**UNIVERSIDADE FEDERAL FLUMINENSE**

**INSTITUTO DE ESTUDOS ESTRATÉGICOS**

# A TECNOLOGIA CIBERNÉTICA E A DEFESA NACIONAL NO SÉCULO XXI

**FELIPE DA SILVA FLAVONI**

**Niterói**

**Novembro de2019**

UNIVERSIDADE FEDERAL FLUMINENSE
INSTITUTO DE ESTUDOS ESTRATÉGICOS

# A TECNOLOGIA CIBERNÉTICA E A DEFESA NACIONAL NO SÉCULO XXI

Autor: Felipe da Silva Flavoni

Monografia apresentada ao Instituto de Estudos Estratégicos da Universidade Federal Fluminense – INEST/UFF, como parte dos requisitos necessários à obtenção do título de Especialista em Estudos Estratégicos e Relações Internacionais.

Orientador: Prof. Dr. Marcio Rocha

Niterói
Novembro de 2019

# A TECNOLOGIA CIBERNÉTICA E A DEFESA NACIONAL NO SÉCULO XXI

Nome do Autor: Felipe da Silva Flavoni

Orientador: Prof. Dr. Marcio Rocha

Monografia apresentada ao Instituto de Estudos Estratégicos da Universidade Federal Fluminense (INEST/UFF), como parte dos requisitos necessários à obtenção do título de Especialista em Estudos Estratégicos e Relações Internacionais.

Aprovada por:

_____

Orientador - Prof. Dr. Marcio Rocha

_____

Leitor - Prof. João Moraes

Niterói

Novembro de 2019

## RESUMO

**Resumo:** Considerando-se as consequências e as possibilidades derivadas das novas tecnologias cibernéticas, diversos países tentam achar uma forma de confrontar as novas ameaças provenientes do ciberespaço, capazes de afetarem suas infraestruturas críticas. A complexidade e a dinâmica desse fenômeno têm produzido um ambiente de incertezas. Esses perigos geram apreensão nos estados que buscam proteger seus sistemas de informação e suas redes. O investimento em recursos do poder cibernético possibilita a uma nação ter maior capacidade de se defender nesta nova realidade, mas também gera uma dependência crescente destes meios. Além disso esse paradigma emergente cria uma redistribuição do poder no contexto das relações internacionais, uma vez que aquilo que gera poder está em plena transformação Como objetivo, este estudo pretende analisar em que medida o domínio da tecnologia cibernética contribui para a adequada capacidade de defesa cibernética do estado, visando identificar os recursos tecnológicos que ampliam a competência de um estado de defender o espaço cibernético que lhe é de direito.



**Palavras-Chave:** Defesa Cibernética. Tecnologia Cibernética. Agenda de Segurança.



## ABSTRACT

**Abstract:** Given the consequences and possibilities derived from new cyber technologies, several countries are trying to find a way to confront new threats from cyberspace that could affect their critical infrastructure. The complexity and dynamics of this phenomenon have produced an environment of uncertainty. These dangers create concern in states that seek to protect their information systems and networks. Investing in cyber power resources enables a nation to be better able to defend itself in this new reality, but it also creates a growing reliance on these means. Moreover, this emerging paradigm creates a redistribution of power in the context of international relations, as that which generates power is in full transformation. As an objective, this study aims to analyze to what extent the domain of cyber technology contributes to the adequate capacity of cyber defense. of the state, in order to identify the technological resources that extend the competence of a state to defend its cyber space.



**Keywords:** Cyber Defense. Cyber technology. Security Schedule.

## LISTA DE FIGURAS

## LISTA DE QUADROS

## LISTA DE TABELAS

**SUMÁRIO**

# 1 **INTRODUÇÃO**

A informação sempre foi indispensável para as civilizações desde os seus primórdios, ela é aquilo que fez no passado e faz nos dias de hoje com que as grandes nações surjam e acabem. Ao longo do tempo, com as inovações tecnológicas das últimas décadas, a Cibernética se tornou protagonista no gerenciamento de informação e também como ferramenta de comunicação para as pessoas como um todo, mudando de maneira drástica as interações e os demais campos de conhecimento. É perceptível que dia após dia a sociedade tem se tornado dependente da Cibernética. Essa revolução tecnológica traz consigo um universo de possibilidades, mas também gera exposição e vulnerabilidade para os seus usuários surgindo dessa forma novos tipos de ameaças.

Essas novas ameaças têm a capacidade de atingir indivíduos, governos e economias a partir de qualquer lugar do mundo, mas apenas se os seus sistemas estiverem nas redes. Entretanto como citado anteriormente as facilidades geradas pela Cibernética trazem consigo uma dependência dos seus meios o que torna a opção de manter um sistema fora da rede pouco provável e em alguns casos impraticável. Sendo assim devido ao fato de os sistemas essenciais para o funcionamento de uma sociedade moderna estarem em pleno funcionamento através das redes, os potenciais danos que podem ser gerados através de um ataque cibernético são consideráveis podendo travar temporariamente o funcionamento pleno de uma nação. Se torna imprescindível nesse cenário a capacidade de se contrapor a essas ameaças por parte dos Estados.

Uma das principais preocupações de um estado moderno é a preservação ou a obtenção daquilo que o garante ou o proporciona vantagem perante os seus pares. O que nos tempos atuais pode ser elencado em alguns tipos de conhecimento, dentre eles as tecnologias da base industrial e as infraestruturas críticas de um Governo. Quanto mais evoluída é uma nação do ponto de vista tecnológico maior tende a ser a sua exposição a ataques cibernéticos devido a modernização e integração dos seus sistemas. De forma que através de um ataque cibernético é possível que um agente malicioso consiga atingir diversos sistemas como o de comunicação, o bancário, o elétrico, o de aviação e qualquer outro que tenha o seu controle realizado em sistemas informatizados.

Essa problemática gera aos Estados demandas de segurança e defesa que não existiam até as últimas décadas. No passado no período da História em que surgiu a tecnologia do canhão e a arma de artilharia passou a compor os exércitos, se fez necessário adaptar as estruturas dos castelos e das fortalezas pois as mesmas, que eram construídas até então com uma menor espessura e grande altura, podiam ser facilmente desmanteladas com alguns

disparos de canhão. A solução na época foi um novo tipo de fortaleza que possuía muralhas mais baixas e robustas conjugado com manobras de infantaria. Assim como os governos do passado precisaram se adaptar os governos atuais estão tendo que se adaptar a essa nova realidade no campo da defesa nacional e na pesquisa e desenvolvimento de novas tecnologias.

Este trabalho aborda o tema Defesa Cibernética, o domínio desse tipo de tecnologia se tornou imprescindível para que um estado se mantenha relevante no atual cenário internacional. A questão geral aqui levantada é que em medida o domínio da capacitação de um estado na Cibernética contribui para sua adequada capacidade de Defesa. Para isso o desenvolvimento desse trabalho ocorre com o primeiro capitulo focando em que estado está a tecnologia cibernética na atualidade, posteriormente no segundo capitulo é abordado como que os estados estão lidando com a problemática da defesa cibernética e no terceiro e último capitulo é estudada a relação de o domínio da tecnologia cibernética e a capacidade de defesa de um estado.

O espaço cibernético, que será melhor explanado no próximo capítulo, é extremamente complexo e difuso, questões de ordem de segurança pública e de defesa nacional se aproximam uma vez que o entendimento sobre essa temática acaba se tornando difícil, pois a mesma é relativamente recente e intricada. Seu funcionamento impele as concepções convencionais, exemplo disso são os limites e as fronteiras, que se tornam gradativamente mais permeáveis. A falta de amparo legal, aceito internacionalmente, para regular e arbitrar as contendas pelo domínio do ciberespaço fazem com que esse espaço seja utilizado por criminosos, terroristas e até mesmo estados e empresas com agendas unilaterais, gerando instabilidade na paz e na ordem mundial.

