, econômico, político, ambiental, internacional ou à segurança do Estado e da sociedade. (MANDARINO Jr., 2010). Quando englobados ativos de informação, é possível que estas infraestruturas afetem diretamente a consecução e a continuidade da missão do Estado e a segurança da sua sociedade.

> Na década de 1990, infraestruturas críticas surgiram como um ponto focal de debate (nos EUA). O conceito de proteção de infraestruturas críticas inclui muitos aspectos diferentes, um dos quais é a cibersegurança. […] Essas infraestruturas críticas da informação são consideradas como a espinha dorsal das infraestruturas críticas em geral, uma vez que a troca ininterrupta de informações é essencial para as operações de governo, serviços de emergência e comércio. Essa dependência da informação – combinada com vulnerabilidades crescentes resultantes das lacunas de segurança técnica, a complexidade da tecnologia, a liberalização do mercado em curso e a crescente capacidade e vontade dos atores maliciosos em conduzir ataques físicos e cibernéticos – faz com que telecomunicações e sistemas de

[30] *This creates the strange irony of cyberwar. The more wired a nation, the more it can take advantage of the Internet. But the more wired a nation, the more it can potentially be harmed by those using the Internet maliciously. […] As director of national intelligence from 2007 to 2009, Mike McConnell oversaw a surge of US cyberwar capabilities, funded by tens of billions of dollars, that culminated in the development of weapons like Stuxnet. But instead of feeling more confident about where the United States stood in cybersecurity after this effort, McConnell testified to the Senate, "If the nation went to war today, in a cyberwar, we would lose. We're the most vulnerable. We're the most connected. We have the most to lose." […] Unlike many of its potential adversaries in this space, the United States and especially the US military is highly reliant on computer networks for everything from communications to electricity (the vast majority of electrical power used by US military bases, for instance, comes from commercial utilities using a fairly vulnerable power grid). So cyberattacks of equivalent strength would have far more devastating consequences on the United States than on potential adversaries like China, whose military is still less networked, let alone a cyber pygmy like North Korea, whose economy never entered the information age. As former NSA official Charlie Miller explains, "One of North Korea's biggest advantages is that it has hardly any Internet-connected infrastructure to target. On the other hand, the United States has tons of vulnerabilities a country like North Korea could exploit."*

> informação tornem-se alvos vulneráveis, ao menos em teoria[31] (CAVELTY, 2008, tradução própria).

Em razão da conectividade dos sistemas de comunicação e informação, quando um sistema é invadido e grande parte dos dados transmitidos é comprometido, em infraestruturas chaves de um Estado, é possível a criação de episódios como o do vírus *Stuxnet* que afetou as usinas nucleares do Irã em 2010. Como consequência, as Infraestruturas Críticas da Informação são fatores que geram preocupação para todos os países, não somente os EUA, e resultaram em uma série de recomendações aos membros da Organização para a Cooperação e o Desenvolvimento Econômico (OECD) em 2008, que propõe:

A. Definir a política e as normas específicas, com objetivos claros, no âmbito do mais alto nível de governo;
B. Atuar como o órgão central de governo com competência (responsabilidade e autoridade) para prover as melhores condições de implantação da política de segurança cibernética e seus objetivos;
C. Promover tanto a cultura de - quanto a educação em - segurança cibernética;
D. Promover mútua cooperação entre os *stakeholders* – setor privado, agência(s), terceiro setor, governo – visando à efetiva implantação da política nacional de segurança cibernética;
E. Atuar com transparência assegurando delegação de competência, ou seja, governança estabelecida, facilitando e fortalecendo a cooperação, em especial entre governo e setor privado;
F. Rever sistematicamente a política, normas e respectivo(s) marco(s) legal(is), com especial atenção às ameaças e vulnerabilidades das infraestruturas críticas da informação de cada país, buscando minimizar riscos e desenvolver novos instrumentos e/ou mecanismos de segurança da informação e comunicações;

---

[31] *In the 1990s, critical infrastructures emerged as focal point in the debate. The concept of critical infrastructure protection includes very many different aspects, one of which is cyber-security […] These critical information infrastructures are regarded as the backbone of critical infrastructures in general, given that the uninterrupted exchange of data is essential to government operations, emergency services, and commerce. This dependence on information – combined with increasing vulnerabilities resulting from the technical security gaps, the complexity of technology, ongoing market liberalization, and the growing ability and willingness of malicious actors to conduct physical and cyber-attacks – makes telecommunications and information systems highly vulnerable targets, at least in theory.*

G. Desenvolver e exercer macrocoordenação da política e estratégia nacional de segurança cibernética, envolvendo cúpula de governo e setor privado;
H. Promover e exercer a macrocoordenação do monitoramento e da avaliação de risco, baseados na análise das vulnerabilidades e ameaças das infraestruturas críticas da informação, visando proteger a economia e a sociedade contra altos impactos;
I. Promover e exercer a macrocoordenação do processo nacional de gestão de risco, orientando desde aspectos da organização, ferramenta(s), até mecanismos de monitoramento, para a implementação de uma estratégia nacional de gestão de risco que compreenda: a) Estrutura organizacional apropriada que promova melhores práticas de segurança, e que incluam prevenção, proteção, resposta e recuperação de ameaças naturais e maliciosas; e, b) Sistema de medidas que permita avaliar continuamente o processo, o que inclui itens de controle, níveis de maturidade, exercícios e testes apropriados;
J. Promover e exercer a macrocoordenação da capacidade de resposta à incidentes em redes computacionais, como as das equipes que atuam em CERTs/CSIRTs[32], incluindo mecanismos de forte cooperação e comunicação entre tais equipes;
K. Estreitar as relações com o setor privado: a) Estabelecendo parcerias público-privadas e acordos de cooperação, com foco na gestão de risco, tratamento de incidentes e recuperação de sistemas e redes de informação e comunicações, e na gestão da continuidade de negócios; b) Estimulando o intercâmbio regular de informação, por meio do estabelecimento de acordos com cláusulas específicas para o caso de conhecimentos sensíveis ou informações classificadas;
L. Estimular e apoiar a aceleração da inovação da segurança cibernética por meio da pesquisa e do desenvolvimento;

[32] CSIRT (*Computer Security Incident Response Team*) / CERT (*Computer Emergency Response Team*) (nota própria).

M. Promover a cooperação bilateral e multilateralmente, em nível regional e global, visando trocas de experiências e fortalecimento das estratégias de segurança cibernética (MANDARINO Jr., 2008, p. 26-28).

Desde 2003 já houve, nos EUA, a iniciativa para a criação da Estratégia Nacional de Segurança do Ciberespaço (*National Strategy to Secure Cyberspace*) que, sob as palavras do então presidente George W. Bush, expôs que "a Estratégia Nacional para Segurança do Ciberespaço ajuda a reduzir a vulnerabilidade da nossa nação para ataques debilitantes contra nossas infraestruturas de informação críticas ou os ativos físicos que lhes dão suporte" (DHS, 2003).

2.2.2.5 Segurança Nacional

Tradicionalmente a segurança nacional é reconhecida como a responsabilidade do governo, apoiando-se em esforços coletivos militares, de estabelecimento de políticas externas e da comunidade de inteligência. É o Estado que tem o dever de manter firme a sua soberania e funcional a sua governabilidade. A segurança nacional é ligada de maneira direta à proteção das infraestruturas críticas da informação de um país. Na ausência dessa proteção, o país compromete sua inteligência a ponto de não conseguir manter sua segurança de intervenções externas.

No caso dos EUA, esse controle é realizado por meio de uma entidade poderosa e detentora de um grande volume de recursos chamada de Agência de Segurança Nacional (*National Security Agency* – NSA). Além da agência, o *Federal Bureau of Investigation* (FBI), certos cargos especializados do Congresso e o presidente são os responsáveis pela manutenção da Segurança Nacional do país. Mesmo com várias diretrizes nos últimos anos – que serão bem-dispostas no decorrer dos próximos capítulos – os EUA terão um longo caminho a percorrer para conseguirem defender seu status de grande potência e ao mesmo tempo impedir intervenções externas por países inimigos que coloquem em risco a sua soberania.

2.2.3 Conclusões parciais

Nesse capítulo foi apresentado a base teórica que fornecerá a metodologia para analisar os eventos e os discursos, bem como os conceitos chave necessários para que a

cibernética seja compreendida de maneira adequada. Esses conceitos, todavia, não esgotam o campo da cibernética, apenas são os mais importantes para embasar o decorrer deste trabalho. Buscar-se-á localizá-los durante a análise dos discursos no terceiro capítulo, e verificar-se-á se essas palavras são utilizadas com frequência (ou não) nos atos de fala dos atores securitizadores.

Como já foi afirmado anteriormente, o método utilizado no desenvolvimento dessa pesquisa será com base no setor militar, mas com possíveis efeitos em outros setores como o econômico e político. Além disso, serão analisados apenas atores em nível unitário estatal. Essas são opções do pesquisador com o intuito de afunilar a pesquisa para que ela atinja um resultado satisfatório.

Assim sendo, com o objetivo de elucidar as novas ameaças que estão surgindo nesses últimos anos, serão apresentados a seguir alguns eventos internacionais em torno da cibernética, em um período selecionado de oito anos, que de certo modo influenciaram os discursos de Estados como os EUA a repensar suas estratégias, e ampliar sua segurança e defesa cibernéticas.

3 EVENTOS INTERNACIONAIS NO CAMPO CIBERNÉTICO

A fim de manter a linha dessa pesquisa serão inseridos, em ordem cronológica, alguns dos eventos internacionais no campo da cibernética (ataques, espionagens, infiltrações), cujos atores responsáveis são Estados – em sua maioria, pois existe a dificuldade de comprovação em alguns casos. São eventos que ocorreram nos últimos oito anos – período de 2007 a 2014 – e que de alguma maneira afetaram direta ou indiretamente outros Estados no sistema internacional e, por conseguinte, repercutiram nos EUA e em seus atos de fala relativos à segurança cibernética do país.

Esses acontecimentos podem ser tanto ataques em meio cibernético ou derivados, quanto à criação de instituições internacionais ou organizações estatais (com a participação dos EUA). Serão aceitos apenas eventos que se relacionem com a cibernética pela forma da Internet global, sendo desconsiderados quaisquer outros meios cinéticos. Dentre esses acontecimentos serão apresentados ataques à redes governamentais, quebra de sigilo e vazamentos massivos em órgãos de inteligência de países, invasões a sistemas industriais responsáveis por infraestruturas críticas de um país, espionagem à agências governamentais e invasões a sistemas integrados. No entanto, não serão considerados ataques à redes corporativas privadas ou outras organizações internacionais, pois fogem ao escopo dessa pesquisa, que é o ator estatal.

Ademais, tem-se como ponto de inflexão o que foi convencionado por alguns especialistas em segurança cibernética como o "primeiro ato de ciberguerra" em abril de 2007 na Estônia, e que será melhor explicado a seguir. Embora seja tratado como o primeiro ato, não há validação como sendo de fato um ato de guerra cibernética, pois mesmo os acontecimentos seguintes decorridos no sistema internacional até o momento não são devidamente reconhecidos e validados - como atos de ciberguerra - pelos Estados. Segundo William J. Lynn (2010), um ex-vice-secretário de defesa dos EUA, "de fato, a maioria das intrusões estão mais perto de serem caracterizadas como espionagem que como atos de guerra. A equação da dissuasão é ainda mais confusa pelo fato de que ataques cibernéticos muitas vezes se originam de servidores cooptados em países neutros, e as respostas a eles poderiam ter consequências inesperadas".

> Há todas as razões para acreditar que a maioria das guerras cinéticas no futuro serão acompanhadas de guerra cibernética, e que outras guerras cibernéticas serão conduzidas de "maneira pura", sem explosões, infantaria,

> poder aéreo e marinhas. Não há ainda, porém, uma guerra cibernética em grande escala em que as nações líderes nesse tipo de combate podem empregar suas ferramentas mais sofisticadas umas contra as outras[33] (CLARKE; KNAKE, 2010, p. 21, tradução própria).

Mesmo que não haja certeza quanto a como classificar de maneira adequada esses novos acontecimentos, vale dissertar sobre eles e buscar observar suas consequências no cenário internacional. É o que esse capítulo propõe. Seguindo uma cronologia, inicia-se as exposições com o ataque às estruturas governamentais da Estônia em 2007, e finaliza-se com os ataques à Alemanha em 2014.

2.2 ATAQUES À ESTÔNIA

A Estônia é uma república parlamentar democrática dividida em quinze condados, cuja capital – e maior cidade do país – é Tallinn. Com uma população composta majoritariamente de estonianos, também possui uma massiva presença de russos (em torno de 25%, segundo o senso de 2015[34]). Essa presença é marcante graças ao legado deixado pela ocupação e posterior queda da URSS, que terminou sua ocupação do país em 16 de novembro de 1988, com a Declaração Estoniana de Soberania[35] através de um evento internacionalmente conhecido como "Revolução Cantada"[36], em que os países dos Bálcãs - Estônia, Letônia e Lituânia - se separaram da União Soviética. Em 17 de setembro de 1991, os principais países ocidentais reestabeleceram relações diplomáticas com a Estônia e as bandeiras de todos os três Estados bálticos foram levantadas em frente à sede da ONU em Nova York. Estônia voltou ao seio das nações livres do mundo.[37]

Esse legado de imigrantes russos que hoje em dia compõem a população da Estônia é de grande relevância, pois acredita-se que eles influenciaram indiretamente em ataques cibernéticos ao governo estoniano há oito anos atrás. Foram uma série de

---

[33] *"...there is every reason to believe that most future kinetic wars will be accompanied by cyber war, and that other cyber wars will be conducted as "stand-alone" activities, without explosions, infantry, airpower, and navies. There has not yet, however, been a full-scale cyber war in which the leading nations in this kind of combat employ their most sophisticated tools against each other*".

[34] *Minifacts About Estonia*, 2015. Disponível em: <http://www.stat.ee/90745> Acesso em 21/07/2015

[35] Disponível em: <http://estonia.eu/about-estonia/history/estonias-return-to-independence-19871991.html> Acesso em 21 jul. 2015

[36] Ibidem**.** Acesso em 21 jul. 2015

[37] Ibidem. Acesso em 21 jul. 2015

vários ataques DDoS[38] que iniciaram em 27 de abril de 2007 – se alongando por aproximadamente um mês - e derrubaram uma série de sites de organizações estonianas, incluindo o parlamento, bancos, ministérios, jornais locais dentre outros. Um dos motivos que levou aos ataques, segundo fontes midiáticas como *New York Times*[39] e *The Guardian*[40], foi a retirada de uma estátua conhecida como "O soldado de bronze de Tallinn". De acordo com o historiador russo Alexander Daniel (2007), o Soldado de Bronze tem um valor simbólico aos estonianos russos, simbolizando não somente a vitória soviética sobre a Alemanha na Grande Guerra Patriótica, como também a aquisição dos direitos desses russos no país. Já para grande parte dos estonianos o Soldado é considerado um símbolo da ocupação soviética e da repressão que seguiu o fim da Segunda Guerra Mundial.

Segundo Gadi Evron[41],

> Relatos iniciais da mídia sugeriram que os ataques de negação de serviço (DDoS) podem ter sido organizados pelo governo russo em retaliação à decisão da Estônia de mover a estátua. A realidade, porém, é que os ataques foram realizados por um número desconhecido de indivíduos russos com o apoio ativo de pessoas experientes no ramo de segurança na blogosfera russa, Evron disse (COMPUTERWORLD, 2007, tradução própria).

Mesmo que os ataques e protestos desencadeados *online* não tenham partido de ordens dadas através do Kremlin, o conjunto de consequências sobre o governo estoniano e sua população levantaram preocupação. Segundo Bruce Brody, um oficial sênior de cibersegurança dos EUA, "foi um ataque de força bruta, um ataque rude, sem elegância e precisão que caracterizam as capacidades cibernéticas sofisticadas das grandes potências" (UPI, 2007). Já o professor James Hendler, cientista chefe da DARPA descreveu o ataque como "mais um ciber-motim (*cyberriot)* do que um ataque militar" (UPI, 2007).

---

[38] *Denial Distribution of Service* (ataque de negação de serviço), um tipo de ataque em que sites são bombardeados por várias tentativas de acesso, sobrecarregando seus servidores e os tornando inacessíveis por um período de tempo correspondente ao bombardeamento de acessos. Dependendo da estrutura do servidor, ele pode sofrer danos irreversíveis e ter de ser restaurado.

[39] Disponível em <http://www.nytimes.com/2007/05/29/technology/29estonia.html?_r=0> Acesso em 22 jul. 2015

[40] Disponível em <http://www.theguardian.com/world/2007/apr/29/russia.lukeharding> Acesso em 22 jul. 2015

[41] *"Initial media reports suggested that the denial-of-service (DoS) attacks may have been organized by the Russian government in retaliation for Estonia's decision to move the statue. The reality, however, is that the attacks were carried on by an unknown number of Russian individuals with active support from*

Não obstante, a Estônia é conhecida - há mais de 20 anos[42] - como um dos países tecnologicamente mais bem inseridos no cenário internacional em termos de acesso à internet, com uma estrutura de informações centralizadas conhecida como *e-Estonia*[43]. É através da rede mundial que o país se tornou uma das mais avançadas *e-societies* no mundo, em que são abarcados desde sites de consulta pública a informações governamentais até eleições que são realizadas por meio da internet[44]. Segundo Jaak Aaviksoo, ministro da Defesa estoniano naquele período, "se tornou uma situação de Segurança Nacional […] e pode ser efetivamente comparado como quando fecham seus portos para o mar aberto" (LANDLER, MARKOFF, 2007). Ainda, segundo os autores Landler e Markoff, o ataque poderia ter levado a uma discussão dentro da OTAN do que precisaria ser feito para modificar o comprometimento dos países quanto à defesa coletiva, consagrada no artigo V do Tratado do Atlântico Norte.

Após desencadeados os ataques, iniciaram-se diversos debates no meio acadêmico e uma série de organizações militares em todo o mundo começaram a reconsiderar a importância da segurança da rede mundial para a doutrina militar moderna. Não somente o país, grandes potências como os EUA também estão caminhando a passos largos, de um ponto de vista histórico, englobando novas tecnologias em torno da Internet e tornando inevitáveis vulnerabilidades como as que atingiram a Estônia no passado.

Em 14 de junho de 2007 os ministros da defesa dos membros da OTAN[45] realizaram uma reunião em Bruxelas, e emitiram um comunicado conjunto prometendo ações imediatas. De acordo com Mike Witt, vice-diretor da Equipe de Resposta à Emergências Cibernéticas dos EUA[46], houve um envolvimento dos EUA após a OTAN - cuja Estônia é país membro - contatar o país a fim de obter assistência para conter os

---

security-savvy people in the Russian blogosphere, Evron said." Evron é executivo da Companhia de Segurança Beyond Security, já participou do *Computer Emergency Response Team* (CERT), em Israel.

[42] A Internet é considerada um direito de todo cidadão desde os anos 2000. Para mais informações, consultar a "lei de telecomunicações" estonianas em: <http://www.lexadin.nl/wlg/legis/nofr/oeur/lxweest.htm>.

[43] Para mais informações, consultar <https://e-estonia.com/>.

[44] Para mais informações, consultar <http://vvk.ee/voting-methods-in-estonia/engindex>.

