Universidade de Brasília
Instituto de Relações Internacionais
Programa de Pós-Graduação em Relações Internacionais
XVII Curso de Especialização em Relações Internacionais

Vigilância ou militarização da segurança cibernética? Uma análise entre as mentalidades militar e liberal de segurança e a regulação das ameaças do ciberespaço.

Iramar Renó Faria

Artigo apresentado como requisito parcial para obtenção do título de Especialista em Relações Internacionais

Orientador: Professor Doutor Alcides Costa Vaz

Brasília, DF

2016

RESUMO

Este artigo pergunta como a percepção de segurança e ameaças no ciberespaço desempenham um papel importante na justificativa de que meios e medidas são empregados por diferentes atores e agências de segurança. Para esta proposta, este artigo foca na maneira como que as ameaças do ciberespaço são conceituadas, identificando mentalidades distintas de segurança. Ele vai apresentar a ideia de abordagens sobre diferentes "mentalidades de segurança", como estas desempenham um papel na normatização do ciberespaço e podem influenciar as normas legais. Para atingir este objetivo, este artigo estabelece uma comparação entre a mentalidade militar de segurança – preocupada principalmente com a estratégia de segurança nacional – e a mentalidade liberal de segurança – que percebe a segurança em conjunto com os direitos individuais e o equilíbrio de interesses.

PALAVRAS-CHAVE: CIBERSEGURANÇA – MENTALIDADES DE SEGURANÇA – CIBERESPAÇO.

ABSTRACT

This article asks how the perception of security and threats in cyberspace play an important role in justifying which means and measures are employed by different security actors and agencies. For this purpose, this article focuses on the way in which threats from cyberspace are conceptualized by identifying distinct mindsets of security. It will present the idea of different "security mindsets" as distinct approaches to security and how these play a role in regulating cyberspace and influencing legal regulations. For reach this objective, this article parallel between a military security mindset – concerned with military and strategic considerations of national security – and a liberal security mindset – which perceives security together with individual rights and balancing interest.

KEYWORDS: CYBER SECURITY – SECURITY MINDSETS – CYBERSPACE.

INTRODUÇÃO

> *"A vitória sorri aos que melhor se adaptam às mudanças do caráter da guerra e não aos que esperam adaptar-se depois dela ocorrer".*
> General Giulio Douhet

A rede mundial de computadores apresenta uma variedade de desafios à segurança: com a presença de mais e mais tecnologias onipresentes de comunicação, dispositivos eletrônicos em redes, a governança da segurança muitas vezes vem com uma carga pesada de efeitos colaterais. Por um lado, este chamado ciberespaço é um espaço democrático e livre; uma plataforma global de comunicação, por outro lado, ele oferece opções para vigilância, controle de informações, crimes, espionagem e até mesmo a guerra.

Este artigo busca introduzir o conceito de segurança com distintas "mentalidades" como uma ferramenta para identificar suas diferentes abordagens e com isso permitir uma análise sem a necessidade de aceitar ou negar suas ameaças, porém o dever de estabelecer contramedidas para prevenção. Isto é de enorme importância no mundo em que a segurança serve cada vez mais como um meio para expandir os poderes e capacidades, justificar interferências nos direitos e exceções legais ou alterações permanentes de leis.

Com esse mote, vou apresentar alguns conceitos de "mentalidades de segurança" e aplicá-los para descrever dois modelos distintos que desempenham um papel muito importante na tecnologia global de informação de hoje: a "mentalidade militar de segurança" e uma "mentalidade liberal de segurança".

O principal objetivo desse artigo é analisar em que medida as consequências das mentalidades militares e liberais de segurança cibernética (baseando-se nos possíveis desdobramentos que elas desencadeariam), podem interferir no ciberespaço desestabilizando a ordem em vários níveis (político, econômico, financeiro... etc.), principalmente a segurança de infraestruturas críticas, e a balança do poder.

Para tanto, no decorrer do artigo para um melhor embasamento teórico sobre o ambiente do ciberespaço e suas características, teço explicações e exemplificações de problemas de segurança ocasionados no período de 1990 até os dias atuais.

Vale salientar que restrinjo a pesquisa ao nicho Estadunidense, pois apresenta além de uma maior gama de documentos sobre o assunto, como também exemplos das guerras que passaram desde o surgimento deste novo ambiente hostil.

Os objetivos específicos são descrever os marcos conceituais e históricos da ciberguerra. Busco mostrar como este novo campo de batalha vem sofrendo mutações e quanto os Estados Unidos da América estão buscando balizá-los (com leis e decretos) uma conduta adequada tanto no campo militar quanto no campo civil.

Para um entendimento mais gradativo dos eventos, na primeira seção do artigo descrevo a rápida evolução das redes de computadores que permeia o mundo globalizado em que vivemos e suas inúmeras possibilidades.

Posteriormente pontuo as mudanças de conceitos sobre a segurança Internacional, focando inicialmente na visão Realista e para obtermos um entendimento apropriado sobre a ciberguerra, busco uma clarificação maior a respeito da segurança multidimensional.

Na seção posterior abordo os vários tipos ameaças que permeiam o ambiente do ciberespaço e que devido a sua constante expansão, estas ameaças evoluem seus métodos e formas de atuar na sociedade ou no indivíduo.

Após apresentadas estas bases de conceitos e ambientes do ciberespaço começo a entrar no cerne do problema exposto no artigo e, embora existam certamente mais do que duas mentalidades de segurança que compõem o cenário global de hoje, escolhemos as duas como uma ferramenta para melhor descrever e compreender dois tipos de mentalidades de segurança cibernética: a militar, e a liberal.

Este artigo conta com fontes primárias (documentos oficiais do site da OTAN[1], CIA[2] e Agências de Inteligência) e fontes secundárias (notícias de jornais, livros, artigos e revistas científicas). A revisão bibliográfica documental foi realizada com o uso de bases primárias de documentos oficiais, estatísticas, artigos especializados e obras clássicas e contemporâneas.

[1] Organização do Tratado do Atlântico Norte (OTAN), por vezes chamada Aliança Atlântica, é uma aliança militar intergovernamental baseada no Tratado do Atlântico Norte, que foi assinado em 4 de abril de 1949. A organização constitui um sistema de defesa coletiva por meio do qual seus Estados-membros concordam com a defesa mútua em resposta a um ataque por qualquer entidade externa à organização.

[2] *Central Intelligence Agency* - Agência Central de Inteligência dos EUA

1. Evolução da rede de computadores e suas possibilidades

O ambiente digital está mudando rapidamente. Os Estados Unidos não dominam mais a arquitetura da internet como fazia quando o sistema foi concebido, no final da década de 1960, sob a designação de ARPANEt[3] (*Advanced Research Projects Agency Network* – "Rede da Agência de Pesquisa de Projetos Avançados").

Todos os anos dezenas de milhões de pessoas se conectam a internet pela primeira vez. Com a expansão do acesso *online* global e um crescente número de pontos conectados, o tráfego da internet está cada vez mais ramificado em todo o mundo. Enquanto este crescimento é positivo do ponto de vista econômico, ele também traz riscos, e oportunidades aos atores maliciosos – estatais, não estatais ou uma combinação de ambos – para lançarem ataques, esconderem suas identidades e se protegerem por trás das estruturas sociais e de governança que ainda não compreenderam plenamente a natureza da internet.

A internet é maior do que qualquer Estado ou grupos de Estados, e evolui em um ritmo muito além do controle, inclusive da mais avançada empresa de tecnologia. Nos próximos anos, a complexidade do espaço cibernético só vai se aprofundar, aumentando o potencial para atritos, fricções, conflitos (CORNISH, 2010) e, por que não, "guerras".