É de conhecimento de todos que a Cibernética esta dentre as principais pautas de grandes atores globais como os Estados Unidos e a China. Exemplo disso foi a nomeação do então vice-almirante Michael Gilday (ex-comandante do Comando de Frota Cibernético dos EUA) como comandante da marinha americana no segundo semestre do atual ano pelo, presidente norte americano Donald Trump. Além dessas duas potências pode se dizer que é paulatino o aumento de investimentos de outros estados na área da capacitação cibernética e este acaba sendo uma via de mão única para o sistema global, pois a medida em que uma nação se desenvolve tecnologicamente, cresce a sua vulnerabilidade aos ataques através do domínio. Cibernético, por sua vez a solução para uma maior vulnerabilidade é o aumento da sua capacidade gerando um ciclo paradoxal.

Além disso, com o constrangimento e o medo do uso dos meios de coerção convencionais no âmbito das relações internacionais por instituições como a ONU ou pelo risco

de uma guerra nuclear. Os ataques cibernéticos se apresentam como uma possibilidade para os estados pensando em um emprego estratégico. Podendo por vezes esses ataques serem utilizados em conjunto aos demais mecanismos coercitivos. Podemos dizer que. o espaço cibernético foi o causador da recente expansão do campo de batalha, tido como o quinto domínio da guerra, juntamente com o mar, a terra, o ar e o espaço sideral.

## 2 **TÉCNOLOGIA CIBERNÉTICA NA ATUALIDADE**

A denominada “Era da Informação” tem como uma de suas características a velocidade com que os dados são transmitidos e disseminados. Em tempos prévios o conhecimento era escasso e aquele que o obtinha se diferenciava perante os seus pares. Com a popularização das fontes de informação e conhecimento ocorreu um processo de horizontalização e assim o diferencial não passou a ser a obtenção da informação pois ela passou a estar acessível em grande quantidade a todos. Desta forma o diferencial passou a ser a capacidade de filtrar, processar e assimilar a informação.

As inovações tecnológicas necessárias para a readequação dos meios de poder têm gerado transformações nas relações internacionais uma vez que o ponto de entrada de cada estado nessa nova era é diferente assim como suas características e capacidades que os levam a ter vantagens ou desvantagens advindas dessas mudanças. Não é a primeira vez que isso ocorre na História. No pós-revolução francesa, Napoleão Bonaparte soube aproveitar as características e a capacidade da França em um momento de mudança. Esses momentos ciclicamente ocorrem originados normalmente por uma conjunção de fatores tecno-científicos, econômicos, sociais e políticos no âmbito global.

Observando o conjunto de estados considerados como potências ao longo do tempo pode se constatar que as fontes do poder vão se alterando e com isso o arranjo da ordem mundial. A velocidade com que uma nação assimila a mudança do paradigma dominante e se adapta ao paradigma emergente conseguindo organizar seus polos científicos e fomentar a sua capacidade industrial e sua força de trabalho conseguem assumir ou manter papel de destaque assim como aconteceu com os países Ibéricos no século XVI e com o Reino Unido durante o século XIX, como dito por Moreira os países mais capacitados a produzir conhecimentos científicos, aplicações tecnológicas e produtos e serviços inovadores tornaram-se ou consolidaram-se como grandes potências mundiais: EUA, Reino Unido, Alemanha, França, Japão e outros. (Moreira, 2012**).**

Um outro ponto importante desta nova Era é muito bem abordado por Nye:

> A característica fundamental dessa Revolução da Informação não é a velocidade das comunicações entre os ricos e os poderosos: durante mais de 130 anos, a comunicação instantânea por telégrafo foi possível entre a Europa e a América do Norte. A mudança crucial é a enorme redução no custo da transmissão da informação. (Nye, 2012).

Este trecho do livro o Futuro do Poder elucida que a verdadeira mudança não é no tempo com que a transmissão dos dados ocorre, mas sim a quem está disponível essa capacidade. Com a produção em escala de diversos meios de comunicação somados a concorrência de diversas empresas de alta tecnologia a barreira do custo de aquisição foi baixando progressivamente ao ponto que nos dias de hoje pode se dizer que não a custo para transmissão de dados em certa proporção. Essa democratização da rápida transmissão de dados gera uma consequência direta que é difusão do fluxo de informações. Segundo Nye:

> Os estados continuarão sendo os atores dominantes no palco mundial, mas encontrarão o palco bem mais povoado e difícil de controlar. Uma parte muito maior da população, tanto dentro quanto entre os países, tem acesso ao poder que vem da informação. Os governos têm sempre se preocupado com o fluxo e o controle das informações, e o período atual não é o primeiro a ser fortemente afetado por mudanças dramáticas na tecnologia da informação. (Nye, 2012, p. 152).

Além disso essa veloz revolução cibernética se espalhou em diversas áreas do conhecimento e do cotidiano se fazendo presente na forma de comprar, fazer transações bancárias ou ensinar. As pessoas hoje em dia não só usufruem da velocidade de dados como também demandam por isso. E essa vontade somada ao ambiente competitivo do sistema internacional capitalista propaga e impõe a modernização e a transformação dos serviços e produtos estatais e privados. Tendo como premissa o Sistema Internacional sendo anárquico, as ferramentas de influência e coerção passam cada vez mais a dependerem da pesquisa e desenvolvimento de tecnologias da área cibernética.

É comum para facilitar o entendimento de algo complexo aglutinarmos uma grande quantidade de invenções de um mesmo período e denominarmos de onda ou revolução tecnológica, mas cada invenção tem capacidade de gerar choques grandes na História da humanidade. Como podemos observar no seguinte quadro:

Quadro 1 – Tecnologias que mais terão impacto na transformação de negócios

| Tecnologias | Global | EUA | China | Japão |
|---|---|---|---|---|
| Nuvem – SaaS / PaaS / IaaS | **11%** | **13%** | **9%** | **13%** |
| Internet das Coisas / M2M | **9%** | 8% | **14%** | 0% |
| Análise de Dados | **9%** | **13%** | 8% | 3% |
| Mobile – plataformas e apps | 7% | 5% | 5% | **7%** |
| Robótica | 6% | 4% | 8% | 3% |
| Segurança cibernética | 6% | **10%** | 5% | **7%** |
| Biotecnologia / medicina digital / cuidados com a saúde IT | 5% | 8% | 3% | 3% |
| Impressão 3D | 5% | 4% | 5% | **7%** |
| Inteligência artificial / Computação Cognitiva | 5% | 8% | 9% | **23%** |
| Plataformas de moeda digital (ex: Bitcoin, sistemas de pagamentos, etc) | 4% | 5% | 5% | 3% |
| Biometria: gestos, face , voz | 4% | 4% | **12%** | 3% |

Fonte: KPMG Technology Innovation Survey, 2015

As vantagens atinentes ao surgimento e aperfeiçoamento da ciência computacional e robótica são indubitáveis, mas é preciso ter uma visão holística de forma que começamos a compreender o verdadeiro impacto dessa revolução digital no nosso mundo.

### 2.1 Cibernética

O termo Cyber tem suas origens na língua grega, equivalendo ao termo controle trazendo para o português. Se valendo deste significado prévio Norbert Wiener, um renomado físico, criou e fez o termo cibernética ser de conhecimento amplo, quando ele publicou o livro intitulado Cibernética em 1948. A palavra "cibernética" por sua vez significa a ciência do controle e da comunicação entre os seres vivos e as máquinas. Com o passar dos anos e com a disseminação desta nova expressão o prefixo "cyber" ou "ciber" converteu-se a uma gama de assuntos relacionados ao domínio da computação e das maquinas.

Trazendo para a realidade brasileira mais especificamente do ponto de vista da Defesa Nacional o termo é definido da seguinte forma na Doutrina Militar de Defesa Cibernética:

> Termo que se refere à comunicação e controle, atualmente relacionado ao uso de computadores, sistemas computacionais, redes de computadores e de comunicações e sua interação. No campo da Defesa Nacional, inclui os recursos de tecnologia da informação e comunicações de cunho estratégico, tais como aqueles que compõem o Sistema Militar de Comando e Controle (SISMC2), os sistemas de armas e vigilância, e os sistemas administrativos que possam afetar as atividades operacionais. (Ministério da Defesa, 2014, p. 18).

