UNIVERSIDADE FEDERAL DE SANTA MARIA

CENTRO DE CIÊNCIAS SOCIAIS E HUMANAS

DEPARTAMENTO DE ECONOMIA E RELAÇÕES INTERNACIONAIS

CURSO DE RELAÇÕES INTERNACIONAIS

A SECURITIZAÇÃO NO ESPAÇO CIBERNÉTICO NO BRASIL E ESTADOS UNIDOS E SEUS IMPACTOS NA CAPACIDADE COERCITIVA E DE VIGILÂNCIA DO ESTADO

TRABALHO DE CONCLUSÃO DE CURSO

RAFAEL SEVERO DA TRINDADE

Santa Maria, RS, Brasil

2016

A SECURITIZAÇÃO NO ESPAÇO CIBERNÉTICO NO BRASIL E ESTADOS UNIDOS E SEUS IMPACTOS NA CAPACIDADE COERCITIVA E DE VIGILÂNCIA DO ESTADO

RAFAEL SEVERO DA TRINDADE

Trabalho de Conclusão de Curso apresentado ao Curso de Relações Internacionais da Universidade Federal de Santa Maria (UFSM, RS) como requisito parcial para a obtenção do grau de **Bacharel em Relações Internacionais.**

Orientador: Prof. Dr. Igor Castellano da Silva

Santa Maria, RS, Brasil

2016

AGRADECIMENTOS

Ao chegar ao fim desta etapa, é impossível não rever os caminhos que me trouxeram até aqui. Agradeço a todos que, de alguma maneira, contribuíram para a conclusão deste trabalho e, de uma maneira especial, agradeço:

- ao meu orientador Igor Castellano da Silva pela dedicação e apoio ao longo deste trabalho e dos projetos de extensão.

- à minha mãe Marlene Tonollier Severo pelo carinho, compreensão, companheirismo e suporte ao longo de toda minha vida.

- à minha família, em especial aos meus irmãos Fabiano Severo Bertoncello e Ricardo Severo Bertoncello pelo incentivo e apoio incondicional. Também, agradeço à minha cunhada Geice Peres Nunes pelo incentivo ao saber, notadamente, a literatura.

- aos meus amigos que sempre me deram incentivo e me alegraram neste período. Em especial, ao João Francisco Mozzaquatro Wendt pelo auxílio técnico neste trabalho.

- à Universidade pública, gratuita e de qualidade pela oportunidade de realizar este trabalho.

Dedico este trabalho ao meu pai Airton Luiz Duarte da Trindade (*in memoriam*).

Esse é o paradoxo de nosso mundo saturado de dispositivos de vigilância, quaisquer que sejam seus pretensos propósitos: de um lado, estamos mais protegidos da insegurança que qualquer geração anterior; de outro, porém, nenhuma geração anterior, pré-eletrônica, vivenciou os sentimentos de insegurança como experiência de todos os dias (e de todas as noites).

(Zygmunt Bauman, 2013)

RESUMO

Trabalho de Conclusão de Curso

Curso de Relações Internacionais

Universidade Federal de Santa Maria

A SECURITIZAÇÃO NO ESPAÇO CIBERNÉTICO NO BRASIL E ESTADOS UNIDOS E SEUS IMPACTOS NA CAPACIDADE COERCITIVA E DE VIGILÂNCIA DO ESTADO

AUTOR: Rafael Severo da Trindade

ORIENTADOR: Igor Castellano da Silva

Data e Local da Defesa: Santa Maria, 16 de Dezembro de 2016.

A pesquisa relacionará a securitização do ciberespaço com a capacidade coercitiva e a capacidade de vigilância do Brasil e Estados Unidos. Esses impactos se tornam de grande importância na medida em que o domínio cibernético ganha mais espaço na segurança internacional. Essa importância se deve pelo fato da popularização da internet que trouxe novos constrangimentos para a segurança do cenário internacional devido à presença da população, empresas e órgãos estatais em um sistema em que é inexistente algum marco legal que discipline o domínio. A hipótese é de que a securitização do espaço cibernético nesses países trouxe efeitos positivos aos meios da capacidade coercitiva e efeitos negativos a efetividade da capacidade de vigilância. Assim, serão analisados os discursos de securitização e as políticas de vigilância no meio cibernético de ambos os países. Chegou-se a conclusão de que a securitização nesses países trouxe benefícios às capacidades coercitivas pela criação de comandos cibernéticos e negativos a efetividade da capacidade de vigilância pela impossibilidade de análise desses dados e devido à violação de liberdades individuais para captar esses dados.

Palavras Chave: Securitização – Capacidade Coercitiva – Capacidade de Vigilância

ABSTRACT

Senior Thesis

International Relations Major

Universidade Federal de Santa Maria

THE SECURITIZATION IN CYBERSPACE IN BRAZIL AND THE UNITED STATES AND ITS IMPACTS ON COERCIVE CAPACITY AND SURVEILLANCE CAPACITY OF THE STATE

AUTHOR: Rafael Severo da Trindade

ADVISOR: Igor Castellano da Silva

Presentation"s Date and Place: Santa Maria, December 16.

The search will relate the securitization of cyberspace with coercive capacity and administrative capacity of Brazil and the United States. These impacts have become of major importance as cyberspace gains more space in international security. This importance is the result of the popularization of the Internet that has brought new constraints to international security due to the presence of the population, companies and state systems in a system in which there is no legal framework that disciplines the domain. The hypothesis is the securitization of cyberspace in these countries brought positive effects to the means of coercive capacity and negative effects to the effectiveness of surveillance capacity. Thus, securitization discourses and surveillance policies will be analyzed in the cyber domain of both countries. We reached the conclusion that the securitization in these countries has brought benefits to coercive capabilities by creating cyber commands and negative effectiveness of surveillance capability by the impossibility of analysis of the data and due to the violation of individual freedoms to capture this data.

Key words: Securitization – Coercive Capacity – Surveillance Capacity

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ABIN	Agência Brasileira de Inteligência
CDCyber	Centro de Defesa Cibernética
CDN	Conselho de Defesa Nacional
CDM	Continuous Diagnostics & Mitigation
CDMA	Cyber Defence Management Authority
CERT	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CGI.br	Comitê Gestor da Internet no Brasil
CREDEN	Câmara de Relações Exteriores e Defesa Nacional
DHS	United States Department of Homeland Security
EB	Exército Brasileiro
END	Estratégia Nacional de Defesa
FAB	Força Aérea Brasileira
GSI-PR	Gabinete de Segurança Institucional da Presidência da República
HSC	Homeland Security Council
IISS	International Institute for Strategic Studies
IP	Internet Protocol
IETF	Internet Engineering Task Force
LOA	Lei Orçamentária Anual
MB	Marinha do Brasil
NSA	Nacional Security Agency
OTAN	Organização do Tratado do Atlântico Norte
RENASIC	Rede Nacional de Excelência em Segurança da Informação e Criptografia
RMA	Revolution in Military Affairs
SMDC	Sistema Militar de Defesa Cibernética
TIC	Tecnologia de Informação e Comunicação
TCU	Tribunal de Contas da União

SUMÁRIO

1 INTRODUÇÃO GERAL

O presente trabalho final de graduação tem por objetivo compreender os impactos da securitização do comando do ciberespaço na capacidade coercitiva e na capacidade de vigilância no Brasil e Estados Unidos. Este projeto faz o uso das teorias de relações internacionais para conseguir explicar os constrangimentos que envolvem a securitização do espaço cibernético.

Não existem regulamentações de âmbito global em relação ao domínio cibernético e com a grande facilidade de acesso à rede, esse domínio requer o uso de grandes recursos do Estado para poder proteger diversos atores como empresas, cidadãos e áreas estratégicas do próprio Estado. A partir de 2008 com a Estratégia Nacional de Defesa (END) o setor cibernético brasileiro se tornou um ponto estratégico da defesa brasileira. Isso se deu pelo fato do país sediar grandes jogos como a Copa do Mundo e as Olímpiadas, além da Jornada Mundial da Juventude.

Devido a sua importância no sistema internacional, os Estados Unidos sofrem diversos tipos de ataques cibernéticos, tanto contra órgãos estatais quanto empresas privadas. Devido a isso, ocorreu uma securitização do seu espaço cibernético que acabou por retirar direitos dos seus cidadãos.

Esse projeto procura contribuir para o avanço no debate sobre a securitização do ciberespaço e de como sua securitização pode contribuir para sociedade de maneira efetiva sem perda de liberdades individuais. O projeto será dividido em três capítulos. O primeiro será sobre a securitização, capacidade coercitiva e capacidade de vigilância no espaço cibernético. O segundo e o terceiro irão tratar sobre os impactos da securitização do espaço cibernético nas capacidades coercitivas e de vigilância dos Estados Unidos e Brasil respectivamente. A comparação será realizada na conclusão.

O trabalho aborda quatro principais temas: segurança internacional, securitização, comando cibernético, capacidade coercitiva. Essas temáticas são importantes para compreender os impactos da securitização.

Segundo Sousa (2005) os estudos de segurança mais que em termos absolutos, é discutido em termos relativos. As análises tradicionais da segurança internacional concentravam-se, regra geral, na sua dimensão militar, em face de ameaças de ataque externo ou instabilidade interna, e na importância dos gastos com a defesa. Com o final da guerra fria, novas ideias foram incorporadas na agenda de segurança, alargando o seu âmbito, a fatores e considerações políticas, económicas, sociais, culturais, ecológicas e ambientais (SOUSA, 2005, p. 168-169).

Para Buzan e Wæver (2003) a securitização é o processo discursivo através do qual uma compreensão intersubjetiva é construída dentro de uma comunidade política para tratar algo como uma ameaça existencial para um objeto referente, e seja emitido um pedido de medidas urgentes e excepcionais para lidar com tal ameaça. Ou seja, problemas se tornam questões securitárias por serem socialmente construídas. Quando um tema é securitizado, ele sai da esfera da política normal e passa para a esfera da política emergencial (DUQUE, 2008, p.38) o que permite a retirada de direitos e por muitas vezes legitima o uso da força.

No pós-Guerra Fria autores da Escola de Copenhague buscaram por ampliar as questões tratadas pela área da Segurança Internacional, autores como: Barry Buzan, Ole Waever e Jaap de Wilde afirmaram que para algo ser considerado como ameaça existencial é preciso ser colocado discursivamente para ser questão de Segurança (ACÁCIO, 2012 p. 2). Essa questão discursiva tem como elemento central a securitização que é caracterizada como:

> O processo discursivo através do qual uma compreensão intersubjetiva é construída dentro de uma comunidade política para tratar algo como uma ameaça existencial para um objeto referente valorizado, e para permitir que um pedido de medidas urgentes e excepcionais para lidar com a ameaça. (BUZAN & WÆVER, 2003, p 491, tradução nossa).[1]

Quando uma questão é securitizada ela demanda medidas emergenciais.

[1] No original: “The discursive process through which an intersubjective understanding is constructed within a political community to treat something as an existential threat to a valued referent object and to enable a call for urgent and exceptional measures to deal with the threat”. (BUZAN & WÆVER, 2003: 491)

Para compreender os impactos da securitização é necessário explicitar a definição de capacidade estatal que se refere à capacidade efetiva do Estado de penetrar na sociedade e alterar a distribuição de recursos, atividades e conexões interpessoais (TILLY, 2007, p.16). A capacidade estatal pode ser avaliada em três dimensões (HANSON & SIGMAN, 2013, p. 3): capacidade extrativa, capacidade coercitiva e capacidade administrativa. Esse trabalho fará uso da definição de capacidade coercitiva que é a habilidade do Estado de preservar suas fronteiras, proteção contra ameaças externas, manter ordem interna e fazer cumprir políticas (HANSON & SIGMAN, 2013, p. 4). A capacidade coercitiva pode ser mensurada com gastos militares, contingente militar e forças de segurança. A segurança nacional e a análise de dados no ciberespaço se tornam global, e esses dados podem colidir até mesmo com aliados, fazendo com que a confiança entre os coligados possa desaparecer. Outro aspecto importante da capacidade estatal é seu poder de vigilância que Giddens (1988) caracteriza em dois componentes. O primeiro se refere à produção de informação possibilitando a coordenação no tempo e no espaço, das atividades dos atores. O segundo diz a respeito de locais onde tempo e espaço está diretamente implicado na supervisão direta da atividade de alguns atores sobre outros como, por exemplo, nas prisões (GIDDENS, 1988, p. 243). A efetividade dessa vigilância vai tratar sobre a qualidade da informação que vai chegar para um tomador de decisões. Dada a quantidade dos dados acumulados, os analistas não conseguem analisar todo o conteúdo, apenas visualizam o gráfico das relações que são identificadas e se concentram no que parecem ser os trechos mais significativos, que mostram relações específicas de conexões entre os dados (BAUMAN, 2014, p.125).

A capacidade coercitiva no espaço cibernético se deu pela criação de comandos cibernéticos, que opera no espaço cibernético que é o domínio operacional onde pessoas e suas organizações usam e criam informações digitais e eletromagnéticas (KUEHL, 2009, p.29), em países como os Estados Unidos e o Brasil tem o objetivo de conter ameaças a esses países e como viabilidade socioeconômica e política de sociedades inteiras (CEPIK, CANABARRO, BORNE, 2014, p. 24). O comando cibernético americano, similar ao brasileiro, tem objetivo de:

> Planejar, coordenar, integrar, sincronizar e realizar atividades para: direcionar as operações e a defesa de redes de informações especifica do Departamento de Defesa e; preparar-se para quando dirigido, conduzir operações militares de amplo espectro no espaço cibernético para habilitar as ações em todos os domínios, garantir a liberdade de ação dos Estados Unidos e de seus aliados no ciberespaço, bem como negar essa capacidade a seus adversários (UNITED STATES, 2010, tradução nossa).[2]

A discussão da teoria de segurança internacional inicialmente se dava entre o embate dos realistas e idealistas. Segundo Rudzit (2006) os realistas tendem a ver a segurança como um derivativo do poder: um ator com suficiente poder que assegure equilíbrio de poder adquiriria como resultado a sua segurança. Já os idealistas tendem a ver a segurança como a consequência da paz. Uma paz duradoura proveria segurança para todos (RUDZIT, 2006, p. 299). A partir do fim da Guerra Fria houve um debate epistemológico mais amplo acerta da segurança internacional (BUZAN, HANSEM, 2009, p.32). Esse debate foi sobre a concepção de segurança entre objetiva, subjetiva e discursiva. A concepção objetiva geralmente define a segurança em termos materiais relativos, a subjetiva salienta contexto social, a história e a psicologia de medo e a discursiva foca no processo intersubjetivo através do quais "ameaças" se manifestam como problemas de segurança na agenda política (BUZAN, HANSEM, 2009, p. 34).

Atualmente, no debate da segurança internacional ocorre um processo de novas tecnologias que estão dando nova dimensão ao conteúdo do debate, essas novas tecnologias fazem parte da digitalização que pode ser classificada como:

> Digitalização é o processo pelo qual um determinado dado (imagem, som, texto) é convertido para o formato de dígito binário para ser processado por um computador. No plano militar, a digitalização diz respeito à confluência entre o radar, o infravermelho, o laser e as micro-ondas de alta potência. No jargão da área militar, é geralmente denominada como Revolução em Assuntos Militares (RMA). (MARTINS, 2008, p.7)

[2] No original: "*USCYBERCOM plans, coordinates, integrates, synchronizes, and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries*" (UNITED STATAES, 2010).

Digitalização cria uma quantidade de dados recolhidos em uma escala transnacional, não deixando claro o que é nacional, assim como os limites entre a aplicação da lei e inteligência (BAUMAN *et al*, 2014, p. 125). No contexto da digitalização, entra a defesa do espaço cibernético por meio dos comandos cibernéticos. O Reino Unido em 2011 anunciou um investimento de cerca de um bilhão de dólares ao longo de quatro anos. A China possui um quadro de funcionários do alto escalão do Exército de Libertação Popular que trata com a defesa cibernética que pode chegar a mil funcionários. Devido a influencia global países como Estados Unidos, Rússia, China, Reino Unido e França são considerados os que possuem maiores capacidades cibernéticas (HACKETT, 2014, p. 20). No Brasil, com a Estratégia Nacional de Defesa (END) de 2008 o setor cibernético se tornou um dos setores estratégicos de defesa juntamente com o nuclear e espacial. O ciberespaço é caracterizado por ser um domínio operacional, marcado pelo uso da eletroeletrônica e do espectro eletromagnético, com objetivo de facilitar e explorar o uso da informação pelas redes interconectadas e independentes (KUEL, 2009, p. 29). O comando cibernético é de responsabilidade do exército brasileiro por meio do Centro de Defesa Cibernética do Exército (CD Ciber) e tem como objetivo o gerenciamento e proteção do setor cibernético do Exército Brasileiro no que diz respeito ao ambiente interno e externo da força. O ambiente externo são Órgãos de Estado e de Governo, Conselho de Defesa Nacional (CDN), Câmara de Relações Exteriores e Defesa Nacional (CREDEN), Casa Civil da Presidência da República, GSI-PR, Departamento de Segurança da Informação e Comunicações (DSIC) e Agência Brasileira de Inteligência (ABIN) Carvalho (2011, p. 10 - 11).

A estruturação inicial da defesa cibernética do Brasil foi formada pela união de quatro vetores:

> Verifica-se que a capacitação de recursos humanos constitui a atividade prioritária na estruturação do setor, uma vez que proporciona as capacitações cibernéticas, no dizer da própria END, indispensáveis para mobiliar os quatro vetores que o integram, quais sejam: a Inteligência - a Doutrina - a Ciência, Tecnologia e Inovação - e as Operações. A mobilização da capacidade cibernética, em nível nacional, atrelada ao amparo legal para a atuação do setor, proporciona os necessários recursos materiais e humanos, com

> respaldo, para a realização das ações no espaço cibernético que caracterizam a Defesa Cibernética. (CARVALHO, 2011, p. 13)

A defesa cibernética americana se encontra no estágio securitizado e a brasileira ainda em um estágio de securitização incipiente (LABATO & KENKEL, 2015, p. 38). Essa securitização do espaço cibernético levanta a questão da possibilidade de guerras serem travadas nesse meio. A guerra cibernética pode ser vista como a fase mais recente na revolução dos assuntos militares.

O setor cibernético recebeu grande importância dos Estados e instituições a partir dos anos 2000 quando começou a se perceber a vulnerabilidade que essas tecnologias poderiam trazer. A securitização também pode ser compreendida pelas Unidades de Análise de Segurança:

> Os autores também definem as Unidades de Análise em Segurança (Units of Security Analysis), em que o Objeto de Referência é a coisa existencialmente ameaçada; Ator de Securitização é aquele que securitiza a questão declarando que o objeto de referência está ameaçado e os Atores Funcionais afetam dinâmica do setor analisado. (ACÁCIO, 2012 p. 3).