Além disso, deve-se prestar atenção também ao fenômeno do poder. A transição de poder de um Estado dominante para outro é um evento histórico conhecido, mas a chamada "difusão do poder" é um processo novo (NYE, 2010).

Na atual era da informação global, o problema para todos os Estados é que muitos eventos estão ocorrendo fora do controle estatal, inclusive dos Estados mais poderosos. A proliferação da informação é tanto uma causa da atual "não polaridade" quanto à proliferação de armamentos (HAASS, 2008).

A nova revolução da informação está mudando a natureza do poder e aumentando a sua difusão. É isto que é preciso ter em mente quando se fala em poder cibernético. O Estado continuará a ser o ator dominante no cenário mundial, mas a cena

[3] ARPANet, acrônimo em inglês de *Advanced Research Projects Agency Network* do Departamento de Defesa dos EUA, foi a primeira rede operacional de computadores à base de comutação de pacotes, e o precursor da Internet foi criada só para os militares.

internacional estará cada vez mais movimentada e difícil de ser controlada. Uma porção muito maior da população, tanto domesticamente quanto entre os Estados, tem acesso ao poder oriundo da informação. A atual revolução da informação reduziu os custos de criar, processar e transmitir informação. (NYE, 2010).

Quem chamou a atenção para a questão da "guerra cibernética", pelo menos do modo como ela está sendo tratada nos dias de hoje, foi, principalmente, Richard Clarke, cujo mérito está no fato de ter levado o assunto para discussão pública, isto é, para além dos círculos das informações classificadas da comunidade de segurança nacional – no caso, estadunidense.

Inicialmente Clarke elaborou este livro nos Estados Unidos, mas acabou chamando a atenção da imprensa do mundo todo. Dessa forma, provavelmente o seu livro *Cyberwar*: *The Next Threat to National Security and What to Do About It* (2010), escrito em parceria com Robert Knake, e todas as produções intelectuais decorrentes, foram e estão sendo lidas em diversos países, influenciando de alguma forma o modo de se pensar o fenômeno da "guerra cibernética".

Em suma, Clarke e Knake buscam atuar diretamente em um debate público sobre estratégia de "guerra cibernética", antes que os Estados Unidos entrem em um conflito deste tipo. Afirmam que a "guerra cibernética" não dá nenhuma vantagem à Washington, mas, na verdade, coloca o país em perigo. Certamente os EUA devem se preocupar com as ameaças cibernéticas às suas infraestruturas críticas, mas isso não significa que a "guerra cibernética" não lhes dê alguma superioridade.

Para o assunto ser discutido mais claramente, no primeiro capítulo de *Cyberwar* é dada uma definição preliminar de "guerra cibernética": os autores a entendem como sendo constituída por determinadas ações conduzidas por Estados-nação para penetrar computadores, ou redes de computadores, de outros países, com o objetivo de causar algum dano. Mais adiante no livro os autores ampliam a definição:

> Guerra cibernética é a penetração não autorizada – por, em nome de ou em apoio a um governo – de um computador, ou uma rede de computadores, de outra nação, ou qualquer outra atividade que afete um sistema de computador – atividade esta na qual o objetivo é adicionar, alterar ou falsificar dados, ou causar alguma ruptura ou dano a um computador, a

> algum dispositivo de rede ou aos objetos controlados por um sistema de computadores [4] (CLARKE; KNAKE, 2010, cap. 7).

Clarke e Knake chamam a atenção para o fato de que há uma grande possibilidade de que a "guerra cibernética" tenha o potencial de mudar o balanço militar mundial e, assim, alterar as relações políticas e econômicas. Isso é importante, pois indica que as ameaças cibernéticas têm algum impacto significativo na política internacional.

2. A evolução do conceito de segurança internacional e a ciberguerra

O conceito de segurança vem se ampliando para além das políticas estratégicas nacionais. Os valores hegemônicos internacionalmente reconhecidos parecem incorporar-se crescentemente a esse conceito. A institucionalização de novos valores decorreria da mudança da configuração do sistema internacional, que pareceria tender para a forma unipolar, embora nela permaneçam significativas características de multipolarismo. Como sabemos a tendência ao unipolarismo não é necessariamente sinônimo de predomínio de uma determinada potência, como ocorreu em outros períodos históricos. Os valores que antes serviram de apoio para a sustentação do equilíbrio bipolar (defesa da civilização ocidental ou anti-imperialismo militante) não mais se ajustam à nova configuração do sistema internacional, cuja sustentação dependeria agora da predominância de pilares diversos, como o liberalismo econômico, os direitos humanos, a proteção ambiental, os direitos sociais e igualmente importantes, o militar-estratégico, ainda que considerado sob novas formas.

O conceito de segurança sob a ótica das Relações Internacionais é bastante complexo, sendo necessários autores renomados como Buzan para esclarecê-lo. Inicialmente existem fatores que devem ser ponderados para nossa análise posterior.

Pode-se dizer que o debate teórico em Relações Internacionais está concentrado em dois campos. De um lado encontra-se o tradicional Realismo, e do outro o Construtivismo. Novamente, Realistas e Construtivistas têm visões diferentes, dentre outras, sobre o foco que se deve observar quando se estiver abordando a segurança de um país.

Irei me embasar na visão realista para conceituar segurança Internacional e conforme eles tendem a ver a segurança como um derivativo do poder: um ator com suficiente poder que atinja uma posição dominante adquiriria como resultado a sua segurança.

[4] A tradução é deste que escreve.

O conceito de Segurança Internacional passou por várias reformulações teóricas durante os anos conforme Buzan destaca.

Inicialmente apresentou o conceito de segurança coletiva, mas com o fracasso da Liga das Nações e posteriormente das Nações Unidas, interrompeu os interesses nessa abordagem (Buzan, 1987), até chegar ao conceito de segurança Multidimensional.

A Segurança Multidimensional ajuda a entender como essa nova modalidade de guerra, a ciberguerra, tem ganhado projeção entre os Estados, tendo em vista, que com a intensificação cada vez mais severa da globalização, não só os Estados e Organizações Internacionais tornam-se alvos, mas os próprios indivíduos e empresas. Trata de uma questão de insegurança do sistema global, já que é algo novo e propício a causar anarquia ao cenário mundial.

O problema do dilema de segurança é que o mesmo possui uma natureza multidimensional trazendo uma diversidade de temas, arenas e atores com fronteiras nem sempre convergentes. Esse problema pode ser visto por dois pontos. Primeiro devido a uma indefinição de fronteiras no espaço cibernético entre o que é nacional e internacional. O segundo ponto diz respeito a uma indefinição das estruturas estatais que vão atuar no espaço cibernético, se são estruturas civis (segurança pública) ou se são de segurança militar (defesa).

O conceito de Segurança Multidimensional[5] foi definitivamente estabelecido na Conferência Especial sobre Segurança realizada na Cidade do México em 2003. Nessa Conferência, o conceito e as abordagens tradicionais devem ser estendidos às ameaças com que possuem aspectos diferentes como os ataques a Cibersegurança.

> Os criminosos recorrem ao uso de novas tecnologias para melhorar a sua capacidade de organização e, consequentemente, tem aumentado o nível de violência. Por isso para a Organização dos Estados Americanos a insegurança é considerada uma das principais ameaças às civilizações de convivência pacífica, e também representa um desafio para a consolidação da democracia e do Estado de Direito (STEIN, 2010).