A percepção global da ameaça derivada da ciência cibernética aconteceu naturalmente décadas após o seu surgimento. Esse período entre um fato e o outro foi o tempo necessário para o crescimento da rede digital. Isso é decorrente das circunstâncias desse ambiente que diferente dos demais ambientes pré-existentes onde ocorrem as atividades bélicas ele não foi descoberto ou explorado, mas sim inventado e criado pelo homem como será mais detalhado ao longo deste trabalho. As apreensões a respeito dos riscos inerentes ao domínio virtual foram crescendo à medida que a rede crescia e o controle dos entes estatais sobre ela diminuía. Conforme Nye (2012):

> Em 1993. havia cerca de 50 sites no mundo; em 2000, esse número já superava 5 milhões. Uma década mais tarde, só a China linha mais de 400 milhões de usuários da internet e a rede social Facebook tinha cerca de meio trilhão de usuários. As larguras de banda das comunicações estão expandindo-se rapidamente e os custos das comunicações continuam a cair até mais vertiginosamente do que os do alcance da computação. Em 1980, as chamadas telefónicas transmitidas por fio de cobre só conseguiam carregar uma página de informação por segundo; atualmente, um cabo fino de fibra ótica consegue transmitir 90 mil volumes em um segundo. Em 1980, 1 gigabyte de armazenagem cabia no bolso de sua camisa. A quantidade de informação digital aumenta dez vezes a cada cinco anos. (Nye, 2012, p. 153).

No período imediato pós-Guerra Fria a infraestrutura das redes e a indústria de alta tecnologia pode se desenvolver mais vocacionada para o uso civil e esse descompasso entre o começo da ampla utilização e o início da percepção de risco por todos gerou solo fértil para o crescimento de agentes maliciosos. A transmissão de dados instantâneos, a rapidez nunca antes vista nas comunicações, as transações bancárias podendo ser realizadas a partir de qualquer lugar do globo terrestre, a administração de dados por meio digital por estados, empresas e pessoas floresceram nessa fase. Entretanto esses recursos não surgiram com base em princípios de segurança, proteção, transparência e privacidade. Atividades criminosas como como roubo de dados, acesso descabido a dados confidenciais, falsificações eletrônicas, sabotagem e espionagem começaram a afetar de maneira considerável indivíduos, empresas e os seus respectivos governos. Contramedidas a esses novos perigos passaram a ser uma preocupação constante de toda a sociedade como é descrito por Canogia (2009).

> Os chamados ataques cibernéticos, atualmente, apresentam escala mundial crescente e destacam-se como o grande desafio do século. Com isso, assegurar a integridade, a confidencialidade e a autenticidade da informação é essencial para a formulação de estratégias e para o processo decisório, especialmente no âmbito do amplo espectro de competências da administração pública federal. (Canogia, 2009).

Essas ameaças cibernéticas estão vinculadas a uma gama de conteúdos que abrangem monitoramento cibernético, sensoriamento remoto, atividades na área das telecomunicações, em redes de computadores e o gerenciamento de dados. Com tudo é na *world wide web* e em outras redes a ela conectada que elas incidem de maneira mais significativa. O fator propiciador dos crimes cibernéticos é a ideia de que o Espaço Cibernético é um ambiente a margem da sociedade, um universo em que a lei e a ordem estão ausentes. Esse pensamento ocorre porque os usuários não têm a percepção que o ambiente é suficientemente vigiado e que a impunidade é a regra e a punição a exceção. O binômio norma-sanção se faz essencial para a manutenção do pacto social no mundo real e para o ambiente virtual não é diferente.

Somado a essa sensação de impenitência ainda temos que considerar o fato de que no século em que vivemos a maior parcela dos meios de controle de estruturas fundamentais da sociedade estão conectados através de sistemas cibernéticos. O entendimento da atual dependência das infraestruturas básicas ao ambiente virtual é fundamental para percebermos a importância desse novo domínio.

### 2.2 Espaço Cibernético

O Mar, o Ar e a Terra são os domínios geográficos convencionais e eles são de conhecimento do homem desde o início dos tempos, porém a sua ocupação e utilização ocorreram ao longo do desenrolar da história da humanidade. Os continentes foram sendo ocupados pouco a pouco no decorrer dos primeiros séculos ao passo em que a exploração dos outros domínios somente se deu nos últimos mil anos. O proveito de cada um dos domínios geográficos convencionais visando a continuidade da raça humana, exigiu dos povos a ordenação e sua tutela que só pode ser realizado através de um pensamento estratégico.

Por termos nos tornados dependentes e executarmos diversas tarefas por meio dele nós não nos atentamos do quão recente é o espaço cibernético. Pode se dizer que seus primórdios datam do final da década de 70 relacionados a uma pequena rede de computadores e a elaboração do protocolo TCP/IP, que são códigos para a transferência de dados. Essa rede foi desenvolvida pelo Departamento de Defesa Americano e ficou sendo conhecida como "Arpanet" Esse novo sistema foi concebido para montar uma *internet* basilar que tinha a capacidade de transmitir agrupamentos de informações digitais. Alguns anos depois em 1972 o projeto até então exclusivamente começou a crescer e expandir a nível internacional até chegar próximo do que conhecemos atualmente como a *Internet*. A World Wide Web propriamente

dita surgiu posteriormente no final da década seguinte e ferramentas de buscas que são tão essenciais e rotineiras como o "Google" nasceram no final da década de 90.

Na conformação atual, Richard Clarke (2010) descreve o ciberespaço como a mescla de tecnologias relacionadas à rede computacional global, incluindo também tudo aquilo que está sob o controle desses equipamentos. Tendo já explanado alguns conceitos fica mais claro que apesar de ser normal lermos em alguns textos a expressão "espaço cibernético" ser empregada como uma expressão de sentido semelhante a *Internet.* Essa equivalência não é correta, pois o espaço cibernético engloba aquilo que representa o termo *Internet* além de tudo aquilo que está conectado. Sendo para Richard Clarke (2010), a ideia de espaço cibernético mais ampla que a da *Internet*.

Essa diferença entre esses dois conceitos se torna ainda mais relevante quando pensamos sobre a *Internet* das Coisas mais conhecida como IOTs (*Intertet of Things*). De forma simplificada podemos dizer que essa inovação, é basicamente uma continuidade da *Internet* dos dias de hoje, que habilita objetos do cotidiano, com capacidade computacional e informacional, a se conectarem à rede. A conectividade com a rede global computacional possibilita, inicialmente, que os objetos sejam controlados remotamente e também permite que os os mesmos sejam conectados como provedores de serviços. Estas inovadoras capacidades, de objetos ordinários, criam uma gama de possibilidades no ramo das indústrias assim como no meio acadêmico.

De forma mais abrangente, conseguimos descrever o ciberespaço como uma mescla de infraestrutura e ferramentas tangíveis, denominados hardware, combinados aos aplicativos, sistemas operacionais e plataformas que somos capazes de conectarmos pelos através dos celulares, *notebooks*, entre outros *gadgets*, os chamados softwares. Daniel Ventre (2011) assim como outros autores, ressaltam também a relevância dos usuários que utilizam desse conjugado intitulado por eles como o *peopleware*. Dentre as diversas descrições uma das mais consideradas para o ciberespaço é compreendê-lo como um sistema mundial, estabelecido, conectado e conservado por aparelhos interligados. Uma característica interessante desse espaço é explanada por Nye (2012):

> Podemos conceituar o espaço cibernético em termos de muitas camadas de atividades, mas uma primeira aproximação simples o retrata como um singular regime híbrido de propriedades físicas e virtuais. A camada de infraestrutura física segue as leis econômicas dos recursos rivais (ou exclusivos) e os crescentes custos marginais e as leis políticas de jurisdição e controle soberanos. A camada virtual, ou informacional, tem características da rede econômica de aumento de receitas em função da escala e práticas políticas que dificultam a realização de controle jurisdicional. (Nye, 2012, p. 162).