[45] Croácia, Albânia, Eslovênia, Eslováquia, Romênia, Lituânia, Letônia, Estônia, Bulgária, Polônia, Hungria, República Tcheca, Alemanha, Espanha, Turquia, Grécia, Estados Unidos, Reino Unido, Portugal, Noruega, Holanda Luxemburgo, Itália, Islândia, França, Dinamarca, Canadá, Bélgica.

[46] O *U.S. Cyber Emergency Response Team (U.S. CERT)* é composto por uma equipe de especialistas em segurança cibernética do Departamento de Segurança Nacional, responsável por coordenar defesas e respostas contra ciberataques através da nação.

ciberataques. Witt comentou ainda que o seu time "trabalhou com um grupo internacional conhecido como Fórum de Resposta a Incidentes e Equipes de Segurança (*FIRST*, em inglês) com o intuito de coordenar uma resposta global aos ataques, que foram realizados por computadores espalhados por todo o globo" (UPI, 2007).

Já em 25 de junho de 2007, o presidente estoniano Toomas Hendrik Ilves se reuniu com o ex-presidente dos EUA, George W. Bush. Entre os temas discutidos estavam os ataques à infraestrutura da Estônia, bem como do início da operação do *Cooperative Cyber Defence Centre of Excellence* (CCDCOE) da OTAN, que começou seus trabalhos em Tallinn em agosto de 2008[47].

3.1.1 *Cooperative Cyber Defence Centre of Excellence* (CCDCOE)

O *Cooperative Cyber Defence Centre of Excellence* é uma organização criada em 2008 através de um memorando em Bruxelas. Em 28 de outubro do mesmo ano foi acreditada com o status de Organização Militar Internacional, e tem a missão de elevar a capacidade, cooperação, e compartilhamento de informações da OTAN e suas nações membros em cibersegurança, além de prezar pela virtude da educação, pesquisa e desenvolvimento na área. Sua sede é em Tallinn, capital da Estônia, onde ocorreram os ataques no ano de 2007.

Centros de Excelência da OTAN, como o CCDCOE, são instituições elegidas e financiadas de maneira nacional ou multinacional, com o intuito de treinar e educar líderes e especialistas dos países membros e parceiros da OTAN, auxiliando no desenvolvimento de doutrinas, identificando "lições aprendidas", melhorando na interoperabilidade e nas capacidades de testar e validar conceitos através da experimentação – no caso da CCDCOE com simulações de ataques e defesas, e desenvolvimento de operações no âmbito da cibernética. Ao oferecer a experiência e os conhecimentos, a aliança se prepara para as transformações no sistema internacional, evitando a duplicação de bens, recursos e capacidades já presentes dentro da estrutura de comando da organização[48].

---

[47] Disponível em < http://www.networkworld.com/article/2279535/lan-wan/nato-to-set-up-cyber-warfare-center.html > Acesso em 22 jul. 2015.

[48] Informações retiradas do site da OTAN. Disponíveis em: <http://www.act.nato.int/centres-of-excellence> Acesso em 22 jul. 2015.

Vale reiterar que os EUA, mesmo presentes nos discursos de apoio a criação do Centro, não estiveram presentes entre os sete países responsáveis pelo memorando de criação: Estônia, Alemanha, Itália, Letônia, Espanha e República Eslovaca. Os EUA somente aderiram ao grupo em 17 de novembro de 2011, cuja adesão foi em conjunto com a Polônia. A Estônia, como líder nessa iniciativa, sofreu um ataque que mesmo de grande sofisticação, seria apenas uma preparação para um ainda maior que ocorreria na Geórgia no ano seguinte.

3.2 ATAQUES À GEÓRGIA

A República da Geórgia está localizada ao sul da Rússia, e as duas nações cultivaram um passado de relações conturbadas no último século. A Geórgia é um país pequeno, com aproximadamente quatro milhões de pessoas (segundo o censo de 2015). Durante sua história, houve duas tentativas de separação da influência do Kremlin. A primeira tentativa de independência foi durante o final da Primeira Guerra Mundial, em 1918. Não durou muito, afinal o exército vermelho rapidamente invadiu o país após o término da guerra, retomando o controle e consolidando a União das Repúblicas Socialistas Soviéticas. Passados quase um século, a segunda tentativa foi em 1991, quando a URSS perdeu o controle sobre o país e a Geórgia declarou sua independência, permanecendo uma república soberana até os dias atuais.

Mesmo independente, a Geórgia perdeu o controle de duas regiões até então sob sua influência, a Ossétia do Sul e a Abcásia, que se tornaram territórios com governos considerados "independentes". Mesmo legalmente fazendo parte da Geórgia, os dois territórios confiavam e buscavam a proteção da Rússia.

> Então, em julho de 2008, os rebeldes da Ossétia do Sul (ou agentes russos, dependendo cuja versão dos eventos for confiada a informação) provocaram um conflito com a Geórgia, encenando uma série de ataques de mísseis sob aldeias georgianas. O exército georgiano, previsivelmente, respondeu aos ataques com mísseis no seu território ao bombardear a capital da Ossétia do Sul. Em seguida, em 7 de agosto, a Geórgia invadiu a região. Não surpreso com o rumo dos acontecimentos, o exército russo se envolveu no dia seguinte, rapidamente expulsando o exército georgiano da Ossétia do Sul. Precisamente ao mesmo tempo que o exército russo se moveu para a região, também se moveram os ciberguerreiros[49]. Seus objetivos eram impedir os

[49] Um "ciberguerreiro" é uma pessoa que se envolve em um conflito cibernético, quer por razões pessoais ou de crença religiosa ou patriótica. Os ciberguerreiros vêm em diferentes formas, dependendo dos seus

> georgianos de entender o que estava acontecendo, para tal eles transmitiram ataques DDoS em meios de comunicação e sites do governo georgiano. O acesso do país aos sites da CNN e a BBC foram interrompidos. No mundo físico, os russos também bombardearam a Geórgia e assumiram um pequeno pedaço do território georgiano que não estava em disputa, alegadamente para criar uma "zona tampão"[50] (CLARKE; KNAKE, 2010, p. 15, tradução própria).

Segundo os autores supracitados, o ponto relevante nessa história não é a importância dos ciberataques como causadores de destruição física (pois não houve) ou de receio de que países como os EUA fossem retaliar as ações russas (apenas consideraram esse um caso como remoto, e em geral não muito importante).

Os ataques atingiram um nível de sofisticação interessante. Como a Geórgia se conecta a Internet através da Rússia e da Turquia, a maior parte do tráfego foi interrompido, e os cidadãos georgianos não conseguiam se conectar a quaisquer fontes de informação externas ao país, sequer mandar e-mails para fora. O país perdeu inclusive o controle sobre o seu domínio ".ge" e foi forçado a alterar a maior parte dos sites governamentais para servidores fora do país. Mesmo tentando usar as maneiras disponíveis para se defender, bloqueando todo o tráfego vindo da Rússia, os ciberataques foram se alternando entre servidores na China, Canadá, Turquia, e até da Estônia. Ou seja, foi uma clara invasão de soberania sofrida pela Geórgia.

> O setor bancário georgiano desligou seus servidores como meio para superar os ataques, reconhecendo que uma perda temporária de transações online seria melhor que correr o risco de um roubo massivo de dados ou danos aos seus sistemas internos. Não sendo possível obter acesso aos bancos georgianos, os russos enviaram uma grande quantidade de tráfego por meio de seus *botnets* à comunidade de bancos internacionais, fazendo parecer com que os ciberataques estivessem sendo enviados da Geórgia. Os ataques desencadearam uma resposta automática da maioria dos bancos estrangeiros, fechando as conexões com o setor bancário da Geórgia. Sem acesso aos sistemas europeus, as operações bancárias do país foram paralisadas.

---

papéis, mas todos lidam com segurança da informação de uma ou outra maneira. Definição disponível em: < https://www.techopedia.com/definition/28615/cyber-warrior>. Acesso em: 05 ago. 2015

[50] *"Then, in July 2008, South Ossetian rebels (or Russian agents, depending upon whose version of events you trust) provoked a conflict with Georgia by staging a series of missile raids on Georgian villages. The Georgian army, predictably, responded to the missile strikes on its territory by bombing the South Ossetian capital city. Then, on August 7, Georgia invaded the region. Not surprised by this turn of events, the Russian army moved the next day, quickly ejecting the Georgian army from South Ossetia. Precisely at the same time that the Russian army moved, so did its cyber warriors. Their goal was to prevent Georgians from learning what was going on, so they streamed DDOS attacks on Georgian media outlets and government websites. Georgia's access to CNN and BBC websites were also blocked. In the physical world, the Russians also bombed Georgia and took over a small chunk of Georgian territory that was not in dispute, allegedly to create a "buffer zone".*

> Sistemas de cartão foram abaixo, seguidos pelo sistema de telefonia móvel[51] (CLARKE; KNAKE, 2010, p. 16, tradução própria).

Mesmo o governo russo negando participação oficial nos ciberataques à Geórgia, o nível de sofisticação empregado no lançamento dos ataques somente poderia ter vindo de um aparato de inteligência governamental. Ainda segundo os autores, o nível de coordenação nos ataques e o financiamento necessário para orquestra-los sugere um "fervor patriótico". Por fim, o governo russo se negou a auxiliar tanto nas investigações, quanto a impedir com que os ataques fossem cessados após o movimento militar.

3.3 OPERAÇÃO "*BUCKSHOT YANKEE*"

Em outubro de 2008, um soldado norte-americano ao caminhar por um estacionamento em uma base militar dos EUA no Oriente Médio, avistou vários *pen-drives* no chão. Sem saber quem havia deixado, ele decidiu pegar um e plugar na porta USB de um computador da base, conectada à rede da central de comando, sem saber que dentro dele havia um sofisticado *malware*. Essa tática de lançar objetos duvidosos que despertam a curiosidade é chamada "*candy drop*", e nessa oportunidade foi utilizada por uma agência de inteligência estrangeira, resultando em uma grande vulnerabilidade aos sistemas interconectados dos EUA (FRIEDMAN, SINGER, 2014).

O Pentágono passou os catorze meses seguintes na tentativa de eliminar esse software das instalações, em uma operação conhecida como *Buckshot Yankee*. O software malicioso, que ficou conhecido como "agente.btz", tinha o poder de escanear todos os dados dos computadores conectados à rede, além de criar *backdoors*[52], e ligar-se ao comando e aos servidores de controle. Seu código oferecia, para servidores sob

---

[51] *"The Georgian banking sector shut down its servers and planned to ride out the attacks, thinking that a temporary loss of online banking was a better bargain than risking the theft of critical data or damage to internal systems. Unable to get to the Georgian banks, the Russians had their botnets send a barrage of traffic to the international banking community, pretending to be cyber-attacks from Georgia. The attacks triggered an automated response at most of the foreign banks, which shut down connections to the Georgian banking sector. Without access to European settlement systems, Georgia's banking operations were paralyzed. Credit card systems went down as well, followed soon after by the mobile phone system"*

[52] Conhecidas como "Portas dos fundos", é um recurso utilizado por diversos *malwares* para garantir acesso remoto a um sistema ou rede infectada, explorando falhas críticas existentes em programas instalados ou em softwares desatualizados.

controle estrangeiro, tanto acesso à rede não-confidencial NIPRNET, quanto à confidencial SIPRNET, e de um modo a não ser detectado pelos sistemas estadunidenses. Mesmo após a eliminação do vírus, há relatos de oficiais do Departamento de Segurança Interna de que, no ano seguinte, o vírus ainda deixava alguns rastros, sendo persistente e evoluindo para novas versões. Não foi divulgado à mídia quais redes o vírus afetou, mas foram reforçadas as seguranças tanto dos domínios "dot.gov" quanto da "dot.mil" (redes não-confidencial e confidencial, respectivamente).

Por fim, segundo William J. Lynn (2010), "nos últimos dez anos a frequência e a sofisticação das intrusões em redes militares dos EUA têm aumentado exponencialmente; todos os dias, redes civis e militares do país são sondadas milhares de vezes e escaneados milhões". O resultado de mais esse ataque às redes estadunidenses gerou uma resposta, a criação do centro integrado para operações de ciberdefesa, o *U.S. Cyber Command* (USCYBERCOM), no ano seguinte.

3.3.1 *U.S. Cyber Command*

Em junho de 2009, o então Secretário da Defesa Robert Gates ordenou a consolidação de forças-tarefa em um único comando, criando o Ciber Comando dos Estados Unidos (*U.S. Cyber Command* ou USCYBERCOM). O centro iniciou seu comando com um general de quatro estrelas e (à época) diretor da NSA, Keith Alexander, que assumiria o papel extra como comandante do órgão.

O USCYBERCOM iniciou oficialmente suas operações em maio de 2010, subordinado ao Comando Estratégico do país (*U.S. Strategic Command*), tornando-se completamente operacional em outubro do mesmo ano.

Em sua estrutura, ele possui três missões principais.

1. A primeira é levar a proteção no dia-a-dia de todas as redes de defesa, e apoiar missões militares e de contraterrorismo com operações no ciberespaço.
2. A segunda é fornecer uma forma clara e responsável de mobilizar recursos financeiros para todas as operações cibernéticas militares. De forma a facilitar o levantamento desses recursos, a cadeia de comando vai do presidente dos Estados Unidos para a Secretaria de Defesa, depois para o

Comando Estratégico, e por fim para o Ciber Comando, com poucos intermediários.

3. E a terceira missão é trabalhar com uma variedade de parceiros dentro e fora do governo dos EUA. Representantes do FBI, o Departamento de Segurança Interna, o Departamento de Justiça, a Agência de Sistemas de Informação de Defesa (LYNN, 2010).

A organização consolida a maior concentração de guerreiros cibernéticos e investigadores do governo sob um único comando militar, exacerbando inclusive as preocupações de alguns especialistas com o excessivo controle militar dos sistemas de computação civis. Para 2016, o USCYBERCOM buscará ter completamente construída a nova força de missões no ciberespaço: 13 equipes nacionais com oito equipes de suporte; 27 equipes para missões de combate com 17 equipes de suporte; 18 equipes de proteção cibernética nacionais com 24 equipes de serviço; e 26 equipes de comando e informação do Departamento de Defesa (HEALEY, 2015).

Essa defesa ativa tem sido possível por meio da consolidação de capacidades de defesa cibernética coletivas do Departamento de Defesa, sob um único teto, e provendo-os com a inteligência necessária para antecipar sinais de invasões e ataques. Estabelecer essa ligação foi uma das razões mais importantes para a criação do *U.S Cyber Command*.

No mesmo ano da criação do centro, um movimento chamaria muita atenção internacional: a descoberta de um sofisticado vírus capaz de invadir e controlar sistemas industriais, responsáveis por infraestruturas críticas, o Stuxnet.

3.4 STUXNET

Em junho de 2010, uma companhia de segurança cibernética bielorrussa recebeu um chamado de um cliente, que buscava descobrir o porquê seus computadores estavam reiniciando por vezes seguidas. Um software foi encontrado, e possuía certificação digital, mostrando-se parte de uma companhia confiável. Esse fato chamou a atenção da comunidade produtora de antivírus, cujos programas automatizados de detecção não conseguiam resolver esse problema. Foi a primeira aparição do *malware* Stuxnet.

Com especialistas intrigados sob a situação, eles compartilharam as informações que descobriam sobre o assunto entre fóruns e e-mails, na tentativa de entender o que estava acontecendo. Segundo Kushner (2013), seguiu-se até que uma empresa de segurança com sede em Moscou, a Kaspersky Lab - em conjunto com outras companhias – começou a realizar a engenharia reversa do código por trás do software, encontrando certas pistas pelo caminho: número de computadores infectados, grande fração de infecções no Irã, referências aos sistemas industriais da Siemens (SCADA - *Supervisory Control and Data Acquisition)* - usados em centrais de energia. Ao mapearem o software, eles descobriram não uma, mas quatro maneiras do mesmo se espalhar entre os sistemas sem deixar qualquer rastro (conhecido como *zero-day exploits*). O software tinha o poder, quando exposto em uma instalação, de se espalhar através de *pen drives* USB, conexões integradas entre os sistemas de intranet da instalação, e até por vulnerabilidades nas redes de impressoras conectadas no local. Era um processo automatizado, um software brilhante e muito bem construído.

Na ocasião em que foi descoberto, "o Stuxnet aparentemente tinha infectado 60.000 computadores, mais da metade no Irã; outros países afetados foram a Índia, Indonésia, China, Azerbaijão, Coréia do Sul, Malásia, Estados Unidos, Reino Unido, Austrália, Finlândia e Alemanha" (FARWELL; ROHOZINSKI, 2011). Mas foi apenas no Irã que ele causou danos físicos, adentrando no controle e comando das instalações de produção de urânio do país, na cidade de Natanz, e alterando a velocidade de giro das usinas, fazendo com que as mesmas alcançassem uma rotação acima do normal cujo equipamento não tinha sido desenhado para suportar.

Segundo Roel Schouwenberg, um pesquisador sênior da equipe de Análise e Pesquisa global da Kaspersky Lab,

> Logo ficou claro, no próprio código, bem como nos relatórios de campo, que o Stuxnet foi projetado especificamente para subverter sistemas Siemens rodando centrífugas no programa nuclear de enriquecimento iraniano. Os analistas da Kaspersky então notaram que não havia objetivo de ganho financeiro. "Foi um ataque politicamente motivado. Naquele momento não havia dúvida de que este era patrocinado por um Estado", Schouwenberg afirmou. Foi um fenômeno que pegou de surpresa a maioria dos especialistas em segurança cibernética. "Somos todos engenheiros aqui, olhamos para códigos", disse o analista da Symantec O'Murchu. "Esta foi a primeira ameaça real que vimos cujas ramificações no mundo real eram políticas. (Era

> algo que tínhamos que concordar com […])"[53] (KUSHNER, 2013, tradução própria).

Ainda, segundo Schouwenberg e seus colegas da Kaspersky, ao concluírem que esse código era sofisticado demais para um grupo de *hackers* ter desenvolvido, apontaram que um time de no mínimo 10 pessoas levaram entre 2 e 3 anos para criar o Stuxnet. A questão que permanecia, quem foi o responsável?

De acordo com uma declaração feita pelo ex-analista de segurança Edward Snowden[54] ao jornal alemão *Der Spiegel*, o Stuxnet foi criado pelos EUA com o auxílio de Israel. Na entrevista ele foi perguntado se a Agência de Segurança Nacional (NSA) tinha ajudado a criar o Stuxnet. Ele respondeu: "a NSA e Israel o co-escreveram" (HAARETZ, 2013). Observando-se de um ponto de vista do direito internacional, apesar de não haver nenhuma doutrina formada sobre o assunto até o momento, de acordo com o Manual Tallinn[55], desenvolvido por um grupo de especialistas patrocinado pelo CCDCOE da OTAN, essa sabotagem constituiu em um "ato de força".

Segundo os criadores do manual: "atos que matam ou ferem pessoas, ou destroem objetos e provocam danos são inequivocamente atos de força" (TALLINN MANUAL, 2013. p. 49). Na visão dos autores, e de acordo com a carta da ONU, o uso da força é proibido, exceto em casos de legítima defesa contra um ataque iminente.