O enfoque de segurança multidimensional adquire importância à medida que explica porque a segurança cibernética antes de ser exclusividade de uma ótica

[5] A Secretaria de Segurança Multidimensional foi criado em 2005 em reconhecimento da necessidade urgente de tratar da segurança de uma forma mais abrangente e incorpora programas previamente existentes para coordenar as respostas dos Estados membros a ameaças de segurança nacional e as ameaças à segurança dos cidadãos (CHISMAN, et al, 2011).

internacionalista, passa a ser visualizada dentro de uma agenda multidimensional, com repercussões em agendas securitárias tênues de natureza civil e militar. (DAVID, 2001).

Com base nos paradigmas de análise dos ciberconflitos, na identificação de suas naturezas e os atores envolvidos, surge a possibilidade de uma apreensão detalhada da espacialização dos campos de poder dos ciberconflitos, de maneira a mostrar, tanto, as forças descentralizadas dos ataques cibernéticos, quanto, as contra forças centralizadas, das estruturas civis e militares nos Estados Nacionais.

A figura 1 a seguir, mostra que existe uma grande quantidade de ciberconflitos no mundo, sendo a ciberguerra uma dimensão com visão centrada no estado e permeada por *harckers*[6] soldados. É importante visualizar no mapa quais Estados detém estruturas de defesa cibernética.

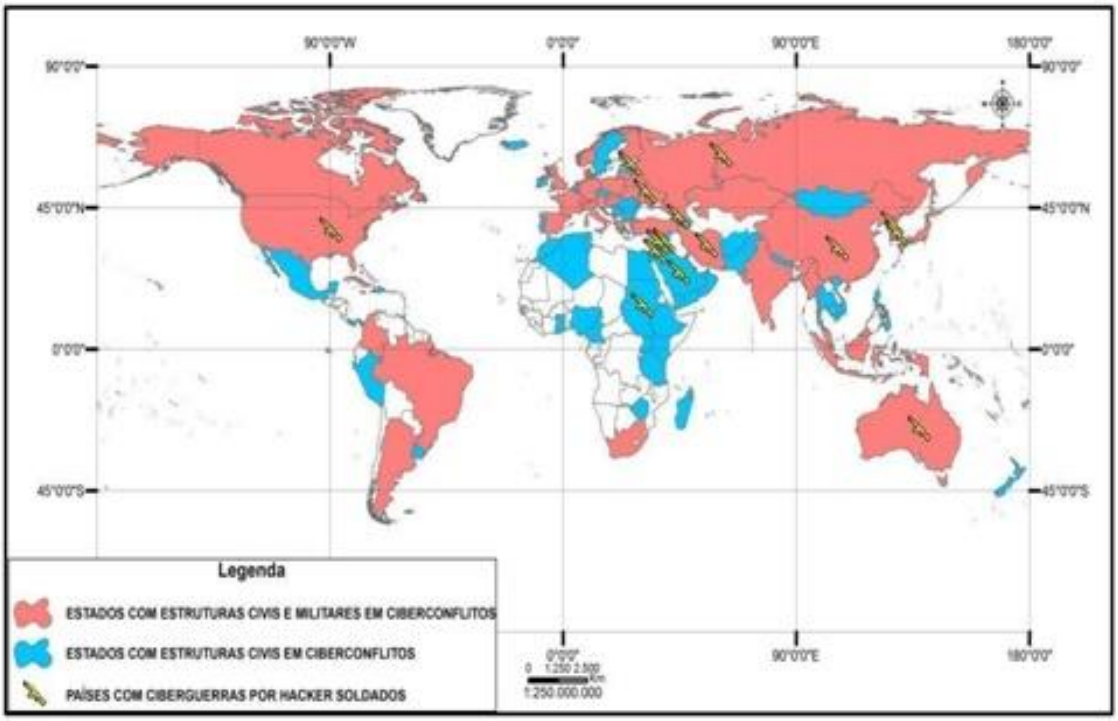

Figura 1- Estruturas civis e militares da ciberguerra

Fonte: SENHORAS, 2014

[6] Pessoa que possui um bom conhecimento em informática, sendo capaz de fazer *hack* (modificação, alteração) em algum sistema informático.

O mais comum é a existência de estruturas civis e militares com ações realizadas principalmente com *hackers* soldados como acontece nos Estados Unidos, Rússia, China, Coréia do Sul, Coréia do Norte, Austrália, Estônia, Geórgia, Ucrânia, entre outros países. Essa atuação só de civis gera ainda mais instabilidade ao sistema internacional, pois é mais difícil de o Estado ter controle sobre os ciberataques.

Cabe retomar uma questão elaborada por DEUTSCH (1978) nos anos 60. Utilizando-se da Lei de Parkinson para a discussão da segurança, afirma que "a sensação de insegurança de uma nação aumenta na razão direta de seu poder. Quanto maior e mais poderosa for uma nação, mais os seus líderes, suas elites, e frequentemente sua população, aumentam seus níveis de aspiração em política internacional" (DEUTSCH, 1978: p. 118).

Por fim, o espaço cibernético é um teatro de guerra caracterizado pela insegurança multidimensional, uma vez que a mesma possui tanto um caráter de ameaça tradicional interestatal quanto de nova ameaça. Isso se deve ao fato de que numa visão clássica nacional realista, a ciberguerra representa uma ameaça tradicional e numa visão liberal representa uma nova ameaça.

3. Ameaças do ciberespaço

O ciberespaço e as tecnologias de informação têm múltiplas influências sobre as sociedades em uma escala global. No entanto, devido à enorme complexidade da área, essas influências são muito difíceis de avaliar, como é para entendê-las.

Scott Charney[7] lista cinco tipos de ameaças diferentes: Em primeiro lugar há vários atores, indivíduos, grupos criminosos organizados, empresas e até mesmo estados, que têm os meios e o interesse em agir de forma maliciosa. Em segundo lugar, esses atores, têm motivos muito divergentes, por exemplo, o enriquecimento pessoal, espionagem ou o ataque à infraestrutura crítica de um estado. Em terceiro lugar, há muitas maneiras diferentes de atacar e atribuir o feito a outro ator específico.

Em quarto lugar, a Internet é um ambiente compartilhado e integrado, e isso não só complica a atribuição, mas também a identificação de grupos específicos, e como a atividade maliciosa ocorre dinamicamente, torna-se extremamente difícil a identificação da

[7] Diretor de crimes cibernéticos, Departamento de Justiça dos EUA.

real ameaça. Em quinto lugar, as consequências de atividades maliciosas são muito difíceis de prever.

De fato, os cenários de ataques do ciberespaço são assustadores e, muitas vezes parecem estranhos, quando, por exemplo, o filho do vizinho é supostamente capaz de invadir o sistema de uma usina de energia nuclear de um país, como foi retratado no filme *War Games*, do diretor John Badham, em 1983. Por mais absurdo que esses tipos de cenários pareçam, eles têm um efeito real sobre as políticas de segurança cibernética de hoje.

> A economia dos EUA em expansão habita um espaço físico comum, e em nossas redes de comunicações. Se um inimigo interrompe nossas transações financeiras e contábeis, nossas ações e mercados de títulos ou o nosso comércio varejista..., resultaria o caos. Nossas redes de energia, transporte aéreo e terrestre, telecomunicações e sistemas de filtragem de água estão em perigo também. (John Michael McConnell, 2010) [8]

São estes cenários apocalípticos que formam a compreensão básica de como proteger e governar o ciberespaço de hoje. Aqui, a segurança cibernética é entendida como a prevenção e a luta contra os ataques de larga escala, a partir da adulteração nas infraestruturas críticas, por exemplo, sistemas de controle de tráfego, à manipulação dos mercados de ações.

Sistemas de hoje estão interligados e muitos aspectos do funcionamento das sociedades modernas dependem de sistemas de computador em rede, a partir da biblioteca da cidade para os mercados financeiros globais. Nesse sentido, a manipulação ou a perturbação poderia ter enormes efeitos sobre as sociedades, com dimensões catastróficas.