No Brasil, a securitização definiu necessidades para que haja maiores constrangimentos para aumentar a capacidade estatal. Segundo Charles Tilly, principal autor sobre Capacidade Estatal, o conceito significa: capacidade efetiva do Estado de penetrar na sociedade e alterar a distribuição de recursos, atividades e conexões interpessoais (TILLY, 2007, p.16). Para poder penetrar na sociedade existe outro elemento chamado de capacidades (capabilities):

> Importa para o Estado não apenas alterar as condições da sociedade, mas ter capacidade para fazê-lo. Isso, porque (i) as capacidades existentes, mesmo se não empreendidas na ação, já causam alterações tanto na relação Estado-Sociedade, quanto na interação do Estado com o ambiente externo e (ii) a compreensão das capacidades específicas de um Estado possibilita antever e prognosticar suas ações potenciais no presente e no futuro. (CASTELLANO DA SILVA *et al*, 2012 p. 2).

Com o avanço das tecnologias houve uma nova forma de relacionamento e interação entre os Estados e a sociedade além de outros atores não estatais. Segundo

Castellano da Silva *et al* (2012) existem três campos de maior impacto da Era Digital a respeito do equilíbrio entre Estado e sociedade:

> Em primeiro lugar, seguem-se possibilidades de fortalecimento da Capacidade Estatal trazidas pelo emprego das TIC nas atividades que envolvem a capacidade de extração do Estado e de promoção da segurança, do bem-estar e da justiça. Em segundo lugar, no que concerne a avaliação do papel da sociedade perante o Estado devem ser levadas em consideração iniciativas de participação, de contestação e de prestação de serviços de caráter público. Há que se lembrar, todavia, que conforme cresce a difusão das TIC cresce o rol de ameaças e de vulnerabilidades aos Estados, aos atores econômicos e aos atores sociais de forma ampla. Em terceiro lugar, a Era Digital afeta a capacidade de interação das duas esferas (Estado e sociedade) na medida em que incentiva o aumento do fluxo e do processamento de informações e as vias de comunicação. (CASTELLANO DA SILVA *et al*, 2012 p. 7).

O trabalho se propõe como um estudo comparado e utiliza o método hipotético-dedutivo. Os objetos de referência serão os Estados Unidos e Brasil. Os Estados Unidos porque representa o maior processo de securitização do ciberespaço e possui as políticas de vigilância que possuem maior abrangência em sua população. O Brasil, pois possui uma securitização incipiente do ciberespaço e possui um incremento recente de políticas de vigilância recente.

A dissertação procura compreender os impactos da securitização do ciberespaço na capacidade coercitiva e na capacidade de vigilância no Brasil e Estados Unidos a partir dos acontecimentos de 11 de setembro de 2001, data em que o espaço cibernético começou a receber mais atenção dos Estados. Como objetivos específicos procura: a) Analisar o processo de securitização no meio cibernético; b) Analisar os processos de capacidade estatal no meio cibernético; c) Analisar os discursos de securitização de Brasil e Estados Unidos; d) Analisar como o Brasil e Estados Unidos estão estruturando sua defesa cibernética e como estão agindo para fazer tal proteção; e) Analisar as políticas de vigilância no meio cibernético dos Estados Unidos e Brasil.

A hipótese do trabalho é a de que a securitização do espaço cibernético nesses países trouxe efeitos positivos aos meios da capacidade coercitiva e efeitos negativos a efetividade da capacidade de vigilância. É importante notar que efetividade é um

conceito que tem relação com eficiência e eficácia. Eficiência se insere nos meios, ou seja, nas operações, enquanto a eficácia se preocupa em atingir os objetivos (DE CASTRO, 2006, p. 3). Efetividade é definida como:

> Efetividade: é o mais complexo dos três conceitos, em que a preocupação central é averiguar a real necessidade e oportunidade de determinadas ações estatais, deixando claro que setores são beneficiados e em detrimento de que outros atores sociais. Essa averiguação da necessidade e oportunidade deve ser a mais democrática, transparente e responsável possível, buscando sintonizar e sensibilizar a população para a implementação das políticas públicas. Este conceito não se relaciona estritamente com a ideia de eficiência, que tem uma conotação econômica muito forte, haja vista que nada mais impróprio para a administração pública do que fazer com eficiência o que simplesmente não precisa ser feito (TORRES, 2004, p. 175).

O estudo realizará duas comparações principais. A primeira será entre os impactos da securitização na capacidade coercitiva do Estado que será avaliada baseada em documentos oficiais, discursos e artigos da imprensa. A segunda entre os impactos da securitização na capacidade de vigilância do Estado que será avaliada com base nas políticas criadas para fazer a vigilância, a qualidade e quantidade de dados que Brasil e Estados Unidos conseguem processar para chegar a seus analistas.

As fontes adotadas serão primárias (documentos governamentais, relatórios) e secundárias (estudos empíricos e analíticos). Especialmente no que diz respeito à securitização do ciberespaço serão utilizadas fontes primárias como discursos das elites políticas, diretrizes das forças armadas sobre o domínio cibernético além da cobertura da imprensa sobre o assunto.

Por fim, as conclusões retomarão o que foi discutido ao longo dos capítulos, também, apresenta um quadro comparativo que demonstra como a securitização do espaço cibernético no Brasil e Estados Unidos acabaram fortalecendo os meios coercitivos principalmente pela criação dos comandos cibernéticos e enfraquecendo a efetividade da capacidade de vigilância devido à incapacidade de mostrar clareza e transparência nas ações de recolhimento de informações.

2 SOBRE A EVOLUÇÃO DOS ESTUDOS DE SEGURANÇA INTERNACIONAL, A SECURITIZAÇÃO DO ESPAÇO CIBERNÉTICO, CAPACIDADE COERCITIVA E DE VIGILÂNCIA

O presente capítulo possui como objetivo apresentar o aporte teórico para análise dos impactos da securitização do espaço cibernético na capacidade coercitiva e na capacidade de vigilância do Brasil e Estados Unidos. Primeiramente, serão explicados os avanços da teoria de segurança internacional para poder compreender a teoria da securitização do espaço cibernético e as ameaças que esse espaço pode provocar aos Estados. Em seguida, será debatida a capacidade coercitiva e a capacidade de vigilância no espaço cibernético.

2.1 SEGURANÇA INTERNACIONAL E A SECURITIZAÇÃO DO ESPAÇO CIBERNÉTICO

O estudo da Segurança Internacional é interdisciplinar e implica discussões sobre ética e moral. Várias teorias abordam o tema como o Realismo, Liberalismo, Teoria dos Jogos, Estudos da Paz, Construtivismo, Teoria Crítica e de Terceiro Mundistas. O marco dos estudos é no pós-segunda Guerra Mundial quando se começa a diferenciar estudos de segurança e defesa. A "era de ouro" dos estudos é na década de 50 e 60 quando houve o amparo da academia ao complexo militar e a iniciação dos Estudos da Paz e de Terceiro Mundo. Com a publicação do livro "People, States and Fear: The National Security Problem in International Relations" em 1983 por Barry Buzan da Escola de Copenhage acabou introduzindo perguntas fundamentais na área como qual seria a definição de segurança. Esses estudos pós-45 segundo Buzan e Hansen foram de importância, pois:

> Em primeiro lugar, levou a segurança ao invés de defesa ou guerra como seu conceito fundamental, uma mudança conceitual que abriu o estudo de um conjunto mais amplo de questões políticas, incluindo a importância da coesão social e da relação entre ameaças e vulnerabilidades militares e não militares. (BUZAN & HANSEN, 2009, p.1, tradução nossa). [3]

[3] No original: *"First, it took security rather than defence or war as its key concept, a conceptual shift which opened up the study of a broader set of political issues, including the importance of societal cohesion and the relationship between military and non-military threats and vulnerabilities."* (BUZAN & HANSEN, 2009, p.1)

O estudo sobre a definição de segurança, como abordar o tema e as novas perspectivas sobre segurança internacional é discutido entre duas escolas, a dos tradicionalistas e dos não tradicionalistas. Os tradicionalistas tem o Estado como o principal ator dos seus estudos e possuem uma epistemologia positivista materialista, após a Guerra Fria os estudos são focados nas políticas das Grandes Potências, na revolução dos assuntos militares e em regiões. Os não tradicionalistas aprofundam seus estudos para além do Estado, ampliando para setores políticos, sociais, econômicos e ambientais. Essa expansão conceitual surgiu no Pós-Guerra Fria e devido a agenda do neoliberalismo para os Estados, o conteúdo dessa expansão conceitual é uma tensão entre segurança individual, social e de definições de ameaças plausíveis para a segurança. Em 1994 com a divulgação do Relatório do Desenvolvimento Humano pelo Programa das Nações Unidas para o Desenvolvimento a Segurança Humana entra na agenda da ONU encobrindo estudos sobre discriminação racial, direito das mulheres e crianças afetadas por conflito. Essa agenda também inclui Pobreza, Ambiente e Saúde.

Com a expansão dos estudos de segurança internacional surgiu a segurança social que foi definida como a capacidade de uma sociedade de persistir em sua característica essencial sob mudanças nas condições e ameaças possíveis ou reais (Wæver *et al*., 1993: 23). A definição de segurança depende do sucesso da construção do seu discurso de ameaça (BUZAN, HANSEM, 2009, p. 213). Com a abordagem da securitização foi possível estudar segurança como um conceito que não é simplesmente uma condição (BUZAN, HANSEM, 2009, p. 214).

> A maneira de estudar a securitização é estudar o discurso e as constelações políticas: Quando é que um argumento com uma estrutura retórica e semiótica particular, consegue um efeito suficiente para fazer uma audiência tolerar violações de regras que de outra forma teriam que ser obedecidas? Se, por meio de uma discussão sobre a prioridade e a urgência de uma ameaça existencial o ator de securitização conseguiu libertar-se de procedimentos ou regras que ele ou ela iria de outra forma seriam

> vinculados por, estamos testemunhando um caso de securitização. (BUZAN *et al*, 1998, p. 25, tradução nossa).[4]

A securitização do ciberespaço se aprofundou a partir dos incidentes de 11 de setembro de 2001 devido ao uso das novas tecnologias por terroristas (Latham, 2003, p. 1). Segundo Cepik *et al* (2014, p. 5) existem duas tendências que fomentam o crescimento das ameaças no meio cibernético que são a ubiquidade e convergência digital. A ubiquidade trata a respeito da onipresença da rede, com dispositivo de todos os tipos conectando-se um ao outro por meio da Internet. A convergência digital é um fenômeno social complexo de integração de mídias distintas em um único canal de transmissão. Esse fenômeno acaba por transformar um celular em televisão, rádio, máquina fotográfica e plataforma de acesso à web ao mesmo tempo. Essas tendências trazem grandes benéficos econômicos e de interação entre as populações do planeta, porém, é nesses benéficos onde agentes procuram se por meios maliciosos obter vantagens próprias.

Apesar de a definição de guerra cibernética estar em aberto e qual o seu papel na revolução em assuntos militares (RMA)[5] houve diversos casos de sabotagem e espionagem cibernética. Dois eventos ilustram a complexidade e o potencial de ataques cibernéticos: os ataques sofridos pela Estônia em 2007 e o vírus Stuxnet. Em 27 de abril de 2007, o governo da Estônia decidiu fazer a transferência de uma estátua da época em que o país ainda participava da União Soviética e que representava a vitória sobre o nazismo na Segunda Guerra Mundial. Com a transferência da estátua que desagradou a minoria russa do país, se iniciou uma grande leva de ataques de negação de serviço. Ataques de negação de serviço (DDoS, em inglês) é uma tentativa de tornar os recursos de um sistema indisponíveis para os seus utilizadores pela sobrecarga do sistema devido a grande quantidade de informação. Devido a grande interação de

[4] No original: *"The way to study securitization is to study discourse and political constellations: When does an argument with this particular rhetorical and semiotic structure achieve sufficient effect to make an audience tolerate violations of rules that would otherwise have to be obeyed? If by means of an argument about the priority and urgency of an existential threat the securitizing actor has managed to break free of procedures or rules he or she would otherwise be boundby, we are witnessing a case of securitization."* (Buzan *et al*., 1998: 25)

[5] "Reunião de uma combinação complexa de inovações táticas, organizacionais, doutrinárias e tecnológicas para a implantação de uma nova abordagem conceitual em relação à guerra ou a um sub-ramo especializado dela" (KNOX, MURRAY, 2001, p. 12).

serviços do país com a Internet o caso se tornou questão de segurança nacional. A Estônia acusa a Rússia de ter participado nos ataques, os russos negam participação (RID, 2012, p. 14).

A primeira arma cibernética pode ser considerada o Stuxnet na medida em que seu objetivo não era roubar, manipular ou apagar informação, seu objetivo era destruir um alvo (Langner, 2011, p.49). Em 2010 o vírus tinha como alvo o sistema desenvolvido pela Siemens para controlar as centrífugas de enriquecimento de urânio iranianas. A partir do momento em que ele se infiltrou no sistema as centrífugas giraram 40% mais rapidamente, o que causou rachaduras nas centrífugas de alumínio. O vírus também conseguiu passar despercebido pelos técnicos que não percebem qualquer modificação em seu funcionamento. Segundo Knoepfel (2014), os desenvolvedores do Stuxnet foram Estados Unidos e Israel, pois seria necessário um alto nível de inteligência para obter conhecimento da planta do local das centrífugas, Israel possuía acessos a centrifugas similares as do Irã e devido à cooperação da Siemens com os Estados Unidos, os americanos teriam acesso ao software utilizado pelas centrífugas, o que seria essencial para desenvolver o vírus (KNOEPFEL, 2014, p. 121).

Para poder esclarecer os acontecimentos que se dão no espaço cibernético, pode-se categorizar esses acontecimentos de acordo com o quadro 1:

Quadro 1: Tipologia de conflitos cibernéticos segundo Möckly (2012)

Tipo de conflito	Caracterização
Hacktivismo	Mistura de ações hacker com ativismo político. Geralmente tem como objetivo a inviabilização de sítios eletrônicos e servidores.
Crime cibernético	Desenvolvimento de ações ilícitas com o emprego de computadores e da Internet.

Espionagem cibernética	Acesso não autorizado a computadores e servidores com a finalidade de se testar a configuração e os sistemas de defesa de um determinado computador, ou ganhar acesso a informações sigilosas.
Sabotagem cibernética	Criação de empecilhos ao desenvolvimento de processos e rotinas de trabalho nos setores público e privado a partir de meios eletrônicos, geralmente com motivações econômicas.
Terrorismo cibernético	Ataques ilícitos contra computadores – e a informação neles armazenadas – e redes computacionais com o objetivo de intimidar ou coagir governos e/ou suas populações para o alcance de objetivos políticos. Dos ataques, deve decorrer a violência contra bens e pessoas, tanto quanto for necessária para se gerar o nível de medo adequado ao rótulo de 'terrorismo cibernético' (grifos nossos). Nas palavras de Möckly (2012, p. 116, tradução nossa): "O termo é também usado de forma imprecisa e vaga para incidentes cibernéticos de natureza política variada".
Guerra cibernética	Emprego de meios eletrônicos para atrapalhar as atividades de um inimigo, bem como atacar sistemas de comunicação. Nas palavras de Möckly (2012, p. 116, tradução CEPIK,

	CANABARRO, BORNE, 2014): “[o] termo é também usado de forma imprecisa e vaga para incidentes cibernéticos de natureza política variada”.

Fonte: Elaborado e adaptado de CEPIK, CANABARRO, BORNE (2014).

Percebem-se novas vulnerabilidades que surgem no processo da digitalização, que é o é o processo pelo qual um determinado dado (imagem, som, texto) é convertido para o formato de dígito binário para ser processado por um computador. No plano militar, a digitalização diz respeito à confluência entre o radar, o infravermelho, o laser e as micro-ondas de alta potência. No jargão da área militar, é geralmente denominada como Revolução em Assuntos Militares (RMA) (MARTINS, 2008, p.7).

O processo da digitalização que possibilita a incorporação de novas tecnologias que possibilitam a adição de sistemas de armamentos ou a condução de tarefas combatentes, de inteligência e comando e controle com desempenho mais elevado e menores custos (DUARTE, 2011, p. 1). Tal processo permitiu uma nova discussão sobre seus impactos na distribuição de poder devida sua importância que ultrapassa apenas o meio militar. No processo militar a digitalização representa uma Revolução nos Assuntos Militares (RMA) devido a novas configurações de cadeia de comando, controle, comunicações e inteligência.

A ideia de se falar em uma revolução apenas em “assuntos militares” perde a dimensão dos impactos da digitalização na economia civil, que se reflete na confluência tecnológica entre televisão, o telefone e o computador, que passam a operar em uma mesma rede e em uma base de hardware comum. A mudança trouxe novos padrões para a produção material, para a administração de empresas e para a alavancagem e financiamento de negócios. Por isso o uso do termo digitalização (em vez de [Revolução nos Assuntos Militares]), devido a uma maior simplicidade e precisão (MARTINS, 2008, p. 7-8).

No meio militar a digitalização significa a capacitação através de computadores e redes de todos os armamentos e soldados, de maneira que todos saibam o que todos

estão fazendo permitindo uma melhor detecção de ameaças e a resposta a elas com o mínimo de contato com as forças oponentes e o máximo de precisão e eficiência (DUARTE, 2011, p.2). Também significa o suporte para operações físicas que dependem de suprimentos sendo entregue corretamente, soldados sendo movidos de um lugar para outro em um cronograma apertado e comunicações funcionando (ANDRESS, WINTERFIELD, 2013, p. 168). Como o caso dos veículos aéreos não tripulados (VANTs) que operando em alta altitude podem ser utilizadas como retransmissoras de dados sem fio, possibilitando uma comunicação além do horizonte tendo qualidades semelhantes aos satélites (ÁVILA, CEPIK, MARTINS, 2009, p. 68). A digitalização tornou a utilização de alta tecnologia com recursos reduzidos garantindo que seja acessível a diversos países. O comando do espaço possui uma característica única: a provisão livre, contínua e persistente de uma cobertura efetivamente global oferecendo grandes vantagens para a guerra de tropas expedicionárias, como a luta contra o terrorismo e outros exemplos de ambientes assimétricos de combate (ÁVILA, CEPIK, MARTINS, 2009, p. 68).

Alguma incursão no espaço, mesmo pequena, pode impactar diretamente o equilíbrio de poder internacional. Ou seja, as operações no espaço são interdependentes das realizadas nos ambientes aéreos, aquáticos e terrestres. A guerra no espaço é apenas um âmbito das esferas da estratégia e operações em época de guerra[6]. (ÁVILA, CEPIK, MARTINS, 2009, p. 68).