> O problema de depender das Nações Unidas é que o processo de recurso é lento, politicamente influenciável, e em grande parte inútil para lidar com ataques em tempo real. Mas isso levanta uma avenida para o debate, exposição e potencial de ação que poderia revelar-se diplomaticamente útil para problemas de longo prazo. O Irã iria concluir que o Conselho de Segurança seria de pouco valor em uma resposta para o Stuxnet. Suas chances de obter uma resolução apoiando sua posição seriam zero. A questão mais interessante é o que as nações que sustentam danos colaterais podem ser

[53] *It soon became clear, in the code itself as well as from field reports, that Stuxnet had been specifically designed to subvert Siemens systems running centrifuges in Iran's nuclear-enrichment program. The Kaspersky analysts then realized that financial gain had not been the objective. It was a politically motivated attack. "At that point there was no doubt that this was nation-state sponsored," Schouwenberg says. This phenomenon caught most computer-security specialists by surprise. "We're all engineers here; we look at code," says Symantec's O'Murchu. "This was the first real threat we've seen where it had real-world political ramifications. That was something we had to come to terms with."*

[54] Edward Snowden foi um analista de segurança da Agência de Segurança Nacional (NSA), e ficou mundialmente conhecido por vazar diversos documentos da agência, além de programas de espionagem dos EUA em 2013, em uma série de mídias internacionais como jornais e periódicos.

[55] "O Manual Tallinn sobre o Direito Internacional aplicável a guerra cibernética" é um conjunto de excertos desenvolvido por um grupo de 20 especialistas e pesquisadores, convidados pela própria OTAN, e publicado oficialmente em 2013. Segundo os próprios autores: Não é uma declaração de políticas oficiais da OTAN ou de qualquer de seus governos membros, mas reflete uma visão de consenso de um grande grupo de estudiosos e profissionais do direito, incluindo vários advogados militares seniores dos países da OTAN que participaram da elaboração do mesmo.

> capazes de obter, talvez na aplicação de pressão para aqueles que empregam ataques cibernéticos para limitar operações futuras a fim de evitar tais danos (FARWELL; ROHOZINSKI, 2011, p. 33).

Por fim, o Stuxnet é (do presente, pois o *malware* ainda existe) um sofisticado programa de computador projetado para penetrar e estabelecer controle sobre os sistemas remotos de maneira quase autônoma. Ele representa uma nova geração de *malware "fire-and-forget"* que pode ser apontado no ciberespaço contra alvos selecionados (FARWELL; ROHOZINSKI, 2011, p. 25). Seu uso foi um caso que até hoje levanta questões para especialistas de segurança e formadores de políticas, pois uma vez na Internet, o software pode ser aperfeiçoado e novamente utilizado para outros fins, que deveriam preocupar a segurança interna dos Estados no Sistema Internacional.

3.5 ATAQUES AO CANADÁ

Em janeiro de 2011, o governo canadense confirmou um extenso ciberataque contra suas agências governamentais. O ministro federal canadense da época, Stockwell Day, - juntamente com o presidente do conselho do Tesouro - disseram à imprensa que os *hackers* tentaram se infiltrar nos computadores do departamento, que supervisiona a burocracia e as operações governamentais; bem como o Departamento das Finanças, responsável pelo orçamento do governo e pelas políticas fiscais (AUSTEN, 2011). O ataque forçou o Departamento de Finanças e Tesouro a se desconectar da Internet, enquanto os oficiais de segurança localizassem os computadores infectados e removessem os softwares que comprometiam os sistemas. Além desse departamento, o setor de Pesquisa e Desenvolvimento em Defesa, que presta assistência às necessidades científicas e tecnológicas das Forças canadenses, também foi afetado. Milhares de funcionários desses departamentos ficaram em casa a fim de usar suas conexões domésticas, por um período de seis semanas, até o problema ser solucionado. Foi usada uma técnica bastante sofisticada nesses ataques.

> (Essa técnica) é chamada de "*executive spear-phishing*". Como funciona: fontes afirmaram que *hackers*, usando servidores na China, ganharam controle de um número de computadores do governo canadense pertencentes a funcionários federais de cargos superiores. Os *hackers*, em seguida, posando como os executivos federais, enviaram e-mails a funcionários

> técnicos departamentais, enganando-os ao fornecer senhas-chave de desbloqueio de acesso a redes do governo [...] Ao mesmo tempo, os *hackers* enviavam a outra equipe memorandos, aparentemente inócuos, em forma de anexo. No momento em que um anexo era aberto por um destinatário, o vírus era desencadeado na rede. O programa caçava tipos específicos de informações confidenciais da administração pública, e as enviava de volta para os *hackers* através da internet. Uma fonte envolvida na investigação disse que o *spear-phishing* é de alta simplicidade: "Não há nada de particularmente inovador sobre isso. É que é terrivelmente eficaz."[56] (WESTON, 2011, tradução própria).

As mídias canadenses reportaram, na ocasião, que o governo do país rastreou os *hackers* utilizando endereços de servidores localizados na China. Segundo Greg Weston, jornalista da CBC News canadense, o ataque proporcionou acesso a informações confidenciais. O Ministério de Relações Exteriores chinês negou que esses ataques tenham partido de redes oficiais do governo.

Segundo Michel Juneau-Katsuya, um analista de segurança e ex-oficial de inteligência da CSIS (*Canadian Security Intelligence Service*), todas as indicações apontam para a China como a origem de uma tentativa de ciber-espionagem. Ele afirmou ainda que tal ataque deve possuir alguma conexão com o governo chinês, que também é conhecido como fomentador dos então chamados “hackers patrióticos”, devotados a buscar alvos como instituições ou governos concebidos como ameaçadores ao seu (WESTON, 2011).

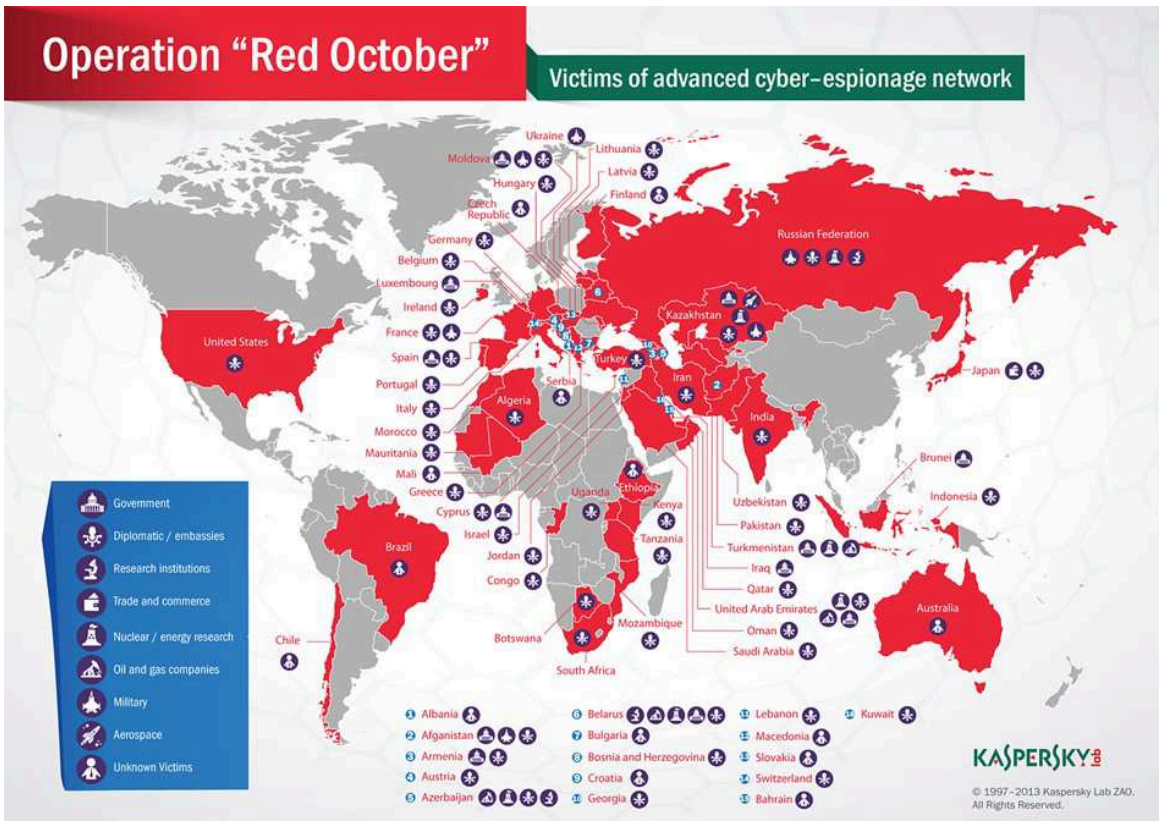
3.6 OPERAÇÃO “OUTUBRO VERMELHO”

Durante aproximadamente cinco anos, de 2007 até 2012, uma campanha de ciber-espionagem de alto nível se infiltrou com sucesso em computadores de redes diplomáticas, governos e organizações de pesquisa científicas, coletando dados e inteligência de dispositivos móveis, sistemas de computadores e equipamentos em rede. Essa ação foi descoberta pela Kaspersky Lab em outubro de 2012, cujo trabalho

[56] *...it is called "executive spear-phishing." Here's how it worked: Sources say hackers using servers in China gained control of a number of Canadian government computers belonging to top federal officials. The hackers, then posing as the federal executives, sent emails to departmental technical staffers, conning them into providing key passwords unlocking access to government networks [...] At the same time, the hackers sent other staff seemingly innocuous memos as attachments. The moment an attachment was opened by a recipient, a viral program was unleashed on the network. The program hunts for specific kinds of classified government information, and sends it back to the hackers over the internet. One source*

necessitou de alguns meses para analisar o *malware*, em que os alvos eram organizações e governos, em sua maioria da Europa Oriental em países da antiga União Soviética, além de países da Ásia Central – também afetou, de maneira menos expressiva, países da Europa Ocidental e América do Norte, como pode se observar pela imagem abaixo.

Figura 1 – Operação Outubro Vermelho



Fonte: Kaspersky Lab (2013)

O *malware* utilizava-se de vulnerabilidades em softwares da Microsoft, especificamente o MS Word e o MS Excel, e além de tradicionais alvos como estações de trabalho. O *software* malicioso era capaz de roubar dados de dispositivos móveis como *smartphones*, alterar configurações de equipamentos de rede, sequestrar arquivos de discos removíveis, roubar bancos de dados de e-mails, e desviar arquivos de redes locais nos servidores. Além disso, esse sistema criado era resistente a tentativas de ser derrubado, permitindo-se recuperar seus acessos as máquinas infectadas usando canais

involved in the investigation said spear-phishing is deadly in its simplicity: "There is nothing particularly innovative about it. It's just that it is dreadfully effective."

de comunicação alternativos. “A fim de controlar as redes das máquinas infectadas, os agressores criaram mais de 60 nomes de domínios e muitos servidores, localizados em diversos países, principalmente na Alemanha e Rússia”[57] (GREAT, 2013, p. 2, tradução própria).

Após a análise dos registros de dados, feita pela empresa Kaspersky, descobriu-se que os servidores de comando e controle e os numerosos artefatos executáveis tinham em seus nomes caracteres do alfabeto cirílico, ou seja, acredita-se que os agressores tinham como origem a língua russa. Ainda, as façanhas do software parecem ter sido criadas por *hackers* chineses. No entanto, não há evidências suficientes para confirmar que se trata de um ataque patrocinado por um Estado-Nação. A Kaspersky trabalhou em conjunto com diversas organizações internacionais como o US-CERT (*United States - Computer Emergency Response Team*), o CERT da Romênia e da Bielorrússia.

3.7 ATAQUES À CORÉIA DO SUL

Em março de 2013, uma rede de computadores da Coréia do Sul foi atingida por um *malware* chamado “DarkSeoul”, em um ataque aparentemente patrocinado pelo governo norte-coreano. As consequências foram a paralização de serviços dos três maiores bancos sul-coreanos e das três maiores emissoras, deixando a população sem acesso a saques em caixas eletrônicos, serviços de *internet banking* e sem transmissão de notícias online até o dia seguinte ao ataque. O *malware* era capaz de evadir os antivírus usados e tornar computadores inutilizáveis. No total, cerca de 32.000 computadores foram atingidos.

Segundo especialistas, os servidores cujo ataque foi gerado indicavam endereços chineses, o que levantaria a hipótese para a participação do país. No entanto, não havia evidências para comprovar essa suposição.

O movimento dos ataques ocorreu logo após a Coréia do Norte, na semana anterior, apontar como culpados a Coréia do Sul e os Estados Unidos por realizarem manobras militares na região de fronteira entre os dois países, e por derrubar alguns dos *websites* e serviços de notícias do país. A agência central de notícias norte-coreana

[57] *To control the network of infected machines, the attackers created more than 60 domain names and several server hosting locations in different countries (mainly Germany and Russia).*

KCNA afirmou, na mesma semana dos ataques, que o país "nunca vai permanecer um espectador passivo de ciberataques de inimigos, que atinge uma fase muito grave, como parte de movimentos para os sufocar" (SANG-HUN, 2013). Apesar dessa afirmação, não foi oficialmente confirmado que os ataques vieram do país.

3.8 ATAQUES AOS EUA

Em maio de 2013, um sofisticado grupo de *hackers* - aparentemente patrocinados pelo governo chinês –, realizou um ato de espionagem contra os EUA considerado como um dos mais elaborados dos últimos anos. Os alvos foram computadores de sistemas do governo e empresas do ramo de defesa norte-americano. Nessa empreitada dos *hackers*, foi adquirido acesso à informações de mais de duas dúzias de sistemas avançados de armamentos dos EUA, incluindo mísseis, jatos de combate, helicópteros e navios militares (MACASKILL, 2013).

Na semana do ataque, após a negação oficial do país sobre a participação, uma porta-voz do Ministério de Relações Exteriores chinês, Hua Chunying, declarou à imprensa americana

> A China tem repetido que de maneira resoluta se opõe a todas as formas de ciberataques […] Estamos dispostos a levar a cabo um diálogo construtivo com os EUA sobre a questão de segurança da Internet. Mas nos opomos firmemente a quaisquer acusações infundadas e especulações, uma vez que só vai prejudicar os esforços de cooperação e a atmosfera entre os dois lados a fim de fortalecer o diálogo e a cooperação[58] (SANGER, 2013, tradução própria)

Esse caso repercutiu negativamente, e fez com que o presidente Barack Obama levasse o assunto a uma reunião com o presidente chinês Xi Jinping na semana seguinte – o *US-China summit* –, criando um atrito entre as relações dos dois países.

De acordo com a jornalista Ellen Nakashima, repórter da área de segurança internacional,

---

[58] *"China has repeatedly said that we resolutely oppose all forms of hacker attacks," she said. "We're willing to carry out an even-tempered and constructive dialogue with the U.S. on the issue of Internet security. But we are firmly opposed to any groundless accusations and speculations, since they will only damage the cooperation efforts and atmosphere between the two sides to strengthen dialogue and cooperation."*

> Especialistas dizem que o ciber-roubo cria três grandes problemas. Em primeiro lugar, o acesso a projetos avançados aufere a China uma vantagem operacional imediata que pode ser explorada em um conflito. Em segundo lugar, ele acelera a aquisição de tecnologia militar avançada da China, que economiza bilhões em custos de desenvolvimento. E em terceiro lugar, os projetos dos Estados Unidos podem ser utilizados em benefício da própria indústria de defesa chinesa[59] (NAKASHIMA, 2013, tradução própria).

Ainda segundo a jornalista, o *Defense Science Board*, um grupo consultivo sênior constituído por peritos governamentais e civis, afirmou que na lista das empresas produtoras desses sistemas de defesa estão empreiteiros de alto escalão, como Boeing, Lockheed Martin, Raytheon e Northrop Grumman. Além de armamentos, amplas tecnologias foram comprometidas como um sistema de *drones* de vídeo, nanotecnologia, links de dados táticos e sistemas de guerra eletrônica – áreas que tanto o Pentágono quando os militares chineses estão investindo intensamente.

3.9 OPERAÇÃO PRISM

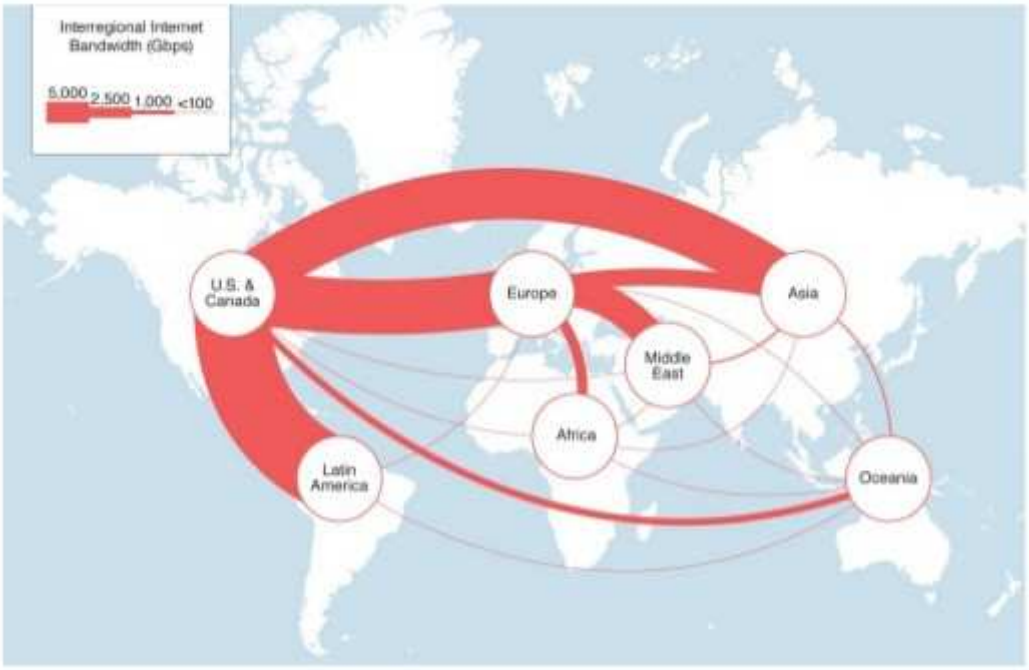
Em junho de 2013, uma semana após a revelação dos ataques aos EUA - que motivou críticas por parte dos líderes estadunidenses - o país virou réu perante a comunidade internacional. O ex-analista de segurança da NSA, Edward Snowden, divulgou documentos secretos que revelam os EUA como mantenedor de um programa de vigilância global, chamado "PRISM". O programa foi implantado em 2007 e estava cumprindo o seu 6º ano de atividades de ciber-espionagem.

Snowden, entre outras declarações, informou que a NSA mantinha operações clandestinas com alvos específicos. Ele afirmou que, como todas as comunicações globais são passíveis de atravessar pontos de concentração (figura abaixo), a maior parte delas buscava realizar o caminho mais curto entre dois pontos, passando então pelos EUA. Nessas transmissões se incluíam ligações telefônicas, e-mails e serviços de chats e VOIP (Voz por IP). No país, elas eram direcionadas através de *backdoors* para os imensos servidores da agência, localizados em Fort Meade, no estado de Maryland.

---

[59] *The experts said the cybertheft creates three major problems. First, access to advanced U.S. designs gives China an immediate operational edge that could be exploited in a conflict. Second, it accelerates China's acquisition of advanced military technology and saves billions in development costs. And third, the U.S. designs can be used to benefit China's own defense industry.*

Figura 1 – Distribuição das redes de fibra óptica internacionais (2015)



Fonte: Telegeography (2015)

Em uma dessas operações, chamada de Serviço de Coleta Especial (*Special Collection Service*), divulgou-se que ao menos trinta e cinco líderes mundiais foram espionados, incluindo os casos divulgados amplamente na mídia dos telefones da presidente Dilma Rousseff e da chanceler Angela Merkel (OPSAHL, 2013).