Organizações internacionais, Estados e seus agentes de segurança estão cientes das possibilidades e perigos do ciberespaço, e estão construindo mecanismos para conseguir governar a área. Com isso surgem não só novos padrões de segurança, mas também novas formas de vigilância: As revelações recentes sobre o uso de vigilância e tecnologia de controle por meio da CIA (*Central Intelligence Agency*) pelo ex-funcionário da NSA (*National Security Agency*)[9] Edward Snowden[10], dão uma ideia da escala real das possibilidades de controle e vigilância cibernética.

---

[8] Diretor Nacional da Inteligência dos Estados Unidos, de 20 de fevereiro de 2007 à 27 de Janeiro de 2009.

[9] Agência de Segurança Nacional dos EUA, criada em 4 de novembro de 1952 com funções relacionadas a Inteligência de sinais incluindo interceptação e criptoanálise.

[10] É um analista de sistemas, ex-administrador de sistemas da CIA e ex-funcionário da NSA que tornou públicos detalhes de vários programas que constituem o sistema de vigilância global da NSA americana.

As ameaças do ciberespaço podem, portanto, ser construídas de múltiplas formas e por meio de múltiplos atores. Eles chegam de violações de direitos autorais sobre crimes individuais até cenários apocalípticos.

4. Mentalidade militar de segurança cibernética

De um ponto de vista militar e estratégico, o mundo pode ser descrito em termos bastante simples com um foco nos Estados-nação e o realismo tradicional das Relações Internacionais, o estado e sua segurança nacional estão no cerne do conceito de segurança.

Essa forma de pensar estava presente não só durante os tempos de bipolaridade e guerra fria, mas também na chamada guerra contra o terror, embora, claro, com a percepção de que o inimigo não é tão claramente identificável. No entanto, pensar em termos de uma mentalidade militar de segurança significa enfocar o Estado como entidade e sua segurança nacional.

Nos EUA, um ataque terrorista é entendido como um ato de guerra, como um ataque ao Estado principalmente de natureza externa, mesmo quando o inimigo vem de dentro de seu próprio estado, por exemplo, na forma de grupos revolucionários agressivos. Predominantemente o que está sendo ameaçada é a (nação) estado e a pronta-resposta militar será empregada contra essas ameaças.

Por conseguinte, a retórica de autodefesa, integridade territorial e soberania desempenham um papel importante para justificar medidas intrusivas e agressivas em uma perspectiva legal, e o Direito Internacional oferece vários desses mecanismos.

Tal retórica bélica é facilmente identificável quando se trata de percepções de ameaças do ciberespaço. Em maio de 2011, os EUA publicaram sua Estratégia Internacional para o ciberespaço, que afirma:

> Quando tal se justifique, os Estados Unidos vão responder a atos hostis no ciberespaço como seria para qualquer outra ameaça ao nosso país. Todos os estados possuem o direito inerente de legítima defesa, e reconhecemos que certos atos hostis realizados por meio do ciberespaço poderia obrigar ação no âmbito dos compromissos que temos com nossos parceiros de tratados militares. Reservamo-nos o direito de utilizar todos os meios necessários... adequados e compatíveis com o direito internacional aplicável, a fim de defender nossa nação, nossos aliados, nossos

> parceiros e nossos interesses.[11](A Estratégia Internacional da Casa Branca para o Ciberespaço).

Após a análise estratégica das ameaças cibernéticas, muitos Estados criaram Estratégias de Segurança Cibernética e constituíram instituições de defesa, com o intuito de se preparar para o ataque e a guerra cibernética. Estas instituições compartilham informações e coordenam a segurança de autoridades relevantes, incluindo empresas privadas e, muitas vezes os militares.

Os EUA construíram os *Estates Cyber Command United* (USCYBERCOM) [12], Alemanha o *National Cyber Defence Centre*[13] e no Reino Unido, uma unidade cibernética conjunta integrada em estruturas militares que desenvolvem e utilizam uma gama de novas técnicas, incluindo medidas proativas, para interromper ameaças a segurança do tráfego da informação.

Todos estes países mostram uma compreensão muito militarista das ameaças do ciberespaço. Isto lembra a lógica da Guerra Fria, e parece que uma nova corrida armamentista que na verdade já está em andamento - mas desta vez com armas diferentes. As ameaças, é claro, poderiam ser reais. Espionagem militar, sabotagem das forças armadas, ataque as infraestruturas e roubo de tecnologia, as quais sempre foram parte da guerra, e não é nenhuma surpresa que, com a tecnologia militar moderna, as metodologias mudassem.

Por exemplo, em um incidente em 2011, os EUA perderam um veículo aéreo não tripulado (VANT) Tipo RQ-170 Sentinela (ver figura 2) sobre o território iraniano. O Irã afirma que capturou a aeronave *hackeando* seus controles. Mais tarde, em fevereiro de 2013, o Irã alegou que tinha descriptografado e extraído todas as informações a partir do VANT, operado pela CIA em uma missão de espionagem.

No entanto, os cenários vão muito além das ameaças às maquinas e armas militares. Claro que, em teoria, o que começa como um ataque a um alvo militar pode se tornar também uma ameaça para a infraestrutura civil. Um atentado cibernético na rede elétrica, das usinas nucleares, em bombas de água, em sistemas de transporte público e até

[11] A tradução é deste que escreve.
[12] Comando Cibernético dos EUA é um comando sub-unificado das forças armadas, subordinado ao Comando Estratégico dos Estados Unidos. Sua responsabilidade é a de proteger a rede militar de computadores dos EUA.
[13] O Centro Nacional Alemão de Defesa Cibernética é uma cooperação de agências de segurança alemãs no nível federal que tem a função de repelir ataques eletrônicos em infraestruturas de TI da República Federal da Alemanha e sua economia.

mesmo sobre o sistema econômico nacional poderia afetar civis de maneira sem precedentes durante, ou antes, de um conflito.