Além do comando do espaço que é definido como: controle das comunicações espaciais para fins militares, comerciais, de inteligência e direitos civis (KLEIN, 2004, p.67). O valor inerente de espaço é como um meio de comunicação; portanto, guerra espacial quer assegurar comando do espaço ou prevenção do inimigo de protegê-lo. Comando de espaço não significa que um adversário não pode agir, apenas que ele

[6] Entre as temáticas contemporâneas das esferas da estratégia e operações em época de guerra estão às novas formas de balanceamento (A2/AD) e novas formas de engajamento. A2/AD significa Anti-Access/Area Denial, o antiacesso seria interdição do acesso de forças navais inimigas a bases avançadas e a negação de área é a capacidade de derrotar forças navais móveis. O exemplo clássico é o da união soviética que definiu três perímetros defensivos para fazer frente a grupos de batalha estadunidenses. O exemplo atual ocorre entre China e Estados Unidos. A China vem fazendo uma modernização naval desde 1990 desenvolvendo fundamentos navais, missilísticos e informacionais.

não pode interferir seriamente em suas ações. O comando de espaço está normalmente em disputa (KLEIN, 2004, p. 67). Além dessa discussão, a digitalização vai discutir o fenômeno de guerra centrada em rede.

O espaço cibernético que é o domínio operacional onde pessoas e suas organizações usam e criam informações digitais e eletromagnéticas (KUEHL, 2009, p.29). Não se tem uma definição exata do que seria guerra no meio cibernético, o que se tem conhecimento é que redes de infraestruturas críticas são os principais alvos para ataque cibernético porque elas têm crescido ao ponto onde eles executam os sistemas de comando e controle, gerenciam a logística, habilitam o planeamento e as operações de pessoal, e é a espinha dorsal das capacidades de inteligência (ANDRESS, WINTERFIELD, 2013, p. 5).

Erik Gartzke (2013) afirma que a guerra cibernética não é uma revolução nos assuntos militares, mas sua premissa é de que vai aumentar as disparidades de poder e influência no sistema internacional. Para Adams (2001) os Estados Unidos são vulneráveis a ataques de grupos privados que impactariam na indústria privada guerra assimétrica, cujo impacto seria sentido não apenas no setor público, mas também na indústria privada. Stephen Walt (2010) argumenta que o conflito cibernético consiste em quatro elementos: diminuir as capacidades militares inimigas, desligar infraestrutura de civis, atividades criminais baseados na web e espionagem cibernética. Thomas Rid (2012) menciona que todos os ataques cibernéticos são versões sofisticadas de três atividades: sabotagem, espionagem e subversão e que a guerra cibernética não é suficientemente violenta ou causadora de baixas para ser considerada guerra. Esses aspectos sobre a guerra no meio cibernético precisam ser avaliados também pela ótica da capacidade coercitiva dos Estados que será discutida na próxima seção.

2.2 CAPACIDADE COERCITIVA

A definição de capacidade estatal diz sobre a capacidade efetiva do Estado de penetrar na sociedade e alterar a distribuição de recursos, atividades e conexões interpessoais (TILLY, 2007, p.16). Um dos aspectos da Capacidade Estatal são as capacidades de conseguir alterar as condições da sociedade, pois, as capacidades existentes, mesmo se não empreendidas na ação, já causam alterações tanto na

relação Estado-Sociedade, quanto na interação do Estado com o ambiente externo e a compreensão das capacidades específicas de um Estado que possibilita antever e prognosticar suas ações potenciais no presente e no futuro (CASTELLANO DA SILVA *et al*, 2012, p. 2). Em um Estado com Capacidade Estatal reduzido, agentes estatais têm efeitos limitados. Em um regime de alta capacidade, sempre que agentes do Estado agem, suas ações afetam os recursos dos cidadãos, atividades e conexões interpessoais de maneira excessiva (TILLY, 2007, p.16).

Tanto níveis muito baixos de Capacidade Estatal, quanto níveis muito altos, desfavorecem os processos necessários para a democratização. Por outro lado, níveis ótimos, que seria um nível bem balanceado, de Capacidade Estatal favorecem os processos que condicionam a democracia. No caso de baixa Capacidade Estatal, os elementos da sociedade são muito mais fortes que as estruturas do Estado, gerando espaço para conflitos civis, redes de poder autônomas e elites patrimonialistas. No caso de altíssima Capacidade Estatal, a força do Estado é desproporcionalmente maior do que a da sociedade, o que gera poucas condições e pode criar problemas para a conquista de direitos por parte do corpo social (CASTELLANO DA SILVA *et al*, 2012, p. 4).

Independente dos níveis de Capacidade Estatal nos processos para a democratização eles procuram integração de redes de confiança em políticas públicas, blindagem de políticas públicas de desigualdade categórica e verificação de centros de poder autónomos de forma a aumentar a influência popular sobre políticas públicas e o controle de políticas públicas sobre as ações do Estado (TILLY, 2007, p.184).

Com o surgimento na Era Digital e as Tecnologias de Informação e Comunicação (TIC) se manifestam novas influências na interação Estado-sociedade e uma inserção internacional de atores estatais e não estatais na busca pela conquista de seus objetivos políticos (CASTELLANO DA SILVA *et al*, 2012, p. 7). Segundo Castellano da Silva *et al* (2012) a Era Digital vai ter três campos de maior impacto na relação Estado-sociedade. Em primeiro lugar, pela possibilidade de fortalecimento da Capacidade Estatal trazidas pelo emprego das TIC nas atividades que envolvem a capacidade de extração do Estado e de promoção da segurança, do bem-estar e da justiça. Em

segundo lugar, no que importa a avaliação do papel da sociedade perante o Estado devem ser levadas em consideração iniciativas de participação, de contestação e de prestação de serviços de caráter público. Em terceiro lugar, a Era Digital afeta a capacidade de interação das duas esferas (Estado e sociedade) na medida em que incentiva o aumento do fluxo e do processamento de informações e as vias de comunicação (CASTELLANO DA SILVA *et al*, 2012, p. 7).

A Capacidade Estatal pode ser avaliada em três dimensões (HANSON & SIGMAN, 2013, p. 3): capacidade extrativa, capacidade coercitiva e capacidade administrativa. Capacidade extrativa diz sobre os meios necessários para alcançar as suas populações, coletar e gerenciar informações, possuir confiáveis agentes para administrar a receita e garantir o cumprimento popular da política fiscal. O aumento das receitas não é apenas uma função crítica do estado, mas também abrange um determinado conjunto de capacidades que são fundamentais ao poder do Estado (HANSON & SIGMAN, 2013, p. 4). Capacidade coercitiva se relaciona diretamente com a capacidade do Estado de preservar suas fronteiras, proteger contra ameaças externas, manter a ordem interna, e aplicar políticas. A capacidade administrativa é uma dimensão mais ampla, que inclui a capacidade de desenvolver políticas, a capacidade de produzir e entregar bens e serviços públicos, e a capacidade de regular atividade comercial. Administração política eficaz exige competência técnica, confiáveis agentes estatais, mecanismos de acompanhamento, de coordenação, alcance eficaz em todo o território do Estado e agrupamentos sociais.

A capacidade coercitiva é importante para o elemento de autoridade do Estado, autoridade é a aceitação do poder como legítimo que produz a atitude mais ou menos estável no tempo para a obediência incondicional às ordens ou às diretrizes que provêm de uma determinada fonte (BOBBIO, 1998, p. 90). Na hipótese hobbesiana que serve de fundamento à teoria moderna do Estado, a passagem do Estado de natureza ao Estado civil, ou da *anarchía* à *archia*, do Estado apolítico ao Estado político, ocorre quando os indivíduos renunciam ao direito de usar cada um a própria força, que os tornava iguais no estado de natureza, para confiá-lo a uma única pessoa, ou a um único corpo, que a partir da mudança de estado será o único autorizado a usar a força contra

eles (BOBBIO, 1998, p. 956). Para Pattnayak (1996) capacidade coercitiva do Estado refere-se também ao potencial do Estado para desempenhar o papel do árbitro final na área de gestão de conflitos sociais. A fim de garantir altas taxas de crescimento industrial, conflitos entre grupos terão de ser geridos ou dissuadidos pelo Estado (PATTNAYAK, 1996, p. 276). Pattnayak ainda argumenta que devido às experiências de desenvolvimento lideradas pelo Estado nas últimas décadas, pode-se argumentar que a capacidade de coerção pode agir como uma importante variável interveniente nos modelos que examinam a relação entre a dívida externa e do crescimento industrial (PATTNAYAK, 1996, p. 277).

Para mensurar a capacidade coercitiva pode se analisar tamanho militar ou sofisticação militar, bem como atributos do estado para promover a manutenção da ordem. Existem amplo estudo e levantamento de dados sobre estes itens para a maioria dos países no período da década de 1960 até o presente. Estados que têm a capacidade de manter a ordem podem ter forças militares e também uma segurança eficaz, embora haja países que conseguem manter a ordem com pouco ou nenhum poder militar. Uma grande força militar, por outro lado, pode ser um sinal de guerra ou insegurança, tanto que poderia chegar a uma condição de esgotar as capacidades do Estado (HANSON & SIGMAN, 2013, p. 6-7).

A capacidade coercitiva no meio cibernético vem recebendo grande atenção dos países atualmente. Segundo o *International Institute for Strategic Studies* (IISS) existem dois problemas principais para mensurar e comparar as capacidades cibernéticas dos países. O primeiro é que informações dessas capacidades geralmente são confidenciais e o segundo é relaciona a ubiquidade, a natureza do uso dual de ferramentas informáticas e cibernéticas, a discrição e rapidez das operações cibernéticas e a incerteza sobre as responsabilidades das organizações civis e militares (HACKETT, 2014, p.19).

> Compreender as capacidades cibernéticas militares exige a análise estratégica, tecnológica e de intenções políticas do Estado. Ele também envolve a compreensão de como os Estados compreendem o domínio cibernético. Nações, diferentes organizações e departamentos dentro os próprios Estados podem ter diferentes noções do termo

> "cibernética". Estes vão desde as tecnologias de informação que abrangem alguns aspectos da cibernética, incluindo os dados e as informações dentro dela, para uma noção doutrinária mais estrita da cibernética como uma corrente principal, camada de domínio cruzado de informações físicas de infraestrutura, computadores e rede (HACKETT, 2014, p. 19, tradução nossa).[7]

As capacidades militares no meio cibernético vão além das competências das forças armadas, pois o acesso a tecnologias, penetração da internet a população, liberdade da mídia digital, pesquisa e desenvolvimento na área cibernética pelas universidades e medidas legislativas podem ser avaliadas como capacidades a se considerar para mensurar capacidade coercitiva no meio cibernético (HACKETT, 2014, p.19-20). Portanto, qualquer discussão sobre as capacidades cibernéticas precisa incluir ambições de defesa nacional, as ameaças atuais previstas e conflitos, os recursos estatais, e a capacidade de suas forças armadas para se adaptar a novos desafios (HACKETT, 2014, p. 20).

O quadro desenvolvido pelo *International Institute for Strategic Studies* (IISS) estabelece os possíveis indicadores de capacidade cibernética envolvendo os meios políticos, militares, econômicos, sociais, de informação/tecnologia e infraestrutura. É importante ressaltar que devido às especificidades do espaço cibernético como a presença de ameaças, o cidadão comum e as forças coercitivas no mesmo domínio os indicadores sociais possuem destacada importância para a mensuração das capacidades coercitivas no meio cibernético.

Quadro 2: Possíveis indicadores de capacidade cibernética segundo o IISS

Indicadores	Variáveis
Político	Sistema Político; Estabilidade social; Ambição nacional; Posição Internacional;

[7] No original: *"Understanding military cyber capabilities requires analysis of states strategic, technological and political intentions. It also involves understanding how states themselves view the cyber domain. Nations – and also different organisations and departments within states – may have varying of the term "cyber". These range from information technologies that encompass some aspects of cyber, including data and the information within it, to a more strict doctrinal notion of cyber as a mainstream, cross-domain layer of physical information infrastructure, computers and network"* (HACKETT, 2014, p. 19).

	Relação de hackers com patrocínio estatal e objetivos políticos; Ação regulatória; Discussão parlamentar; Documentos de segurança nacional.
Militar	Doutrina e estratégia militar no ciberespaço; Organização estrutural; Adestramento, treinamento e exercícios; Operações conhecidas ou suspeitas; Inteligência; Material, logística e infraestrutura.
Econômico	Orçamento de defesa; Orçamento do programa de defesa; PIB; Matéria prima; Restrições de importação e exportação; Patentes; Financiamento de pesquisas e desenvolvimento; Empresas públicas de alta tecnologia; Produção de manufaturdos; Produtos de alto valor agregado.
Social	Estudantes pós-graduados; Ensino técnico superior; Maturidade da sociedade de informação; Graduação em ciência e engenharia; *Hackers* conhecidos; Intensidade de pesquisa e desenvolvimento; Concentração de pesquisadores.
Informação/Tecnologia	Controle do domínio; Densidade de alta tecnologia; *Know-how;* Inovação; Estado da arte da tecnologia; Varejo de eletrônicos; Tecnologia avançada

	(Sistema não tripulado, robótica).
Infraestrutura	Rede militar; SIGINT (*signals intelligence*)[8]; Comunicações; Acesso a conexão de alta velocidade; Serviços de boa qualidade; Número de fornecedores de acesso à internet (ISPs); Capacidades de exploração espacial; Base Industrial.
Outros	Compras e vendas estratégicas; Atenção política de segurança.

Fonte: Adaptado e traduzido de HACKETT (2014, p. 22).

As capacidades defensivas no espaço cibernético têm como objetivo principal a proteção de informação. As forças que fazem a proteção precisam se manter atualizadas com a criação de novas tecnologias e ter familiaridade com o *hardware* e *software* das forças inimigas (HACKETT, 2014, p. 21). As capacidades ofensivas precisam fazer uma avaliação de possivei alvos e para as forças obterem sucesso precisam esconder suas reais capacidades e ter capacidade de combinar os ataques cibernéticos com outros métodos de combate (HACKETT, 2014, p. 21-22).

2.2 CAPACIDADE DE VIGILÂNCIA

Capacidade de vigilância envolve a coleta de informações sobre populações para fins institucionais e pessoais (HAGGERTY, GAZSO, 2005, p. 170). Segundo Giddens (1988), a expansão da capacidade de vigilância é uma das razões fundamentais porque os Estados-nação são diferentes dos Estados tradicionais, devido ao fato de a sua capacidade de vigilância ser muito mais vasta e intensa do que alguma vez foi possível nos estados tradicionais, em virtude dos Estados modernos serem mais organizados (GIDDENS, 1988, p. 244).

Capacidade de inteligência é um importante fator para manter controle e segurança envolvido na capacidade de vigilância. Segundo Marco Cepik (2003) inteligência tem duas definições mais abrangentes. A primeira é que inteligência é toda

[8] Termo usado para descrever a atividade da coleta de informações ou inteligência através da interceptação de sinais de comunicação entre pessoas ou máquinas.

informação coletada, organizada ou analisada para atender as demandas de um tomador de decisões qualquer. A segunda mostra que inteligência é uma camada específica de agregação e tratamento analítico em uma pirâmide informacional, formada, na base, pode dados brutos e, no vértice, por conhecimentos reflexivos. Cepik vai utilizar uma definição mais específica que diz que inteligência é a coleta de informações sem o consentimento, a cooperação ou mesmo o conhecimento por parte dos alvos da ação (CEPIK, 2003, p. 28).

No espaço cibernético a inteligência deve ter o conhecimento prévio sobre a ameaça, conhecer e compreender, em tempo útil, as táticas, técnicas e procedimentos do adversário, proporcionar, em tempo hábil, que as operações baseadas em inteligência cibernética contribuam de maneira eficaz para a missão; evitar o gasto elevado em recursos para ações de recuperação e resposta a incidentes, e fornecer de forma imediata, dados partilháveis para desenvolver informações na condução proativa de segurança cibernética (FRIAS, 2013, p. 55). No meio cibernético o Estado consegue obter informações pra sua vigilância por meio de diversas práticas para interceptar a comunicação, que são complexas e interligadas e são projetadas para secretamente processar dados pessoais. Esses dados consistem em conteúdos como gravações de telefonemas, mensagens de texto, imagens das *webcams*, substância de mensagens de e-mail, entradas no Facebook, a história do acesso de um usuário da Internet a sites da *Web*, e *metacontent* que são dados de gravação dos meios de criação de dados transmitidos, a hora e a data da sua criação, o seu criador, e o local onde criado. Quando recolhidos, os dados e os metadados são mantidos durante um determinado período de tempo (como em *Tempora*[9]) e, em seguida, organizados por meio de plataformas de integração (como o PRISM[10]) para se tornar perceptível por meio da visualização de redes, começando com pessoas ou endereços de Internet que já estão sob suspeita (BAUMAN *et al*, 2014, p. 123).

[9] Tempora é o código para um sistema de computador secreto que é usado pelo British Government Communications Headquarters (GCHQ). Este sistema é utilizado para armazenar a maioria das comunicações de Internet que são extraídos a partir de cabos de fibra óptica, de modo que podem ser processados e pesquisados em um momento posterior.

[10] PRISM (programa de vigilância) é um dos programas do sistema de vigilância global da Agência de Segurança Nacional dos Estados Unidos (NSA) que foi mantido secreto desde 2007 e teve sua revelação na imprensa por meio de documentos fornecidos por Edward Snowden.

Com todas as informações que o espaço cibernético proporciona para a capacidade de vigilância é preciso analisar como e de que maneira vão ser analisadas essas informações. Essas informações podem acabar sendo uma instrumentaização dos serviços de inteligência por parte dos governantes para ganhos próprios ou a autonomização dos serviços e sua transformação em centros de poder independentes no sistema político (CEPIK, 2003, p. 186). Outro fator relacionado à quantidade de informações que chegam para o analista dessas informações coletadas é que ele não consegue ler todas e precisa se concentrar no que parecem ser os trechos mais significativos que mostram os nós específicos de conexões entre os dados (BAUMAN *et al,2014*, p.125), o que mostra o problema da efetividade das análises dessas informações. Portanto, o problema da efetividade na capacidade de vigilância é causado por dois pontos principais: o primeiro seria a incapacidade humana de analisar o alto número de informações e o segundo é devido a maneira como os órgãos do Estado estão captando essas informações que muitas vezes é feita de maneira sigilosa e assim suprimindo direitos e liberdades individuais.