Esse é um dos atributos desse domínio que chama a atenção para o seu emprego nas relações entre os estados, uma vez que ações realizadas através da camada virtual custam muito pouco e podem ser realizadas de maneira anônima podendo afetar de maneira drástica as infraestruturas físicas de qualquer alvo desejado causando um grande prejuízo. Isso tudo podendo ser feito a baixo custo político e econômico. Conforme detalhado na tabela 1.

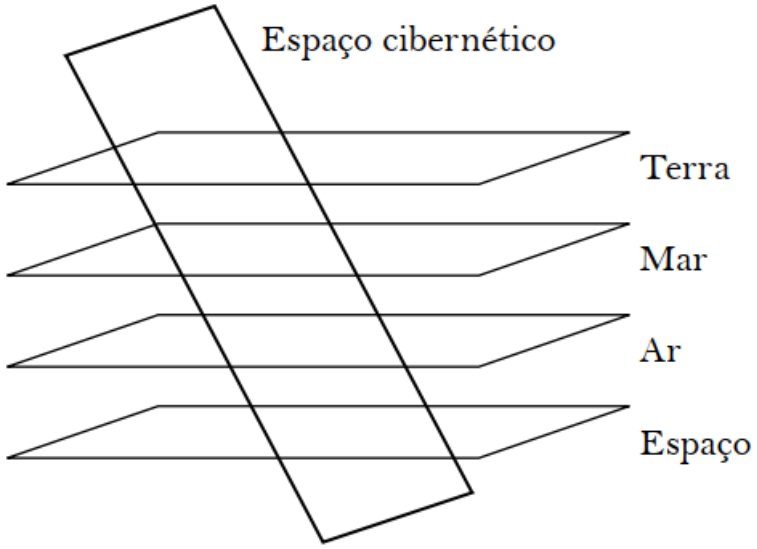
Tabela 1 – Dimensões físicas e virtuais do poder cibernético

| **Alvos do poder cibernético** | | |
|---|---|---|
| | **Intraespaço cibernético** | **Extra espaço cibernético** |
| **Instrumentos de informação** | Duro: ataques de negação de serviço<br>Brando: determinação de normas e padrões | Duro: ataque em sistemas Scada<br>Brando: campanha de diplomacia pública para influenciar a opinião pública |
| **Instrumentos físicos** | Duro: controle das companhias por parte do governo<br>Brando: software para ajudar ativistas dos direitos humanos | Duro: roteadores de bomba ou corte de cabos<br>Brando: protestos para denunciar os provedores cibernéticos |

Fonte: Nye, 2012

Além disso por cruzar através de todos os outros domínios, o espaço cibernético pode ser considerado como um excelente instrumento de controle pelos governos, visto que tem a capacidade exercer sua influência nos demais espaços. Em oposição aos domínios geográficos convencionais, como por exemplo o terrestre, no qual um estado necessita ter controle total sob um determinado território para poder extrair e usufruir dos seus recursos naturais, o ciberespaço tem como foco a aquisição e o gerenciamento da informação, que aparece no seu interior e através de conexões. Sendo assim o pensamento político e estratégico aplicado nesse ambiente não visa conquistar ou incidir em um espaço cibernético parecido com os outros, mas simplesmente comtemplar as suas fronteiras e divisas em relação as outras nações e seus pontos de conexão marítimo, terrestre, aéreo e espacial. Pode se dizer com tudo, que essa é uma via de mão dupla, pois as conexões cibernéticas também são posições vulneráveis para os Estados, que como consequência direta disso devem ter controle e proteger esses pontos.

Figura 1 – Relação do Espaço Cibernético com os demais espaços geográficos.




Fonte: Ventre (2012, p. 35).

O domínio de certa parcela de um espaço é algo fundamental para a conservação e continuidade na ordem mundial vigente, podendo ser um dos atributos de maior relevância do atual modelo e a característica intrínseca que diferencia os antigos estados dos estados modernos (Giddens, 2001). Outro ponto, a medida em que o espaço se apresenta como algo que possa ser utilizado pela raça humana como origem de recursos que podem ser transformadas por meio de novas tecnologias, o controle desse ambiente passa a ser vital para a manutenção da soberania e a existência dos estados como nós os conhecemos atualmente. Um contraponto a esta forma de pensar que pode se considerar que ameniza a ideia de dissolução ou transformação dos estados como eles são nos é apresentada por Nye (2010):

> "Mudanças nas informações sempre tiveram um impacto importante sobre o poder, mas o domínio cibernético é tanto um novo como um volátil ambiente virtual. As características do ciberespaço reduzem alguns dos diferenciais de poder entre os atores e, portanto, são um bom exemplo da difusão do poder que caracteriza a política global neste século. [...] Mas o ciberespaço também ilustra o ponto de que a difusão do poder não significa igualdade de poder ou a substituição de governos como os atores mais poderosos da política mundial. Enquanto o ciberespaço pode criar algumas mudanças de poder entre os estados, abrindo oportunidades limitadas para pequenos estados através da guerra assimétrica, é pouco provável que seja uma virada de jogo nas transições de poder. Por outro lado, o domínio cibernético é susceptível de aumentar a difusão do poder de atores não estatais e ilustra a importância das redes como uma dimensão chave de poder no século 21"
> (Nye, 2010, p. 19).

Ainda existem muitas incertezas no que diz respeito a proporção em que se darão as mudanças no sistema internacional. Entretendo o que de fato podemos afirmar é que o conjunto de propriedades do espaço cibernético geram no âmbito das relações internacionais

uma difusão do poder, e independente da manutenção de cada estado moderno nas suas atuais formas, o mais relevante é de que forma esse estado vai se adaptar ou resistir a esse novo universo. A própria política já se transforma e tem se demonstrando cada vez mais volúvel e menos refreada dentro das respectivas fronteiras de cada nação e a agenda da internacional se expandiu e agora abarca um grupo cada vez maior de atores. Sendo que essas transformações não dizem somente respeito ao número de atores que participam, número este que aumenta exponencialmente, mas também dizem respeito a mudanças qualitativas. Visto que os atores não estatais estão sofrendo cada vez menos influência direta das grandes estruturas formalmente organizadas.

### 2.3 Recursos de Poder Cibernético

Tendo um entendimento básico do que é a cibernética e o seu espaço podemos abordar sobre o poder derivado deste campo do conhecimento e os seus recursos que o proporcionam. A Doutrina Militar de Defesa Cibernética define o poder cibernético como "capacidade de utilizar o Espaço Cibernético para criar vantagens e eventos de influência neste e nos outros domínios operacionais e em instrumentos de poder." (Ministério da Defesa, 2014, p. 19). Uma outra definição que detalha melhor esse poder é dado por Nye (2012):

> O poder cibernético pode ser definido como um conjunto de recursos que se relacionam à criação, ao controle e à comunicação de informações eletrônicas e baseadas em computador infraestrutura, redes, *software*, habilidades humanas. Isso inclui não somente a internet dos computadores ligados à rede, mas também intranets, tecnologias de telefonia celular e comunicações via satélite. Definido do ponto de vista comportamental, o poder cibernético é a capacidade para obter resultados preferidos mediante o uso dos recursos de informação eletronicamente conectados do domínio cibernético. (Nye, 2012, p. 162).

Tendo em vista o que foi supracitado compreendemos a necessidade de analisarmos de forma um pouco mais detalhada os tipos de recursos decorrentes do poder cibernético. Esses recursos são interconectados, porém o seu arranjo se dá de maneira indistinta entre os variados estados-nações do ordenamento mundial.