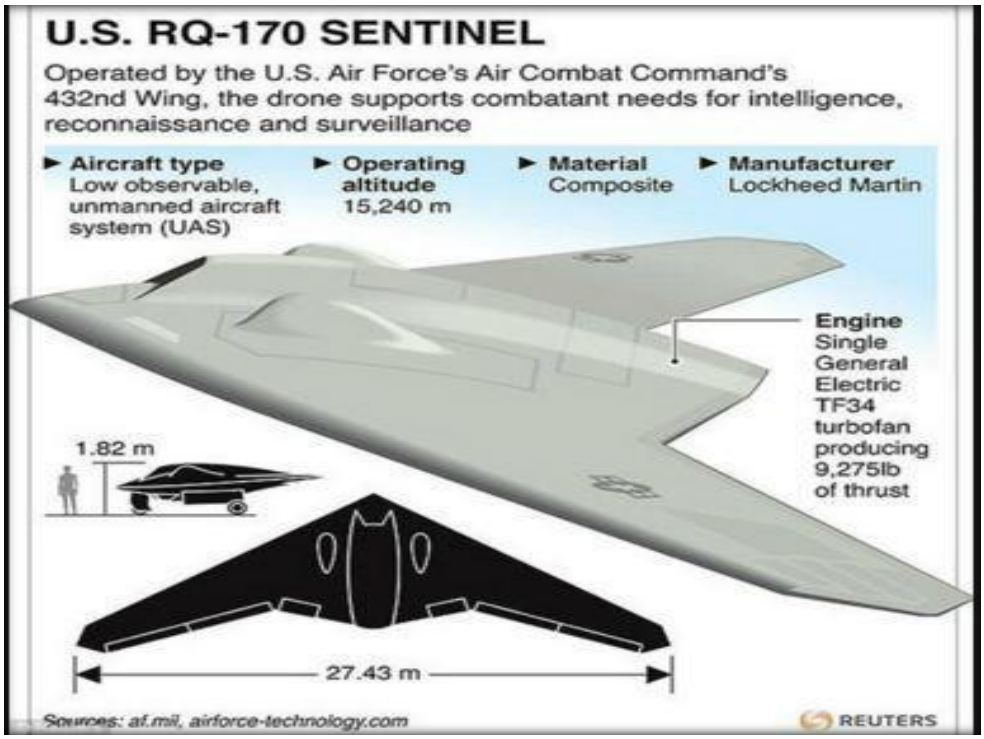

Figura 2 – VANT - U.S. RQ-170 Sentinel

Fonte: AVIATION WEEK, US Air Force

A mentalidade militar de segurança no ciberespaço, portanto, vem como uma atitude profissional onde conscientização de segurança é baseada em concepções militares e estratégicas de ameaças. As ameaças à segurança são articuladas em uma língua que distingue nitidamente entre concepções de "amigo" e "inimigo". O objeto ameaçado, portanto, é uma comunidade ampla (por exemplo, nação, estado, e sociedade) ou certas partes existenciais dele (abastecimento de água e infraestrutura). Além do mais, uma mentalidade militar de segurança exige e legitima meios excepcionais para proteger e defender a entidade, muitas vezes sugerindo medidas radicais (interruptor de corte geral da internet, capacidades de ataques cibernéticos preventivos, etc.).

5. Guerra cibernética e militarização do seu ambiente

Ao aproximar-se do ciberespaço com uma mentalidade militar de segurança, torna-se fácil remeter a retórica da Guerra Fria. O fato de que afirma, em uma escala global, que estão construindo sistemas ciberdefesa e incluem cenários de ataques cibernéticos nos seus planos estratégicos de segurança, mostrando que há uma crescente conscientização sobre essas questões[14] (OTAN, 2010). Na verdade, os estrategistas afirmam que a guerra cibernética já está acontecendo em uma escala global (CLARKE; KNAKE, 2010).

Apesar destas afirmações, a partir de uma perspectiva legal, a guerra cibernética pode ser abordada a partir de duas perspectivas diferentes, ambas inerentes a uma mentalidade militar de segurança: em uma forma limitada e em uma forma abrangente. Uma definição limitada, por um lado, vai junto com o princípio da distinção na lei humanitária internacional, daí a obrigação de distinguir entre alvos militares e civis. Isto seguiria a lógica da Lei de Conflito Armado Internacional e as Convenções de Genebra de 1949, estabelecendo uma clara distinção entre o que pode ser alvo e o que não pode em uma situação de conflito armado. Além disso, ciberguerra entendido a partir dessa perspectiva limitada provoca não só o *jus in bello*[15], mas também o *jus ad bellum*, portanto, o mecanismo de justificativas para se envolver na guerra.

O Manual de Tallinn[16] sobre o Direito Internacional aplicável a guerra cibernética é um exemplo de um documento sugerindo que regulamenta ciberguerra usando as ferramentas do direito internacional humanitário.

Uma definição mais abrangente iria englobar qualquer tipo de ataque cibernético contra infraestruturas civis e militares de uma nação, não apenas qualquer tipo de ator - de estado militar e de inteligência estrangeira - mas também incluiriam atos de espionagem industrial, corte da rede mundial, ativismo, etc. Assim, com o problema da atribuição no ciberespaço, contramedidas militares necessariamente teriam como alvo qualquer elemento que fosse percebido como uma ameaça e, portanto, tornariam o princípio da distinção impraticável.

---

[14] Trecho do tratado da OTAN, 2010, Conceito Estratégico de Defesa e Segurança dos Estados Membros da Organização do Tratado do Atlântico Norte.

[15] O Direito Internacional Humanitário (DIH), ou *jus in bello*, é o direito que rege a maneira como a guerra é conduzida. O DIH tem fins puramente humanitários, buscando limitar o sofrimento causado pela guerra. Independe de questões sobre a justificativa ou os motivos para a guerra, ou a prevenção da mesma - áreas cobertas pelo *jus ad bellum*.

[16] Manual de Tallim – Lei Internacional aplicável à guerra cibernética.

A origem e motivos, bem como a natureza desses ataques são múltiplos. Eles vêm de *hackers*[1] individuais, do crime organizado, espiões industriais, ativistas políticos e muitos mais.

E aqui está o problema: alguns desses "ataques" estão melhor classificados como ativismo político, alguns são protestos e manifestações, alguns são fraudes para o enriquecimento pessoal e outros são hostilidades militares.

Para contra atacá-los e reagir com meios militares corremos o risco de afetar os espaços livres na sociedade. O que é realmente surpreendente são as medidas para proteger o ciberespaço, muitas vezes combinam enormes quantidades de energia a partir de setores militares de inteligência e de setores para aplicação da lei.

Um exemplo de proteção bastante eficaz proposto no Congresso dos EUA em 2010, mas nunca promulgado, foi a exigência de um "interruptor de corte da Internet"- teria a finalidade de encerrar toda a atividade de rede para proteger o presidente - Sua principal consequência, no caso que a regulamentação internacional, poderia dar início a uma corrida cibernética armamentista em que novas instituições de segurança conjuntas e muito poderosas, encabeçadas por militares, obteriam enorme quantidade de poder de controle sobre o ciberespaço global, permitindo o acesso até mesmo aos *smartphones* [17]da sociedade civil.

Estamos começando a ver uma tomada de poder no ciberespaço por militares do mundo: monitoramento em redes de larga escala e controle militar dos padrões da Internet. (SCHNEIER, 2008) Na verdade, este ponto de vista parece ser muito mais próximo da realidade depois das revelações (Edward Snowden) recentes dos arquivos da NSA, veiculadas pelo jornal *the Guardian*[18].

Este fato mostra nada menos que a militarização do ciberespaço, na qual uma mentalidade militar de segurança transforma o espaço público em uma zona de guerra e em um estado de exceção.

6. A mentalidade liberal de segurança: crimes no ciberespaço

[17] Celular com conectividade e funcionalidades semelhantes às de um computador pessoal, notadamente com um sistema operacional capaz de operar várias aplicações. Tradução livre: Telefone inteligente.
[18] É um jornal britânico fundado em 1821.

Uma resposta ao recém revelado arquivo da NSA, por Edward Snowden, e com isso a percepção de que as agências de inteligência têm construído e utilizado de ferramentas tecnológicas para uma vigilância abrangente de comunicações digitais, é chamada de mecanismo de justificação legal. Espionagem global injustificada de membros do governo sobre os cidadãos vem com muito debate jurídico, incluindo questões de direitos fundamentais [19].

Não só o direito à privacidade, liberdade de expressão, mas também os direitos à proteção de dados, tal como consagrado em convenções internacionais e de direitos humanos, bem como regimes regionais tais como a Convenção Europeia dos Direitos Humanos oferece uma variedade de mecanismos de proteção contra o excesso intrusivo e sobre controle do estado. Concentrando-se nos direitos e, portanto, outra possibilidade de enfrentar as questões de segurança no ciberespaço. Esta abordagem é inerente à outra mentalidade: a mentalidade liberal de segurança.

Contrastando a mentalidade militar de segurança e seu foco sobre os meios estratégicos militares e estratégias para solução de problemas, sempre com um inimigo claramente projetado, uma mentalidade liberal de segurança vem com uma compreensão mais sensível aos indivíduos, os seus direitos e a liberdade que o ciberespaço está oferecendo. A partir desta perspectiva, existe, como uma coisa natural, uma variedade de ameaças no ciberespaço que precisam ser abordadas; no entanto, essas ameaças não afetam drasticamente a vida e a existência da nação como uma entidade. Assim, o objetivo final não é primariamente preservar e proteger a soberania do Estado e integridade, mas a integridade do indivíduo.