2.3 CONCLUSÃO AO CAPÍTULO

Para compreender os impactos da securitização do espaço cibernético na capacidade coercitiva e de vigilância é necessário entender as especificidades desse domínio. A primeira especificidade é o momento em que o espaço começa a receber uma maior atenção para seus perigos, que é após o 11 de setembro de 2001. A segunda é a característica de o espaço cibernético conter informações secretas do Estado e do cidadão comum de todo o globo no mesmo domínio, o que acaba por dificultar a tomada de decisão devido a quantidade de informação que chega para o analista.

3 SECURITIZAÇÃO DO ESPAÇO CIBERNÉTICO E SEUS IMPACTOS NA CAPACIDADE COERCITIVA E DE VIGILÂNCIA NOS ESTADOS UNIDOS

O presente capítulo possui como objetivo apresentar impactos da securitização do espaço cibernético na capacidade coercitiva e na capacidade de vigilância dos Estados Unidos. Primeiramente, será explicada como se deu a securitização do espaço cibernético e as ameaças desse domínio para os Estados Unidos. Em seguida, será debatida a capacidade coercitiva e a capacidade de vigilância no espaço cibernético americano.

3.1 O PROCESSO DE SECURITIZAÇÃO DO ESPAÇO CIBERNÉTICO NOS ESTADOS UNIDOS

As atenções do governo norte americano no espaço cibernético começaram a partir do governo de Ronald Reagan (1981-1989) que tinha como uma das principais preocupações evitar divulgações prejudiciais de informações confidenciais. Enquanto o governo Bill Clinton (1993 – 2001) percebeu as ameaças cibernéticas como um dos perigos principais do século XXI, o do governo George W. Bush (2001 – 2009) a partir dos ataques de 11 de setembro passou de um foco muito forte em *cybertools* e métodos para a integração dos aspectos físicos de terrorismo (CAVELTY, 2007, p. 44-92), pois, os atentados destacaram o fato de que os terroristas poderiam atacar infraestruturas críticas fisicamente. Portanto, demonstrou a necessidade de reexaminar as proteções físicas estabelecendo o Departamento de Segurança Interna dos Estados Unidos (DHS[11]), o Conselho de Segurança Interna (HSC[12]), o estabelecimento de um escritório de cyber defesa na Casa Branca e mudanças no aspecto legal (CAVELTY, 2007, p. 104).

> Uma mudança significativa após 9/11 ocorreu no campo legal. A 'Unindo e fortalecendo a América Fornecendo as Ferramentas Apropriadas Necessárias para Interceptar e Obstruir o Terrorismo' [USA PATRIOT Act; PL 107 – 56, §506(a)], que se tornou lei em 26 de outubro de 2001, contém algumas das mudanças mais substanciais às leis de crimes cibernéticos dos Estados Unidos desde as revisões de 1996 e emendou a Fraude de Computador e o Ato de Abuso (CFAA 18 USC, §1030) em várias áreas altamente

[11] United States Department of Homeland Security.
[12] Homeland Security Council.

> controversas e críticas. O Ato Patriota foi uma versão de compromisso da Lei Antiterrorismo de 2001 (ATA). (CAVELTY, 2007, p. 104, tradução nossa).[13]

A Lei Antiterrorismo permitiu a expansão da competência das agências de aplicação da lei e de inteligência para monitorar comunicações privadas, acesso a informações pessoais e começou a tratar crimes cibernéticos como atos de terrorismo e propondo prisão perpétua para os criminosos no primeiro esboço da lei. A partir desse momento foi abandonada devido a iminente ameaça terrorista a proteção das liberdades individuais proposta pelo presidente Clinton (CAVELTY, 2007, p. 104-105). Em 2006 aconteceu o primeiro Cyber *Storm* que foi uma simulação em que organizações receberam ataques cibernéticos relacionado com vários cenários ao longo de quatro dias e obrigando-os a trabalhar com outras organizações para desenvolver estratégias e respostas aos ataques (LEBLANC *et al*, 2011, p. 98) e esse evento acabou mostrando que os Estados Unidos não estavam prontos para sofrer esse tipo de ataque (CAVELTY, 2007, p. 108).

Para Cavelty (2007), o objeto de referência[14] no processo de securitização para as orgaizações de aplicação de lei seria os crimes cibernéticos, para os militares seriam a guerra de informação, operações de informação e guerra cibernética. Para os cientistas da computação e técnicos em informática estavam preocupados com ataques, abuso e interrupções contra redes de computadores, conflitos de software, e outros *bugs* [15] que podem levar a falhas no sistema (CAVELTY, 2007, p. 126).

Com a chegada de Obama em 2009 houve uma revisão dos esforços da proteção da infreaestrutura de informação e comunicação:

> Em maio de 2009, o Presidente aceitou as recomendações resultantes da Revisão da Política do Espaço Cibernético, incluindo a seleção de um Coordenador de Segurança Cibernética do Poder Executivo que terá acesso regular ao Presidente. O Poder

[13] No original: *"A significant change after 9/11 occurred on the legal floor. The 'Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act' [USA PATRIOT Act; P.L. 107–56, §506(a)], which became law on 26 October 2001, contains some of the most substantial changes to US federal cyber-crime laws since the last major revisions of 1996 and amended the Computer Fraud and Abuse Act (CFAA 18 USC, §1030) in several critical, and highly controversial, areas. The PATRIOT Act was a compromise version of the Anti-Terrorism Act of 2001 (ATA)".*

[14] Objeto existencialmente ameaçado.

[15] Erro no funcionamento do hardware ou software.

> Executivo também foi direcionado para trabalhar em estreita colaboração com todos os setores na segurança cibernética dos Estados Unidos, incluindo o Estado, os governos locais e o setor privado, para garantir uma resposta organizada e unificada para futuros incidentes cibernéticos; fortalecer parcerias público/privadas para encontrar soluções tecnológicas que garantem a prosperidade e a segurança dos EUA; Investir na pesquisa de ponta e desenvolvimento necessário para a inovação e descoberta digital aos desafios do nosso tempo; e começar uma campanha para promover a conscientização de segurança cibernética e alfabetização digital de nossas salas de reuniões a nossas salas de aula e começar a construir a força de trabalho digital do século XXI (WHITE HOUSE, 2010, p. 1, tradução nossa).[16]

Esse documento (WHITE HOUSE, 2010) elencou três objetivos para a proteção dos Estados Unidos: estabelecer uma linha de frente de defesa contra ameaças imediatas compartilhando as informações sobre possíveis ameaças entre o governo federal, governos locais e parceiros privados, defender contra todo o tipo de ameaças, aumentando a capacidade de contra inteligência dos EUA e aumentar a segurança da cadeia de abastecimento para as principais tecnologias de informação e fortalecer o futuro ambiente de segurança cibernética pela expansão da educação cibernética e trabalhar para definir e desenvolver estratégias para deter a atividade hostil ou maliciosa no ciberespaço (WHITE HOUSE, 2010, p. 1-2). Esses objetivos vão ao encontro com o discurso de Obama de 2009 em que fala que o ciberespaço "é onde estão os documentos militares e de inteligência secretos, assim como a internet que nos fez mais interligado do que em qualquer momento na história humana. Assim, 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 empoderam aqueles que procuram perturbar e destruir. E esse paradoxo é

[16] No original: *"In May 2009, the President accepted the recommendations of the resulting Cyberspace Policy Review, including the selection of an Executive Branch Cybersecurity Coordinator who will have regular access to the President. The Executive Branch was also directed to work closely with all key players in U.S. cybersecurity, including state and local governments and the private sector, to ensure an organized and unified response to future cyber incidents; strengthen public/private partnerships to find technology solutions that ensure U.S. security and prosperity; invest in the cutting-edge research and development necessary for the innovation and discovery to meet the digital challenges of our time; and begin a campaign to promote cybersecurity awareness and digital literacy from our boardrooms to our classrooms and begin to build the digital workforce of the 21st century"*.

algo que experimentamos todos os dias” [17]. Em 2011, o governo americano propôs uma legislação em relação à cibersegurança devido a um pedido dos membros dos dois partidos no congresso que reconheceram a necessidade de uma renovação das leis. A legislação teve como objetivo proteger o povo americano, a infraestrutura crítica, e as redes e computadores do governo federal por meio do recrutamento de pessoal, esclarecer as penas para os crimes cibernéticos, planos de segurança cibernética das infraestruturas críticas, aquisição de *data centers*, entre outros.

Prosseguindo, em 2015, fica claro que a grande preocupação norte americana continua sendo a proteção das infraestruturas críticas (BERWANGER, 2015, p. 81). Em audiência com o Comitê de Inteligência do Senado o atual diretor da NSA, o Almirante Michael S. Rogers[18] reafirmou essa importância:

> 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[19] 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! […]

[17] No original: “*It's the classified military and intelligence networks that keep us safe, and the World Wide Web that has made us more interconnected than at any time in human history. 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. And this paradox -- seen and unseen -- is something that we experience every day.”* Disponível em: <https://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure>.

[18] Diretor da NSA de 2014 – atualmente.

[19] Diretor da NSA entre 2005 – 2014.

> 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 destrutivo direcionado 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. Transcrição e tradução (BERWANGER, 2015, p. 80).

Em sequencia, em julho de 2016 a presidência norte americana lançou uma diretiva (WHITE HOUSE, 2016) em relação aos incidentes cibernéticos mostrando cinco princípios que vão guiar as respostas do governo: 1) responsabilidade partilhada entre indivíduos, setor privado e agências governamentais na proteção contra atividades cibernéticas maliciosas. 2) Avaliação de risco na resposta do governo contra ataques que representam riscos para as entidades americanas. 3) Respeito as entidades afetadas salvaguardando os detalhes do incidente, bem como as liberdades de privacidade e civis, e as informações sensíveis do setor privado. 4) O primeiro orfão federal que tomar conhecimento de um incidente irá notificar rapidamente outras agências federais, a fim de facilitar uma resposta Federal unificada. 5) As respostas do governo serão conduzidas de forma a facilitar a restauração e recuperação de uma entidade que tem experimentado um incidente cibernético. No fim da diretiva é reafirmada a importância da segurança para a proteção da infraestrutura crítica.

Portanto, o objeto de referência da securitização do espaço cibernético americano é a proteção às Infraestruturas Críticas da Informação que passa pela

tentativa do governo norte americano, o ator securitizador[20], de conseguir ter a informação completa de todos os setores da sociedade.

3.2 AS CAPACIDADES COERCITIVAS DO ESPAÇO CIBERNÉTICO NOS ESTADOS UNIDOS

Em 2009 entra em funcionamento o Comando Cibernético dos Estados Unidos localizado em Fort Meade com três objetivos principais: 1) liderar a proteção de todas as redes de defesa e suporte militares e missões contra terrorismo no espaço cibernético. 2) Fornecer uma maneira clara e responsável de mobilizar recursos de guerra cibernética no meio militar. 3) Trabalhar com todos os possiveis parceiros dentro e fora do governo como a indústria privada (LYNN, 2010, p. 102). A cadeia de comando passa do presidente a todas as forças.

> Uma única cadeia de comando é executado do Presidente dos Estados Unidos para o Secretário da defesa para o comandante do Comando Estratégico para o comandante do Comando Cibernético e para unidades militares em todo o mundo. Para garantir que as considerações de segurança cibernética sejam uma parte regular do treino e equipamento dos soldados, o Comando Cibernético supervisiona comandos dentro de cada ramo das forças armadas, incluindo o Comando Cibernético do Exército, Décima Frota da Marinha dos Estados Unidos, Vigésima-Quarta Força Aérea e o Comando do Espaço Cibernético dos Fuzileiros Navais. Porque redes militares não estão imunes ao ataque, uma parte crítica da missão de treinamento é assegurar que todas as forças operacionais são capazes de funcionar em um ambiente de informação degradada (LYNN, 2010, p 102, tradução nossa).[21]

Além de uma cadeia de comando que permite uma resposta rápida a qualquer incidente o Pentágono implantou um sistema que inclui três linhas de defesa. A primeira

[20] Ator que securitiza a questão, declarando que o Objeto de Referência está ameaçado (ACÁCIO, 2012, p. 4).

[21] No original: *"A single chain of command runs from the US president to the Secretary of Defense to the commander of Strategic Command to the commander of Cyber Command and on to individual military units around the world. To ensure that considerations of cybersecurity are a regular part of training and equipping soldiers, Cyber Command oversees commands within each branch of the military, including the Army Forces Cyber Command, the U.S. Navy's Tenth Fleet, the 24th Air Force, and the Marine Corps Forces Cyberspace Command. Because military networks are not impervious to attack, a critical part of the training mission is to ensure that all operational forces are able to function in a degraded information environment"*.

é uma habitual *computer hygiene*[22] mantendo *software* e *firewalls* atualizados. A segunda é a utilização de sensores que detecta e localiza invasores. A terceira linha de proteção utiliza as capacidades de inteligência do governo para fornecer defesas eficazes por meio de tecnologias que funcionam na internet e nas redes de informação militares que detectam e param códigos maliciosos antes que entrem em ação nos sistemas militares. Como inevitavelmente algumas intrusões vão acontecer, a defesa precisa encontrar o invasor e isso é possível devido às instalações do Departamento de Defesa na área cibernética estar localizadas em um mesmo lugar[23]. Outro ponto importante da defesa é a articulação com aliados atráves de parcerias de inteligência principalmente com a OTAN[24] (LYNN, 2010, p. 102-105).

> Acordos mais fortes para facilitar a partilha de informação, tecnologia e inteligência devem ser feitos com um maior número de aliados. O relatório da OTAN de 2020, estudo encomendado pelaa OTAN presidido pela antiga Secretária de estado dos EUA Madeleine Albright, justamente, identificou a necessidade de novo "conceito estratégico" para incorporar a defesa cibernética ainda mais na aliança. O governo dos EUA deve garantir que a OTAN mova mais recursos para a segurança cibernética para que os Estados-Membros possam defender redes integrais para operações da Aliança (LYNN, 2010, p. 105, tradução nossa).[25]

A OTAN, em documento revelado em 2016 (OTAN, 2016) revelou suas ações de defesa no domínio cibernético com a criação do Centro de Excelência Cooperativo de Defesa Cibernética com o objetivo de pesquisa e centro de treinamento lidando com educação em cyber defesa, pesquisa e desenvolvimento. Criou também a Escola de Sistemas de Informação e Comunicações na Itália com o propósito de treinar pessoal de nações aliadas (assim como não-OTAN) relativas à operação e manutenção de alguns sistemas de comunicação e informação da OTAN. Para Hughes (2009) uma

[22] Manutenção do computador.
[23] A Agência de Segurança Nacional, A Escola de Defesa da Informação A Agência de Defesa dos Sistemas de Informação ficam localizados em Fort Head, Maryland.
[24] Organização do Tratado do Atlântico Norte.
[25] No original: *"Stronger agreements to facilitate the sharing of information, technology, and intelligence must be made with a greater number of allies. The report NATO 2020, a nato-commissioned study chaired by former U.S. Secretary of State Madeleine Albright, rightly identified the need for the alliance's new "strategic concept" to further incorporate cyberdefense. The U.S. government must ensure that nato moves more resources to cyberdefense so the member states can defend networks integral to the alliance's operations"*.

área que atrai mais atenção dos membros da OTAN é a criação de Equipes de Resposta a Emergências de Computador (CERT)[26] nacionais. O autor ainda argumenta que a OTAN atingiu dois grandes objetivos: A criação da Autoridade de Gestão de Cyber Defesa[27] e uma plataforma intelectual para pensar em longo prazo a doutrina e estratégia sobre o domínio cibernético através da formação do Centro de Excelência Cooperativo de Defesa Cibernética visando defender infraestruturas civis de ataques estatais ou não estatais (HUGHES, 2009, p 1-5). Fica claro que os Estados Unidos expandem sua estratégia de defesa cibernética com foco principal na defesa das infraestruturas críticas aliado a um grande compartilhamento de informações entre as principais entidades estatais e atores não estatais como Microsoft, Google e IBM, bem como com grupos de padrões internacionais como a Organização Internacional para Padronização e a Força de Tarefas de Engenharia da Internet[28] (IETF) (HUGHES, 2009, p. 4).

Em 2015 o orçamento da Presidência proposto para 2016 (WHITE HOUSE, 2015) foi de US $ 14 bilhões em segurança cibernética para pesquisa e iniciativas críticas. US$ 582 milhões é destinado ao Departamento de Segurança Interna dos Estados Unidos para coordenar a implementação do programa Contínuo Diagnóstico & Mitigação (CDM[29]) que vai dar assistência a agências em gerenciamento de riscos de segurança cibernética. Esse investimento no Departamento de Segurança Interna dos Estados Unidos também oferece suporte à implantação do Sistema de Proteção Nacional de Segurança Cibernética (mais conhecido como Einstein) para permitir que as agências detectem e previnam ameaças cibernéticas em evolução. US$ 149 milhões para o setor privado. US$ 243 milhões são repartidos para apoiar a investigação e desenvolvimento em agências civis de tecnologias inovadoras de segurança cibernética. Um dos maiores investimentos propostos pelo documento é para o Comando Cibernético do país. Na figura 1 está ilustrado os gastos informados.

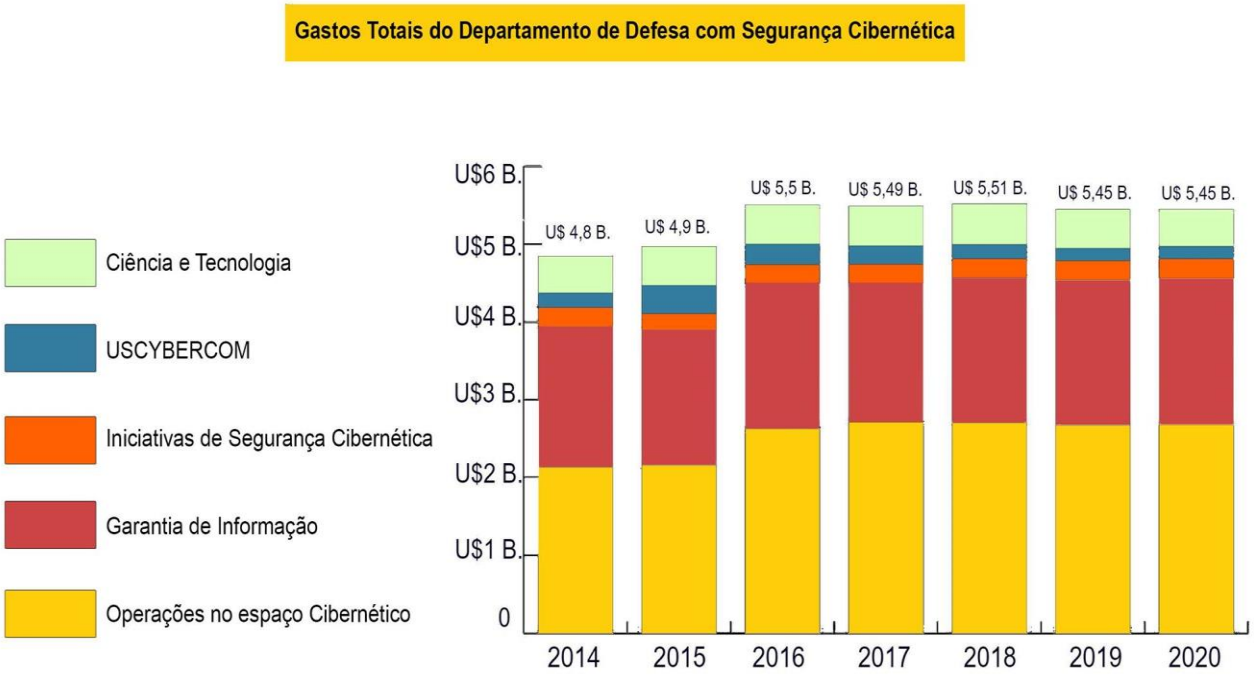
[26] Computer Emergency Response Teams (CERT).
[27] Cyber Defence Management Authority (CDMA).
[28] Internet Engineering Task Force (IETF).
[29] Continuous Diagnostics & Mitigation (CDM).