O conhecimento técnico ligado às inovações digitais é um recurso que pode ser descrito como o saber com o qual um grupo ou um indivíduo fica habilitado à acessar e utilizar o ciberespaço para disseminar informações e cultura ou influenciar a sociedade global ou local, como exemplo podemos citar o *YouTube,* que tem um fluxo enorme de informação que é direcionado de acordo com o que é intencionado pelos seus desenvolvedores para cada um dos usuários. Outra forma de enxergar esse recurso é a capacitação técnica necessária para o

desenvolvimento de *gadgets* que tem um valor intangível gerando um certo grau de influência à nível global como por exemplo o *Iphone* da empresa *Apple*. Em suma esse conhecimento

Outro recurso é o processamento de dados digitais a fim de se conseguir informações importantes como por exemplo tendências de mercado, intensidade dos ventos ou de notícias mais impactantes. Desta forma, existe um grande interesse em passar os dados do meio físico para o meio digital, transformando assim bibliotecas físicas que podem ser utilizadas por um público limitado para grandes acervos virtuais acessados a qualquer momento do dia por pessoas do mundo todo. A acumulação de dados é um aspecto de grande importância deste recurso, o chamado *Big Data,* que consiste no armazenamento e concentração de informações, pode ser utilizado com outras tecnologias e assim refinar informações brutas em dados relevantes para determinado nicho. Um exemplo simples dessa utilização é a informação que a empresa *Spotify* possui referente ao gosto musical dos seus clientes e com alguns filtros pode seccionar por faixa de idade e sexo e assim poder vender o dado de qual o melhor trecho de alguma musica especifica seria o ideal para ser utilizado em um comercial de roupas para jovens mulheres. O mesmo pode ser feito para a realização de operações psicológicas entre nações beligerantes.

A infraestrutura da rede de informações, é mais um dos recursos do poder cibernético, a sua relevância reside no fato de que os dados trafegam através dos cabos de fibra ótica, satélites, antenas e torres de telecomunicações e o constante melhoramento dessas estruturas é essencial para atender à crescente demanda tanto em quantidade, quanto em velocidade de transmissão de dados. Além da questão da transmissão dos dados, também há a problemática relativa ao formato em que os dados são transmitidos e as padronizações designadas para esse fim, envolvendo a escolha das faixas de frequência do espectro magnético e local de posicionamento do parque de antenas e de passagem do cabeamento das redes. Essas de decisões são baseadas nas especificidades técnicas de cada meio bem como o norteamento estratégico de cada estado, uma vez que nem sempre o que melhor atende os requisitos técnicos vai estar alinhado com uma menor exposição da estrutura informacional para ataques na dimensão tangível. É importante salientar também, o aumento do envolvimento de atores não estatais que estavam focados apenas na produção de software e conteúdo e passaram a investir na infraestrutura de rede, com foco principalmente no cabeamento submarino. Exemplo desde fato são empresas como o Google, que em um período curto de tempo investiu US$ 30 bilhões em cabeamento e continua ampliando.

Um outro recurso a ser considerado é a capacidade computacional esse recurso está diretamente ligado com a as capacidades técnicas de velocidade de processamento,

armazenamento de dados, uma vez que essas capacidades são pré-requisitos para se ter um amplo espectro de utilização e emprego no meio cibernético. Investimentos assíduos são feitos no avanço e criação de novos gadgets e computadores, e também em estruturas de processamento mais modernas, repercutindo assim também em outros pontos da sociedade atual. Seu acúmulo possibilita ao possuidor desse recurso grandes vantagens competitivas em variados segmentos, exemplo evidente da capacidade deste recurso é a própria mineração de criptomoedas, computadores superpotentes gerando riqueza imediata.

Após analisarmos o conhecimento técnico ligado às inovações digitais, o processamento de dados digitais, a infraestrutura da rede de informações e a capacidade computacional examinaremos por fim um último recurso de poder, o dos algoritmos de programação. Os algoritmos são responsáveis por dar serventia aos dados coletados e inseridos, possibilitar a automação de ações de rotina, auxiliar na tomada de decisões, permitir a interação entre usuário e software, e também como viabiliza a inteligência artificial. Existe uma ampla variedade de algoritmos. Desde algoritmos desenhados para efetuar uma tarefa pontual e rotineira em uma fábrica, operando maquinas com base em variáveis previamente inseridas, até algoritmos de *machine learning* que de forma simplificada é uma forma de fazer com que computadores efetuem ações sem necessitarem ser programados para tal. Esses algoritimos mais avançados são utilizados normalmente para criarem sugestões a um determinado usuário. São usados em diversos sites de venda virtual, redes sociais, jogos e plataformas de *streaming* de vídeos e de música. Nessa modalidade o algoritmo utiliza os dados dos seus seguimentos e os dados de histórico de navegação na internet para realizar sugestões ao usuário. As preferências do usuário durante a navegação e o compartilhamento de dados são usadas para fazer a sugestão de serviços ou programas que sejam semelhantes.

## 3 **A DEFESA CIBERNÉTICA E OS ESTADOS**

Segundo Mandarino, o domínio digital não tem limites nem fronteiras. Dessa forma uma rede compromissada pode afetar outras, sejam elas públicas ou privadas. Por este motivo, a cooperação e a permanente contato entre diversos atores são primordiais para manter um alto grau de proteção cibernética para o sistema por inteiro (Mandarino Junior, 2010).

De maneira isolada nenhum segmento de um estado irá conseguir ter êxito na segurança e defesa das suas próprias redes. São fundamentais atuações paralelas e simultâneas entre todos os setores. da sociedade. Nos dias de hoje se tornou um pré-requisito para um bom funcionamento da indústria e dos polos científicos a segurança das suas redes de forma a garantirem patentes evitarem fraudes e roubos de dados gerando assim uma demanda latente por sistemas seguros. Cabe ao governo orquestrar os recursos do estado a fim de precaver, reconhecer fraquezas e prontificar-se para a ocorrências de ameaças devendo alçar essas ideias ao nível de questões de Estado e não apenas de prioridades de um governo.

Em uma visão abrangente, a salvaguarda no ciberespaço está diretamente conectada aos meios de ataque que existem. Em termos práticos o ataque e a defesa cibernética dependem dos mesmos recursos. O êxito no ataque reside apenas na descoberta dos pontos fracos na defesa do sistema a ser atacado. Desta maneira, para se elaborar uma tática de proteção apropriada, é necessário estar inteirado com as ferramentas e técnicas de ataques mais modernas.

O contato e a colaboração, com os demais participantes do sistema, são obviamente o caminho a ser trilhado, entretanto não é o bastante, para ser capaz de progredir no desenvolvimento de tecnologias de segurança e defesa cibernética de ponta. Apenas através da permuta de conhecimentos e partilha de bons costumes é viável aumentar as capacidades de detecção de lapsos ou vulnerabilidades que possam ser aproveitadas por agentes maliciosos. Nessa visão, tanto governo, quanto a sociedade, a indústria e a academia tem um papel relevante a ser cumprido. Além disso podemos salientar que a defesa e a segurança dos sistemas cibernéticos dependem muito mais da qualificação de pessoal de investimentos em hardware. Dessa forma, o ponto focal do esforço da política de estado de segurança e defesa cibernética precisa ser na capacitação de pessoas e na formação de técnicos. Mas isso só pode ocorrer na medida em que se passa a considerar que a temática de proteção cibernética, está relacionada com a soberania de uma nação, de forma a ser do interesse do alto escalão político e estratégicos de um governo. Apenas com essa conscientização que um estado consegue criar as condições necessárias, bem como a provisão de recursos para orquestras as atuações essenciais para à segurança e defesa cibernética dele próprio

### 3.1 Conceitos de Defesa Cibernética

Podemos dizer que a problemática gerada por esse novo universo já chama a algum tempo o olhar das autoridades, o general do Exército Brasileiro, José Carlos dos Santos, quando ocupava a função de Comandante do Centro de Defesa Cibernética no Brasil afirmou durante uma entrevista à revista época o seguinte:

> "É uma nova governança. Eu diria que diversos países estão na mesma situação. Os Estados Unidos criaram seu comando cibernético em 2009. A Alemanha ativou seu centro de defesa cibernética neste ano, a Inglaterra no ano passado. O Brasil criou o Centro de Defesa Cibernética em agosto do ano passado. Essa era digital é um contexto novo. [...] Podemos, sim, contratar civis. Está dentro de nossas previsões a contratação de especialistas em regime de prestação de serviços. Basicamente estamos cuidando da formação do nosso pessoal. A partir de 2012, a matéria tecnologia para informação e comunicação se tornará obrigatória para todos os nossos futuros oficiais. Nas escolas de formação dos nossos sargentos, o assunto também será introduzido. É uma possibilidade contratar [hackers]. A imprensa diz que os Estados Unidos já fazem isso. Eles teriam até um grupo de hackers que trabalharia em prol do governo americano. Eles não se identificam como tal, mas trabalham. [No Brasil] São registrados milhares de incidentes de rede por dia. Logicamente um porcentual desses incidentes é de tentativas de intrusão em serviços internos do Exército. Recentemente, tivemos no Recife uma intrusão num serviço social, de distribuição de água. Um grupo, o FatalErrorCrew, conseguiu acessar um banco de dados dessa operação. Foi dado crítico? Bom, crítico, não. Mas mostrou uma vulnerabilidade. Eram dados de militares vinculados àquela operação" (SANTOS, 2011).