No entanto, é plausível que a ocorrência de uma guerra cibernética com ataques estratégicos coordenados à infraestrutura de comunicação e com efeitos não só as estruturas militares, mas também sobre sociedades inteiras. Partindo de uma perspectiva liberal, não é a sociedade como tal que tem de ser protegida contra as ameaças do ciberespaço, mas o indivíduo e a formação de tal sociedade.

[19] Trecho de documento apresentado pela Comissão do Parlamento das Liberdades Cívicas, da Justiça e dos Assuntos Internos da União Europeia.

Há uma percepção de ameaças existenciais (terrorismo), mas medidas contra essas ameaças e riscos precisam ser equilibradas contra as interferências e restrição dos direitos e liberdades dos cidadãos.

Segurança Cibernética percebida por meio de uma mentalidade liberal de segurança é, portanto, focada na proteção e a segurança do indivíduo. Essa mentalidade, portanto, incluem ameaças e riscos que vão além dos estados, os métodos militares e as regras da guerra, e isso permite, ao mesmo tempo contramedidas que vão além do emprego de lógicas e métodos militares.

Ela (mentalidade liberal de segurança) percebe as ameaças de uma perspectiva muito mais ampla e de uma forma muito mais detalhada, sendo assim, se torna relevante para o debate sobre segurança cibernética, pois permite uma visão sob a perspectiva interna: baseada no direito penal, na governança e no policiamento.

Conforme descrito anteriormente, um dos problemas de ciberespaço é que as suas fronteiras são difíceis de definir. Além disso, os atores são extremamente variados, desde indivíduos até empresas estatais. Olhando para os perigos do ciberespaço com uma mentalidade militar de segurança, significa suspeitar de uma ameaça potencial para a sociedade ou país em cada ato malicioso, que é então considerado como um ato de guerra, vindo de um inimigo externo.

Olhando para o ciberespaço com uma mentalidade liberal de segurança permite a correta diferenciação entre as ameaças, e consegue diferenciar o cibercrime da ciberguerra, proporcionando diferentes respostas a ameaças.

Cibercrime pode então ser visto como um fenômeno que não necessariamente precisa ser combatido usando algum tipo de centro de comando cibernético executado pelos militares, mas utilizando as estruturas existentes do Estado de direito. Tal abordagem poderia, portanto, superar os perigos da militarização do ciberespaço e com este, expulsar suas estruturas e métodos existentes e usar os princípios jurídicos. Além disso, poderá opor-se ao emprego de meios militares secretos que vão além do policiamento e métodos intrusivos que permeiam as esferas da vida da sociedade.

A concepção de mentalidade liberal de segurança é baseada em uma compreensão liberal dos indivíduos, seus direitos legais e a liberdade. Essa mentalidade,

portanto, por um lado, incorpora concepções de segurança humana e, por outro lado, considera os direitos humanos e o equilíbrio de direitos como uma parte essencial nas sociedades modernas. A partir desta perspectiva, é imprescindível a proteção dos indivíduos contra eventuais violações; por exemplo, por meio da legislação criminal.

Naturalmente, o ciberespaço vem com uma variedade de possíveis violações contra o indivíduo. A fraude, o roubo de identidade, as violações de direitos autorais, a perseguição, o assédio, o *hacking* e muitos mais são exemplos de violações contra o indivíduo e a sociedade. Por isso, o cibercrime é considerado como um fenômeno novo e uma nova área do direito penal. Sem ir muito além sobre os debates em torno da natureza do crime cibernético, é importante distinguir entre as muitas facetas do cibercrime, por exemplo, a tentativa de criar uma classificação específica no aspecto de crimes cibernéticos.

No contexto mais amplo, o direito penal e as discussões sobre cibercrime podem ser vistas como ferramentas para equilibrar e proteger os direitos individuais específicos.

O que é importante no contexto deste artigo é que uma mentalidade liberal de segurança abarca especialmente a proteção das pessoas das violações do ciberespaço e, portanto, procura o equilíbrio entre a liberdade individual, direitos e deveres, bem como os interesses da segurança coletiva. O que existe em comum com a mentalidade militar de segurança, porém, é que o conceito de "segurança" como tal, é um dado adquirido. Em casos de interferências dos direitos individuais no ciberespaço, no entanto, essas violações precisam ser justificadas e deverá ocorrer a inclusão de mecanismos de salvaguarda adequados. Portanto, a Criminalização poderá fornecer uma ferramenta para combater problemas de segurança no ciberespaço, e ao mesmo tempo, fornecerá garantias legais.

Em um comentário sobre a vigilância em larga escala sobre os cidadãos trouxeram à luz por meio dos, já mencionados, arquivos da NSA, a Alta Comissária da ONU[20] para os Direitos Humanos advertiu sobre consequências negativas:

> Enquanto as preocupações sobre a segurança nacional e a atividade criminosa podem justificar o uso excessivo adotado dos programas de vigilância, monitoramento sem salvaguardas adequadas para proteger o direito à privacidade, na verdade, o risco de um impacto negativo sobre o gozo dos direitos humanos e das

[20]Organização das Nações Unidas (ONU), ou simplesmente Nações Unidas, é uma organização intergovernamental criada para promover a cooperação internacional.

> liberdades fundamentais.[21] (Escritório das Nações Unidas do Alto Comissariado para os Direitos Humanos).

Uma mentalidade liberal de segurança, embora permita a exceção em certos casos, apela para fazê-lo estritamente dentro do Estado de direito, apenas quando salvaguardas adequadas estão em vigor.

A concepção de uma mentalidade liberal de segurança, portanto, pode ser caracterizada por um forte foco no indivíduo. Segurança não é muito conceituada para a comunidade, mas como garantia para o indivíduo que vive em uma sociedade. Qualquer interferência nos direitos, liberdades e modos de vida dos indivíduos que se baseia em segurança, portanto, precisaria ser de alguma forma justificada e equilibrada. Além disso, o próprio objeto de segurança é o indivíduo e, neste sentido, os indivíduos precisam ser protegidos das violações no ambiente do ciberespaço.

Mecanismos estabelecidos de proteção aos indivíduos contra violações, como, por exemplo, o policiamento e criminalização, são consequências da expansão do ciberespaço.

7. Criminalização e policiamento do ciberespaço

A mentalidade liberal de segurança tentar lidar com as ameaças no ciberespaço dentro do Estado de direito e no âmbito das leis existentes do direito penal. Como o ciberespaço adiciona uma nova área para o direito penal, também novos campos de crime aparecem, exigindo nova legislação, e um dos primeiros tratados internacionais sobre crimes na Internet e crimes em redes de computadores foi a Convenção do Conselho da Europa[22].

Além de listar uma série de crimes cometidos dentro de áreas digitais, tais como computadores relacionados à fraude, falsificação, interferência do sistema de rede, pornografia infantil e violações de direitos autorais, ele tenta vincular estados para inclusão de contramedidas específicas dentro de seus sistemas jurídicos. Ao mesmo tempo, a Convenção também obriga os Estados a garantir a possibilidade de aplicação da lei no ciberespaço. Contudo, os Estados-Membros devem assegurar que as possibilidades legais sejam aplicadas em tempo real e também legitimar a interceptação de dados.

---

[21] A tradução é deste que escreve.

[22] Convenção do Conselho Europeu sobre Cibercrime (Budapeste 23 de Novembro 2001).