> "Segurança nacional e ameaças cibernéticas. US $ 514 milhões estão incluídos para o Departamento de Justiça para investigar invasões cibernéticas que representam sérias ameaças à segurança nacional e a estabilidade econômica do país e processar os criminosos. O orçamento também aborda segurança econômica por sustentar os esforços para modernizar e aumentar consideravelmente a eficiência e a capacidade do Tratado de Assistência Mútua Legal, e para apoiar os nossos esforços diplomáticos para proteger o livre fluxo de informações e comércio no espaço cibernético. Dentro do Departamento de Defesa, o orçamento inclui financiamento para continuar a desenvolver o Comando Cibernético com capacidade total" (WHITE HOUSE, 2015, p. 2, tradução nossa).[30]

O documento ainda reforça o pedido para modernizar e atualizar as autoridades de aplicação da lei e as sanções penais para que possam garantir a aplicação da lei tendo ferramentas para investigar, processar e interromper o cibercrimes além de para processar a venda no exterior de informações financeiras dos EUA roubadas, como números de cartão de crédito e contas bancárias.

[30] No original*: "National Security and Cyber Threats. $514 million is included for the Department of Justice to investigate cyber intrusions which pose serious threats to National security and the Nation's economic stability and to prosecute the offenders. The Budget also addresses economic security by sustaining efforts to modernize and vastly increase the efficiency and capacity of our Mutual Legal Assistance Treaty capabilities, and to support our diplomatic efforts to protect the free flow of information and commerce in cyberspace. Within the Department of Defense, the Budget includes funding to continue developing U.S. Cyber Command to its full strength"*.

Figura 1: Gastos Totais do Departamento de Defesa com Segurança Cibernética.



Fonte: Traduzido e adaptado de STERNTEIN (2015).

Outro fator necessário devido à securitização americana do espaço cibernético é a necessidade do capital humano que devido à população menor que de países como China e Índia os Estados Unidos precisam aliar a formação dos agentes de defesa cibernética com a superação tecnológica sobre seus rivais. Essa superação tecnológica se dá pela parceria com os investimentos no setor privado.

> "Fazendo uso da capacidade inovadora do setor privado também exigirá melhorias dramáticas em procedimentos do governo para a aquisição de tecnologia da informação. Em média, o Pentágono leva 81 meses para fazer um novo sistema de computador operacional após ser financiado. Tendo em conta o crescimento da computação sugerida pela lei de Moore, isto significa que quando os sistemas são entregues, eles já estão pelo menos quatro gerações atrás do estado da arte. Em comparação, o Iphone foi desenvolvido de 24 meses. Ou seja, menos tempo do que levaria o Pentágono para preparar um orçamento do novo sistema de computador e receber aprovação do Congresso para isso." (LYNN, 2011, p. 107, tradução nossa).[31]

[31] No original: *"Making use of the private sector's innovative capacity will also require dramatic improvements in the government's procedures for acquiring information technology. On average, it takes*

Para manter a agilidade na aquisição de tecnologias o Pentágono desenvolveu um sistema baseado em quatro princípios: 1) O processo de desenvolvimento de tecnologia deve ser rápido e durar de 12 a 36 meses ao invés de sete ou oito anos. 2) O Pentágono deve empregar desenvolvimento incremental e de testes ao invés de tentar implantar grandes sistemas complexos. 3) Os militares devem estar dispostos a sacrificar ou adiar alguma personalização para alcançar melhorias incrementais rápidas. 4) Necessidades de tecnologia de informação do departamento da defesa - que variam de modernizar os sistemas de comando e controle nucleares para atualizar o software de processamento de texto - exigem diferentes níveis de supervisão (LYNN, 2011, p 107). Lynn (2011) destaca que esses quatro princípios são essenciais para a eficácia da segurança americana quando se trata de defesa cibernética forjando essa estratégia que consiste em desenvolver uma construção organizacional para treinar, equipar e comandar as forças de defesa cibernética; empregar em camadas as proteções com um núcleo forte de defesas ativas; usar capacidades militares para apoiar os esforços dos outros departamentos e proteger as redes que executam as infraestruturas críticas dos Estados Unidos e para construir as defesas coletivas com os aliados dos EUA para assim proteger a economia e o país.

A securitização também afetou e foi afetada pela política externa dos Estados Unidos. O Stuxnet que foi descrito no capítulo anterior foi usado para poder dissuadir Israel de atacar o Irã e conseguir retardar o projeto nuclear desse país (LOPES, DE OLIVEIRA, 2014, p. 63).

> Nas gestões de George W. Bush e Barack Obama, ou pelo menos na transição entre ambas, o uso do poder cibernético teve duas dimensões. Uma aberta, encabeçada por Richard Clarke (mesmo não trabalhando com Obama, Clarke não deixa de transmitir uma visão do establishment de segurança nacional dos EUA). A outra fechada, embora esteja sendo revelada aos poucos (SANGER, 2012). A dimensão aberta objetivava mostrar que a “guerra cibernética” não interessava aos EUA, desviando a atenção da dimensão fechada, que utilizou da

---

the Pentagon 81 months to make a new computer system operational after it is first funded. Taking into the account the growth of computing power suggested by Moore's law, this means that by the time systems are delivered, they are already at least four generations behind the state of the art. By comparison, the iPhone was developed 24 months. That is less time than it would take the Pentagon to prepare a budget and new Computer System receive congressional approval for it.”.

> “guerra cibernética” e espionagem cibernética para alcançar fins de política externa: atrasar o programa nuclear do Irã, e possivelmente outros objetivos que ainda não vieram à público (DE ARAÚJO JORGE, 2012, p. 47).

Portanto, a securitização do espaço cibernético permitiu aos Estados Unidos novas estratégias para agir no sistema internacional e o transformou junto com a Rússia e a China como grande potência em capacidades cibernéticas. A doutrina americana foi desenvolvida ao longo das últimas décadas e teve como foco principal a defesa das infraestruturas críticas.

3.3 CAPACIDADE DE VIGILÂNCIA DO ESPAÇO CIBERNÉTICO NOS ESTADOS UNIDOS

A popularização da internet acabou atraindo todos os setores da sociedade em um espaço onde existe uma grande troca de informações inclusive entre ações criminosas. Kerr (2003) descreve que “o objetivo fundamental de uma rede de comunicações é enviar e receber comunicações. Como resultado, cada rede de comunicações apresenta dois tipos de informações: o conteúdo das comunicações e o endereçamento e informações de roteamento que as redes usam para entregar conteúdos de comunicações. O primeiro é "informações de conteúdo", e o último é "informações do envelope.". A distinção essencial entre as informações de conteúdo e envelope permanece constante através de diferentes tecnologias, de correio postal para o e-mail. As informações de conteúdo para um e-mail são a mensagem no corpo do e-mail em si, bem como a conversa telefônica ou a carta no envelope. O e-mail também carrega informações de endereçamento em um cabeçalho de "correio". Cabeçalhos de e-mail são carimbos digitais que acompanham cada e-mail e transportam informações sobre a entrega do correio” (Kerr, 2003, p. 611-612). Um entendimento completo de vigilância da Internet deve ir além de vigilância e-mail para englobar a vigilância das comunicações homem-para-computador e o computador a computador. Kerr (2003) ainda destaca que a internet é uma rede de "comutação de pacote", que significa que todas as comunicações enviadas pela Internet são divididas em pacotes individuais e

que os computadores se comunicam uns com os outros pelo envio e recebimento de pacotes de informação através da Internet (KERR, 2003, p. 613).

> Vigiar a Internet em nível de pacote fornece uma segunda maneira de se realizar a vigilância da Internet que pode ser considerada distinta da vigilância de e-mail. Como outras formas de vigilância, vigilância de pacote divide-se em informações do envelope e informações de conteúdo. Quando um computador envia informações através da Internet, quebra a comunicação em pacotes e cria um "cabeçalho" para direcionar o pacote ao seu destino. O Cabeçalho contém informações de endereçamento, como o de e para endereços de Internet dos dois computadores, muitas vezes referida como os endereços de protocolo de Internet, ou simplesmente endereços IP, bem como informações sobre que tipo de pacote é (por exemplo, parte de uma página da web, parte de um arquivo de imagem). Quando o pacote chega ao seu destino, o computador receptor descarta o cabeçalho do pacote e mantém a mensagem original. A nível de pacote, esta mensagem é a informação de conteúdo no pacote, geralmente referido como "carga" do pacote. Algumas comunicações, tais como páginas da web em trânsito, normalmente são "empacotadas" apenas uma vez: o computador anfitrião cria os pacotes, e o computador de destino descarta os cabeçalhos de pacote e os reconstrói o arquivo original quando os pacotes chegam. Outras comunicações podem ser empacotadas várias vezes sobre o curso de entrega. Por exemplo, um e-mail pode ser dividido em pacotes e remontado para o e-mail original algumas vezes na sua viagem de remetente para o receptor. (KERR, 2003, p. 613, tradução nossa).[32]

Os programas da Agência Nacional de Segurança americana têm como objetivo colher dados de cabos de Internet (subaquáticos) e/ou interceptar dados durante as

[32] No original: *"Surveilling the Internet at the packet level provides a second way of conducting Internet surveillance that can be considered distinct from email surveillance. Like other forms of surveillance, packet surveillance divides into envelope information and content information. When a computer sends information across the Internet, it breaks the communication into packets and creates a "packet header" to direct the packet to its destination. The packet header contains addressing information, such as the to and from Internet addresses of the two computers, often referred to as the Internet Protocol addresses, or simply IP addresses, as well as information about what kind of packet it is (e.g., part of a web page, part of a picture file). When the packet arrives at its destination, the receiving computer discards the packet header and keeps the original message. At the packet level, this message is the content information in the packet, generally referred to as the packet's "payload." Some communications, such as web pages in transit, typically are "packetized" only once: the host computer creates the packets, and the destination computer discards the packet headers and reassembles the original file when the packets arrive. Other communications can be packetized several times over in the course of delivery. For example, an email may be broken down into packets and reassembled into the original email a few times on its trip from sender to receiver"*.

viagens (Tempora). Eles envolvem o posicionamento de interceptores nos grandes cabos de fibra óptica conectando os hubs[33] diferentes da Internet (BAUMAN *et al*, 2014, p. 122). Para conseguir esses dados muitas vezes a agência trabalha com o serviço privado.

> Isso envolve a aquisição de dados pessoais de consumidores, forçando as empresas privadas (como Google, Microsoft, Apple ou Skype) regularmente coletar grandes quantidades de dados para fins comerciais e entregar para os serviços de inteligência, sem o conhecimento dos usuários. Acredita-se que a NSA e vários serviços europeus obtiveram grandes quantidades de dados precisos através deste processo. Isso não é reunido através de dados brutos transitando cabos, mas está principalmente ligado com a disposição dos usuários em utilizar os serviços de nuvem de computação — fornecida, por exemplo, por plataformas como Microsoft ou Dropbox — e sua ignorância da coleção secreta de seus dados. Este é também o caso com informações provenientes de redes sociais, tais como aquelas gerenciadas pelo Facebook. Tais dados e metadados permitem um mapeamento das relações entre as pessoas, seus endereços IP e o compartilhamento de conteúdo, localização e interesses (BAUMAN *et al*, 2014, p. 123, tradução nossa).[34]

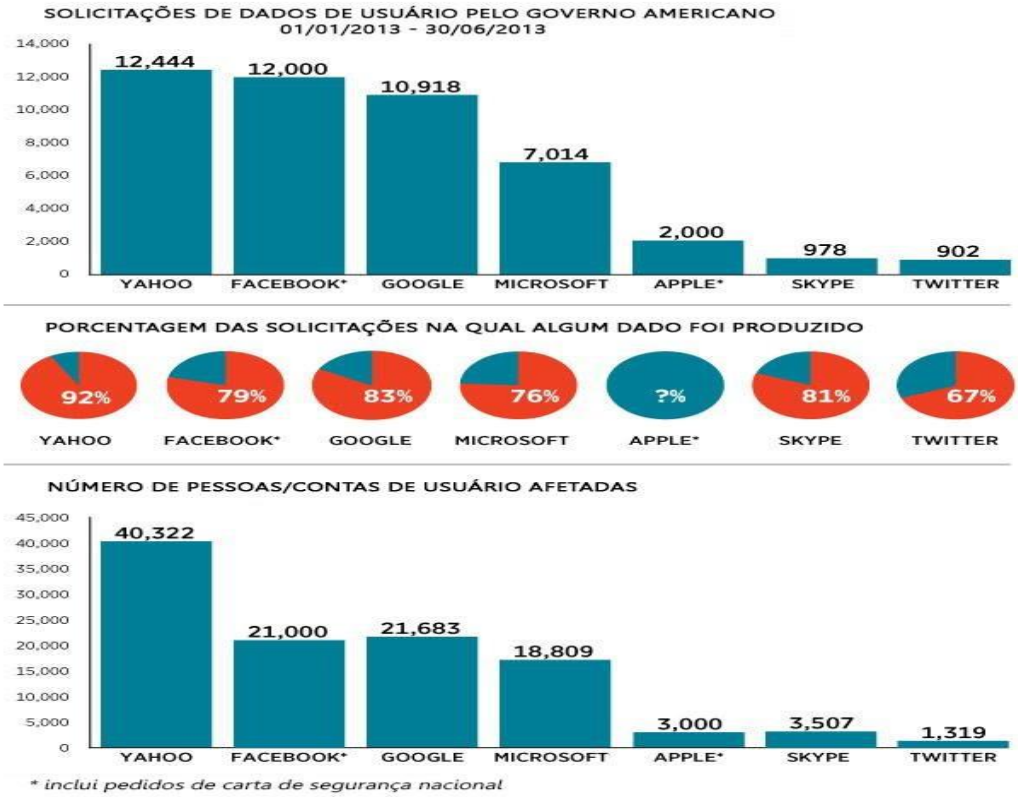
Assim, fica claro o motivo dos Estados Unidos de procurar as empresas privadas para trabalharem com as agências de segurança, pois, além de conseguirem informações como o IP e de interesses pessoais, essas empresas são transnacionais e conseguem informações valiosas (BAUMAN *et al*, 2014, p. 123). Na figura número 2 é possível ver o alto número de pedidos feito pelo governo americano para conseguir informações. Bauman *et al* (2014) ainda relata a importância geográfica dos cabos submarinos que pode dar vantagens a certos países na política internacional (BAUMAN *et al*, 2014, p.123).

---

[33] Processo pelo qual se transmite ou difunde determinada informação.

[34] No original: *"This involves the acquisition of consumers' personal data by forcing those private companies (such as Google, Microsoft, Apple, or Skype) regularly collecting vast amounts of data for commercial purposes to hand it over to the intelligence services without the knowledge of users. The NSA and several European services are believed to have obtained large amounts of precise data through this channel. It is not gathered through raw data transiting cables but is mostly connected with the willingness of users to use the services of cloud computing—provided, for example, by Microsoft platforms or Dropbox—and their ignorance of the secret collection of their data. This is also the case with information coming from social networks, such as the ones managed by Facebook. Such data and metadata permit a mapping of relations between people, their IP addresses, and the sharing of content, location, and interests".*

Figura 2: Solicitações de Dados de Usuário Pelo Governo Americano



Fonte: Traduzido e adaptado de HILL (2015).

Com as declarações de Edward Snowden, ex-contratado da Agência de Segurança Nacional que revelou detalhes da vigilância global realizado pelos Estados Unidos, se pôde ter uma dimensão da quantidade de informações que as principais agências são capazes de conseguir. No entanto, essa grande quantidade de informações também se torna quase impossível de avaliar por um analista.

> Desde o 11 de Setembro, o número de horas de que os funcionários da Força Aérea necessitam para reciclar as informações fornecidas pelos *drones* aumentou 3.100% - e a cada dia mais 1.500 horas de vídeos são acrescentadas ao volume de informações que demandam processamento. Quando a limitada visão “em túnel” dos sensores dos *drones* for substituída por uma “visão de Górgona”, capaz de abarcar uma cidade toda de uma só vez (desenvolvimento iminente), serão necessários 2 mil analistas para tratar as informações transmitidas por um único *drone*, em lugar dos noventa que hoje fazem esse trabalho. Mas isso apenas significa, permita-me comentar, que pescar um objeto “interessante” ou “relevante” num poço de dados sem fundo vai exigir trabalho duro e custar muito dinheiro; não que qualquer objeto potencialmente interessante possa

> garantir-se contra a possibilidade de ser arrastado para esse poço. (BAUMAN, LYON, 2014. p. 27-28)

Bauman *et al* (2014) coloca que a vigilância em larga escala é devido a conjunção dos três processos tornaram-se interligados: transnacionalização, digitalização e privatização. Para os autores “este conjunto cria um efeito global de dispersão que desafia a ideia de uma razão de estado conduzido por um "estado" em que o governo determina os interesses nacionais e da segurança nacional” e que, portanto pode se “sugerir que o que ainda chamamos de segurança nacional tem sido colonizada pelas agências de inteligência operando em uma arena transnacional cada vez mais autónoma” com isso as agencias de inteligência “desafiam a autoridade dos cidadãos nacionais reconfigurando as ideias de privacidade, sigilo de comunicação, a presunção de inocência e até mesmo democracia” (BAUMAN *et al*, 2014, p. 126). Bauman *et al* (2014) ainda sugere que as agências nacionais de segurança dos Estados Unidos e da Europa colonizaram a segurança nacional em uma arena transnacional com troca de informações recolhidas de todo o globo. Esse papel é liderado pela a Agência de Segurança Nacional americana que tem cerca de doze a quinze vezes mais funcionários e um orçamento maior também assim os Estados Unidos construíram uma estrutura assimétrica em que consegue adquirir informações além das suas capacidades técnicas (BAUMAN *et al*, 2014, p. 127). Esses dados em massa adquiridos em sigilo e sem o consentimento da sociedade se tornam incapaz de se analisar especificamente então as ameaças e alvos são traçados em perfis genéricos, assim, não sendo respeitados os direitos individuais. (BAUMAN *et al*, 2014, p. 129).