De acordo com Kurt Ophsahl (2013), ativista da EFF (*Electronic Frontier Foundation),* a base legal que suportava essa massiva vigilância se encontrava sob o *Foreign Intelligence Surveillance Act Amendments Act (FISAAA),* na subseção 702, de 2008[60]. Dentre as definições da FISAAA, a que chama atenção é o que o país considera como "*foreign intelligence information"*, cuja definição era apresentada na lei como sendo: ataques, terrorismo, atividades inteligência, ou tudo o que é relacionado a condução aos assuntos externos dos EUA. Uma definição, que segundo Ophsahl, "é extremamente ampla, e sugere que qualquer coisa pode ser relacionada a condução dos assuntos externos dos EUA".

[60] Lei disponível em: <https://www.congress.gov/bill/110th-congress/house-bill/6304>

A execução do programa causou preocupação e revolta da comunidade internacional. O governo chinês, além de criticar as ações, afirmou que a administração Obama é hipócrita ao repreender seu governo por cometer ciberataques, enquanto aparentemente os EUA cometem em abundância em seu próprio país. Segundo o porta-voz do Ministério de Defesa chinês, Yang Yujun

> O caso *Prismgate* (referência ao PRISM) é em si apenas como um prisma que revela a verdadeira face e a conduta hipócrita (dos EUA) sobre a Internet […] Por um lado, o abuso das vantagens da tecnologia da informação para fins egoístas, por outro, ao fazer acusações infundadas contra outros países, mostrando padrões duplos que não são de nenhuma ajuda para a paz e a segurança no ciberespaço[61] (DAVISON, 2013, tradução própria).

Barack Obama se defendeu em uma entrevista realizada com Charlie Rose pela PBS[62], em junho de 2013, afirmando que "todos os países do mundo, grandes ou pequenos, engajam-se na coleta de informações; e que é uma fonte ocasional de tensões, mas é geralmente praticada dentro de limites".

3.10 ATAQUES À ALEMANHA

Em dezembro de 2014 foi publicado um relatório anual[63] pelo Escritório Federal de Segurança de Informação alemão (*Bundesamt für Sicherheit in der Informationstechnik - BSI*). Nele continha uma informação de grande relevância, relacionada aos ciberataques destrutivos ocorridos no século XXI, mas que foi pouco difundida na mídia internacional.

Um adversário (não identificado) conseguiu acesso à rede corporativa de uma instalação de produção de aço alemã, por meio da técnica de *spear phishing*[64]. Adquirindo também acesso a rede das plantas da instalação, ele foi capaz de causar a

---

[61] *The Prismgate affair is itself just like a prism that reveals the true face and hypocritical conduct regarding Internet ... To, on the one hand, abuse one's advantages in information technology for selfish ends, while on the other hand, making baseless accusations against other countries, shows double standards that will be of no help for peace and security in cyberspace.*

[62] Entrevista disponível em: <https://www.youtube.com/watch?v=IlThTTJgKYo> Acesso em: 13 out. 2015

[63] Relatório disponível em: < https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ Lageber ichte/Lagebericht2014.pdf?__blob=publicationFile> Acesso em: 13 out. 2015

[64] Spear phishing é um golpe de e-mail direcionado com o objetivo único de obter acesso não autorizado aos dados sigilosos. Diferente dos golpes de phishing, que realizam ataques amplos e dispersos, o *spear phishing* foca em um grupo ou organização específicos. A intenção é roubar propriedade intelectual, dados financeiros, segredos comerciais ou militares e outros dados confidenciais.

falha em múltiplos componentes no sistema da fábrica. Como consequência, o processo de produção desregulou-se, e resultou em enormes prejuízos materiais. Segundo o relatório BSI: houve uma acumulação de avarias em componentes individuais do sistema de controle e de instalações inteiras; o forno era incapaz de ser desligado corretamente, o que resultou em condições inesperadas e danos físicos ao sistema.

Até então só havia sido documentado um caso de ataque em que o resultado foram danos físicos a equipamentos e instalações, o Stuxnet em 2010. Esse pode ser considerado o segundo caso de ciberataques com danos à Infraestruturas Críticas.

> A partir das informações divulgadas, podemos caracterizar e avaliar um possível perfil para o ator como um ator APT (*advanced persistent threat*) com foco em roubo de propriedade intelectual, não tendo buscado danificar o processo intencionalmente […] Nenhuma informação foi apresentada publicamente sobre as motivações do(s) agressor(es). Várias teorias podem ser tiradas incluindo sabotagem industrial para os contratos de concorrentes ou de interesses nacionais, extremistas ambientais, ou um indivíduo ou grupo testando suas capacidades e táticas se o dano físico foi intencional ou não[65] (LEE; ASSANTE; CONWAY, 2014, p. 3-5, tradução própria).

Na tentativa de encontrar mais informações sobre esse ataque, diversas mídias internacionais foram consultadas[66], mas não se obteve quem foram os responsáveis (sequer especulações foram encontradas), e com qual motivação real o ataque foi perpetrado.

3.10.1 Conclusões parciais

Para fins dessa pesquisa, foram coletados e estudados os mais diversos ataques cibernéticos que ocorreram desde 2007 até 2014. Como pode ser notado acima, há apenas uma menção ao ano de 2014, pois, mesmo que realizados massivos ataques contra grandes empresas como o banco J. P. Morgan Chase, a companhia Sony, e o site de e-commerce Ebay; de acordo com o foco dessa pesquisa, serão apenas considerados

---

[65] *From the information release if we characterize and evaluate one possible profile for the actor as an APT threat actor with a typical focus on intellectual property theft, not intentional process damage. For this reason, we can possibly consider an adversary that utilizes traditional APT tactics and tools, however their ultimate goal is beyond intellectual property theft. No information has been publicly presented on the attacker(s)' motivation. Multiple theories can be drawn including industrial sabotage for competing contracts or national interests, environmental extremists, or an individual or group testing out capabilities and tactics whether the physical damage was intended or not.*

[66] Entre as mídias pesquisadas: <https://www.rt.com/news/216379-germany-steel-plant-hack/>, <http://www.bbc.com/news/technology-30575104>, <http://blogs.wsj.com/cio/2014/12/18/cyberattack-on-german-iron-plant-causes-widespread-damage-report/> Acesso em: 13 out. 2015

ataques contra atores estatais que sejam realizados (possivelmente) por outros atores estatais.

Foi possível observar, no entanto, que desde um grande ataque em 2007 seguiram-se outros significativos ataques e invasões, e tornaram países de vários níveis de desenvolvimento alvos de vulnerabilidades. A assimetria com que o poderio cibernético se desenvolve, em relação a outras capacidades militares, é alvo de grande preocupação de estadistas e responsáveis por manter a segurança nacional dos seus respectivos países. Esses eventos mostram a fragilidade dos Estados diante das novas ameaças, que possuem caráter difuso. Muitos dos ataques possuem motivações políticas, e ataques de magnitude similar ao Stuxnet, por exemplo, poderiam gerar consequências e externalidades em diversos setores da sociedade, aumentando a animosidade entre países até escalar a um conflito maior com o uso da força militar.

Como, antes de 2007, o conhecimento disponível sobre esses fenômenos militares no meio cibernético não era muito difundido, após os ataques à Estônia, buscou-se tomar providências e iniciar debates sobre o assunto. A seguir, serão observados e analisados os resultados desses debates dentro dos EUA, seja na forma da criação de documentos e políticas com o intuito de defender o país, sejam discursos de securitização vindos dos seus governantes e chefes militares ocorridos nesse mesmo período, e buscar-se-á verificar se são ou não parte formadora de uma onda internacional a fim de securitizar a cibernética.

4. DISCURSOS DE SECURITIZAÇÃO NOS EUA

O objetivo desse capítulo final é localizar tanto os resultados institucionais, quanto os discursos que permearam os Estados Unidos da América no tocante à cibersegurança durante os anos de 2007 a 2015, realizados durante as duas administrações do presidente Barack Obama, desde seus discursos de campanha no final de 2007, até os últimos acontecimentos do seu segundo mandato correspondentes a data de realização dessa pesquisa.

Como alicerce teórico esse trabalho fez-se uso do livro "*Security: A new framework for analysis"*, dos autores Barry Buzan, Ole Waever e Jaap the Wilde (1998), delineado no capítulo primeiro deste trabalho. No entanto, vale lembrar alguns pontos específicos.

Os autores problematizam as cinco seguintes questões: 1) "O capital social do enunciador, o ator securitizador, deve estar em uma posição de autoridade" (BUZAN *et al*., 1998, p. 33, tradução própria). As análises que seguem, por decisão do pesquisador no recorte selecionado, serão focadas em um patamar macro e não em pessoas específicas. Haja vista que o objeto referente são os EUA, os atores securitizadores serão os seus estadistas e representantes de alto escalão dos governos Obama (secretário de defesa, generais de alta patente, diretores de agências de inteligência e segurança nacional). 2) "O Estado (geralmente) tem regras explícitas sobre quem pode falar em seu nome, de modo que quando o governo diz "temos de defender a nossa segurança nacional", ele tem o direito de agir em nome do Estado. O governo é o Estado nessa circunstância" (BUZAN *et al*., 1998, p. 41, tradução própria). Assim sendo, a análise será centrada nesses governantes - das últimas administrações - que comandam e coordenam o andamento do país, respondendo às atitudes alheias e a eventos internacionais nesse período considerado.

Ainda, segundo os autores, 3) "a securitização faz parte de um processo que pode ser *ad hoc* ou institucionalizado. Se um determinado tipo de ameaça é persistente ou recorrente, não há surpresa ao descobrir que a resposta e sentido de urgência tornar-se-ão institucionalizadas" (BUZAN *et al*., 1998, p. 27, tradução própria). A cibernética, como parte de um movimento maior, já observado no segundo capítulo, tem em seu âmago a evolução tecnológica do ser humano no decorrer da sua história recente. É

provável que ela será cada vez mais parte do cotidiano das relações entre indivíduos e, consequentemente, entre Estados. Dessa maneira, quando o processo de securitização se iniciar em torno da cibernética, não será apenas de maneira *ad hoc*.

> 4) Na prática, as atribuições (em torno da securitização)[67] variam substancialmente de Estado para Estado (e também ao longo do tempo). Alguns Estados irão politizar a religião (Irã, Arábia Saudita, Birmânia), e alguns não (França e Estados Unidos). Alguns vão securitizar cultura (o ex-URSS, o Irã, e outros não (Reino Unido, Países Baixos) […] Assim, a definição e critérios exatos de securitização são constituídos pelo estabelecimento intersubjetivo de uma ameaça existencial, com uma saliência suficiente para ter efeitos políticos substanciais[68] (BUZAN et al, 1998, p. 24-25, tradução própria).

No caso dos EUA, é senso comum que sua posição como superpotência militar, ao longo do último século, não foi adquirida apenas através do uso uno de relações diplomáticas. Por meio do uso da força, o país "conquistou" nesse trajeto um considerável número de comandantes irritados de países que não cultivam boas relações com os *yankees*. Haja vista que uma resposta militar contra o país demanda uma grande quantidade de recursos físicos e financeiros, difíceis de se obterem - e que a cibernética é uma maneira relativamente fácil e barata para realizar insurgência[69].

Os EUA se tornaram um país vulnerável nesse novo cenário do século XXI. Ao mesmo tempo que desenvolvem suas defesas e planejam suas ofensivas, ainda não estão prontos para uma efetiva "guerra cibernética", como será demonstrado nos documentos e discursos no decorrer do capítulo. Assim sendo, alguns desses foram realizados com o intuito de criar um "movimento de securitização", cuja eficiência ou não até o momento é difícil de ser provada, mas o que se pode verificar é que há um movimento de securitização em curso, e buscará ser elucidado a seguir.

---

[67] Nota própria.

[68] *In practice, placement varies substantially from state to state (and also across time). Some State will politicize religion (Iran, Saudi Arabia, Burma) and some will not (France, and United States). Some will securitize culture (the former URSS, Iran) and some will not (the UK, the Netherlands) […] Thus, the exact definition and criteria of securitization is constituted by the intersubjective establishment of an existential threat with a saliency to have substantial political effects.*

[69] Um exemplo real, nos últimos anos, deriva da difusão do grupo terrorista Estado Islâmico, cuja tentativa de criar um Califado no Oriente Médio almeja também táticas para o meio online, por meio do que alguns insurgentes chamam de "ciber-califado". Mais informações sobre o assunto: <http://www.theguardian.com/world/2015/apr/12/isis-cyber-caliphate-hacking-technology-arms-race> Acesso em: 30 out. 2015

Por fim, é importante pontuar o método proposto pelos autores - e utilizado nessa pesquisa - ao desenvolverem esse paradigma, e que será aplicado no decorrer desse capítulo.

> 5) Como devemos estudar os casos? O método mais óbvio é através de análise de discursos, desde que estamos interessados em quando, como e por quem algo foi estabelecido como uma ameaça à segurança. O critério para definição de segurança é textual: uma estrutura retórica específica que tem de ser localizada no discurso. Não vamos usar nenhuma técnica sofisticada de linguística ou quantitativa […] A técnica é simples: ler, buscando por argumentos que levam a formas retóricas e lógicas de definir algo como um assunto de segurança[70] (BUZAN et al, 1998, p. 176-177, tradução própria).

Antes de iniciar a exposição dos discursos em torno da cibernética, segue um breve histórico com o intuito de permear como foi realizada a inclusão da cibernética na agenda de segurança dos EUA e, consequentemente, na agenda global.

4.1 BREVE HISTÓRICO

Segundo Myriam Dunn Cavelty (2014), as características da cibernética como "*policy issue*" surgiram nos EUA nos anos 1970, foram impulsionadas durante os 1980, e espalharam-se para outros países na segunda metade dos anos 1990.

> Desde o início, os projetistas das redes globais priorizaram a robustez e capacidade de sobrevivência sob a segurança, já que não havia aparente necessidade de uma atenção especial à segurança nessa época, quando os sistemas de informação estavam sendo hospedados em grandes máquinas que estavam conectadas a alguns poucos computadores. [...] Em meados dos anos 1990, tornou-se claro que os setores-chave da sociedade moderna, incluindo aqueles vitais para a segurança nacional e para o funcionamento essencial das economias (pós) industrializadas contavam com um espectro, de alta interdependência nacional e internacional, de sistemas de controle baseados em software para o seu bom funcionamento de maneira confiável e contínua. O novo **objeto referente** que emergiu foi a totalidade de **infraestruturas críticas (da informação)** que fornecem o modo de vida, e que caracteriza as nossas sociedades. Este é o contexto em que a maioria das políticas de cibersegurança emergiram[71] (CAVELTY, 2014, tradução e grifo próprio).

---

[70] *How should we study our cases? The obvious method is discourse analysis, since we are interested in when and how something is established by whom as a security threat. The defining criterion of security is textual: a specific rhetorical structure that has to be located in discourse […] The technique is simple: Read, looking for arguments that take the rhetorical and logical form defined here as security.*

[71] *From the very beginning, the network designers emphasized robustness and survivability over security, since there was no apparent need for a specific focus on security at that time, when information systems were being hosted on large proprietary machines that were connected to very few other computers. […] In the mid-1990s, it became clear that key sectors of modern society, including those vital to national security and to the essential functioning of (post-)industrialized economies, had come to rely on a spectrum of highly interdependent national and international software-based control systems for their smooth, reliable, and continuous operation. The new referent object that emerged was the totality of*

Essa emergência segue uma linha cronológica, e dois importantes pontos de inflexão nos anos 2000, em relação a relevância da cibernética para a agenda de segurança dos EUA, foram: 1) os acontecimentos de 11 de setembro de 2001; e 2) os eventos na Estônia em 2007.

Em relação ao "11/09", pode-se dizer que foi o primeiro momento em que a segurança em torno da cibernética foi cogitada para a agenda de segurança dos EUA.

> Quem, então, ajudou a colocar a segurança cibernética na agenda política nacional? Quem foram os agentes que conceberam? No contexto do debate sobre o novo "terrorismo internacional" e o outro novo medo na política de pensamento em segurança - "guerra assimétrica" - o conceito de "segurança nacional" ou "defesa da pátria" 'foi desenvolvido por *think tanks* americanos no final de 1990. A ideia básica era o fim da invulnerabilidade americana baseada em sua posição geográfica especial [...] Na verdade, a ideia de segurança interna, incluindo a proteção contra o ciberterrorismo, foi retomada pelo novo governo sob George W. Bush, em Maio de 2001 [...] Um projeto de lei na Câmara dos Representantes faria o Congresso dos Estados Unidos declararem ciberterrorismo "uma ameaça emergente para a segurança nacional dos Estados Unidos"[72] (GIACOMELLO; ERIKSSON, 2007, tradução própria).

Entre as consequências que seguiram os atentados, além do ciberterrorismo, foi o surgimento de demandas para unificar 22 entidades federais com propósitos similares de proteger a segurança interna do país. Desse modo, foi fundado o Departamento de Segurança Interna (*Departament of Homeland Security - DHS*), ratificado pelo presidente George W. Bush em 25 de novembro de 2002. Uma das atribuições dadas ao secretário do DHS em relação ao ciberespaço a época foi de "desenvolver um plano nacional para assegurar recursos chaves e a infraestrutura crítica dos Estados Unidos" (WHITE HOUSE, 2003). Surgiu, assim, a Estratégia Nacional para Segurança do Ciberespaço (*National Strategy to Secure Cyberspace*), em 2003. Dessa maneira, o DHS se tornaria o primeiro centro federal de excelência para a segurança cibernética e seria um ponto focal da administração federal sob estados, cidades, organizações governamentais, setor privado, academia e para a população. Ao propor essa estratégia,

---

critical (information) infrastructures that provide the way of life that characterizes our societies. This is the context in which most cyber-security policies emerged.

[72] *Who, then, helped to put cybersecurity on the national policy agenda? Who were the framing agents? In the context of the debate about the new 'international terrorism' and the other new fear in security policy thinking – 'asymmetric warfare' – the concept of 'homeland security' or 'homeland defense' was developed by American think tanks in the late 1990s. The basic idea was the end of the American invulnerability based on its special geographical position [...] Indeed, the idea of homeland security, including protection against cyberterrorism, was taken up by the new government under George W. Bush*

o governo federal lançou em 2002 um rascunho online para avaliação de indivíduos e instituições, cujo objetivo era "elevar o nível de conscientização sobre a importância da segurança cibernética" (WHITE HOUSE, 2003, p. 2). Nas semanas que seguiram o lançamento desse rascunho, o Congresso norteamericano passou uma lei pública (nº 107-305)[73], posteriormente ratificada pelo presidente, chamada *Cyber Security Research and Development Act.* Seu objetivo era "um esforço ao longo dos próximos anos em criar ciber-tecnologias mais seguras, expandir a pesquisa e desenvolvimento sob a segurança cibernética, e melhorar a força de trabalho na área" (WHITE HOUSE, 2002, p. 2). Esses foram os primeiros impulsos em torno de criar um "movimento de securitização" da cibernética no país.

O próximo ponto de continuidade, sob a perspectiva institucional, foi com a criação do *Comprehensive National Cyber Initiative (CNCI)*, resultado parcial dos eventos ocorridos contra a Estônia em 2007 e contra o Pentágono em 2008, já descritos no capítulo anterior.

4.2 INSTITUCIONALIZAÇÃO DA CIBERNÉTICA

Como resultados dos eventos internacionais ocorridos no período de 2007 a 2015, vamos apontar a seguir as iniciativas da administração federal em fomentar a institucionalização da cibernética nos EUA. Serão apresentadas ações, algumas exclusivas em torno desse ponto, outras integradas a iniciativas militares mais amplas.