Nesse contexto, outro problema se torna aparente: A criminalização de atos maliciosos no ciberespaço pode fornecer razões para expandir suas capacidades de vigilância para as agências de segurança, podendo ser no ato da aplicação da lei ou agências de inteligência. Assim, a falta de regulamentação as novas tecnologias, somado aos novos cenários de ameaça ciberespaço, levou a um aumento das possibilidades da vigilância técnica e a vigilância real. Isto se tornou especialmente visível após revelações dos arquivos da NSA, mostrando as capacidades de vigilância em grande escala. No entanto, já antes disso, as questões de segurança foram abordadas pelos tribunais, questionando sobre a vigilância e controle das práticas intrusivas por agentes de segurança do Estado. Assim fez, por exemplo, o Tribunal Constitucional alemão ao derrubar normas legais e práticas excessivas de pesquisas *online* por meio da polícia e do Escritório para Proteção da Constituição que desenvolveu um novo direito fundamental à confidencialidade e integridade dos sistemas de tecnologia da informação em 2008.[23]

No que diz respeito ao aumento da criminalização dos delitos cibernéticos, devem ser considerados que, como permeiam redes de computadores o ciberespaço é um fenômeno global, e a criminalização apenas em nível nacional, portanto, sem a cooperação e coordenação internacional está fadada ao fracasso.

Contudo a cooperação internacional também abre lacunas em torno de mecanismos nacionais de salvaguarda. Nesse sentido, há uma necessidade de uma avaliação cautelosa quando se trata de crimes cibernéticos. Os atos maliciosos devem ser revistos cuidadosamente para que realmente os consolidados em direito penal e executadas com os mecanismos transnacionais, especialmente no que diz respeito a questões sensíveis, tais como liberdade de expressão, incitamento contra o discurso do ódio, *hacking* , protesto político, direitos autorais ou interesses comerciais.

De fato, muitos problemas de segurança no ciberespaço tornam-se de interesse particular do que de relevância para a sociedade e precisam de debates abertos na sociedade para sua criminalização, como exemplo cito os debates sobre a criminalização das violações de direitos autorais por meio do compartilhamento de música.

Além disso, até mesmo os efeitos do cibercrime sobre os indivíduos e as sociedades estão sujeitas a forte disputa. Florêncio e Herley, dois pesquisadores da Microsoft,

[23] Corte de Julgamento Constitucional Alemão - 2008

analisaram recentemente estudos sobre danos causados por cibercrimes financeiros e constataram que a maioria deles é metodologicamente falha. "Examinamos o cibercrime a partir de um ponto de vista econômico e encontramos uma história em conflito com a sabedoria convencional. Alguns criminosos fazem bem ao sistema, mas o cibercrime é uma luta implacável de pouco lucro para a maioria."

Há uma forte necessidade de uma avaliação crítica das ameaças por meio do cibercrime, especialmente quando criminalização torna-se um instrumento político e com isso corre perigo de consolidar o interesse particular dentro do direito penal. Além disso, a criminalização do ciberespaço oferece justificativa para o controle e mecanismos de vigilância. Uma mentalidade liberal de segurança, embora se esforçando para o equilíbrio de interesses, pode ficar sem ferramentas para se opor aos cenários de ameaças que carregam o interesse político ou desvirtua da missão de segurança. Nesse sentido, uma mentalidade liberal de segurança, apesar de reconhecer os perigos do excesso de interferências no ciberespaço, ainda pode seguir por mais que haja o excesso da criminalização e ampliação do controle simplesmente por causa da dificuldade de análise dos cenários de ameaça. Além disso, a expansão dos poderes de policiamento no ciberespaço pode levar a mais controle e vigilância sobre a criminalização no ciberespaço.

CONCLUSÃO

Este artigo inicialmente apresentou a base histórica sobre o ambiente do ciberespaço, mencionando seu nascimento e destacando sua rápida evolução. Na seção seguinte foi destacada a evolução do conceito de segurança Internacional sob a ótica realista, recorrendo ao teórico Buzan, chegando ao conceito de segurança Multidimensional – a mais apropriada para entendermos os fenômenos propostos pelo artigo. Posteriormente elaborei uma síntese sobre as ameaças que permeiam o ambiente do ciberespaço, apontando a crescente expansão das redes de computadores e, por conseguinte a constante evolução das ameaças.

Logo a seguir, foram introduzidas duas abordagens distintas de segurança no ciberespaço: mentalidade militar de segurança e mentalidade liberal de segurança. Foram mostradas que ambas as perspectivas se concentram em diferentes ameaças e trazem suas próprias estratégias de solução. No entanto, ambas carregam seus próprios problemas. A

tabela 2 mostra a seguir, uma tentativa de classificar e distinguir as concepções básicas de uma mentalidade militar e liberal de segurança cibernética por meio de uma lista de atributos.

Mentalidade Militar de segurança	**Mentalidade Liberal de segurança**
•Ameaça é dirigida contra uma definida comunidade ou suas partes existenciais.	•Ameaça definida é dirigida contra indivíduos.
•Ameaça vem de um inimigo.	•Ameaça vem de indivíduos.
•Proteção da comunidade.	•Proteção dos individuais contra ofensas.
•Forte foco militar, tático e meio e métodos estratégicos.	•Meios e métodos de policiamento: equilíbrio e justificação do poder.
•Luta contra ameaças.	•Regulando ameaças.
•Meios excepcionais para combater ameaças.	•Meios excepcionais para combater as ameaças, mas precisam ser justificadas dentro de quadros jurídicos.
•Cenários críticos de ameaça.	•Cenários de ameaça moderada.

Tabela 2. Atributos de mentalidades de segurança.

Fonte: Elaborada por este autor.

A mentalidade militar de segurança demonstrou que percebe o ciberespaço por meio da lente da estratégia militar, com suas táticas e a distinção clara de amigo e do adversário. Qualquer ameaça ao ciberespaço será vista como vital para o sistema, e como tal, será adequadamente combatida. Quando a situação do ambiente cibernético piorar a tal ponto, de poder abrir o caminho para conflitos militares reais, e finalmente com a militarização do ciberespaço uma corrida armamentista cibernética acontecerá, e com ela a destruição de seu potencial democrático, econômico e livre.

A mentalidade liberal de segurança acompanhou uma perspectiva de direitos orientada basicamente nos indivíduos; no entanto, corre-se o risco de generalizar a criminalização permitindo um controle e vigilância exagerados por meio de forças policiais ou outros organismos de segurança do Estado. Embora o equilíbrio dos direitos individuais

possa ser possível, uma mentalidade liberal de segurança ainda carrega a própria ameaça e tem dificuldade em desarmá-la, especialmente quando a ameaça é real. Então, poderá ocorrer um excesso de criminalização e com isso, o controle generalizado pode muito bem ser capaz de destruir o espaço público. Por um lado, o ciberespaço não pode ser um espaço sem lei. Por outro lado, o ciberespaço se torna cada vez mais central, se não vital, à vida das sociedades como canaliza muitas atividades individuais essenciais, de comunicações diárias, operações financeiras, ativismo político e de protesto. Neste sentido, o ciberespaço deve ser manuseado com muito cuidado, especialmente quando se trata de conceber uma nova legislação. Quando se trata de policiamento, deve-se avaliar cuidadosamente a aplicação dos direitos em vez das medidas opressivas e vigilância. Notamos que ao fazermos uso de novas tecnologias sempre trará consigo, uma variedade de medidas cujas dimensões não são fáceis de avaliar.