Dessa forma, percebe-se que no âmbito militar há uma clara preocupação com a defesa e segurança cibernética dos sistemas virtuais e de infraestrutura do país. A questão principal gira em torno de como se Defender de agressores anônimos e com armas intangíveis. Na entrevista podemos perceber que existe uma ideia de mobilização com foco em recrutamento de pessoal especializado. Mas é difícil garantir que alguém com altos talentos na área cibernética se mantenha junto ao interesse de Defesa do estado. Contudo antes de se aprofundar um pouco mais no assunto se faz necessário a colocação de algumas definições:

a) Defesa Cibernética

Segundo o que consta na Doutrina Militar de Defesa Cibernética o conceito de Defesa Cibernética pode ser assim descrito:

> "conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente" (MINISTÉRIO DA DEFESA, 2014).

b) Segurança Cibernética

Uma outra definição necessária por questão de diferenciação é a de segurança cibernética uma vez que os temas muitas vezes se confundem. Na visão de Mandarino (2009), a expressão Segurança Cibernética é compreendida como requisito para a proteção e salvaguarda das informações de uma nação:

> "A Segurança Cibernética é entendida 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" (MANDARINO, 2009).

O mesmo autor considera que os conceitos de Segurança Cibernética e de Defesa Cibernética estão sendo elaborados por diferentes segmentos do estado e que a zona de ação da Segurança Cibernética compreende óticas e atuações de prevenção e repressão. E para a Defesa Cibernética abrange medidas de nível operacional de combates ofensivos.

c) Infraestruturas Críticas

Os alvos mais preocupantes para um Estado para um ataque cibernético são as suas infraestruturas críticas as quais o autor De Carvalho (2011) conceitua como "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" (DE CARVALHO, 2011)

### 3.2 Atores do Poder Cibernético

Dentro de um estado o seu governo exerce sua autoridade em todo o país, ostentando dessa maneira uma soberania interna. De um outro ângulo no nível da relação entre os estados as interações ocorrem de uma maneira complexa em um sistema anárquico. A anarquia é inerente nas relações internacionais, pois estas nações não estão submetidas a um governo global. Dessa forma os estados encontram-se em um meio que pode se vivenciar hostilidades ou colaboração.

Coexistindo com os estados encontram-se atores não estatais que possuem a sua parcela de importância no sistema internacional. Esses atores, como por exemplo as empresas transnacionais, tem um papel fundamental em diversos ocorridos ao longo da História. Entretanto, é necessário considerar que nos instantes em que se faz necessário o uso da força, os estados são os únicos capazes de a emprega-la. Eles, que monopolizam o uso da força, são

os protagonistas no cenário das relações internacionais e são as fundamentais entidades que salvaguardam os princípios essenciais da sociedade como a justiça, a liberdade, o bem-estar, a segurança, e a ordem. E também. é orientado por um interesse nacional que está envolvido com o esforço contínuo de agrupar o poder militar e o econômico

A respeito dos usuários que dominam o ciberespaço, podemos caracteriza-los como agentes, que possuem ou não apoio estatal, e dispõem de habilidades técnicas e são envolvidos em diversas atividades, como a censura, a propaganda, a sabotagem, a vigilância e a espionagem. No arsenal empregado por eles empregados em ataques cibernéticos, estão os *softwares scanners*, *buffers*, e *trojan horses* qualquer indivíduo, grupo ou entidade, tem a capacidade de causar estragos no ciberespaço, desde um garoto de onze anos de idade fissurado em programação até um sofisticado batalhão cibernético de alguma potência mundial. Esse espectro inclui grupos terroristas que usam a *internet* para angariar seus novatos e planejar atentados. Organizações de ativistas ambientais fazem estragos em sites de empresas e governos. A tabela 2 a seguir detalha as diferentes características de cada um desses principais atores do poder cibernético.

Tabela 2 – Recursos de poder relativos dos atores no domínio cibernético

| |
|---|
| **Principais governos** |
| 1. Desenvolvimento e apoio de infraestrutura, educação e propriedade intelectual. |
| 2. Coerção legal e física de indivíduos e intermediários localizados dentro das fronteiras. |
| 3. Tamanho do mercado e controle do acesso - por exemplo, União Europeia, China, Estados Unidos. |
| 4. Recursos para ataque e defesa cibernéticos: burocracia, orçamentos, agências de inteligência. |
| 5. Provisão de bens públicos, como as regulações necessárias para o comércio |
| 6. Reputação para a legitimidade, benignidade e competência que produzem poder brando |
| **Principais vulnerabilidades**: alta dependência de sistemas complexos facilmente danificáveis, instabilidade política, possível perda de reputação. |
| **Organizações e redes altamente estruturadas** |
| 1. Grandes orçamentos e recursos humanos, economias de escala. |
| 2. Flexibilidade transnacional. |
| 3. Controle de desenvolvimento de código e produto, geração de aplicativos |

4. Marcas e reputação.

**Principais vulnerabilidades**: perseguição legal, roubo de propriedade intelectual, danos a sistemas, possível perda de reputação (denúncias).

**Indivíduos e redes fracamente estruturadas**

1. Baixo custo de investimento para a entrada.
2. Virtual anonimato e facilidade de saída.
3. Vulnerabilidade assimétrica em comparação aos governos e às grandes organizações.

**Principais vulnerabilidades**: coerção legal e ilegal por parte dos governos e das organizações, caso sejam apanhados.

Fonte: Nye, 2012

No que diz respeito aos governos Joseph Nye (2012), vislumbra que como esses governos permanecem soberanos em relação aos seus respectivos territórios e também como a infraestrutura das redes até então se mantém associada com o território. O espaço geográfico ainda se mantém como um relevante recurso do espaço cibernético. Os governos ainda têm a competência de direcionar recursos financeiros à infraestrutura, ao ensino na área de informática e à salvaguarda da propriedade intelectual que instigue o acréscimo de capacidade técnica computacional dentro de suas fronteiras. Vale salientar ainda que através do controle do espaço tangível e das normas, os governos também podem realizar medidas coercitivas e controles legais. Além de possuírem a maior capacidade dentre os atores do espaço cibernético de realizarem ataques cibernéticos, que em geral são executados com o intuito de neutralizar sistemas, espionar ou roubar informações e técnologia.

O conjunto, dos atores não estatais com redes altamente estruturadas, possui a mesma competência de executar ataques cibernéticos que neutralizam sistemas, mas com menor capacidade e por motivos diferentes como ativismo, terrorismo ou mesmo crimes financeiros. Golpes cirúrgicos contra alvos de excelente proporção custo-benefício, como sistemas bancários e de dados sociais. É fato que o domínio cibernético é difuso e relativamente mais igualitário, contudo isso não faz com que um grupo de *hackers* esteja em nível de igualdade com um governo desenvolvido. Conforme Joseph Nye (2012), dizer que estamos vivendo um fenômeno de difusão de poder não quer dizer que vivemos uma equalização de poder. Estudiosos da área afirmam que, dentro de uma década, com alguns adventos e melhoramentos nas tecnológicas de identificação e criptografia será possível reduzir em muito essas ameaças assimétricas frente aos estados.