3.4 CONCLUSÃO DO CAPITULO

Ao longo deste capitulo pôde-se perceber alguns impactos da securitização nas capacidades coercitivas e de vigilância dos Estados Unidos. A agenda da segurança cibernética ocorreu a partir da década de 1980 e o assunto se tornou securitizado a partir dos acontecimentos dos 11 de setembro. Em relação às capacidades coercitivas

se deu em relação à proteção das infraestruturas críticas do país e tornou o país um dos mais capazes de atuar no espaço cibernético devido a políticas para conseguir adquirir tecnologias rapidamente. Na questão da capacidade de vigilância os Estados Unidos criaram um sistema que consegue captar uma grande quantidade de informações o que torna improvável para analistas de inteligência processar toda informação e devido a essa captação de dados ocorrerem de forma sigilosa e em larga escala acaba suprimindo os direitos individuais de liberdade.

4 SECURITIZAÇÃO DO ESPAÇO CIBERNÉTICO E SEUS IMPACTOS NA CAPACIDADE COERCITIVA E DE VIGILÂNCIA NO BRASIL

O presente capítulo possui como objetivo apresentar impactos da securitização do espaço cibernético na capacidade coercitiva e na capacidade de vigilância do Brasil. Primeiramente, será explicada como se deu a securitização do espaço cibernético e as ameaças desse domínio para o Brasil. Em seguida, será debatida a capacidade coercitiva e a capacidade de vigilância no espaço cibernético brasileiro.

4.1 O PROCESSO DE SECURITIZAÇÃO DO ESPAÇO CIBERNÉTICO NO BRASIL

O processo de securitização no Brasil começou a partir do ano 2000 com o lançamento do primeiro documento oficial que trata sobre o tema, que foi elaborado pelo Ministério da Ciência e Tecnologia: Sociedade de Informação: Livro Verde que tinha o objetivo de elaborar as metas de implementação do Programa Sociedade da Informação e constituir uma súmula consolidada de possíveis aplicações de Tecnologias da Informação para impulsionar a Sociedade da Informação no Brasil em todos os seus aspectos: ampliação do acesso, meios de conectividade, formação de recursos humanos, incentivo à pesquisa e desenvolvimento, comércio eletrônico, desenvolvimento de novas aplicações (2000, p. v). Segundo Acácio (2012, p. 5), no âmbito da legislação é necessário distinguir dois momentos: (2000-2005) e (2005 - atualmente). No primeiro momento o tema seria caracterizado como politizado e atinge patamares de uma securitização incipiente a partir de 2005. O primeiro momento começa com o decreto 3505 de 13 de junho de 2000 quando começou a se evidenciar que o tema era sensível à segurança do Estado. Esse decreto instituiu um Comitê Gestor da Segurança da Informação, subordinado à Secretaria-Executiva do Conselho de Defesa Nacional e definiu o conceito de Segurança da informação como:

> Segurança da Informação: proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento. (BRASIL, 2000).

Outro marco importante veio com o Decreto nº 4.829, de 03 de setembro de 2003 foi criado o Comitê Gestor da Internet no Brasil – CGIbr[35], com as atribuições de estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil; estabelecer diretrizes para a organização das relações entre o Governo e a sociedade, na execução do registro de Nomes de Domínio, na alocação de Endereço IP (*Internet Protocol*) e na administração pertinente ao Domínio de Primeiro Nível (*ccTLD - country code Top Level Domain*), "**.br**", no interesse do desenvolvimento da Internet no País; promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais, para a segurança das redes e serviços de Internet, bem assim para a sua crescente e adequada utilização pela sociedade; propor programas de pesquisa e desenvolvimento relacionados à Internet, que permitam a manutenção do nível de qualidade técnica e inovação no uso, bem como estimular a sua disseminação em todo o território nacional, buscando oportunidades constantes de agregação de valor aos bens e serviços a ela vinculados; articular as ações relativas à proposição de normas e procedimentos relativos à regulamentação das atividades inerentes à Internet; ser representado nos fóruns técnicos nacionais e internacionais relativos à Internet; adotar os procedimentos administrativos e operacionais necessários para que a gestão da Internet no Brasil se dê segundo os padrões internacionais aceitos pelos órgãos de cúpula da Internet, podendo, para tanto, celebrar acordo, convênio, ajuste ou instrumento congênere e deliberar sobre quaisquer questões a ele encaminhadas, relativamente aos serviços de Internet no País.

A partir do Decreto Nº 5484, de 30 de Junho de 2005 o Estado brasileiro começou a ter uma maior atenção com o tema definindo como objetivo: “Para minimizar os danos de possível ataque cibernético, é essencial a busca permanente do aperfeiçoamento dos dispositivos de segurança e a adoção de procedimentos que

[35] O CGIbr é formado por representantes do setor governamental, representante de notório saber em assuntos da internet, representantes do setor empresarial como de provedores de acesso da Internet e provedores de infraestrutura de telecomunicações, representantes do terceiro setor, representantes da comunidade científica e tecnológica e um secretário executivo. Portanto, o CGIbr é um importante comitê com a participação de diversos membros da sociedade brasileira para discutir o desenvolvimento da Internet no Brasil.

reduzam a vulnerabilidade dos sistemas e permitam seu pronto restabelecimento" e como diretriz: "aperfeiçoar os dispositivos e procedimentos de segurança que reduzam a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra ataques cibernéticos e, se for os casos permitam seu pronto restabelecimento" (BRASIL, 2005). Esse documento foi o primeiro a mostrar as percepções de ameaça cibernética do Brasil.

Em 2008 com a Estratégia Nacional de Defesa (2008) e que "trata de questões políticas e institucionais decisivas para a defesa do País, como os objetivos da sua "grande estratégia" e os meios para fazer com que a Nação participe da defesa". Teve como uma de suas diretrizes "fortalecer três setores de importância estratégica: o espacial, o cibernético e o nuclear" e com isso "os setores espacial e cibernético permitirão, em conjunto, que a capacidade de visualizar o próprio país não dependa de tecnologia estrangeira e que as três Forças, em conjunto, possam atuar em rede, instruídas por monitoramento que se faça também a partir do espaço" (BRASIL, 2008, p. 12). Em relação às capacitações cibernéticas a END se manifesta especialmente em relação à capacidade do uso da rede pelas forças:

> As capacitações cibernéticas se destinarão ao mais amplo espectro de usos industriais, educativos e militares. Incluirão, como parte prioritária, as tecnologias de comunicação entre todos os contingentes das Forças Armadas de modo a assegurar sua capacidade para atuar em rede. Contemplarão o poder de comunicação entre os contingentes das Forças Armadas e os veículos espaciais. No setor cibernético, será constituída organização encarregada de desenvolver a capacitação cibernética nos campos industrial e militar. (BRASIL, 2008, p.36)

Esse documento dá ênfase "as medidas para a segurança das áreas de infraestruturas críticas, incluindo serviços, em especial no que se refere à energia, transporte, água e telecomunicações, a cargo dos Ministérios da Defesa, das Minas e Energia, dos Transportes, da Integração Nacional e das Comunicações, e ao trabalho de coordenação, avaliação, monitoramento e redução de riscos, desempenhado pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR)" (BRASIL, 2008, p. 65). Os três setores de importância estratégica foram destinados a uma das Forças Armadas: o setor nuclear na Marinha do Brasil (MB), o setor aeroespacial, com

a Força Aérea Brasileira (FAB) e o cibernético, com o Exército Brasileiro. Acácio ressalta que a Força Aérea e a Marinha ficaram com projetos que já tinham *expertise* com projetos em andamento enquanto o Exército do ponto de vista doutrinário e mesmo institucional ainda tinha com incipiente a questão da segurança cibernética. A Marinha com o projeto do submarino e do Centro Tecnológico da Marinha, e a especificidade da área da Força Aérea com o setor aeroespacial. Ainda em 2008 pela Portaria GSI/PR nº 31, de 06 de outubro de 2008, institui a Rede Nacional de Excelência em Segurança da Informação e Criptografia – RENASIC que tem por objetivo elevar a competência brasileira em Segurança da Informação e Criptografia (SIC).

Para poder se adequar para a proteção do espaço cibernético o Exército Brasileiro passou por diversas atualizações institucionais e de conceitos. Com o Glossário Militar das Forças Armadas (2007) foi definido guerra cibernética como: "Conjunto de ações para uso ofensivo e defensivo de informações e sistemas de informações para negar, explorar, corromper ou destruir valores do adversário baseados em informações, sistemas de informação e redes de computadores. Estas ações são elaboradas para obtenção de vantagens tanto na área militar quanto na área civil" (BRASIL, 2007, p. 123). No âmbito institucional o Exército Brasileiro criou o Centro de Defesa Cibernética do Exército e o Núcleo do Centro de Defesa Cibernética do Exército

> Internalizando a percepção da ameaça e organizando-se institucionalmente para responder a nova missão atribuída pela END, o Exército Brasileiro instituiu o "setor cibernético" em seu âmbito por meio da Portaria do Comandante do Exército nº 03-RES, de 29 de junho de 2009. Em 4 de agosto de 2010, esse Exército decidiu, por meio das portarias 666 e 667, respectivamente, abrir o Centro de Defesa Cibernética do Exército e o Núcleo do Centro de Defesa Cibernética do Exército. (Acácio, 2012, p. 9)

Em 2009 com o Decreto nº 7.009, de 12 de novembro inclui os temas de atividade de inteligência; segurança para as infraestruturas críticas, incluindo serviços; segurança da informação e segurança cibernética os objetivos da Câmara de Relações Exteriores e Defesa Nacional - CREDEN do Conselho de Governo com a finalidade de formular políticas públicas e diretrizes de matérias relacionadas com a área das

relações exteriores e defesa nacional do Governo Federal. Ainda em 2009, a Portaria CREDEN nº45, de 8 de setembro de 2009, instituiu o Grupo Técnico de Segurança Cibernética, com objetivo de propor diretrizes e estratégias para a Segurança Cibernética, no âmbito da Administração Pública Federal e descreve Infraestrutura Críticas como: “as instalações, serviços, bens e sistemas que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade” e descreve Segurança Cibernética como a “arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus Ativos de Informação e suas Infraestruturas Críticas”.

No ano de 2012 foram aprovadas duas leis. A Lei nº 12.737, de 30 de novembro de 2012, a qual dispõe sobre a tipificação criminal de delitos informáticos e a Lei nº 12.735, de 30 de novembro de 2012, a qual tipifica as condutas realizadas mediante uso de sistema eletrônico, digital ou semelhante, que sejam praticadas contra sistemas informatizados e similares. Pela Portaria Normativa nº 3.389/MD é aprovado a Política Cibernética de Defesa com a finalidade de orientar, no âmbito do Ministério da Defesa (MD), as atividades de Defesa Cibernética, no nível estratégico, e de Guerra Cibernética, nos níveis operacional e tático, visando à consecução dos seus objetivos e com objetivos como: a) assegurar, de forma conjunta, o uso efetivo do espaço cibernético (preparo e emprego operacional) pelas Forças Armadas; b) capacitar e gerir talentos humanos necessários à condução das atividades do Setor Cibernético (St Ciber) no âmbito do MD e c) d) desenvolver e manter atualizada a doutrina de emprego do St Ciber. A Política Cibernética de Defesa teve como diretrizes: a) conceber e implantar o Sistema Militar de Defesa Cibernética (SMDC), contando com a participação de militares das FA e civis; b) levantar as infraestruturas críticas de informação associadas ao St Ciber para contribuir com a formação da consciência situacional necessária às atividades de Defesa Cibernética; c) estabelecer critérios de risco, inerentes aos ativos de informação, e realizar o seu gerenciamento, reduzindo os riscos às infraestruturas críticas da informação de interesse da Defesa Nacional a níveis

aceitáveis. Portanto, o ano de 2012 foi importante para estabelecer critérios e controlar a mobilização e desmobilização de pessoal para a atividade de Defesa Cibernética.

O Acórdão 3.051/2014-TCU-Plenário de 5 de novembro de 2014, referente ao processo do TCU nº 023.050/2013-6 contextualizando auditorias em diversos órgãos e entidades da Administração Pública federal constatou os seguintes pontos de interesse:

> A segurança da informação segue sendo objeto de preocupação. Há baixa conformidade das organizações para com os normativos e com as boas práticas aplicáveis. Na maioria das organizações fiscalizadas na primeira fase, falhas foram observadas: a) 80% - falhas na gestão de continuidade de negócio; b) 70% - falhas no controle de acesso; c) 75% - falhas na gestão de incidentes; e, d) 85% - falhas na gestão de riscos de segurança da informação; Principais causas estão ligadas a falhas típicas de governança, como a falta de designação de um responsável pela segurança da informação, fato observado em 40% das organizações; Houve tendência de mudança de comportamento dos dirigentes públicos sobre a segurança da informação; A redução dos percentuais observados não se traduz necessariamente em retrocesso, mas pode ser interpretado como amadurecimento dos gestores de TI no sentido de compreender melhor os conceitos relacionados à segurança da informação; Ainda não há, por exemplo, um planejamento estratégico do Estado brasileiro que reúna e coordene ações dos diversos atores responsáveis por assuntos ligados a essa área; Recomendações ao GSI/PR: elabore e acompanhe periodicamente planejamento que abranja a estratégia geral de segurança da informação para o setor sob sua jurisdição; e alerte as organizações sob sua jurisdição que a elaboração periódica de planejamento das ações de segurança da informação é obrigação expressa prevista no item 3.1 da Norma Complementar 02/IN01/DSIC/GSI/PR. (BRASIL, 2015, p. 30)

Portanto, a defesa cibernética apesar de ser reconhecida como algo necessária continuou sofrendo negligências significativas do ponto de vista governamental. Ainda nesse ano é sancionada a Lei nº 12.965, de 23 de abril de 2014 que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil que será discutida na seção sobre vigilância.

Desse modo, o processo de securitização do espaço cibernético brasileiro pode ser dividido em três momentos. Até 2000, em que o setor foi apenas reconhecido, de 2000 a 2005 é um estágio que os órgãos do governo reconhecem o tema e começam a

tomar providencias para a própria segurança. A partir de 2005 se entra em um estágio de securitização incipiente com a participação das Forças Armadas do Brasil. No quadro organizado por Acácio é possível observar esse evolução.

Quadro 3: Estágios do tema Segurança Cibernética no Estado Brasileiro.

Tempo	Até 2000	2000~2005	2005-Atual
Órgãos	----------	Vários, GSI/PR (Gestão na APF)	GSI/PR (elementos do Politizado) MD-EB (elementos do Securitizado)
Estágio	Não-Politizado	Politizado	Securitizado

Fonte: Adaptado de ACÁCIO (2012, p. 5).

Portanto, desde os anos 2000 o Ator de Securitização é o Estado brasileiro devido a ser o principal produtor legal dos documentos por meio do Gabinete de Segurança Institucional da Presidência da República para a Administração Pública Federal e o Exército Brasileiro, enquanto a proteção às Infraestruturas Críticas da Informação é o objeto de referência.

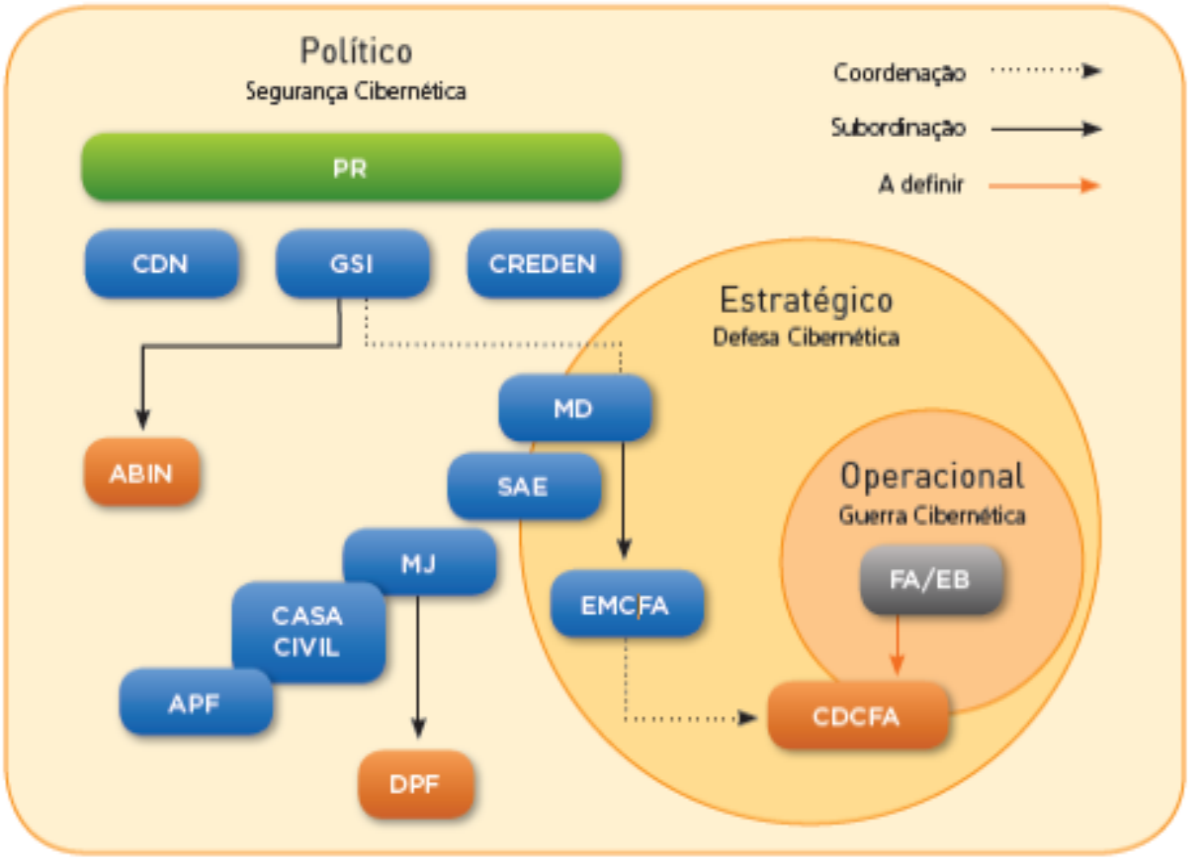
4.2 AS CAPACIDADES COERCITIVAS DO ESPAÇO CIBERNÉTICO NO BRASIL

Para reduzir a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra ataques cibernéticos é criado pelo meio da Portaria nº 666, de 4 de agosto de 2010 o CDCiber[36]. O CdCiber foi inaugurado em 2012 com o objetivo de proteger os sistemas de informações e neutralizar a fonte de ataques, tentando inibir possíveis ataques digitais. Com a figura 3 é possível observar como está estruturado o sistema

[36] Centro de Defesa Cibernética.

brasileiro de segurança cibernética e em especial a atuação do Exército na área operacional da guerra cibernética.