Do ponto de vista militar, foi demonstrado que, as ameaças no ciberespaço estão ligadas às vulnerabilidades dos estados. Sabotagem cibernética, ataques cibernéticos e até mesmo ciberguerra são percebidas como uma clara ameaça à segurança Estatal. Partindo de uma perspectiva vigilante, o desenvolvimento do mundo digital requer novos tipos de policiamentos, técnicas apropriadas e legislação criminal. Isso cria um dilema: por um lado, a vigilância do ciberespaço e combate dos crimes cibernéticos, as agências de segurança precisam expandir seus meios e métodos para formarem as reservadas necessárias para o domínio da segurança militar e estratégica. Em contrapartida, para defender um estado contra ameaças de ciberespaço a segurança militar orientada para o exterior precisa empregar seus meios e métodos estritamente para o policiamento interno. Os resultados destes movimentos podem ser vistos na criação de centros de cibersegurança conjuntos extremamente poderoson, tais como o USCYBERCOM. Nesse sentido, as fronteiras entre a vigilância nacional e defesa militar tornam-se indefinidas e como consequência, as competências dos órgãos de segurança expandem-se e suas fronteiras entre o direito penal e de segurança nacional irão desaparecendo.

Diante de todo o exposto, podemos concluir que ao identificarmos as diferenças entre as mentalidades de segurança poderemos questionar, de forma embasada, os meios e métodos empregados no tratamento das Liberdades fundamentais dos indivíduos.

Foi possível concluir também, baseado em teorias mencionadas por Barry Buzan sobre o conceito de segurança Multidimensional que os EUA, devido as suas dimensões (Estado) poderiam embasar sua necessidade sem limite de segurança, legitimando

assim a intrusão e vigilância militar sob qualquer indivíduo ou nação que apresente qualquer tipo de ameaça ou desestabilização a sua segurança e, por conseguinte, a balança do poder.

Foi apresentado há pouco tempo, pelos EUA, um exemplo que suas agência de Inteligência compreenderam muito bem a importância da vigilância cibernética montando uma mega estrutura de produção do conhecimento, conhecido mundialmente como o caso de Edward Snowden, ex- analista da NSA e suas revelações demonstraram o quão descomunal e sujo é o jogo da ciberespionagem mundial pela busca de informações que possam demonstrar uma possibilidade de desequilíbrio na balança de poder em qualquer parte do planeta.

O presente trabalho buscou levantar as principais diferenças entre as mentalidades militar e liberal de segurança, com o escopo das Relações Internacionais, utilizando, em especial, os pensadores do Realismo. Este trabalho não se encerra aqui e abre um caminho para novas pesquisas e questionamentos, por meio de análises de como percebemos a segurança no ciberespaço hoje, e, portanto, que tipo de mentalidade de segurança poderá ser empregada, determinando a concepção do ciberespaço nas sociedades modernas para as próximas gerações.

REFERÊNCIAS BIBLIOGRÁFICAS

BBC. 7 feb. 2013. **Iran Shows Hacked US Spy Drone.** Disponível em: < http://www.bbc.com/news/world-middle-east-21373353> accesso 20 jul. 2015.

BUZAN, Barry; WAEVER, Ole. **Regions and Powers.** Nova Iorque: Cambridge University Press, 2003.

CHISMAN, A.; et alli. **Multidimensional Security in the Americas**: The OAS Secretariat for Multidimensional Security Implements Programs to Combat and Eliminate Terrorism and Develops Policies That Strengthen and Protect Citizen Security in the Americas. **In:** Americas (English Edition), Vol. 63, No. 3, May-June 2011. Disponível em: <http://www.questia.com/magazine/1G1-255495542/multidimensional-security-in-the-americas-the-oas#/>. Acesso em: 26 de set. de 2015.

CLARKE, Richard A.; KNAKE, Robert K. **Cyber War: The Next Threat to National Security and What To Do About It**. HarperCollins e-books, 2010.

CORNISH, Paul; LIVINGSTONE, David; CLEMENTE, Dave; YORKE, Claire. **On Cyber Warfare**: A Chatam House Report, November 2010. Disponível em: <http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r1110_cyberwarfare.pdf>. Acesso em: 20 set. 2015.

DAVID, C. P. **Segurança Cooperativa e Segurança Comum**. Lisboa: Instituto Piaget, 2001.

DEUTSCH, Karl. **Análise das Relações Internacionais**. Brasília: Editora UnB, 1978.

DOUHET, Giulio. **O domínio do ar.** Rio De Janeiro: Instituto Histórico da Aéronáutica, 1988.

FLORÊNCINO, Dinei; HERLEY Cormac .**The Cybercrime Wave That Wasn't**. *The New YorkTimes*,15abr.2012,Disponívelem:<http://www.nytimes.com/2012/04/15/opinion/sunday/the-cybercrime-wave-that-wasnt.html > Acesso em: 13 dez. 2015.

HAASS, Richard. **The Age of Nonpolarity**: *Foreign Affairs*, Vol. 87, No. 3, May/June 2008.

JATOBÁ, Daniel. **Teoria das Relações Internacionais.** São Paulo: Saraiva, 2013.

LIBE. 14 oct. 2013. Committee Inquirity on Eletronic Mass Surveillance of EU Citizens , Statement by Professor Martin Scheinin, Disponível em: <http://www.europarl.europa.eu/document/activities/cont/201310/20131017ATT72929/20131017ATT72929EN.pdf> Acesso em: 11 dez. 2015.

LAKATOS, E. M. & MARCONI, M. de A. **Metodologia do trabalho científico**: procedimentos básicos, pesquisa bibliográfica, projeto e relatório, publicações e trabalhos científicos. 3ª. ed. São Paulo: Atlas, 1990

NATO. **Cyber security.** NATO, 08 Apr. 2015. Disponível em: <http://www.nato.int/cps/en/natohq/topics_78170.htm?> Acesso em: 26 de set. de 2015.

NYE, Joseph. **Guerra e paz no ciberespaço**. *O Estado de S. Paulo*, 15 abr. 2012, Internacional, p. A22. Disponível em: <http://www.estadao.com.br/noticias/impresso,guerra-e-paz--no-ciberespaco-,861242,0.htm>. Acesso em: 21 out. 2015.
_____. **Cyber Power**. Harvard Kennedy School, Belfer Center for Science and InternationalAffairs,May2010.Disponívelem: <http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf>. Acesso em: 23 nov. 2015.

OTAN, **Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation**, 19–20 nov. 2010. Disponívelem:<http://www.nato.int/nato_static/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf> Acesso em: 27 jul. 2015

SANGER S.; SHANE, D.E. :**Drone Crash in Iran Reveals Secret U.S. Surveillance Effort,** *TheNewYorkTimes*(7December2011).Disponívelem:<http://www.nytimes.com/2011/12/08/world/middleeast/drone-crash-in-iran-reveals-secret-us-surveillance-bid.html> Acesso 20 jul. 2015

SENHORAS, E. M. **Mapas de ciberconflitos no mundo: relatório de pesquisa organizado para Congresso Acadêmico de Defesa Nacional**. Boa Vista: UFRR, 2014.

SENHORAS, E. M.; NASCIMENTO, F. S. S.: **Multidimensional security dilemma in the cyberwarfare paradigm**. Proceedings of the Latin American Studies Association 2015. San Juan: LASA, 2015.

SCHMITT, M. N.:**The Tallinn Manual on the International Law Applicable to Cyber Warfare** (CUP, Cambridge 2013).

SCHNEIER, B. 2008. **The Security Mindset.** Disponível em: <https://www.schneier.com/blog/archives/2008/03/the_security_mi_1.html Acesso em : 15 mar. 2015.

THE GUARDIAN. After 2013 **NSA FILES: DECODED_What the revelations mean for you** Disponível em: <http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1>. Acesso em: 13 mar. 2015.

UN OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS. 12 jul.2013. Mass Surveillance: Pillay urges respect for right of privacy and protection of individuals revealing human rights violations. Disponível em: < http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=%2013534&LangID=E> Acesso em 8 jan.2016.