4.2.1 *Comprehensive National Cybersecurity Initiative* (CNCI)

Uma iniciativa do final do segundo mandado do presidente norte-americano George W. Bush, em janeiro de 2008, foi a *Comprehensive National Cybersecurity Initiative.* O CNCI tem por objetivo estabelecer a política, estratégia e diretrizes para proteger os sistemas federais […] além de delinear uma abordagem que antecipa futuras ameaças e tecnologias, e exige do governo federal a interação entre suas capacidades técnicas e organizacionais, a fim de melhor atender as sofisticadas ameaças e

in May 2001 [...] A bill in the House of Representatives that would make the United States Congress declare cyberterrorism "an emerging threat to the national security of the United States"

[73] Lei disponível para consulta em: <http://www.gpo.gov/fdsys/pkg/PLAW-107publ305/pdf/PLAW-107publ305.pdf> Acesso em 05 nov. 2015

vulnerabilidades (ROLLINS; HENNING, 2009). Seu intuito é o de responder aos iminentes ataques que estavam ocorrendo ao redor do mundo com uma abordagem promovida pelo governo federal dos EUA, com a finalidade de identificar e se proteger de ciberameaças correntes e emergentes no Sistema Internacional.

Dando continuidade a iniciativa de Bush, o então presidente Barack Obama iniciou, em fevereiro de 2009, uma revisão interagências na área de segurança cibernética a fim de desenvolver um quadro estratégico para assegurar que o CNCI fosse apropriadamente integrado e coordenado com o congresso, e recebesse os recursos devidos. Segundo um relatório da comissão do *Center for Strategic and International Studies* para a 44º presidência dos EUA (2008), a cibersegurança ficou conhecida como "um dos mais urgentes problemas de segurança nacional da nova administração"[74]. Barack Obama, durante sua campanha, prometeu "fazer da cibersegurança uma prioridade alta, tal como deveria ser no século XXI […] e eleger um conselheiro nacional de cibersegurança que o reporte diretamente"[75].

Segundo John Rollins, especialista em terrorismo e segurança nacional, e Anna C. Henning, procuradora do legislativo norte-americano,

> O foco do novo governo sobre a segurança cibernética continuará com sua ênfase nos recentes assuntos sobre a questão no poder executivo e no legislativo. Esse foco recente surgiu em parte como **resposta a eventos como os ataques de hackers estrangeiros contra a rede de computadores do Pentágono e da ciberguerra contra a Estônia**, que recebeu significativa atenção da mídia. Relatórios de agências de um grande número de tentativas de infiltração no ciberespaço governamental também levaram a ação. Ambos os ataques de alto perfil e mais infiltrações de rotina lançaram luz sobre a **vulnerabilidade** das **infraestruturas de informação críticas.** Por exemplo, a *Defense Science Board* observou que a "infraestrutura de informação do exército norte-americano é o calcanhar de Aquiles de nosso poderio militar esmagador" (ROLLINS; HENNING, 2009, p. 2, tradução e grifo próprio).[76]

---

[74] Informação disponível em: http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf Acesso em: 07 nov. 2015

[75] Discurso proferido dia 17 de julho de 2008 na Universidade Purdue.

[76] "*The new administration's focus on cybersecurity would continue recent emphasis on the issue by the executive and legislative branches. This recent focus emerged partly in response to events such as attacks by outside hackers against a Pentagon computer network and the CyberWar against Estonia, which garnered significant media attention. Agency reports of large numbers of attempts to infiltrate government cyberspace have also prompted action. Both the high-profile attacks and more routine infiltrations have shed light on the vulnerability of critical information infrastructures. For example, the Defense Science Board noted that the U.S. military's information infrastructure is the "Achilles' heel of our otherwise overwhelming military might".*

Em janeiro de 2009 o ex-Diretor Nacional de Inteligência (DNI), Mike McConnell, equiparou as "armas cibernéticas" as "armas de destruição em massa", expressando preocupação sobre o uso por terroristas da tecnologia para degradar a infraestrutura do país[77]. Seu sucessor, Dennis Blair, ofereceu no mesmo ano a seguinte declaração para o Comitê de Inteligência do Senado.

> A crescente conectividade entre sistemas de informação, a Internet e outras infraestruturas cria oportunidades para os ofensores romperem telecomunicações, redes de energia elétrica, dutos de energia, refinarias, redes financeiras e outras infraestruturas críticas. Ao longo dos últimos anos, temos visto ataques cibernéticos contra infraestruturas críticas no exterior, e muitas das nossas próprias infraestruturas são tão **vulneráveis** quanto as estrangeiras. Um ataque bem-sucedido contra um grande prestador de serviços financeiros poderia afetar seriamente a economia nacional, enquanto ataques cibernéticos contra sistemas de computadores responsáveis por infraestruturas físicas, como as que controlam redes de energia ou refinarias de petróleo têm o potencial de interromper os serviços por horas, ou até semanas[78] (BLAIR, 2009, grifo próprio).

Além de promover uma estratégia nacional, focando em um aspecto intraestatal, os EUA inovaram ao lançar a "Estratégia Internacional para o Ciberespaço", momento em que apresentou para sua população e para o exterior quais são os princípios que o país defenderá internacionalmente, e será melhor delineada a seguir.

4.2.2 *International Strategy for Cyberspace* (ISFC)

A Estratégia Internacional para o Ciberespaço (*International Strategy for Cyberspace – ISFC*) é uma iniciativa, por parte da administração do presidente Barack Obama, de promover os Estados Unidos como um formador de políticas que possam ser aplicadas no ciberespaço, em uma tentativa de buscar cooperação internacional ao desenvolver não só uma estratégia, mas uma agenda em torno da cibernética no sistema internacional. Ela foi apresentada em maio de 2011 através de um documento de consulta pública[79] pelo ex-coordenador de cibersegurança da Casa Branca, Howard Schmidt.

---

[77] Entrevista disponível no *The Charlie Rose Show*, realizada pelo canal PBS em 8 de janeiro de 2009.
[78] Audiência sobre ameaças à nação do *Annual Threat Assessment of the Intelligence Community, Senate Select Committee on Intelligence*, nº 111 (12 de fevereiro de 2009). Disponível em: <http://www.intelligence.senate.gov/hearings/open-hearing-current-and-projected-threats-united-states> Acesso em: 07 out. 2015.
[79] Disponível em: <https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>. Acesso em: 07 out. 2015.

No evento de lançamento, Howard comentou quais eram as intenções dessa nova política.

> A estratégia internacional estabelece a visão do Presidente para o futuro da Internet, e estabelece uma agenda para a parceria com outras nações e povos a fim de alcançar essa visão […] os Estados Unidos irão construir um ambiente internacional ao garantir que as redes mundiais estejam abertas a inovações, interoperáveis em todo o mundo, seguras o suficiente para apoiar o trabalho das pessoas e confiáveis o suficiente ganhar suas confianças. Para conseguir isso, vamos construir um ambiente em que as normas de ações responsáveis guiem o comportamento dos Estados, mantenham parcerias e apoiem o Estado de Direito […] Essa Estratégia Internacional é maior do que qualquer departamento ou agência. É uma base sólida para as diversas atividades que serão realizadas em todo nosso governo. É sobre os princípios que unem nossa nação, a visão que une nossa política e as prioridades que unem nosso governo […] Com os nossos parceiros em todo o mundo, vamos trabalhar para criar um futuro para o ciberespaço que promova a prosperidade, aumente a segurança e salvaguarde a abertura em nosso mundo conectado. Este é o futuro que buscamos, e nós convidamos todas as nações e povos para se juntar conosco nesse esforço[80] (SCHMIDT, 2011, tradução própria).

Segundo Barack Obama, "ela (a estratégia) fornece o contexto para os nossos parceiros em casa e no exterior de nossas prioridades, e como podemos nos unir para preservar o caráter do ciberespaço e reduzir as ameaças que enfrentamos […] Juntos, podemos construir um futuro para que o ciberespaço seja aberto, interoperável, seguro e confiável" (WHITE HOUSE, 2011). Segundo James A. Lewis, procurador do país, "esse documento serve para sinalizar a outros países que os Estados Unidos querem apenas colaborar na segurança das redes, e não as dominar" (NAKASHIMA, 2011).

No mesmo ano de lançamento da Estratégia Internacional, Schmidt disse que os EUA instam a mais países para assinarem a um tratado - que possui mais de 10 anos de existência - chamado *Budapest Convention on Cybercrime*. O tratado apela para a cooperação em crimes cometidos através da Internet, e já foi ratificado por 30 países,

---

[80] *The International Strategy lays out the President's vision for the future of the Internet, and sets an agenda for partnering with other nations and peoples to achieve that vision [...] the United States will build an international environment that ensures global networks are open to new innovations, interoperable the world over, secure enough to support people's work, and reliable enough to earn their trust. To achieve it, we will build and sustain an environment in which norms of responsible behavior guide states' actions, sustain partnerships, and support the rule of law [...] The International Strategy is larger than any one department or agency. It is a strong foundation for the diverse activities we will carry out across our entire government. It is about the principles that unite our nation, the vision that unites our policy, and the priorities that unite our government. [...] With our partners around the world, we will work to create a future for cyberspace that builds prosperity, enhances security, and safeguards openness in our networked world. This is the future we seek, and we invite all nations, and peoples, to join us in that effort.*

incluindo os EUA e outros 29 países europeus - signatários incluem o Reino Unido, Canadá e Turquia. A China e a Rússia estão entre as nações que ainda não assinaram. Assim sendo, é possível apontar para um claro esforço em que os EUA buscam angariar nações, encorajar comportamentos responsáveis, e enfatizar oposição aos que "pretendem desmantelar redes e sistemas". Entretanto, ao usarem amplamente o termo "*malicious actors*" nas fontes consultadas, a fim de denominar os opositores ao *status quo* sugerido pelos EUA, o país acaba gerando desconfiança por parte da comunidade internacional.

Segundo Adam Segal (2011), pesquisador sênior em Estudos sobre a China e especialista em cibersegurança do *Council on Foreign Relations* (CFR), a China recebeu com ceticismo essa nova estratégia proposta pelos EUA. Ele comentou que as preocupações chinesas giram em torno de três questões: 1) Que a estratégia é realmente sobre as capacidades militares e de dissuasão, e não sobre o ciberespaço ser um grande "mercado" para os EUA. 2) Que, apesar dos apelos de cooperação, os EUA estão tentando manter sua liderança e exclusividade no controle da tecnologia na rede mundial, e insistem em possuir alguns dos núcleos de controle do ciberespaço sob seu território. 3) Que o impulso para enfatizar a "liberdade na internet", ao ser usado em uma agenda para pressionar outros países, é um tema que poderá levar a mais conflitos que soluções.

Mesmo com contradições, foi alcançado um significativo progresso. Em 07 de junho de 2013, um grupo de peritos governamentais da ONU - responsáveis pelo desenvolvimento no campo da informação e das telecomunicações, em um contexto sobre a Segurança Internacional que inclui China, Índia, Russa e os Estados Unidos – chegaram em um consenso sobre o princípio geral de que "as leis internacionais, em particular a Carta da ONU, podem ser aplicadas ao ciberespaço"[81]. É considerado um marco quando pela primeira vez que a China, em particular, concordou que normas do Direito Internacional se apliquem ao ciberespaço.

Voltando o foco ao âmbito interno dos EUA, a próxima seção discutirá um documento publicado periodicamente pelo comando militar do país, chamado de Estratégia Militar Nacional.

[81] Consenso disponível em: <http://www.state.gov/r/pa/prs/ps/2013/06/210418.htm> Acesso em 18 out. 2015

4.2.3 *National Military Strategies* (NMS)

A Estratégia Militar Nacional (*National Military Strategy – NMS*) trata-se de um documento produzido pelo *Chairman of the Joint Chiefs of Staff* (CJCS), o oficial militar de maior patente das forças armadas dos Estados Unidos. De um modo geral, o documento propõe a organização dos meios, formas, e fins militares alicerçados às metas, mais amplas, das políticas da administração nacional. O NMS deve fornecer uma descrição do ambiente estratégico e as oportunidades e desafios que afetam os interesses nacionais dos Estados Unidos e de sua segurança nacional. Ela deve descrever as ameaças regionais mais significativas aos interesses nacionais e de segurança do país, bem como as ameaças causadas pelo terrorismo internacional, as armas de destruição em massa, e os desafios assimétricos.

O relatório produzido pela NMS também inclui uma avaliação da natureza e da magnitude dos riscos estratégicos e militares associados à execução bem-sucedida das missões previstas pela estratégia. O CJCS examina os pressupostos relativos à prontidão das forças (ativas e de reserva), a duração do conflito e o nível de intensidade das operações de combate, além dos níveis de apoio dos aliados e de outras nações amigas.

Para a análise serão consideradas as transformações ocorridas desde a primeira publicação em 1991 até 2015 (foram seis edições até o momento), cujo foco estará na observação da evolução da cibernética como assunto da agenda de segurança do país, sendo as referências mais importantes as duas últimas edições do NMS (em 2011 e 2015).

Nas publicações dos anos 90, em 1991[82], 1995[83] e 1997[84] respectivamente, em uma análise aos documentos oficiais das NMS, não houve nenhuma menção ao prefixo "*cyber*" ou mesmo ao termo "*Internet*". Dessa maneira, conclui-se que naquela década ainda não tinha sido assimilado pelos sistemas militares dos EUA quaisquer movimentos militares que se utilizassem da cibernética como meio, e justificassem sua inclusão às estratégias desenvolvidas. A única menção que poderia ser considerada como relevante foi encontrada no documento de 1997, que tratou de desafios assimétricos (*asymmetric challenges*). Um dos excertos fez referência as "cartas

[82] Disponível em: <https://fas.org/man/docs/918015-nss.htm> Acesso em 18 out. 2015
[83] Disponível em: <https://fas.org/man/docs/nms_feb95.htm> Acesso em 18 out. 2015
[84] Disponível em: <http://www.au.af.mil/au/awc/awcgate/nms/index.htm> Acesso em 18 out. 2015

curinga" (*wild cards*), ou seja, uma demonstração da incerteza quanto aos desafios que poderiam surgir nos próximos anos.

> Uma série de ameaças "curingas" poderiam surgir para colocar os interesses dos EUA em risco. Tais ameaças vão desde o surgimento de novas tecnologias que neutralizam algumas de nossas capacidades militares […] Agindo em conluio com outras entidades hostis, por exemplo, um adversário pode tentar combinar vários meios assimétricos com a apreensão de um objetivo estratégico antes que possamos responder. […] Isso poderia prejudicar gravemente a credibilidade dos EUA, seu acesso e influência no mundo. O ambiente estratégico que enfrentamos é complexo, dinâmico e incerto[85] (NMS, 1997, tradução própria).

Já no documento correspondente a NMS de 2004[86] já é possível encontrar algumas menções ao prefixo "*cyber*". No entanto, nessas ocasiões as referências são para o termo "*cyberspace*", representado como um "novo foco de transformação", em que o Departamento de Defesa dos EUA deveria prestar atenção nos próximos anos. Segundo o documento, "o Departamento deve trabalhar para garantir o acesso estratégico para regiões-chave, linhas de comunicação e bens comuns globais em águas internacionais, como o domínio aéreo, espacial e o ciberespaço" (NMS, 2004). Contudo, não se observou nenhuma atenção especial ao assunto, ao mesmo tempo que não se propôs quais iniciativas devem ser tomadas, ou mesmo como será trabalhada essa estratégia relativa ao ciberespaço.

O ponto de inflexão fica por conta dos dois últimos documentos apresentados, a NMS de 2011 e a de 2015. Somente o prefixo "*cyber*" aparece num total de 45 vezes entre os dois documentos, sendo a maioria delas no documento de 2011. O tratamento que é dado ao assunto é muito mais aprofundado, inclusive com seções específicas tratando do assunto.

No documento de 2011[87], em uma seção de "bens comuns e domínios globalmente conectados", sugere-se que o "domínio do espaço e o ciberespaço são

---

[85] *A number of "wild card" threats could emerge to put US interests at risk. Such threats range from the emergence of new technologies that neutralize some of our military capabilities [...] Acting in collusion with other hostile entities, for example, an adversary might attempt to combine multiple asymmetric means with the seizure of a strategic objective before we could respond [...] This could critically undermine US will, credibility, access, and influence in the world. The strategic environment facing us is complex, dynamic, and uncertain.*

[86] Disponível em: <http://archive.defense.gov/news/Mar2005/d20050318nms.pdf> Acesso em 20 out. 2015

[87] Disponível em: <http://www.defense.gov/Portals/1/Documents/pubs/2011-National-Military-Strategy.pdf> Acesso em 20 out. 2015

simultaneamente os mais críticos para as operações militares, e ainda os mais vulneráveis para ações maliciosas" (NMS, 2011. Pág. 3). Ainda, comenta-se que o "acesso conjunto e garantido aos bens comuns globais e ao ciberespaço constituem um aspecto central da segurança nacional dos EUA, e continua a ser uma missão permanente para a força conjunta do país […] que terá um papel importante nos esforços internacionais para garantir acesso, supervisão e responsabilidade, e promover normas nos bens comuns globais e no ciberespaço" (NMS, 2011, p. 9, tradução própria). Há, inclusive, uma seção específica para o assunto, como segue abaixo.

> Ciberespaço - As capacidades sob o ciberespaço habilitam comandantes para operarem de forma eficaz em todos os domínios. O Comando Estratégico e o Ciber Comando dos EUA (USCYBERCOM) irão colaborar com as agências do governo, entidades não-governamentais, industrias e entidades internacionais a fim de desenvolver novas normas cibernéticas, capacidades, organizações e habilidades. No caso de uma ciber intrusão em larga escala ou de um ciberataque debilitante ocorrerem, devemos fornecer uma ampla gama de opções para garantir nosso acesso e utilização ao domínio do ciberespaço, e aplicar a responsabilidade aos atores maliciosos. Devemos buscar ações executivas e do Congresso a fim de prover novas autoridades e permitir uma ação eficaz no ciberespaço[88] (NMS, 2011, p. 10, tradução própria).

Ainda no mesmo documento, há uma seção sobre "desafios transnacionais", em que a "ciber-agressão" é associada como um dos desafios de segurança transnacionais que cabe aos EUA mostrar iniciativa e auxiliar no combate. Por fim, são propostas em quais áreas em que as forças conjuntas do país devem "projetar o seu poder globalmente", sendo uma delas o ciberespaço. "As forças conjuntas vão garantir o domínio ".mil", exigindo uma arquitetura resiliente para o Departamento de Defesa, que empregará uma combinação de detecção, dissuasão, negação e defesa em várias camadas" (NMS, 2011, p. 19, tradução própria).

É com surpresa, no entanto, que se observou uma menor incidência de menções do prefixo "*cyber*" no documento de 2015[89] se comparado ao de 2011. Porém, nesse documento mais recente, há uma maior variedade no uso proposto ao prefixo. Exemplos

---

[88] *Cyberspace – Cyberspace capabilities enable Combatant Commanders to operate effectively across all domains. Strategic Command and Cyber Command will collaborate with U.S. government agencies, nongovernment entities, industry, and international actors to develop new cyber norms, capabilities, organizations, and skills. Should a large-scale cyber intrusion or debilitating cyber-attack occur, we must provide a broad range of options to ensure our access and use of the cyberspace domain and hold malicious actors accountable. We must seek executive and Congressional action to provide new authorities to enable effective action in cyberspace.*

[89] Disponível em: <http://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf> Acesso em 15 out. 2015

são: "*cyberattacks", "cyber tools", "cyber realm", "cyber security", "cyber systems", "Cyber Mission Force", "cyber capabilities"*. Segue um excerto da seção "deter, negar e derrotar adversários estatais".