Figura 3: Sistema Brasileiro de Segurança e Defesa Cibernética.



Fonte: DINIZ, MUGGAH, GLENNY (2014, p. 19) [37].

As principais ameaças cibernéticas no Brasil estão divididas em três campos: crimes cibernéticos convencionais, crimes cibernéticos complexos e ameaças emergenciais. No quadro a seguir se compreende os campos das ameaças e exemplos que constituem os campos, assim, facilitando a caracterização dos problemas enfrentados pelo Brasil.

[37] Legenda para a figura. PR – Presidência da República; CDN – Conselho de Defesa Nacional; GSI – Gabinete de Segurança Institucional; CREDEN – Câmara de Relações Exteriores e Defesa Nacional; ABIN – Agência Brasileira de Inteligência; APF – Administração Pública Federal; Casa Civil; MJ – Ministério da Justiça; SAE – Secretaria de Assuntos Estratégicos; MD – Ministério da Defesa; EMCFA – Estado-Maior Conjunto das Forças Armadas; CDCFA – Centro de Defesa Cibernética das Forças Armadas; FA/EB – Forças Armadas/Exército Brasileiro.

Quadro 4: Os três principais conjuntos de ameaças virtuais no Brasil

Categoria	Definição	Exemplos	Respostas do governo	Realidade brasileira
Crimes cibernéticos convencionais	Estas são as formas mais difundidas de crimes cibernéticos no mundo e seguem a tipologia proposta pela União Internacional de Telecomunicaçõ es.	Acesso ilegal (*cracking*[38]), interceptação de dados, pornografia infantil, *spam*[39], discurso de ódio, fraudes bancárias, roubo de identidade, violações de direitos autorais.	Exclusivamente aplicação da lei, que normalmente envolvem crimes tradicionais que já são classificados em códigos penais.	Existem dois grandes subconjuntos do crime cibernético convencional: 1) economicamente motivados (especialmente fraude bancária) e 2) relacionadas com o conteúdo (por exemplo, racismo e da pornografia infantil em redes sociais).
Crimes cibernéticos complexos	Isto considera e expande a definição da União Internacional de Telecomunicaçõ es de ofensas cibernéticas ou, aqueles que podem cair em mais de uma categoria de crimes cibernético convencionais.	Cyber-terrorismo, guerra cibernética, ataques contra as infraestruturas críticas, cyber-espionagem e Hacktivismo.	Uma mistura de inteligência, execução militar e da lei, como são várias e distintas fontes potenciais de ataques (internas e externas), bem como alvos.	Hacktivismo e espionagem comercial são os dois principais. Com as denúncias de Edward Snowden[40] a espionagem cibernética americana se tornou um problema.
Ameaças emergenciais	Ameaças relacionadas com a expansão do ciberespaço que não se encaixam bem nas categorias	Usadas por grupos criminosos mais tradicionais, como as gangues e crime organizado	Deveria estar mais ligado à aplicação da lei, mas este campo está apenas emergindo e ainda há falta de	Brasil sofre de altos níveis de violência interpessoal e organizado, especialmente relacionada com

[38] Software usado para quebrar um sistema de software qualquer.
[39] Enviar e postar publicidade em massa.
[40] Serão discutidas as denúncias na próxima seção.

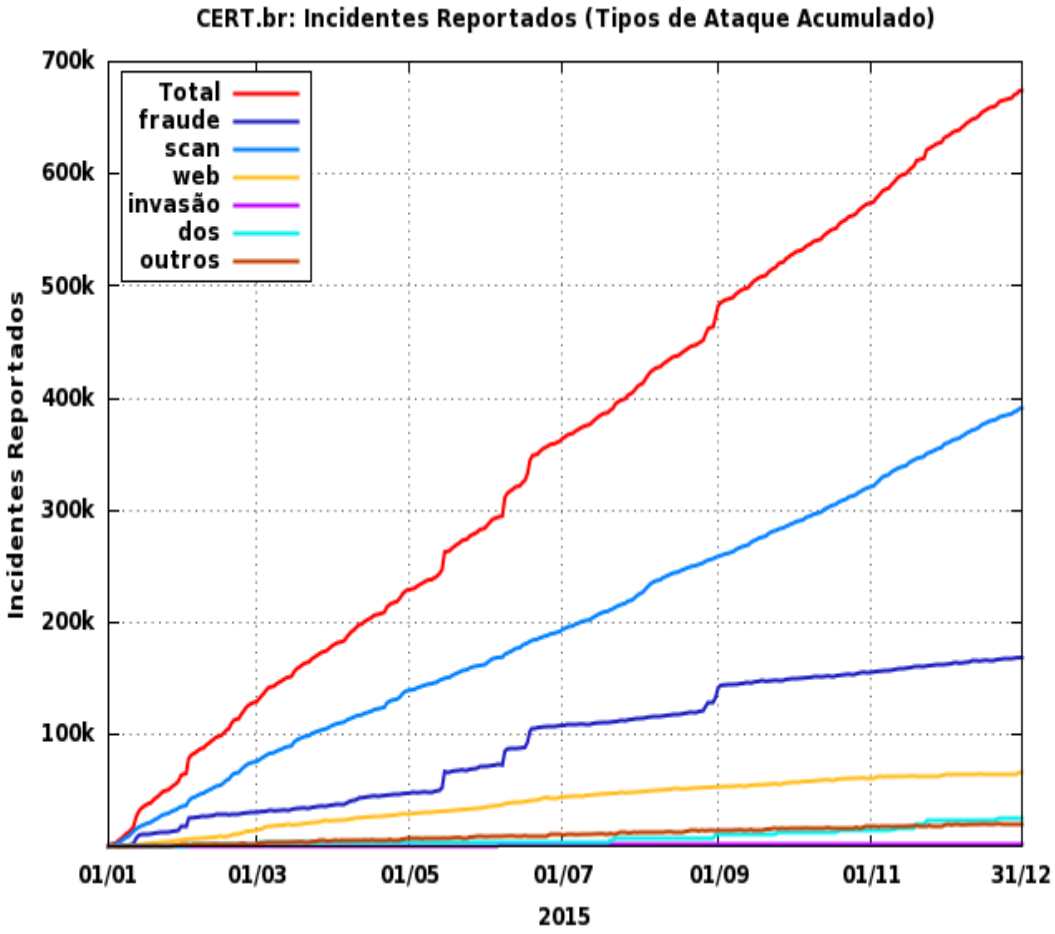
	da União Internacional de Telecomunicaçõ es, porque eles são emergentes ou se relacionam mais com o mundo em desenvolvimento .	(drogas e tráfico de armas, extorsão on-line, disseminação de uma cultura de violência), cyber lavagem de dinheiro e evasão fiscal, etc.	resposta do estado.	as gangues e com o crime organizado. Estes grupos já apreenderam o poder das TICs[41] para ampliar e fortalecer seus negócios.

Fonte: Adaptado e traduzido de DINIZ, MUGGAH, GLENNY(2014, p. 9).

Portanto, os crimes cibernéticos convencionais são os mais comuns no Brasil, principalmente porque tem fins econômicos e o aumento de usuários da rede. No ano 2000 foram reportados ao Cert.br[42] 5997 incidentes cibernéticos, enquanto que no ano de 2015 foram reportados 1047031 incidentes (CERT.BR, 2015a). Como é possível ver na figura 4, os principais incidentes são relacionados aos crimes cibernéticos convencionais.

[41] Tecnologias da Informação e Comunicação.
[42] Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil.

Figura 4: Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2015



Fonte: CERT.BR (2015b)[43].

[43] Legenda fornecida pelo CERT.br:

- **Dos** (DoS -- *Denial of Service*): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.
- **Invasão**: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.
- **Web**: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.
- **Scan**: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.
- **Fraude**: segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.

Consequentemente, como aponta Carvalho (2011) que as Infraestruturas Críticas Nacionais são o alvo principal da defesa cibernética brasileira e muitos desses incidentes que ocorrem no Brasil afetam as ICN.

> As ICN constituem preocupação permanente dos órgãos de Estado e de governo envolvidos na segurança e na defesa nacionais, uma vez que, conforme expressa seu próprio conceito, sua destruição, ou mesmo a interrupção de seu funcionamento, ainda que temporariamente, provoca sério impacto social, econômico, político, internacional ou na segurança do Estado e da sociedade. Foram eleitas seis áreas prioritárias a serem protegidas, quais sejam: energia, telecomunicações, transportes, água, finanças e informação, enfatizando essa última por caracterizar as ICI. A dependência crescente de sistemas de informação controlados por redes de computadores e com aplicativos expostos à internet, onde o risco de exploração de eventuais vulnerabilidades por ameaças cibernéticas é uma realidade, torna a proteção das ICI que controlam a operação das ICN o foco das ações de Segurança e de Defesa Cibernéticas. (CARVALHO, 2011, p. 17)

Para poder realizar a segurança das ICNs e de grandes eventos como o Rio +20 (2012), Copa das Confederações (2013), Jornada Mundial da Juventude (2013), Copa do Mundo (2014) e Olímpiadas o CdCiber até 2015 recebeu um aporte de 400 milhões de reais principalmente para a proteção de redes públicas em grandes eventos. Na Copa do Mundo foram 756 ataques neutralizados com 112 militares e civis empregados (CSIRTs, 2014). Nas Olimpíadas de 2016 o Brasil conseguiu sustentar 500 *gigabytes* por segundo, esse foi o maior ataque registrado e o Brasil teve sucesso na segurança, nas Olimpíadas de Londres em 2012 os ataques chegaram a 60 *gigabytes* por segundo (DOBBINS, 2016).

4.3 AS CAPACIDADES DE VIGILÂNCIA DO ESPAÇO CIBERNÉTICO NO BRASIL

Com as revelações de Snowden em 2013 que os Estados Unidos estariam realizando operações de vigilância no celular da Presidente Dilma Rousseff, na

---

- **Outros**: notificações de incidentes que não se enquadram nas categorias anteriores.

empresa petrolífera Petrobrás, empresa estatal de economia mista, e indiscriminadamente de cidadão brasileiros (Bauman *et al*, 2014, p. 128), o Brasil imediatamente cancelou uma visita presidencial no mesmo ano para Washington e fez duras críticas ao país norte-americano em seu discurso da ONU no mesmo ano (CANABARRO, BORNE, 2015, p. 58).

Em seu discurso da ONU a presidente destacou que as ações de espionagem no Brasil “imiscuir-se dessa forma na vida de outros países fere o Direito Internacional e afronta os princípios que devem reger as relações entre eles, sobretudo, entre nações amigas. Jamais pode uma soberania firmar-se em detrimento de outra soberania. Jamais pode o direito à segurança dos cidadãos de um país ser garantido mediante a violação de direitos humanos e civis fundamentais dos cidadãos de outro país... Estamos diante de um caso grave de violação dos direitos humanos e das liberdades civis; da invasão e captura de informações sigilosas relativas as atividades empresariais e, sobretudo, de desrespeito à soberania nacional do meu país” (ROUSSEFF, 2013). Diante desse discurso, Dilma Rousseff reafirmou os valores que utiliza na política externa contra o desenvolvimento assimétrico e ainda criticou a papel proeminente dos Estados Unidos na Corporação da Internet para Atribuição de Nomes e Números (ICANN) (CANABARRO, BORNE, 2015, p. 58).

Outro ponto importante no discurso de Dilma Rousseff foi que o “Brasil, senhor presidente, redobrará os esforços para dotar-se de legislação, tecnologias e mecanismos que nos protejam da interceptação ilegal de comunicações e dados. Meu governo fará tudo que estiver a seu alcance para defender os direitos humanos de todos os brasileiros e de todos os cidadãos do mundo e proteger os frutos da engenhosidade de nossos trabalhadores e de nossas empresas.” Para essa melhoria o Brasil anunciou várias melhorias como o e-mail brasileiro desenvolvido pela empresa Serpro com o potencial dessas trocas de informações confidenciais serem realizadas por uma rede interna, dificultando o acesso de espiões (PASSARINHO, 2013), a criação

de uma rede submarina de 34.000 km de fibra óptica entre os país dos BRICS[44] (LOPES, 2013) e outro cabo ligado com a Europa (ESTES, 2014).

Consequentemente em 2014 é sancionado o Marco Civil que tem por princípios: a) garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; b) proteção da privacidade; c) proteção dos dados pessoais, na forma da lei; d) preservação e garantia da neutralidade de rede; e) preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas; f) responsabilização dos agentes de acordo com suas atividades, nos termos da lei; g) preservação da natureza participativa da rede e h) liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei. Essa Lei se tornou modelo para diversos países como Itália e Filipinas devido à qualidade para a governança da Internet (CANABARRO, BORNE, 2015, p. 58).

No entanto, o Brasil ainda investe pouco em Inteligência. A Lei Orçamentária Anual (LOA) de 2013 alocou R$ 520,4 milhões para a Agência Brasileira de Inteligência (ABIN) e desse valor, quase 90% era pra pagamento dos salários do pessoal e encargos sociais (SENADO FEDERAL, 2014). Pelo fato do Brasil ainda ser uma democracia recente, a inteligência brasileira ainda está se adaptando a fazer segurança nacional ao invés de segurança do regime, assim, o Estado acaba realizando uma criminalização dos movimentos sociais (DEFESANET, 2016). Segundo Cepik (2003), a segurança nacional é definida por: “condição relativa de proteção coletiva e individual dos membros de uma sociedade contra ameaças à sua sobrevivência e autonomia”

A CPI dos Crimes Cibernéticos que teve como objetivo de investigar a prática de crimes cibernéticos e seus efeitos sobre a economia brasileira pediu mais recursos para a comunidade de inteligência e também uma maior flexibilização do Marco Civil o que levou a uma grande discussão no país. O CGI.br lançou uma nota expressando grande preocupação com as propostas de flexibilização e modificação do regime jurídico

[44] Brasil, Rússia, Índia, China e África do Sul.

adotado no Brasil com o Marco Civil. Ainda assim, uma fiscalização mais complexa não seria possível com um baixo orçamento para as agencias de inteligência brasileira. Portanto, a efetividade da capacidade de vigilância do Brasil é prejudicada pelos baixos recursos destinados e uma política pública que faz um foco nas informações coletadas de maneira não efetiva, pois demanda uma maior retirada dos direitos individuais de seus cidadãos.

4.4 CONCLUSÃO DO CAPITULO

Neste capítulo foi possível perceber os impactos da securitização no espaço cibernético na capacidade coercitiva e na capacidade de vigilância no Brasil. A abordagem do tema começou no início da década de 2000 e a partir de 2005 se tornou securitizado. A capacidade coercitiva foi construída ao longo das ameaças das Infraestruturas Criticas de Informação e dos grandes eventos. A capacidade de vigilância o Brasil foi vítima de uma espionagem e a partir desse momento foi construindo suas capacidades para se defender de invasores externos, porém, tem sua efetividade afetada pelos baixos recursos e ainda uma pressão para a utilização desses recursos de maneira a cercear os direitos individuais.

5 CONCLUSÃO

Ao longo deste Trabalho de Conclusão foram examinados os impactos da securitização do ciberespaço na capacidade coercitiva e na capacidade de vigilância no Brasil e Estados Unidos com o objetivo de compreender os impactos da securitização do ciberespaço na capacidade coercitiva e na capacidade de vigilância no Brasil e Estados Unidos a partir dos acontecimentos de 11 de setembro de 2001. Data em que o espaço cibernético começou a receber mais atenção dos Estados.

No primeiro capítulo foi apresentado um aporte teórico mostrando os avanços dos estudos da Segurança Internacional. Para isso foi preciso compreender as especificidades do espaço cibernético como a ubiquidade e convergência digital. Também, foi demonstrado o processo histórico em que a securitização se dá, principalmente após os acontecimentos de 11 de setembro de 2001 nos Estados Unidos. Ademais, foi demonstrado como funcionam as capacidades coercitivas e de vigilância no espaço cibernético. As capacidades coercitivas têm como objetivos a proteção de informação e fazer uma avaliação de possivei alvos. A capacidade de vigilância envolve a coleta de informações sobre populações para fins institucionais e pessoais.

O capítulo dois tratou sobre os impactos da securitização do espaço cibernético nos Estados Unidos. Os americanos começaram a tratar o tema cibernético a partir do governo Reagan na década de 1980, porém, foram com os atentados de 2001 que se teve uma maior atenção do país ao tema. Com a securitização, os Estados Unidos criaram o Comando Cibernético e se tornaram grande potência em capacidades cibernéticas. Em relação à capacidade de vigilância o país se aproveitou das informações de suas empresas privadas e conseguiu criar um sistema capaz de obter informações em longa escala, porém, isso afetou a efetividade, pois se torna inviável analisar todas as informações recebidas.

No capítulo seguinte, foram discutidos os impactos da securitização do espaço cibernético no Brasil. O processo de securitização no Brasil começou a partir do ano 2000 e foi se desenvolvendo ao longo da década. No campo das capacidades coercitivas o país criou o CDCiber e se preparou de maneira eficaz para receber

grandes eventos. No campo da vigilância o país recebe pressões de seus parlamentares para realizar uma maior fiscalização, porém, sofre de falta de recursos e muitas vezes acaba-se por aplicar seus analistas de maneira ineficaz para a proteção do governo.

Para poder comparar os impactos da securitização mencionados nos capítulos três e quatro foi elaborado o quadro 5.

Quadro 5: Comparativo entre os impactos da securitização do espaço cibernético na capacidade coercitiva e de vigilância no Brasil e Estados Unidos.