O subgrupo dos atores não estatais criminosos com redes altamente estruturadas possui algumas especificidades em relação aos demais. Uma delas é que por existirem a margem da lei a mesma não pode restringir a capacidade desse tipo de organização. Algumas delas costumam realizar ataques pequenos e de pequena duração, mas que possibilitam altos rendimentos em um curto espaço de tempo antes mesmo que as entidades reguladoras consigam agir. Dentro desse subgrupo ainda temos os terroristas que utilizam o meio digital como um instrumento de recrutamento e descentralização das suas redes. Angariando recursos humanos e financeiros no mundo todo para as suas causas, dando treinamento, e realizando atentados cruéis e inesperados. O maior exemplo deste tipo de entidade é sem dúvidas o Estado Islâmico que durante muito tempo conseguiu realizar todas essas atividades de maneira ampla.

O grupo dos Indivíduos e redes fracamente estruturadas, é um exemplo de como as inovações computacionais redesenham a distribuição de importância entre os diversos atores. A grande vantagem deste grupo é que não existem barreiras de entrada para eles e assim como não existem barreiras para sair dessa maneira esses usuários conseguem agir quase que livremente no espaço cibernético decorrente principalmente do baixo custo e ao anonimato. Alguns agem sob a tutela do estado, mas em sua maioria agem por conta própria. Em relação as maneiras em que a interdependência assimétrica ajuda a produzir poder vale a pena notar que os atores individuais no domínio cibernético e beneficiam da vulnerabilidade assimétrica comparada a governos e grandes organizações. O ponto fraco desse grupo de atores é a coerção legal praticada pelos governos e dos demais atores. Entretanto o sentimento que reina nas redes é o da impunidade visto que falta um amparo legal homogêneo e a rede é tão pulverizada que poucos são aqueles que realmente são punidos em relação ao todo. Contudo a capacidade prática desses indivíduos de ameaçar estados e empresas é bem limitada. O que não impede que os seus ataques causem danos a essas entidades como vazamento de informações sigilosas e prejuízo a suas reputações.

### 3.3 Casos relacionados a Defesa Cibernética

O acontecimento de situações de beligerâncias no espaço cibernéticos está conectado de maneira explícita ao nascimento e ao progresso da *Internet*, sendo que o seu desenrolar começa na prática a partir do pós-Guerra Fria. Inicialmente, o ar de tensão vivido na Guerra Fria colaborou para o desenvolvimento de inovações na área de tecnologias de comunicação e informação para fins militares. Posteriormente, por causa da disseminação

da *Internet* no âmbito civil com cobertura mundial, o ciberespaço foi envolto por atividades maliciosas originadas de diversos atores, sendo esses centralizados ou não e com diferentes modelos de combate de acordo com variadas motivações

É claro que a problemática derivada do espaço cibernético se apresenta como um dos maires desafios deste século, os ataques cibernéticos apareceram e aumentaram em proporção global. A proteção do espaço cibernético se destacada como meta a ser alcançada pelos Governos de todo o mundo, principalmente em relação à salvaguarda do bom funcionamento do estado. Essas potenciais ameaças têm forçado os estados a ficarem em condições de preservar seus sistemas de redes de ofensivas no campo cibernéticos. Diversas ocorrências oriundas do ciberespaço estão abalando a segurança dos países. As ameaças cibernéticas têm evoluído e várias delas, que eram consideradas como de baixa probabilidade de ocorrerem, estão começando a acontecer com uma frequência cada vez maior. Essa situação ocorre devido a criação de instrumentos e técnicas cada vez mais avançadas.

Para exemplificar alguns desses fatos abordaremos alguns acontecimentos envolvendo o espaço cibernético:

### 3.3.1 Caso Estônia

No final da década de 2000, um fato relevante aconteceu no âmbito das guerras cibernéticas. A Estónia, sofreu ataques cibernéticos em larga escala, abatendo serviços eletrônicos de relevância para sua administração. Os ataques aconteceram momentos depois da resolução governamental de mover um monumento de guerra soviético da cidade de Tallin para um distante cemitério militar.

A atrição entre os estonianos nativos e os russos étnicos moradoras da Estônia datava desde o momento da independência da Estônia no fim da Guerra Fria. Muitos estonianos solicitaram a retirada de todos os marcos de dominação soviética. Em fevereiro de 2007, o legislativo deu prosseguimento com à Lei das Estruturas Proibidas assinalando que qualquer coisa que lembrasse a ocupação soviética deveria ser destruída, incluso ai o monumento supracitado (Clarke; Knake, 2015).

Foi nesse ambiente tenso que em abril de 2007, a Estónia, um estado extremamente informatizado, recebeu ataques que foram chamados de *Distributed Denial of Service* Essa maneira de realizar ataques necessita do emprego muitos computadores, mesmo que sejam empregados de maneira remota com o desconhecimento do dono. Esses ataques de negação de serviços deixam sites indisponíveis através do engarrafamento do fluxo de dados gerado

por muitos pedidos de acesso falsos. Com a excesso de pedidos de acesso, os sistemas travam e ficam fora do ar. (Carreiro, 2012). Por motivo do ataque e também ao fato de a maioria dos serviços e sistemas da Estônia serem informatizados, serviços eletrônicos do governo, e de empresas de telecomunicações e do sistema bancário ficaram parados por vários dias, o que fatalmente atingiu o dia-a-dia da população.

A Estónia acusou a Rússia pela organização dos ataques, que se desvencilhou de maneira diplomática do seu envolvimento no evento. Entretanto, a Estônia definiu a situação como uma violação a seu território e solicitou o apoio militar da OTAN para resolver o problema. A OTAN prontificou um grupo de técnicos de tecnologia da informação afim de analisar o ocorrido e coopera na reintegração dos serviços. (Carreiro, 2012).

No mês de setembro do mesmo ano, um representante do governo da Estônia afirmou que não existiam evidências do envolvimento do governo russo no ocorrido, sendo o ataque realizado através de computadores do mundo todo. Nem os especialistas da OTAN nem os da Comissão Europeia encontraram qualquer tipo de provas do envolvimento russo. (Carreiro, 2012). De fato, não é possível garantir que a Rússia tenha participado desses ataques virtuais de negação de serviço, nem elencar qual foi ou foram os culpados do ocorrido. Entretanto, vale ser ressaltado que devido ao fato da Estônia ser um país extremamente informatizado e dessa forma dependente da *Internet*, a Estónia mostrou-se bastante frágil a ataques cibernéticos. Em um pouco tempo os ofensores conseguiram atingir sites chaves para o funcionamento do país, causando desordem no país.

Depois destes eventos, notou-se um relevante aumento da consciência de como a falta de comprometimento com a proteção cibernética evidencia os pontos fracos e também o mérito de se precaver para proteger a infraestrutura da rede. Araujo (2014). Nesse sentido foi criada, na capital da Estônia, o Cooperative Cyber Defense Centre of Excellence pela OTAN, a fim de fortalecer e orientar pesquisas sobre contramedidas ao ciberterrorismo e manter um procedimento padronizado para ataques cibernéticos. Geers (2011).

### 3.3.2 Caso Belarus

Durante o pleito presidencial da Bielorrússia em 2006, foi escolhido como presidente a maioria dos votos o candidato Alexander Lukashenko, que se mantinha no poder desde 1994. A oposição ao governo alegou que as eleições, haviam sido fraudadas, entretanto a Rússia e a Comunidade de Estados Independentes aceitaram a oficialidade dos resultados. Geers (2011ApudAraujo 2014).

Conforme o mesmo autor, o site do partido opositor foi objeto de diversos problemas na rede, por ir de encontro ao governo e fazer aliança com os dissidentes políticos. Exemplo disso foi no dia pleito de 2001, uma estatal de telecomunicações impediu o acesso de diversos sites opositores. Mesmo que fosse possível acessa-los de fora da Bielorrússia, ninguém de dentro da mesma conseguia obter acesso, e os sites só voltaram a funcionar no dia subsequente. Um fato a ser considerado é que em tese quando se possui o controle absoluto das telecomunicações, se torna possível efetivar filtros no provedor de serviços à internet, com o fim de bloquear o acesso a certos sites.