> Dissuadir um ataque direto contra os Estados Unidos e nossos aliados é uma missão prioritária, exigindo defesas internas e regionais, aliadas a fim de assegurar capacidades contra ataques convencionais e nucleares. As forças estratégicas dos EUA permanecem sempre prontas. As defesas militares dos EUA são reforçadas pelo Acordo Norteamericano de Defesa e Comando Aeroespacial com o Canadá, e uma estreita cooperação com o Departamento de Segurança Interna. Essas parcerias de segurança interna são complementadas por investimentos crescentes no domínio cibernético projetado para proteger redes e infraestruturas vitais[90] (NMS, 2015, p. 7, tradução própria).

A ênfase proposta nessa última NMS foi sobre a proteção de sistemas cibernéticos e o desenvolvimento de capacidades militares na área. Uma novidade em relação ao documento anterior é a *Cyber Mission Force*, um novo plano proposto em uma outra estratégia, específica do Departamento de Defesa dos EUA, e que será melhor descrita a seguir.

4.2.4 *Department of Defense Cyber Strategy* (DODCS)

Em abril de 2015 foi apresentada, pela Secretaria de Defesa dos EUA, a Ciber Estratégia do Departamento de Defesa dos EUA (*Department of Defense Cyber Strategy – DoDCS*); a segunda de sua linha, pois uma primeira teria sido publicada em 2011 sob um diferente nome, "*Department of Defense Strategy for Operating in Cyberspace*[91]".

O esforço do Departamento na elaboração dessa nova Estratégia iniciou em 2013. Ainda em 2011, durante a primeira edição, a dependência do país do ciberespaço para suas operações levou a Secretaria da Defesa declarar oficialmente o "ciberespaço como um domínio operacional para fins de organizar, treinar e equipar as forças militares dos EUA" (DODCS, 2015, p. 4, tradução própria). A documento atual possui

---

[90] *Deterring a direct attack on the United States and our allies is a priority mission, requiring homeland and regional defenses tied to secure conventional and nuclear strike capabilities. Thus U.S. strategic forces remain always ready. U.S. military defenses are enhanced by our North American Aerospace Defense Command Agreement with Canada and close cooperation with the U.S. Department of Homeland Security. These homeland defense partnerships are complemented by growing investments in the cyber realm designed to protect vital networks and infrastructure.*

[91] Disponível para consulta em: <http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf> Acesso em 25 nov. 2015

três missões em destaque: defender as redes, sistemas e informações do Departamento; defender a segurança interna dos EUA e os seus interesses nacionais contra ciberataques; prestar suporte operacional e planos de contingência.

> Essa nova estratégia estabelece metas e objetivos prioritários para as atividades e missões do Departamento de Defesa alcançarem ao longo dos próximos cinco anos. Centra-se na criação de capacidades para operações de segurança cibernética eficazes ao ponto de defenderem a nação contra ciberataques de significativa consequência; e apoiam os planos operacionais e de contingência. Essa estratégia se baseia em decisões anteriores sobre o desenvolvimento da *Cyber Mission Force* e da *Cyber Workforce,* e fornece novas e específicas orientações a fim de mitigar riscos previsíveis e buscar oportunidades para fortalecer a segurança nacional dos EUA[92] (DODCS, 2015, p. 3, tradução própria).

A *Cyber Mission Force* (CMF) terá um papel único no Departamento de Defesa. Sua criação iniciou em 2012 com o intuito de prestar suporte a ciber-missões. Na CMF estão sendo formados 133 times com mais de 6000 ciber-operadores, com prazo final para 2018, em um investimento aproximado de 2 bilhões de dólares. Segundo uma audiência veiculada em 26 de fevereiro de 2015 pelo Subcomitê de Forças Estratégicas sobre o Orçamento Fiscal de 2016[93], até o momento foram atingidos 50% desse objetivo, com a formação de 58 times e um total de 3100 operadores qualificados. Será dividida e alinhada da seguinte maneira:

> As Forças de Ciber-Proteção irão aumentar as medidas defensivas tradicionais e defender as redes e os sistemas do Departamento de Defesa contra ameaças prioritárias; As Forças de Missão Nacionais e suas equipes de suporte irão defender os Estados Unidos e seus interesses contra ciberataques que possuam consequências significativas; As Forças de Missão em Combate suas equipes de suporte apoiarão os comandos de combate, gerando efeitos integrados no ciberespaço em suporte a planos operacionais e de contingência. Ainda, comandos de combate integram a Forças para Ciber-Missões e os Times de Ciber-Proteção em planos e operações e os empregam no ciberespaço, enquanto a Forças de Missão Nacionais operam sob o comandante da USCYBERCOM[94] (DODCS, 2015, p. 6, tradução própria).

---

[92] *This new strategy sets prioritized strategic goals and objectives for DoD's cyber activities and missions to achieve over the next five years. It focuses on building capabilities for effective cybersecurity and cyber operations to defend DoD networks, systems, and information; defend the nation against cyberattacks of significant consequence; and support operational and contingency plans. This strategy builds on previous decisions regarding DoD's Cyber Mission Force and cyber workforce development and provides new and specific guidance to mitigate anticipated risks and capture opportunities to strengthen U.S. national security.*

[93] Disponível em: <http://fas.org/irp/congress/2015_hr/stratfor.pdf> Acesso em 08 nov. 2015

[94] *Cyber Protection Forces will augment traditional defensive measures and defend priority DoD networks and systems against priority threats; National Mission Forces and their associated support teams will defend the United States and its interests against cyberattacks of significant consequence; and Combat Mission Forces and their associated support teams will support combatant commands by generating integrated cyberspace effects in support of operational plans and contingency operations.*

A CMF é uma força que projetará os EUA com características defensivas e ofensivas no cenário internacional da cibernética, e objetiva ser a base operacional para que se cumpram todas as estratégias propostas pelo país ao longo dos últimos anos, reestruturando as forças de trabalho civis e militares, e as infraestruturas disponíveis para a realização das missões.

Ainda, durante a análise do documento oficial da Estratégia, uma passagem mereceu atenção especial. O documento fez uma comparação entre as forças militares do país durante a Guerra Fria e as forças atuais. Foi observado que as forças de hoje estão acostumadas com o constante acesso às informações e comunicações, de uma maneira ágil e mecânica, e foi recordado que na Guerra Fria existiam diversas operações com ambientes criados em que a comunicação era inacessível, pois na época a possibilidade de uma interrupção pelas capacidades de um adversário parecia mais cogitada e parte da realidade.

Nessa cultura de resiliência das novas gerações com a tecnologia, as forças não são mais capazes de operar sem as ferramentas de acesso imediato às comunicações e à informação instantânea, se comparadas às da época. Isso se torna uma grande vulnerabilidade para o país, e a retomada a essas operações é vista como uma missão a ser cumprida. Ainda assim, a referência feita ao "cenário da Guerra Fria" infere um discurso em que certas possibilidades são "postas a mesa", e os acontecimentos em curso corroboram um cenário conturbado no ciberespaço como possível para o futuro próximo.

Na conclusão do documento oficial, um excerto causou impacto e de certa forma auxilia a fortalecer o objetivo dessa pesquisa, e confirmar que os discursos em relação a securitização da cibernética estão se tornando cada vez mais acalorados.

> "Somos **vulneráveis** no ciberespaço, e a escala da **ameaça cibernética** requer **ações urgentes** por líderes e organizações em todo o governo e o setor privado [...] Esta estratégia apresenta um **plano agressivo**, específico para alcançar a mudança [...] O sucesso requer uma estreita colaboração entre o Departamento de Defesa, entre as agências do governo dos EUA, com o setor privado, e com aliados e parceiros norte-americanos"[95] (DODCS, 2015, p. 33, tradução e grifo próprio).

Combatant commands integrate Combat Mission Forces and Cyber Protection Teams into plans and operations and employ them in cyberspace, while the National Mission Force operates under the Commander of USCYBERCOM.

[95] *We are vulnerable in cyberspace, and the scale of the cyber threat requires urgent action by leaders and organizations across the government and the private sector […] This strategy presents an aggressive,*

4.3 DISCURSOS E MOVIMENTOS DE SECURITIZAÇÃO

A fim de justificar o objetivo dessa pesquisa foi realizado um trabalho de *data mining*[96], em busca de atos de fala proferidos por atores securitizadores - considerados como tais nesse trabalho -, e foram encontrados algumas passagens relevantes, pronunciamentos que auferem a esse trabalho sua *raison d'etre*. Poder-se-á concluir se esses atos fazem parte de um movimento a fim de corroborar essa pesquisa, e se são realmente objetos de uma securitização bem-sucedida. É importante notar, no entanto, que não serão esgotados os recursos disponíveis, devido ao escopo que esse trabalho se propõe a abranger. Optou-se por trazer à tona alguns dos discursos que foram proferidos por atores de alto escalão da administração Obama ao público (logo, disponíveis para consulta). Seguiremos, como nos capítulos anteriores, a cronologia.

Em 29 de maio de 2009, o presidente Barack Obama, já no início do seu primeiro mandato, fez um pronunciamento com o intuito de sublinhar o estado da "segurança das infraestruturas cibernéticas da nação". O mesmo ocorreu no salão leste da Casa Branca, que posteriormente foi disponibilizado pela secretaria de imprensa da presidência[97].

Na abertura do seu discurso ele introduziu a importância do assunto, ao afirmar que "o ciberespaço é real, e assim são os riscos que vêm com ele […] é a grande ironia da nossa Era da Informação, as mesmas tecnologias que nos capacitam para criar e construir, também fortalecem aqueles que buscam perturbar e destruir[98]". Obama afirmou ainda que "a nossa vantagem tecnológica é a chave para o domínio militar dos Estados Unidos; no entanto, nossas redes militares e de defesa estão sob constante ataque[99]".

---

specific plan for achieving change […] Success requires close collaboration across DoD, between agencies of the U.S. government, with the private sector, and with U.S. allies and partners.

[96] Mineração de dados é uma expressão inglesa ligada à informática, e consiste em uma funcionalidade que agrega e organiza dados, encontrando neles padrões, associações, mudanças e anomalias relevantes. É um método que está sendo utilizado nesse trabalho a fim de auxiliar a pesquisa sob certos tipos de dados.

[97] Disponível em: <https://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure> Acesso em 20 nov. 2015

[98] *So cyberspace is real. And so are the risks that come with it… 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.*

[99] *Our technological advantage is a key to America's military dominance, but our defense and military networks are under constant attack.*

> Por todas essas razões, essa **ameaça** nos é clara, e é um dos desafios de **segurança nacional** e econômica mais graves que enfrentamos como nação […] É também claro que não estamos tão preparados como deveríamos estar, como governo ou como país. Nos últimos anos, alguns progressos foram feitos a nível federal. Mas, assim como nós falhamos no passado ao investir em nossas infraestruturas físicas – estradas, pontes e ferrovias – nós falhamos ao investir na segurança da nossa **infraestrutura digital** […] Hoje estou lançando um relatório, e posso garantir que minha administração perseguirá uma nova abordagem abrangente para garantir a **infraestrutura digital** da América. Essa nova abordagem começa do topo, firmando um compromisso meu: a partir de agora, nossa **infraestrutura digital** – as redes de computadores dos quais dependemos todos os dias – será tratada como deveria ser, **um ativo nacional estratégico**. Vamos garantir que essas redes sejam seguras, confiáveis e resilientes. Vamos dissuadir, prevenir, detectar e se defender contra ataques, e nos recuperar rapidamente de quaisquer interrupções ou danos[100] (WHITE HOUSE, 2009, tradução e grifo próprio).

Pode-se notar que as afirmações acima, à época, foram não somente uma reação aos ataques ocorridos nos EUA em 2008 (comentados no segundo capítulo), mas uma busca por inserir a cibernética no conjunto de estratégias que o país detém, a fim de assegurar sua soberania e sua liderança. Foi um pronunciamento que não dizia mais respeito apenas a campanha à presidência, e sim afirmações de um presidente eleito sobre os objetivos que teria durante seu mandado. Apesar de o ator ser Barack Obama, quando ele se refere a "nós" - como conjunto - ele amplia a responsabilidade para a sua administração e, consequentemente, para outros atores presentes e responsáveis por auxiliá-lo no movimento de elevar a cibernética na agenda de segurança. O objeto são os EUA, e durante o ato de fala a preocupação são com as "ameaças à infraestrutura digital", que movem esse objeto para o campo de securitização.

Além do mais, o resultado desse discurso fomentou também a *Comprehensive National Cybersecurity Initiative*, reforçando-a perante a audiência que já havia tido contato durante o final do governo Bush. E, apesar de ser sugerida a vantagem tecnológica do país sob os outros, ao afirmar que "ainda não estamos preparados como

---

[100] *For all these reasons, it's now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation. It's also clear that we're not as prepared as we should be, as a government or as a country. In recent years, some progress has been made at the federal level. But just as we failed in the past to invest in our physical infrastructure -- our roads, our bridges and rails -- we've failed to invest in the security of our digital infrastructure [...] Today I'm releasing a report on our review, and can announce that my administration will pursue a new comprehensive approach to securing America's digital infrastructure. This new approach starts at the top, with this commitment from me: From now on, our digital infrastructure -- the networks and computers we depend on every day -- will be treated as they should be: as a strategic national asset. Protecting this infrastructure will be a national security priority. We will ensure that these networks are secure, trustworthy and resilient. We will deter, prevent, detect, and defend against attacks and recover quickly from any disruptions or damage.*

deveríamos estar", denotou pontos de insegurança do país sobre o estado de desenvolvimento de um ativo que, além de poder ser utilizado de maneira assimétrica perante as outras formas de guerra tradicionais, também faz parte de um desenvolvimento tecnológico sem ponto de retorno. Ou seja, demonstra a vulnerabilidade do país em relação a cibernética.

Dando seguimento, a administração do presidente Obama lançou uma proposta legislativa para a cibersegurança[101]. Ela foi anunciada oficialmente pelo ex-coordenador de Cibersegurança e assistente pessoal do presidente, Howard A. Schmidt, no dia 12 de maio de 2011 no *Capitol Hill*. Ela foi uma resposta a um chamado do Congresso a fim de verificar as necessidades em torno da cibersegurança do país. Nas palavras de Howard, "[…] quando o presidente lançou seu *Cyberspace Policy Review* há quase dois anos, declarou o ciberespaço como um ativo estratégico chave para os Estados Unidos e vital para sua segurança […]". Durante o ano de 2011, foi lançado também um documento chamado *The Administration's Cybersecurity Accomplishments*, que continha os objetivos que a administração já tinha conseguido realizar, derivados da *Cyberspace Policy Review*. Ou seja, a proposta legislativa foi nada mais que um seguimento dado ao estudo lançado em 2009, conforme comentou o assistente pessoal do presidente Obama.

> Membros de ambos os partidos no Congresso também reconheceram a necessidade, e apresentaram cerca de 50 projetos de lei relacionados com a cibernética na última sessão do Congresso. O líder da maioria no Senado e seis presidentes de comissões escreveram ao Presidente e pediram sua opinião sobre a legislação de segurança cibernética. A Administração recebeu bem a oportunidade de ajudar os esforços do Congresso, e temos desenvolvido uma proposta legislativa para a cibersegurança, pragmática e focada para a consideração do Congresso. Essa proposta legislativa é a mais recente conquista no fluxo constante de progresso que estamos fazendo para assegurar o ciberespaço[102] (SCHMIDT, 2011, tradução própria).

A legislação proposta pelo Congresso foi criada com o foco em melhorar a cibersegurança para: O povo norte-americano (proteção contra vazamentos de dados; instituição de penas contra ciber-criminosos); proteção da infraestrutura crítica da nação

---

[101] Disponível em: <https://www.whitehouse.gov/blog/2011/05/12/administration-unveils-its-cybersecurity-legislative-proposal> Acesso em 18 nov. 2015

[102] *Members of both parties in Congress have also recognized this need and introduced approximately 50 cyber-related bills in the last session of Congress. Senate Majority Leader Reid and six Senate committee chairs thus wrote to the President and asked for his input on cybersecurity legislation. The Administration welcomed the opportunity to assist these congressional efforts, and we have developed a pragmatic and*

(assistência voluntária governamental e compartilhamento de informações com a indústrias, estados e governos locais; planos de cibersegurança das infraestruturas críticas); proteger computadores e redes federais (planejamento, recrutamento de pessoal, sistemas de prevenção contra intrusões, aquisição de *data centers*); proteção dos direitos civis e a garantia de privacidade dos indivíduos norte-americanos.

Por fim, a conclusão do documento sobre a proposta legislativa é finalizada com as seguintes palavras:

> Nossa nação está em risco. As **ciber-vulnerabilidades** em nosso governo e em nossas **infraestruturas críticas** são um risco a nossa **segurança nacional**, segurança pública, e a prosperidade econômica. A administração (Obama) tem respondido ao chamado do Congresso para inserir a legislação sobre **cibersegurança** que nossa nação necessita, e nós estamos ansiosos para colaborar com o Congresso em seus movimentos sobre a questão (WHITE HOUSE, 2011, p. 5, tradução e grifo próprio).

Dando seguimento, em 12 de março de 2013 foi lançado um documento, derivado de uma audiência com o então Diretor Nacional de Inteligência (DNI), James R. Clapper, produzida pelo Comitê de Inteligência do Senado. Ficou conhecida como "Avaliação das Ameaças Mundiais da Comunidade de Inteligência dos EUA" (*Worldwide Threat Assessment of the US Intelligence Community*), e tem por objetivo pôr em discussão as mais variadas ameaças (nucleares, terrorismo, crimes transacionais, contra inteligência, pandemias e outras atrocidades) que concernem o país, e destaca-las por meio do pronunciamento de um ator de alto escalão no cenário de inteligência norte-americano.

Já em sua introdução, é curioso como Clapper se referiu às ameaças globais de um modo geral: "[…] são as mais diversas, **interconectadas**, e mais **virais** que em qualquer momento da história" (CLAPPER, 2013, grifo próprio). No entanto, esses elementos que lembram a linguagem computacional presentes no pronunciamento são apenas curiosidade, já que há, no início do primeiro capítulo do documento, uma seção dedicada a "*cyber*" e cujos excertos mais importantes seguem abaixo.

> Estamos em uma grande transformação, pois as nossas **infraestruturas críticas**, economia, vidas, e compreensões básicas e interações com o mundo, estão se tornando cada vez mais interligados com as tecnologias digitais e com a Internet. Em alguns casos, o mundo está aplicando as tecnologias digitais mais rapidamente do que nossa capacidade de compreender as implicações de segurança e reduzir os potenciais riscos [...] Para agravar estes

---

focused cybersecurity legislative proposal for Congress to consider. This legislative proposal is the latest achievement in the steady stream of progress we are making in securing cyberspace

> desenvolvimentos existe a incerteza e a dúvida à medida que enfrentamos novos e imprevisíveis **ameaças cibernéticas**. Em resposta às tendências e eventos que acontecem no ciberespaço, as escolhas que nós e outros atores faremos nos próximos anos irão moldar o ciberespaço para as próximas décadas, com implicações potencialmente profundas para a segurança econômica e nacional dos EUA [...] Nós acompanharemos a evolução cibernética entre atores não estatais, incluindo grupos terroristas, hacktivistas e ciber-criminosos. Nós vimos indícios de que algumas organizações terroristas aumentaram o interesse no desenvolvimento de capacidades cibernéticas ofensivas, mas elas provavelmente estão limitadas pelos recursos inerentes, limitações organizacionais e prioridades de rivais[103] (CLAPPER, 2013, p. 1-3, tradução e grifo próprio).