Países	Estados Unidos	Brasil
Securitização	Securitizado	Securitizado
Capacidade Coercitiva	Grande potência em capacidades cibernéticas com cadeia de comando que permite uma resposta rápida a qualquer incidente. A doutrina americana foi desenvolvida ao longo das últimas décadas e teve como foco principal a defesa das Infraestruturas Críticas. US $ 14 bilhões em segurança cibernética para pesquisa e iniciativas críticas em 2016.	A proteção às Infraestruturas Críticas da Informação é o objeto de referência. Para poder realizar a segurança das ICNs e de grandes eventos o país criou o Centro de Defesa Cibernético. O CdCiber até 2015 recebeu um aporte de 400 milhões de reais.
Capacidade de Vigilância	Os Estados Unidos criaram um sistema que consegue	A capacidade de vigilância do Brasil foi vítima de uma

	captar uma grande quantidade de informações de maneira que retira liberdades individuais e torna improvável para analistas de inteligência processar toda informação.	espionagem e a partir desse momento foi construindo suas capacidades para se defender de invasores externos e existe uma pressão governamental para maior controle da rede. A capacidade de vigilância tem problemas de efetividade pela falta de recursos e um direcionamento para retirada de liberdades individuais.

Fonte: Elaborado pelo autor.

O quadro mostra que os dois países securitizaram o tema, e o objeto de referência da securitização do espaço cibernético em ambos os países é a proteção às Infraestruturas Críticas da Informação. Essa securitização se acentuou ao longo da década de 2000 com o aumento da percepção de ambos os países sobre o que a falta de segurança. Com o aumento de usuários na rede e da circulação de informações sigilosas os dois países lançaram diversas ferramentas no âmbito institucional como as doutrina militares, busca por possíveis acordos e necessidade de formação de pessoal capacitado.

Em relação às capacidades coercitivas os dois países criaram seus Comandos Cibernéticos. É importante salientar que os dois países tem ameaças distintas, enquanto o terrorismo é um dos fatores principais para os americanos, o que motivou principalmente o Brasil foi, sobretudo, ser sede de grandes eventos e a espionagem do

governo americano. Em relação ao orçamento, os Estados Unidos receberam um aporte de bilhões de dólares, sendo que a maior parte desse valor é para operações no espaço cibernético e para garantia de informação. O Brasil recebeu um aporte de 400 milhões de reais.

A capacidade de vigilância dos dois países precisou se adaptar ao uso das novas tecnologias. Os Estados Unidos por serem capazes de produzir as novas tecnologias e essas tecnologias serem usadas em massa no mercado mundial tem uma posição de vantagem. Essa posição de vantagem foi usada para criar um programa de vigilância capaz de atuar globalmente e devido a parcerias com empresas privadas, recolher informações de seus clientes. Porém, devido ao grande número de informações coletadas e pela retirada de direitos a liberdades individuais sua capacidade perde efetividade. No Brasil, a efetividade é problemática pela falta de recursos e uma inclinação à retirada de liberdades individuais.

Diante das conclusões, este trabalho pode trazer contribuições para o tema em questões sociais e mostrar rumos para estudos futuros. Em questões sociais, trata principalmente do resultado e desenvolvimento de uma sociedade da era da informação e o que essa forma de relações sociais impacta tal sociedade. Essa nova sociedade implica em uma relação nova com o Estado, em que são esperadas trocas de informação pelo domínio cibernético. Devido a essas trocas, o espaço cibernético se tornou muito visado para ações maliciosas e obrigou ao Estado a se adaptar para se proteger nesse domínio.

Essa proteção impactou na capacidade coercitiva e na de vigilância. Devido à interconectividade entre Estado e população a capacidade coercitiva foi ampliada no sentido em que ações nesse meio podem incapacitar as Infraestruturas Críticas Nacionais que podem ter impactos sociais, econômicos, políticos, internacionais ou à segurança nacional. O modelo de guerra cibernética assim se tornou uma ferramenta à guerra tradicional por ser capaz de paralisar algum país. Portanto, o estudo mostrou uma nova maneira de confronto entre nações e possíveis perigos advindos de organizações criminosas.

No tocante à capacidade de vigilância, alguns Estados como os Estados Unidos encontraram neste espaço uma oportunidade de conseguir realizar uma vigilância em larga escala. Essa vigilância em larga escala foi debatida neste trabalho ao afirmar que os Estados não são capazes de processar todas as informações obtidas de maneiras muitas vezes ilícitas. Essas maneiras ilícitas acabam por retirar liberdades individuais e essa perda de direitos diminui a efetividade da capacidade de vigilância em uma democracia.

Quanto ao meio acadêmico, o trabalho reuniu uma literatura que trata sobre o tema de maneira geral, em relação à capacidade de vigilância e coercitiva e também sobre literaturas desses pontos específicas de cada país. Para futuras pesquisas se sugere que em relação às capacidades coercitivas se crie um modelo capaz de mensurar essa capacidade de maneira efetiva e em relação a capacidade de vigilância de criar debates que possam sugerir como avaliar as informações de modo efetivo e de como se estabelecer um debate democrático com a sociedade para que o recolhimento dessas informações não ocorra de maneira arbitrária.

6 REFERÊNCIAS

ACÁCIO, I.D.P. . **Segurança Cibernética na Política de Defesa Brasileira: Um caso de Securitização?**. In: I Encontro Sulamericano de Defesa e VI Encontro da Associação Brasileira de Estudos da Defesa, 2012, São Paulo-SP. Anais dos Resumos do I Encontro Sulamericano de Defesa e VI Encontro da Associação Brasileira de Estudos da Defesa, 2012. p. 1-17.

ADAMS, James. **Virtual defense**. Foreign Affairs-New York**-**, v. 80, n. 3, p. 98-113, 2001.

ANDRESS, Jason; WINTERFELD, Steve. **Cyber warfare: techniques, tactics and tools for security practitioners**. Elsevier, 2013.

ÁVILA, Fabrício Schiavo; MARTINS, José Miguel; CEPIK, Marco. **Armas estratégicas e poder no sistema internacional: o advento das armas de energia direta e seu impacto potencial sobre a guerra e a distribuição multipolar de capacidades**. Contexto internacional, v. 31, n. 1, p. 49, 2009.

BAUMAN, Zygmunt *et al*. **After Snowden: Rethinking the impact of surveillance**. International political sociology, v. 8, n. 2, p. 121-144, 2014.

BAUMAN, Zygmunt; LYON, David. **Vigilância Líquida**. Zahar, 2014.

BERWANGER, Tiago. **O discurso de securitização da cibernética nos Estados Unidos da América no período entre 2007 e 2015**. Trabalho de Conclusão de Curso - Universidade Federal de Santa Catarina, Florianópolis, 2015.

BOBBIO, Norberto. D**icionário de política: Norberto Bobbio, Nicola Matteucci e Gianfranco Pasquino**. Brasília: Editora Universidade de Brasília, 1998.

BRASIL. Gabinete de Segurança Institucional. **Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal**. Brasília, 2015

_____. Ministério da Casa Civil. Subchefia para Assuntos Jurídicos. **Decreto Nº 3505, de 13 de junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal**. Brasília, 2000. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto/D3505.htm> Acesso em 21 set 2016.

_____. Ministério da Casa Civil. Subchefia para Assuntos Jurídicos. **Decreto Nº 5484, de 30 de Junho de 2005**. **Política de Defesa Nacional**. Brasília, 2005.

_____. Ministério da Defesa. **Estratégia Nacional de Defesa. Paz, segurança para o Brasil**. 2ªEd. Brasília: Ministério da Defesa, 2008.

_____. Ministério da Defesa. **Glossário das Forças Armadas (MD35-G-01)**. Brasília, 2007

BUZAN, Barry; HANSEN, Lene. **The evolution of international security studies**. Cambridge University Press, 2009.

BUZAN, Barry; WAEVER, Ole. **Regions and powers: the structure of international security**. Cambridge University Press, 2003.

CANABARRO, Diego R. BORNE, Thiago F. **As Reações Brasileiras ao Caso Snowden: Implicações para o Estudo das Relações Internacionais em um Mundo Interconectado**. In: Revista Conjuntura Austral, v.6, nº30. Jun.-jul. Porto Alegre. p. 50-74. 2015.

CARVALHO, P. S. M. **A defesa cibernética e as infraestruturas críticas nacionais**. Rio de Janeiro, 24 maio 2011.

CASTELLANO DA SILVA, Igor; DALL'ONDER SEBBEN, Fernando; KERR DE OLIVEIRA *et al*. Capacidade Estatal: **Democracia e Poder na Era Digital**. Instituto Sul-Americano de Política e Estratégia. 2012.

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

CEPIK, Marco. **Espionagem e democracia**. FGV Editora, 2003.

CEPIK, Marco; CANABARRO, Diego Rafael; BORNE, Thiago. **A securitização do ciberespaço e o terrorismo: uma abordagem crítica.** In: CEPIK, Marco (Org.). Do 11 de Setembro de 2001 à 'Guerra Contra o Terror': reflexões sobre o terrorismo no século XXI. Brasília: IPEA, 2014 [no prelo].

CERT.BR. **Total de Incidentes Reportados ao CERT.br por Ano**. 2015a. Disponível em <http://www.cert.br/stats/incidentes/> Acessado em 04 Out 2016.

_____. **Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2015**. 2015b. Disponível em <http://www.cert.br/stats/incidentes/2015-jan-dec/tipos-ataque-acumulado.html> Acessado em 03 Out 2016.

CESIRTs. **3º Fórum Brasileiro de CSIRTs**. 2014. Disponível em: <http://www.cert.br/forum2014/slides/ForumCSIRTs2014-CDCiber.pdf> Acessado em 03 Out 2016.

DE ARAÚJO JORGE, Bernardo Wahl Gonçalves. **Estados Unidos, poder cibernético e a "guerra cibernética: Do Worm Stuxnet ao Malware Flame/Skywiper–e além**. Meridiano 47-Journal of Global Studies, v. 13, n. 131, p. 43-48. 2012.

DE CARVALHO, Paulo Sérgio Melo. **A defesa cibernética e as infraestruturas críticas nacionais.** Coleção Meira Mattos-Revista das Ciências Militares, 2011.

DE CASTRO, Rodrigo Batista. **Eficácia, eficiência e efetividade na administração pública**. 2006.

DEFESANET. **Exército começa a monitorar lobos solitários e favelas do Rio**. 2016. Disponível em: <http://www.defesanet.com.br/crise/noticia/22640/Exercito-comeca-a-monitorar-lobos-solitarios-e-favelas-do-Rio> Acesso em: 27 Nov 2016

DINIZ, Gustavo; MUGGAH, Robert; GLENNY, Misha. **Deconstructing cyber security in Brazil**. Strategic Paper. 2014

DOBBINS, Roland. **DDoS Attacks From IoT Botnets Don't Have to Mean Game Over**. Arbor Networks. 2016. Disponível em

<https://www.arbornetworks.com/blog/asert/rio-olympics-take-gold-540gbsec-sustained-ddos-attacks/> Acesso em 04 Out 2016.

DUARTE, Érico Esteves. **Impacto de novas tecnologias em política de defesa: lições e limites do modelo norte-americano**. 2011

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

ESTES, Adam. **Brazil Is Keeping Its Promise to Avoid the U.S. Internet**. Gizmodo. 2014. Disponível em <https://gizmodo.com/brazils-keeping-its-promise-to-disconnect-from-the-u-s-1652771021> Acesso em 05 Out 2016.

FRIAS, Óscar. **Cyber Intelligence. A obtenção de informações a partir de fontes abertas no Ciberespaço**. Tese (Mestrado em Guerra de Informação). Academia Militar. Direção de Ensino, Lisboa. 2013.

GARTZKE, Erik. **The myth of cyberwar: bringing war in cyberspace back down to earth**. International Security, v. 38, n. 2, p. 41-73, 2013.

GIDDENS, Anthony. **Dimensões da modernidade**. Sociologia, Problemas e práticas, v. 4, p. 237-251. 1988.

HACKETT, J. (Ed.). (2012). **The Military Balance 2014**. London, UK: The International Institute for Strategic Studies.

HAGGERTY, Kevin D.; GAZSO, **Amber. Seeing beyond the ruins: Surveillance as a response to terrorist threats**. The Canadian Journal of Sociology, v. 30, n. 2, p. 169-187, 2005.

HANSON, Jonathan K.; SIGMAN, Rachel. **Leviathan's Latent Dimensions: Measuring State Capacity for Comparative Political Research**. In:APSA 2011 Annual meeting paper. 2013.

HILL, Kashmir. **Thanks, Snowden! Now All The Major Tech Companies Reveal How Often They Give Data To Government**. Forbes. 2015. Disponível em: <http://www.forbes.com/sites/kashmirhill/2013/11/14/silicon-valley-data-handover-infographic/#323a9d506d06> Acesso em 17 Agosto 2016.

HUGHES, Rex. **NATO and Cyber Defence**. Atlantisch Perspectief, v. 33. 2009.

KERR, Orin S. **Internet surveillance law after the USA Patriot Act: The big brother that isn't**. Available at SSRN 317501. 2003.

KLEIN, John J. **Corbett in orbit: a maritime model for strategic space theory**. NavalWar College Review, Newport, v. LVII, n. 1, p. 59-74, 2004

KNOX, MacGregor; MURRAY, Williamson (Ed.). **The Dynamics of Military Revolution, 1300–2050**. Cambridge University Press, 2001.

KUEHL, D. **From cyberspace to cyberpower: defining the problem.** In: KRAMER, F.; STARR, S.; WENTZ, L. Cyberpower and national security. Washington: National Defense University Press, 2009.

LATHAM, Robert. **Introduction. In Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security, edited by Robert Latham**. New York: The New Press. 2003.

LANGNER, Ralph. Stuxnet: **Dissecting a cyberwarfare weapon**. Security & Privacy, IEEE, v. 9, n. 3, p. 49-51. 2011.

LEBLANC, Sylvain P. *et al*. **An overview of cyber attack and computer network operations simulation**. In: Proceedings of the 2011 Military Modeling & Simulation Symposium. Society for Computer Simulation International. p. 92-100. 2011.

LOBATO, LUÍSA CRUZ; KENKEL, KAI MICHAEL. **Discourses of cyberspace securitization in Brazil and in the United States**. Revista Brasileira de Política Internacional, v. 58, n. 2, p. 23-43. 2015.

LOPES, Gills. **BRICS Cable: levando a cabo uma resposta brasileira à espionagem internacional?**. Mundorama. 2013. Disponível em <http://www.mundorama.net/2013/09/28/brics-cable-levando-a-cabo-uma-resposta-brasileira-a-espionagem-internacional-por-gills-lopes/> Acesso em 05 Out 2016.

LOPES, Gills Vilar; DE OLIVEIRA, Carolina Fernanda Jost. **Stuxnet e defesa cibernética estadunidense à luz da análise de política externa**. Revista Brasileira de Estudos de Defesa, v. 1, n. 1, 2014.

LYNN, William J. **Defending a New Domain: The Pentagon's Cyberstrategy**. Foreign Affairs, v. 89, n. 5, p. 97-108, 2010.

MARTINS, José Miguel. **Digitalização e Guerra Local como Fatores do Equilíbrio Internacional**. Tese de Doutorado, PPG de Ciência Política, Universidade Federal do Rio Grande do Sul. Porto Alegre: 2008

MÖCKLY, D. **Strategic trends 2012: key developments in global affairs**. Zurich: Center for Security Studies (CSS), 2012.

OTAN. **Factsheet Cyber Defence**. 2016. Disponível em: <http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf> Acesso em 15 agosto 2016.

PATTNAYAK, Satya R. **Modernization, dependency, and the state in Asia, Africa, and Latin America**. International journal of comparative sociology, v. 37, n. 3, p. 274-286, 1996.

PASSARINHO, Nathalia. **Novo sistema de e-mails vai 'livrar governo da espionagem', diz Serpro**. G1. 2013. Disponível em: <http://g1.globo.com/politica/noticia/2013/10/novo-sistema-de-e-mails-vai-livrar-governo-da-espionagem-diz-serpro.html> Acesso em 05 Out 2016.

RID, Thomas. **Cyber war will not take place**. Journal of strategic studies, v. 35, n. 1, p. 5-32, 2012.

ROUSSEFF, Dilma. **Discurso da Presidenta da República, Dilma Rousseff, na abertura do Debate Geral da 68ª Assembleia-Geral das Nações Unidas - Nova Iorque/EUA. 2013**. Disponível em <http://www2.planalto.gov.br/acompanhe-o-planalto/discursos/discursos-da-presidenta/discurso-da-presidenta-da-republica-dilma-rousseff-na-abertura-do-debate-geral-da-68a-assembleia-geral-das-nacoes-unidas-nova-iorque-eua> Acesso em 05 Out 2016

SENADO FEDERAL. **Brasil investe pouco em inteligência. 2014**. Disponível em <http://www12.senado.leg.br/emdiscussao/edicoes/espionagem-cibernetica/realidade-brasileira-sem-cultura-de-inteligencia/brasil-investe-pouco-em-inteligencia> Acesso em 05 Out 2016.

SOUSA, Fernando de (dir.). **Dicionário de Relações Internacionais**. Porto: Edições Afrontamento**,** 2005.

STERNSTEIN, Aliya. **The Military's Cybersecurity Budget in 4 Charts**. Defense One, 2015. Disponível em: <https://admin.govexec.com/media/gbc/docs/pdfs_edit/cyberspending.png> Acesso em 17 Ago 2016.

TAKAHASHI, Tadao. **Sociedade da informação no Brasil: livro verde**. Ministério da Ciência e Tecnologia (MCT), 2000.

TILLY, Charles**. Democracy**. New York: Cambridge University Press, 2007.

TORRES, Marcelo Douglas de Figueiredo. **Estado, democracia e administração pública no Brasil**. Rio de Janeiro: Editora FGV, 2004. 224 p.

UNITED STATES. U.S. **Cyber command fact sheet.** May 2010.

WÆVER, Ole, Barry Buzan, Morten Kelstrup and Pierre Lemaitre (1993) **Identity, Migration and the New Security Agenda in Europe**, London: Pinter.

WALT, Stephen M. **Is the Cyber Threat Overblown?.** Foreign Policy, v. 30, 2010.

WHITE HOUSE (Org.). **Cybersecurity Legislative Proposal**. 2011.

_____. **The Comprehensive National Cybersecurity Initiative**. 2010.

_____. **The President's Budget Fiscal Year 2016**. 2015. Disponível em <https://www.whitehouse.gov/sites/default/files/omb/budget/fy2016/assets/fact_sheets/cybersecurity.pdf > Acesso em 16 Ago 2016.

_____. FACT SHEET: **Presidential Policy Directive on United States Cyber Incident Coordination**. 2016. Disponível em: <https://www.whitehouse.gov/the-press-office/2016/07/26/fact-sheet-presidential-policy-directive-united-states-cyber-incident-1> Acesso em 15 Ago 2016.

WILLIAMS, Paul D. **Security studies: an introduction.** Routledge, 2008.