Novamente, presentes nesse discurso estão elementos e palavras que demonstram fontes para a securitização, em que as palavras-chave discorridas no primeiro capítulo são utilizadas a fim de imbuir um senso de importância ao assunto. Denota-se a "incerteza" e "dúvida", citadas quanto ao futuro da cibernética no país, e o papel que ela terá nos perigos que afligem a segurança do país.

No mesmo ano, em 12 de junho de 2013, foi realizada uma audiência promovida pelo Comitê de Apropriações do Senado – um dos maiores comitês do senado norteamericano -, cuja seção foi nomeada "Cibersegurança: preparação e resposta à ameaça contínua". Ela foi presidida pela vice-presidente da comissão, senadora Barbara Mikulski, e tinha como participantes o general Keith Alexander, então diretor da Agência de Segurança Nacional (NSA) e Comandante da USCYBERCOM; o Secretário Adjunto do Departamento de Segurança Interna (DHS), Rand Beers; o Secretário Adjunto do Departamento de Comércio, Patrick Gallagher; e o Diretor Executivo assistente do setor resposta cibernética do Bureau Federal de Investigação (FBI), Richard McFeely.

Entre os excertos encontrados no pronunciamento, os pontuais e de relevância a nossa pesquisa serão expostos, iniciando-se pela fala da senadora Bárbara Mikulski.

---

[103] *We are in a major transformation because our critical infrastructures, economy, personal lives, and even basic understanding of—and interaction with—the world are becoming more intertwined with digital technologies and the Internet. In some cases, the world is applying digital technologies faster than our ability to understand the security implications and mitigate potential risks [...] Compounding these developments are uncertainty and doubt as we face new and unpredictable cyber threats. In response to the trends and events that happen in cyberspace, the choices we and other actors make in coming years will shape cyberspace for decades to come, with potentially profound implications for US economic and national security [...] We track cyber developments among nonstate actors, including terrorist groups, hacktivists, and cyber criminals. We have seen indications that some terrorist organizations have heightened interest in developing offensive cyber capabilities, but they will probably be constrained by inherent resource and organizational limitations and competing priorities.*

> Espero que o nosso país tenha um **senso de urgência**. Nós já estamos sob ataque. Esta é uma nova e duradoura guerra. Estamos em **guerra cibernética** todos os dias. Toda vez que alguém rouba a nossa identidade, rouba nossos segredos de Estado ou de nossos segredos comerciais, estamos em guerra. [...] O presidente dos Estados Unidos solicitou, em sua mensagem ao Congresso sobre o orçamento, US$ 13 bilhões a fim de executar a estratégia de segurança cibernética entre os órgãos do governo federal. [...] A finalidade desta audiência, hoje, é de olhar para as **ameaças cibernéticas**. Nem todos os programas da NSA, nem todos programas executados pelo DHS ou pelo Departamento de Justiça, ou o grande trabalho que está sendo feito pelo NIST[104]. O foco é na **segurança cibernética**[105] (MIKULSKI, 2013, tradução e grifo próprio).

Durante a fala dos outros atores presentes – e testemunhas nessa audiência -, Rand Beers comentou que a cibersegurança é uma das cinco maiores missões do Departamento de Segurança Interna (DHS) atualmente, e que é levada muito a sério. Richard McFeely complementou que líderes do FBI, juntamente com líderes da NSA e do DHS estão trabalhando em conjunto a fim de modelar e esclarecer o caminho sobre a jurisdição da cibernética; e assegurou que esse é um nível de cooperação interagências que não era visto desde o pós 11/09. É visto, pois, que a reunião de diversos atores de órgãos de prestígio como o FBI, a NSA e o DHS corroboram a importância do debate que está surgindo no campo da cibernética. E não é uma coordenação fácil, tendo em vista que no mesmo ano houve os vazamentos da NSA por Edward Snowden; ou seja, o comando e o controle centralizado das informações essenciais para o país são um desafio que o mesmo tem dificuldades em cumprir, ainda mais quando envolve o controle de comunicações no exterior (parte que também se propunha a agência).

Dando continuidade, em 10 de setembro de 2015 o Diretor Nacional de Inteligência (DNI), James R. Clapper, fez novamente um pronunciamento na Avaliação das Ameaças Mundiais da Comunidade de Inteligência dos EUA" (*Worldwide Threat Assessment of the US Intelligence Community*)[106], dois anos após sua última declaração.

---

[104] *National Institute of Standards and Technology* (Instituto Nacional de Padrões e Tecnologia)

[105] *I hope that our country has a sense of urgency. We are already under attack. This is the new, enduring war. We are in a cyberwar every day. Every time someone steals our identity, steals our state secrets or our trade secrets, we are at war. […] The president of the United States, in his budget message to Congress, has asked for the $13 billion in order to execute the cybersecurity strategy across the agencies of the federal government. […] The purpose of this hearing today is to look at the cybersecurity threat. Not every program from the National Security Agency, not every program being run by Homeland or the Department of Justice or the great work being done by NIST. It is the focus on the cybersecurity.*

[106] Disponível em: <https://www.youtube.com/watch?v=Q3aG0CtZbU4> Acesso em: 25 out. 2015

Em seu discurso de abertura, ele expôs: "as **ciberameaças** para a **segurança nacional** e econômica dos EUA estão aumentando em frequência, escala, sofisticação e gravidade de impacto […] temos de estar preparados e blindados contra um grande ataque que pode debilitar a infraestrutura norte-americana inteira […] e essas ameaças incluem os Estados-Nação em duas categorias: programas altamente sofisticados, notavelmente de Rússia e China; e aqueles menos sofisticados tecnicamente, como as capacidades do Irã e da Coréia do Norte, mais agressivos e imprevisíveis" (CLAPPER, 2015, tradução e grifo próprio).

Por fim, em 24 de setembro de 2015, o Comitê de Inteligência do Senado fez uma audiência com o atual Diretor da NSA, Almirante Michael S. Rogers[107]. O objetivo da audiência era ouvir o representante maior da NSA sobre as atividades e habilidades da agência, e conhecer os requisitos disponíveis de suas missões. Será transcrito a parte mais relevante da audiência, em um momento de considerações finais do Almirante com a Senadora Susan Collins, com uma intervenção final do Senador James Paul Lankford.

> *Ms. Collins*: Outra questão é a proteção das nossas **infraestruturas críticas** derivadas de **ciber ameaças** e ciber invasões, que têm sido de grande preocupação para mim. O Departamento de Segurança Interna identificou mais de 60 entidades no campo de **infraestruturas críticas** em que danos causados por um único ciber incidente resultariam em 50 bilhões de dólares em danos econômicos, ou 25000 mortes imediatas, ou uma grave degradação da nossa defesa nacional. Anteriormente, o general Keith Alexander (ex-Diretor da NSA)[108] nos disse que a preparação de nossa nação quando se trata de nos proteger contra **ciberataques** contra nossa **infraestrutura crítica** está em cerca de 3, em uma escala de 1 a 10. Onde você acha que estamos hoje nessa escala?
> *Mr. Rogers:* Isso varia por setor, mas, em média eu provavelmente diria que agora – mais uma vez, dependendo do setor – provavelmente um 5 ou 6. Não é onde nós precisamos estar, claramente!
> *Ms. Collins:* Então ainda há um problema grave nesta área que nos deixa muito **vulneráveis** como nação?
> *Mr. Rogers:* Sim, senhora.
> *Ms. Collins:* Obrigado!
> […]
> *Mr. Lankford:* Então, vamos falar sobre a **guerra cibernética** com a qual estamos lidando internacionalmente neste momento. Maiores ameaças que temos, quais atores estatais e não-estatais neste ponto internacionalmente?
> *Mr. Rogers:* Deixe-me responder desta forma, se eu posso: a maior quantidade de atividades que existem hoje são em ciber crimes, mas quando eu olho em uma perspectiva de **segurança nacional**, eu diria no momento que nosso Estado-Nação está sob um grande desafio em relação a nossa segurança. Há três coisas, olhando para o futuro, que mais me preocupam quando se trata da cibernética: 1) Algo que seja direcionado a uma atividade

[107] Disponível em: <http://www.intelligence.senate.gov/hearings/admiral-rogers-nsa> Acesso em: 25 out. 2015
[108] Nota própria.

> destrutiva direcionada a nossa **infraestrutura crítica**. 2) Manipulação e alteração de dados, pois até o momento a maioria das atividades foram roubo. E se alguém entrasse em um sistema e começasse a manipular e alterar aos dados a um ponto onde nenhum operador conseguisse acreditar no que está vendo em sua frente no sistema? 3) E, o que acontece quando um ator não estatal decide que a web é apenas uma arma, não mais apenas para recrutar pessoas, não apenas para gerar lucro, não somente para compartilhar ideologias (informação verbal, tradução e grifo próprio.)[109].

Visto que existem grandes quantidades de ciber-crimes por meio da Internet, não somente no país, o general aponta que essa não seria a vulnerabilidade que o país enfrenta. É possível observar, por esse último debate, que uma das maiores preocupações dos EUA são com sua vulnerabilidade quanto a proteção de suas infraestruturas críticas, ameaçadas tanto por ciberataques, como ciber-intrusões ou outros atos ciber-relacionados. Por meio da visualização do vídeo é possível notar a expressão de tensão quando o ator expõe o nível que o país se encontra quanto às suas infraestruturas críticas.

Pode-se concluir que os EUA são citados, por inúmeras vezes, como um "país fortemente conectado" (*wired country*), isso durante os vários excertos e audiências checados ao levantar os dados demonstrados nesse trabalho. Ao ser fortemente conectado, torna-se também fortemente dependente dessa tecnologia, que não é mais de

---

[109] (Audiência concebida no dia 24 de setembro de 2015, transcrita e traduzida pelo autor).
Ms. Collins: Another issue, that is the protection of our critical infrastructure from cyber threats and cyber intrusions, which has long been of huge concern to me. The Department of Homeland Security is identifying more than 60 entities in our critical infrastructure where damage caused by a single cyber incident could reassembly result in 50 billion dollars on economic damages, or 25 hundred immediate deaths or a severe degradation of our national defense. Your written testimony talks a little bit about this issue. Your predecessor General Keith Alexander previously said that our nation's preparedness when it comes to protecting against cyber-attack against our critical infrastructure is about a three, on a scale of one to ten. Where do you think we are on that scale?
Admiral Rogers: It varies by sector, but on average, I would probably say right now - again, depending on the sector - probably a five or six. That is not where we need to be, clearly.
Ms. Collins: So, there's still a severe problem in this area that makes us very vulnerable as a nation?
Admiral Rogers: Yes ma'am.
Ms. Collins: Thank you!
[...]
Mr. Lankford: So, let us talk about cyberwar we are dealing with it internationally at this point. Biggest threats that we have, they state actors and non-state actors at this point internationally.
Admiral Rogers: Let me answer in this way if I could, the greatest amount of activity is still criminal based, but when I look at in a national security perspective, I would argue at the moment the nation state represents the greater national security challenge if you will. There is three things, when I look to the future, that concern me most when it comes of cyber: 1) Something directed to destructive activity directed against critical infrastructure. 2) Manipulation changes the data, cause at the moment the most of activities been theft, what if someone gets in the system and starts just manipulating and changing data to the point where now as an operator you no longer believe what you've seen in your system?3) What

interesse somente pelo seu uso civil. É, muito mais do que no passado, um ativo estratégico (*strategic asset*), cuja segurança e defesa nacionais se tornaram dependentes de ações militares mais fortes e concisas. Assim sendo, deve-se notar que a cibernética segue um caminho, um movimento de securitização crescente, cujo meio que a suporta – o desenvolvimento tecnológico por trás – possui uma ligação quase intrínseca com nossas vidas, e não vislumbra ponto de retorno. Por fim, é uma revolução que não se mostra somente nos EUA, pois é suscetível a quaisquer países atrelados à cibernética e às vulnerabilidades que ela proporciona.

4.3.1 Conclusões parciais

Esse último capítulo buscou elucidar muitas das questões que essa pesquisa se propõe a responder. Observa-se que os ânimos relativos ao assunto "cibernética" aumentaram a partir do segundo ponto de inflexão – os ataques à Estônia em 2007 – e resultaram em caminhos em busca de reforçar a segurança da mesma.

Esses movimentos foram tanto discursivos - com a repetição das palavras trabalhadas no primeiro capítulo, e que permeiam o discurso de securitização -, quanto institucionais - na criação de órgãos e delegação de responsabilidades a autores de alto escalão -, e auxiliaram a delinear a "onda de securitização" em torno do tema.

Após Barack Obama assumir seu primeiro mandato, ele assegurou que a cibernética se tornaria uma prioridade na segurança nacional dos Estados Unidos da América. E, ao longo do decorrer desses dois mandatos seus, foi demonstrado que diversos atores - presentes na sua administração - tomaram medidas para assegurar que a cibernética fosse tratada como deveria ser: um ativo estratégico para o país. Foram palavras do Diretor da Nacional de Inteligência, da Agência de Segurança Nacional, da CIA e do FBI, além de diversos Senadores estadunidenses e do próprio presidente.

A incerteza e a dúvida quanto a efetividade dessas ações ainda permanece; no entanto, o trabalho está sendo realizado de maneira intensiva a fim de assegurar que a vulnerabilidade do país seja reduzida ao máximo, e sua soberania não seja atingida com gravidade.

---

happens when non-state actors decides that the web now is a weapon system, not just something to recruit people, not just something to generate revenue, not just something to share the ideology

5. CONSIDERAÇÕES FINAIS

Retomando os elos fundamentais, vale lembrar que o objetivo central desse trabalho foi o de revisar os atos de fala de atores securitizadores norte-americanos, a partir de uma base teórica consolidada, além de apontar os eventos internacionais em um período correspondido, checando se esses geraram alguma influência nos debates em torno da segurança nacional norte-americana no campo da cibernética. Vale lembrar que esse campo de pesquisa não propõe facilidades, pois atravessa períodos de transformações correntes, e ainda é incipiente na história das Relações Internacionais. De acordo com o pesquisador em Segurança Internacional norteamericano, Adam P. Liff (2012), o tema possui importância crescente para os formadores de políticas e planejadores de defesa; mesmo assim, não chamou a atenção devida da maioria dos estudantes de Relações Internacionais. Assim sendo, grande parte da literatura é limitada e surgiu a partir de escolas de guerra norte-americanas, instituições politicamente orientadas e *think tanks*. Segundo ele, ainda é sub-teorizada.

Mesmo sendo um campo historicamente novo, tem tido crescimento exponencial em termos de conteúdo nos EUA nos últimos anos. Ainda, após os ciberataques a Estônia, a maior potência militar do mundo "arregaçou as mangas" e acentuou um processo de preparação que havia começado após os ataques em 2001. O evento ocorrido no país nórdico pode não ter sido um marco que define a securitização da cibernética nos EUA, mas certamente foi um dos pontos de inflexão mais importantes registrados até o momento.

Foi possível identificar que, mesmo o avanço da cibernética não sendo uma ameaça emergencial para os Estados Unidos, nota-se que há vulnerabilidades presentes no país, derivadas dos avanços tecnológicos ocorridos simultaneamente em diversos países do sistema internacional, e que não foram acompanhadas da segurança necessária em torno dessas infraestruturas digitais. Além do mais, ao serem desencadeadas ações ciber-relacionadas (ataques, invasões, espionagem) com cada vez mais facilidade, custo relativo baixo, e sofisticação; o país – representado pelos seus estadistas – registrou preocupações que refletiram na alteração da agenda de segurança nacional dos Estados Unidos, buscando incluir – seja por meio de discursos de seus atores de alto escalão,

seja através de projetos e documentos oficiais – pautas que justifiquem a crescente securitização da cibernética.

Entre os documentos e discursos analisados, registrou-se uma grande quantidade de palavras que atuam no movimento de securitização, corroboram os "atos de fala", e reforçam os EUA como o objeto referente. Enfatizam a **vulnerabilidade** por meio dos modos de **ataques cibernéticos**, que resultam em ações de proteção às **infraestruturas digitais** e a manutenção da **segurança nacional** por meio do desenvolvimento da **segurança cibernética**.

Quanto a identificação dos atores funcionais - que justificam as preocupações do governo norte-americano -, ao levantar a base de dados para essa pesquisa, notou-se que além de atores não-estatais (que não eram o foco dessa pesquisa), os estatais mais aclamados pelos norte-americanos são a Rússia e China. As grandes potências militares são alvos de frequentes disputas com o país nos mais variados cenários – China nos setores econômico, político, de direitos humanos e de maneira incipiente no militar; Rússia nos setores militar, político e social. A Rússia busca a retomada de sua influência regional, muitas vezes indo de encontro aos interesses dos Estados Unidos na região. Já a China agrega iniciativas de ampliar seu poderio e suas influências no cenário internacional, em crescentes disputas com os norte-americanos.

Como foi corroborado por certos autores ao longo dessa pesquisa, é possível que o foco maior do uso da cibernética atualmente - para fins de espionagem – seja alterado em um futuro próximo a fim de atingir de maneira mais agressiva as infraestruturas críticas dos países mais poderosos, como centrais de energia, usinas nucleares, indústrias e inclusive a população civil. Já aconteceu, e ainda há brechas de segurança para que aconteça novamente.

Conclui-se que a cibernética pode não estar securitizada de um modo macro, não abarcando todos os países de grande influência no cenário internacional. Vários países hoje têm preocupações maiores: alguns europeus ainda se recuperando de uma grave crise econômica, e outros gerenciando uma crise do crescente número de migrantes; alguns latino-americanos passando por conturbações políticas, e outros preocupados com seu desenvolvimento; alguns asiáticos preocupados com retomadas do crescimento econômico; e assim por diante. Nota-se que, mesmo que haja um movimento de securitização no âmbito interno - em alguns desses países - a fim de alcançar a

securitização plena, o âmbito externo não está adequado a recepção desse tema, tendo em vista outras preocupações que demandam mais recursos e esforços. Não obstante, o gerenciamento da segurança cibernética será um desafio crescente, e a necessidade de comando e controle deverá impactar a quaisquer países interessados em se integrar ao desenvolvimento tecnológico proporcionado pelas TICs.

Entre 2007 e 2015 a cibernética pode não ter assumido o topo da agenda de segurança nacional dos Estados Unidos, mas certamente galgou um patamar elevado. Sua crescente influência e os seus dilemas de segurança relacionados colaborarão para que as decisões dos governantes norte-americanos se intensifiquem sobre assunto, e resultem em efeitos colaterais nas decisões de estadistas ao redor do mundo.

6. REFERÊNCIAS

_____. **A Glossary of Common Cybersecurity Terminology.** White House Cyberspace Policy Review, May 2009. Disponível em: <https://niccs.us-cert.gov/glossary> Acesso em: 20 set. 2015

_____. **2015 US NATIONAL MILITARY STRATEGY.** Disponível em: <http://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf> Acesso em 30 jul. 2015.

_____. **A Brief History of the Internet.** Disponível em: <http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet> Acesso em: 13 set. 2015

_____. **Internet Voting in Estonia**. Disponível em: <http://vvk.ee/voting-methods-in-estonia/engindex>. Acesso em: 22 jul. 2015.

_____. **Meeting of the North Atlantic Council in Defence Ministers Session.** Disponível em <http://www.nato.int/cps/en/natolive/news_47011.htm> Acesso em 27 jul. 15

_____. **Minifacts about Estonia 2015**. Disponível em: <http://www.stat.ee/90745>. Acesso em: 21 jul. 2015.

_____. **President Bush to Welcome President Toomas Ilves of Estonia.** Disponível em <http://georgewbushwhitehouse.archives.gov/news/releases/2007/05/20070504-6.html> Acesso em 27 jul. 15

_____. FIGURA 1. **Operation "Red October"**, 2013. Disponível em: <http://media.kaspersky.com/en/Kaspersky_Lab_Infographic_Red_October_Victims_By_Country.png> Acesso em: 23 out. 2015

_____. FIGURA 2. **Inter-Regional Internet Bandwidth**, 2015. Disponível em: <https://www.telegeography.com/page_attachments/products/website/research-services/global-internet-geography/0006/2619/GIG_Executive_Summary.pdf> Acesso em: 23 out. 2015

AFTERGOOD, Steven. **Pentagon's Cyber Mission Force Takes Shape.**2015. Disponível em: <https://fas.org/blogs/secrecy/2015/09/dod-cmf/>. Acesso em: 10 nov. 2015.

ALEXANDER, Keith. **Cybersecurity: Preparing for and responding to the enduring threat.** 2013. Disponível em: <http://www.appropriations.senate.gov/imo/media/doc/hearings/Alexander, General Keith Testimony 6.12.13 Cybersecurity Hearing.pdf>. Acesso em: 21 nov. 2015.

AUSTEN, Ian. **Canada Hit by a Cyberattack.** 2011. THE NEW YORK TIMES. Disponível em: <http://www.nytimes.com/2011/02/18/world/americas/18canada.html?_r=0>. Acesso em: 24 out. 2015

AUSTIN, John L. **How to do things with words.** Oxford, 1962.

BBC NEWS. **Siprnet: Where the leaked cables came from.** 2010. Disponível em: <http://www.bbc.com/news/world-us-canada-11863618>. Acesso em: 16 set. 2015.

BBC NEWS. **Stuxnet worm hits Iran nuclear plant staff computers.** 2010. Disponível em: <http://www.bbc.com/news/world-middle-east-11414483>. Acesso em: 22 set. 2015.

BBC NEWS. **China IP address link to South Korea cyber-attack.** 2013. Disponível em: <http://www.bbc.com/news/world-asia-21873017>. Acesso em: 23 out. 2015.

BUZAN, Barry; WAEVER, Ole; De WILDE, Jaap. **Security: A New Framework for Analysis.** Lyanne Rienner Publishers, 1998.

BUZAN, Barry. **People, States and Fear People, States and Fear: an Agenda for International Security Studies in the Post-Cold War Era.** Boulder, Colorado, Lynne Rienner Publishers, 1991.

CAVELTY, Mirian Dunn. **Cyber-Security and Threat Politics: US efforts to secure the information age.** Routledge, 2008.

CAVELTY, Myriam Dunn. **Global Cyber-Security Policy Evolution.** 2014. Disponível em: <http://www.springer.com/cda/content/document/cda_downloaddocument/9783319106199-c2.pdf?SGWID=0-0-45-1482512-p176905994>. Acesso em: 17 nov. 2015.

CCDCOE (Org.). **History**. Disponível em: <https://ccdcoe.org/history.html> Acesso em: 13 out. 2015

CCDCOE (Org.). **NATO Centres of Excellence.** Disponível em: <https://ccdcoe.org/nato-centres-excellence.html> Acesso em: 13 out. 2015

CHOUCRI, Nazli; MADNICK, Stuart; ELBAIT, Gihan. **What is Cybersecurity? Explorations in Automated Knowledge Generation.** Massachusetts Institute of Technology. Political Science Department, Working Paper No. 2012-30. (28 Pág.)

CLAPPER, James R. **World Wide Cyber Threats Hearing.** 2013. Permanent Select Committee on Intelligence. Disponível em: <http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-090.pdf> Acesso em: 24 nov. 2015

CLAPPER, James R. **World Wide Cyber Threats Hearing.** 2015. Permanent Select Committee on Intelligence. Disponível em: <https://www.youtube.com/watch?v=Q3aG0CtZbU4> Acesso em: 24 nov. 2015

CLARKE, Richard A.; KNAKE, Robert K. **The Next Threat to National Security and What to Do About It.** Harper Collins. EPub Edition. Março de 2010.

COMPUTERWORLD. **Black Hat: Estonia attacks an example of online rioting, says researcher.** Disponível em: <http://www.computerworld.com/article/2542850/security0/black-hat--estonia-attacks-an-example-of-online-rioting--says-researcher.html>. Acesso em: 21 jul. 2015.

CRAIGEN, Dan; DIAKUN-THIBAULT, Nadia; PURSE, Randy. **Defining Cybersecurity.** Technology Innovation Management Review, 2014. (9 Págs.)

DALE, Catherine. **National Security Strategy: Mandates, Execution to Date, and Issues for Congress.** 2013. Disponível em: <https://www.fas.org/sgp/crs/natsec/R43174.pdf>. Acesso em: 04 nov. 2015.

DANIEL, Alexander. **Russian Historian: The problem is how to live together if the two peoples have such a different memory.** Regnum News Agency, 2007. Disponível em: <http://pda.regnum.ru/news/issues/823273.html>. Acesso em: 22 jul. 2015.

DAVIDSON, Jacob. **China Accuses U.S. of Hypocrisy on Cyberattacks.** 2013. TIME. Disponível em: <http://world.time.com/2013/07/01/china-accuses-u-s-of-hypocrisy-on-cyberattacks/>. Acesso em: 25 out. 2015.

DEFENSE DATA NETWORK NEWSLETTER. **ARPANET/MILNET SPLIT - How It Will Happen.** Disponível em: <https://www.rfc-editor.org/rfc/museum/ddn-news/ddn-news.n26.1> Acesso em: 13 set. 2015

DENNING, Peter J; HEARN, Anthony; KERN, William. **History and Overview of CSNET**. Washington, 1982.

DHS. **National Strategy to Secure Cyberspace.** 2003. Disponível em: <http://www.dhs.gov/national-strategy-secure-cyberspace>. Acesso em: 22 set. 2015.

FARWELL, James P.; ROHOZINSKI, Rafal. **Stuxnet and the Future of Cyber War.**2011. Disponível em: <http://pt.scribd.com/doc/57100263/Stuxnet-and-the-Future-of-Cyber-War#scribd>. Acesso em: 25 out. 2015.

FEAVER, Peter. **How to Read the New National Military Strategy.** 2015. Disponível em: <http://foreignpolicy.com/2015/07/06/how-to-read-the-new-national-military-strategy/>. Acesso em: 04 nov. 2015.

FERREIRA NETO, Walfredo B.; **Territorializando o "Novo" e (Re)territorializando os Tradicionais: a Cibernética como Espaço e Recurso de Poder.** Coleção Meira Mattos, Rio de Janeiro, v. 8, n. 31, p. 07-18, jan./abr. 2014

GABINETE DE SEGURANÇA INSTITUCIONAL. **Norma Complementar nº 04/IN01/DSIC/GSIPR**. Presidência da República, 2009. Disponível em: <http://dsic.planalto.gov.br/legislacaodsic/53> Acesso em: 22 set. 2015

GIACOMELLO, Giampiero; ERIKSSON, Johan (Ed.). **International Relations and Security in the Digital Age.** 2007. Disponível em: <http://www.skoob.com.br/international-relations-and-security-in-the-digital-age-525363ed533039.html>. Acesso em: 03 set. 2015.

GLOBAL RESEARCH AND ANALYSIS TEAM (Org.). **The "Red October" Campaign – An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies.**2013.

KASPERSKY LAB. Disponível em: <https://securelist.com/blog/incidents/57647/the-red-october-campaign/>. Acesso em: 24 out. 2015

GORMAN, Siobhan; DREAZEN, Yochi. **Military Command Is Created for Cyber Security.** 2009. THE WALL STREET JOURNAL. Disponível em: <http://www.wsj.com/articles/SB124579956278644449>. Acesso em: 21 out. 2015.

GREENWALD, Glenn; MACASKILL, Ewen. **NSA Prism program taps in to user data of Apple, Google and others.** 2013. THE GUARDIAN. Disponível em: <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>. Acesso em: 25 out. 2015.

HEALEY, Jason. **Commentary: Cyber Command as a 5-Year-Old.** 2015. DEFENSE NEWS. Disponível em: <http://www.defensenews.com/story/defense/commentary/2015/06/09/cyber-command-5-year-old-internet-attacks-network-disa-task-force-computer/28730781/>. Acesso em: 19 out. 2015.

ICS-CERT. **Cyber Threat Source Descriptions.** Government Accountability Office (GAO), Department of Homeland Security's (DHS's) Role in Critical Infrastructure Protection (CIP), Washington D.C., 2005. Disponível em: <https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions> Acesso em: 22 set. 2015

JEWISH TELEGRAPHIC AGENCY (Org.). **Snowden Says Israel, U.S. Created Stuxnet Virus That Attacked Iran.** 2013. HAARETZ. Disponível em: <http://www.haaretz.com/israel-news/1.534728>. Acesso em: 25 out. 2015.

KASPERSKY LAB. **O que é Spear Phishing?** Disponível em: <http://brazil.kaspersky.com/internet-security-center/definitions/spear-phishing>. Acesso em: 27 out. 2015.

KUSHNER, David. **The Real Story of Stuxnet.** 2013. INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. Disponível em: <http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>. Acesso em: 25 out. 2015.

LANDLER, Mark; MARKOFF, John. **Digital Fears Emerge After Data Siege in Estonia.** Disponível em: < http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all&_r=0> Acesso em: 16 out 2015

LEE, Robert M.; ASSANTE, Michael J.; CONWAY, Tim. **German Steel Mill Cyber Attack**. 2014. SANS ICS. Disponível em: <https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf>. Acesso em: 27 out. 2014

LIFF, Adam P.; **Cyberwar: A New 'Absolute Weapon'?** The Proliferation of Cyberwarfare Capabilities and Interstate War. 2012. Journal of Strategic Studies, 401-428

LYNN III, William J. **Defending a New Domain.** 2013. FOREIGN AFFAIRS. Disponível em: <https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain>. Acesso em: 23 out. 2015.

MACASKILL, Ewen. **Obama to confront Chinese president over spate of cyber-attacks on US.** 2013. THE GUARDIAN. Disponível em: <http://www.theguardian.com/technology/2013/may/28/obama-chinese-president-cyber-attacks>. Acesso em: 25 out. 2015.

MICHAEL N. SCHMIDT (Ed.). **TALLINN MANUAL.** 2009. Disponível em: <https://ccdcoe.org/tallinn-manual.html>. Acesso em: 10 out. 2015.

MIKULSKI, Barbara. **Mikulski Chairs Hearing on Cybersecurity with NSA, FBI, NIST and Homeland Security Leaders.** Disponível em: <https://www.youtube.com/watch?v=vMbphNuGsrc> Acesso em: 24 nov. 2015

MILLER, Hayley. **Security Clearances: 4.2 Million People Have Access To The Government's Classified Information.** 2011. Disponível em: <http://www.huffingtonpost.com/2011/09/20/security-clearances-government-classified-information_n_972492.html>. Acesso em: 16 set. 2015.

NAKASHIMA, Ellen. **Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies.** 2013. WASHINGTON POST. Disponível em: <https://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html>. Acesso em: 25 out. 2015.

NAKASHIMA, Ellen. **Defense official discloses cyberattack.** 2010. WASHINGTON POST. Disponível em: <http://www.washingtonpost.com/wp-dyn/content/article/2010/08/24/AR2010082406154.htmlsig2=5zytOxY4iutY5eQGjDsAIQ>. Acesso em: 24 out. 2015.

NAKASHIMA, Ellen. **Obama administration outlines international strategy for cyberspace.** 2011. Disponível em: <https://www.washingtonpost.com/world/obama-administration-outlines-international-strategy-for-cyberspace/2011/05/16/AFokL54G_story.html>. Acesso em: 05 nov. 2015.

NATO (Org.). **Cyber Timeline.** Disponível em: <http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm>. Acesso em: 24 out. 2015.

OPSAHL, Kurt. **Everything We Know About NSA Spying: "Through a PRISM Darkly".** Chaos Communication Congress. Evento realizado em 30 de dezembro de 2013. Disponível em <https://www.youtube.com/watch?v=_P1NA29X7Mw> Acesso em: 26 out. 2015

RATNAM, Gopal. **U.S. Plans 'Tough' Global Talks on Cyber-Crime Fight.**2011. Disponível em: <http://www.bloomberg.com/news/articles/2011-01-25/u-s-plans-diplomatic-push-to-broaden-fight-against-cyber-crime>. Acesso em: 06 nov. 2015.

ROLLINS, John; HENNING, Anna C. **Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations.** Congressional Research Service, 2009.

ROUSE, Margaret. **Botnet (zombie army) definition.** Disponível em: <http://searchsecurity.techtarget.com/definition/botnet>. Acesso em: 22 set. 2015.

RYAN, Johnny. **A History of the Internet and the Digital Future.** Reaktion Books LTD. Londres, 2010.

SANGER, David E.. **U.S. Blames China's Military Directly for Cyberattacks.** 2013. THE NEW YORK TIMES. Disponível em: <http://www.nytimes.com/2013/05/07/world/asia/us-accuses-chinas-military-in-cyberattacks.html>. Acesso em: 25 out. 2015.

SANG-HUN, Choe. **Computer networks in south korea are paralyzed in cyberattacks.** 2013. THE NEW YORK TIMES. Disponível em: <http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html>. Acesso em: 25 out. 2015.

SCHMIDT, Howard A. **Launching the U.S. International Strategy for Cyberspace.** 2011. Disponível em: <https://www.whitehouse.gov/blog/2011/05/16/launching-us-international-strategy-cyberspace>. Acesso em: 05 nov. 2015.

SCHMIDT, Howard A. **The Administration Unveils its Cybersecurity Legislative Proposal.** 2011. Disponível em: <https://www.whitehouse.gov/blog/2011/05/12/administration-unveils-its-cybersecurity-legislative-proposal>. Acesso em: 24 nov. 2015.

SEGAL, Adam. **Axiom and the Deepening Divide in U.S.-China Cyber Relations.** 2014. Disponível em: <http://blogs.cfr.org/cyber/2014/10/29/axiom-and-the-deepening-divide-in-u-s-china-cyber-relations/>. Acesso em: 18 nov. 2015.

SINGER, Peter; FRIEDMAN, Allan. **Cybersecurity and Cyberwar: What Everyone Needs to Know.** Oxford University Press; 1 edition (January 3, 2014)

STEWART, Phil; WOLF, Jim. **Old worm won't die after 2008 attack on military.** 2011. REUTERS. Disponível em: <http://www.reuters.com/article/2011/06/17/us-usa-cybersecurity-worm-idUSTRE75F5TB20110617>. Acesso em: 21 out. 2015.

TANNO, Grace. **A contribuição da escola de Copenhague aos estudos de segurança internacional.** *Contexto int.* [online]. 2003, vol.25, n.1, pp. 47-80. ISSN 0102-8529.

TECMUNDO. **Entenda o que são vírus, spywares, trojans, worms e saiba como se proteger.** Disponível em: <http://www.techtudo.com.br/artigos/noticia/2013/06/entenda-o-que-sao-virus-spywares-trojans-worms-e-saiba-como-se-proteger.html>. Acesso em: 22 set. 2015.

TECMUNDO. **O que é Cracker?** Disponível em: <http://www.tecmundo.com.br/o-que-e/744-o-que-e-cracker-.htm>. Acesso em: 22 set. 2015.

TECMUNDO. **O que é Phishing?** Disponível em: <http://www.tecmundo.com.br/phishing/205-o-que-e-phishing-.htm>. Acesso em: 22 set. 2015.

TECMUNDO. **O que é Spam?** Disponível em: <http://www.tecmundo.com.br/spam/223-o-que-e-spam-.htm>. Acesso em: 22 set. 2015.

U.S. GOVERNMENT PUBLISHING OFFICE (Ed.). **Fiscal Year 2016 Budget Request for Strategic Forces.** 2015. Disponível em: <http://fas.org/irp/congress/2015_hr/stratfor.pdf>. Acesso em: 13 nov. 2015.

UNITED PRESS INTERNATIONAL (UPI). **Analysis: Who cyber smacked Estonia?** Disponível em: < http://www.upi.com/Business_News/Security-Industry/2007/06/11/Analysis-Who-cyber-smacked-Estonia/26831181580439/>. Acesso em: 07 out. 2015.

WESTON, Greg. **Foreign hackers attack Canadian government.** 2013. CBC NEWS. Disponível em: <http://www.cbc.ca/news/politics/foreign-hackers-attack-canadian-government-1.982618>. Acesso em: 24 out. 2015.

WHITE HOUSE (Org.). **Cybersecurity Legislative Proposal.** 2011. Disponível em: <https://www.whitehouse.gov/sites/default/files/fact_sheet_administration_cybersecurity_legislative_proposal.pdf>. Acesso em: 23 nov. 2015

WHITE HOUSE (Org.). **National Military Strategy.** 1997. Disponível em: <http://www.au.af.mil/au/awc/awcgate/nms/index.htm>. Acesso em: 06 nov. 2015.

WHITE HOUSE (Org.). **National Security Strategy.** 1991. Disponível em: <http://nssarchive.us/NSSR/1991.pdf>. Acesso em: 05 nov. 2015.

WHITE HOUSE (Org.). **National Military Strategy**. 1995 Disponível em: <http://www.au.af.mil/au/awc/awcgate/nms/nms_feb95.htm> Acesso em: 05 nov. 2015.

WHITE HOUSE (Org.). **National Strategy to Secure Cyberspace.** 2003. Disponível em: <https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf>. Acesso em: 03 nov. 2015.

WHITE HOUSE (Org.). **Remarks by the President on Securing Our Nation's Cyber Infrastructure.** 2009. Disponível em: <https://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure>. Acesso em: 20 nov. 2015.

WHITE HOUSE (Org.). **The Comprehensive National Cybersecurity Initiative.** 2008. Disponível em: <https://www.whitehouse.gov/sites/default/files/cybersecurity.pdf>. Acesso em: 09 nov. 2015.

WHITE HOUSE (Org.). **The National Military Strategy of the United States of America:** A Strategy for Today; a Vision for Tomorrow. 2004. Disponível em: <http://archive.defense.gov/news/Mar2005/d20050318nms.pdf>. Acesso em: 05 nov. 2015

WHITE HOUSE (Org.). **The National Military Strategy of the United States of America:** Redefining America's Military Leadership. 2011. Disponível em: <http://www.defense.gov/Portals/1/Documents/pubs/2011-National-Military-Strategy.pdf>. Acesso em: 08 nov. 2015.

WHITE HOUSE (Org.). **The National Military Strategy of the United States of America.** 2015. Disponível em: <http://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf>. Acesso em: 10 nov. 2015.

YADRON, Danny. **Three Months Later, State Department Hasn't Rooted Out Hackers.** 2015. THE WALL STREET JOURNAL. Disponível em: <http://www.wsj.com/articles/three-months-later-state-department-hasnt-rooted-out-hackers-1424391453>. Acesso em: 23 out. 2015.