Geers (2011ApudAraujo 2014) afirmou que a filtragem na Internet e a vigilância do governo são de fato eficientes, a barragem seletiva aos opositores em momentos críticos, como no dia das eleições, se faz muito pertinente quando o desejado é bloquear o acesso ao que for inconveniente a um governo. A chancela da negação de serviço por um governo para coma a sociedade não está restrito ao uso local, ele pode ser realizado contra outros estados.

As situações detalhadas anteriormente ressaltam como ataques cibernéticos afetam de maneira considerável parte relevante de uma população, especialmente se direcionados para as infraestruturas críticas do estado. A poucos anos atrás, em 2017 ataques cibernéticos sem igual afetaram computadores em diversos países, provocando prejuízos ao funcionamento de empresas e órgãos governamentais, deixando governantes perplexos diante do ocorrido, como divulgado pela imprensa internacional na época isso demonstra que os ataques cibernéticos já são uma ameaça real e que os governantes devem trata-la como uma questão primordial.

## 4 **DOMÍNIO DA TÉCNOLOGIA E CAPACIDADE DE DEFESA**

É notável que a medida em que um estado busca se modernizar ocorre um aumento no número de infraestruturas críticas, junto a isso temos o crescimento de uma dependência dos sistemas de informação e comunicação e da Internet e isso obviamente vem colocando os Estados em situação cada vez mais frágil. Essa fragilidade, entretanto, é resultante das indeterminações do domínio cibernético e explica a vontade dos Estados de se prepararem para um possível conflito.

Essa sensação constante de insegurança é uma das facetas mais interessantes do estudo das relações internacionais no domínio cibernético. Tal domínio garante ao usuário, devidamente habilitado, realizar ataques em anonimato ou fraudando sua identificação. Essa característica possibilita hipoteticamente que um oponente qualificado atribua a terceiros a autoria de uma ofensiva realizada por ele. Isso tem por consequência o fato de que cada vez mais Estados busquem o investimento visando o domínio da tecnologia cyber e o consequente incremento em sua capacidade cibernética de forma a arregimentar uma força cibernética para sua defesa e segurança nacional, assim como para ter a qualificação necessária para conseguir dados sigilosos e informações municiando assim o seu sistema de inteligência, a sua indústria e o seu polo de desenvolvimento científico.

Analisando de maneira mais profunda percebemos que considerando a velocidade instantânea de um ataque cyber e do impedimento de se identificar o ofensor, podemos constatar que os atacantes têm vantagem perante os defensores nesse domínio, e que por isso a iniciativa nas ações se torna primordial nesse ambiente dinâmico. Além disso já verificamos que o custo do investimento em cibernética é relativamente baixo em comparação a outras fontes e domínios de poder. Dessa forma esse momento de transformação da indústria e tecnologia e mudança de paradigma se torna benéfico para os estados que não tinham condições de exercer poder no contemporâneo cenário mundial

Existem outras características que tornam o desenvolvimento de capacidade cyber ideal para os atores de menor relevância. A eficiência de poder realizar uma ofensiva e imobilizar a capacidade ofensiva e administrativa do seu oponente simultaneamente, de forma a deixa-lo frágil no ambiente tangível é uma delas. O ganho com a aquisição de tecnologias e plantas de países mais desenvolvidos é um ponto que grandes nações dos dias de hoje como a China se fizeram valer para chegar até o nível industrial que se encontra atualmente não só no âmbito civil como no militar.

Mas por mais que seja possível elencar diversas razões para se investir no domínio da tecnologia cibernética, sendo por defesa e segurança ou pelo conjunto de possibilidades, a forma de recrutamento e a habilitação de pessoal qualificado é sem dúvidas o recurso chave do poder cibernético, pois esse recurso é o que desencadeia todos os outros. Apesar da difusão inerente ao meio digital possibilitar que qualquer ator estatal ou não estatal e até mesmo indivíduos possam gerar ataques. É de se evidenciar que aquele que desenvolve melhor os seus recursos ampliam de sobremaneira as suas capacidades. Contudo, a forma como acontece os conflitos cibernéticos nos mostra que aquele que tem como foco gerir os seus recursos humanos e a sua rede de usuários tem a maior vantagem perante os demais.

### 4.1 Desenvolvimento Cibernético

A guerra cibernética empregada de maneira isolada é consideravelmente menos dispendiosa que o uso dos meios de guerra convencionais, tendo também a possibilidade de causar destruição no meio físico, mesmo levando em conta que para o amadurecimento deste nível de capacidade se faça indispensável, uma quantidade relevante de investimento em pesquisa, ensino, tempo e produção.

Não obstante, apesar das inúmeras vantagens de um ator coadjuvante se capacitar ciberneticamente o meio físico ainda representa um meio restritivo as suas possibilidades. O risco de sofrer retaliação de uma grande potência pelos meios de guerra convencionais torna pouco provável que um estado nessas condições tenha a iniciática em um possível conflito. Isto é, se faz necessário colocar na balança não só o custo para o desenvolvimento cibernético e o custo do ataque, mas ainda considerar no dispêndio relativo as repercussões de tal ato. A maneira de se mitigar esse risco é garantir de maneira absoluta a não identificação da proveniência do ataque. Necessitando este ser um ponto focal de um ofensor dentro de um conflito cibernético.

Uma das indeterminações da guerra cibernética é a não garantia de êxito no ataque. Não se pode estar certo de que o alvo foi atingido da maneira desejada. Dependendo da forma de ataque um vírus digital pode não funcionar da maneira como era esperada pelo seu desenvolvedor ou ele não teve a capacidade de se manter oculto dos meios de proteção e foi destruído ou modificado. Um ataque visando o colapso de uma cadeia logística pode tomar proporções inesperadas e causar danos indesejados para o atacante e seus aliados.

Um ponto de entendimento é que a cyber guerra deve gerar efeitos tangíveis. Não seria lógico provocar um ataque à elementos que só existem no mundo digital. Quer dizer que, as atuações no meio cibernético têm como premissa produzir resultados no meio físico e

visando algum benefício direto ou indireto para o seu executor. Os ataques se realizam em um campo virtual, o ciberespaço, mas possuem sempre uma origem e objetivos situados em um campo real (VENTRE, 2012). O emprego do poder cibernético de maneira a atingir a população civil é tão real quanto em uma guerra convencional. Entretanto, se os resultados de um conflito cibernético podem ou não atingir escalas alarmantes dependerá apenas dos anseios do ofensor.

O desenvolvimento de formas para desencadear ataques objetivos e, notadamente, focar no centro de gravidade do adversário sem causar danos a outros campos, de modo que através desses meios é possível almejar a vitória através de outros recursos que não a imposição da força bruta e a destruição total, mesmo sem um exército físico, mas se fazendo necessário a criação de um exército cibernético. Essa nova modalidade de batalha possibilita a atuação de um grupo mais numeroso de atores e pode viabilizar as retaliações que, em outro caso ou não seriam feitas ou levariam a uma guerra extremamente destrutiva. Entretanto os ataques cibernéticos ocorrem principalmente nos momentos de paz.

## 4.3 Cenário Atual

Os últimos anos tem sido caracterizado pelo crescimento da ameaça de ataques cibernéticos por grupos, países e organizações menores com razões variadas. Distintas estratégias têm sido traçadas pelos estados que visam se moldar ao mundo como ele se apresenta atualmente. A cibernética em de fato permeia todas as áreas do saber e a utilização errada desse novo campo pode gerar danos em escala ainda não vista para todos.

Dentre todas as nações, a rede computacional, os computadores e *gadgets* se transformaram em algo essencial para o avanço nas mais diversas áreas. Contudo, como resultado dessa transformação, os diferentes setores se tornaram mais eficiente, porém alvos mais fáceis de serem alcançados. Cabe então aos governos o papel de organizadores do espaço cibernético que lhes é incumbido.

### 4.3.1 América do Sul

Não existe conformidade no ciberespaço da América do Sul em relação a políticas e estruturas das instituições, divergindo em conceitos e de como abordar a problemática da situação. Em alguns estados toda a questão cyber fica sob a responsabilidade das respectivas forças armadas, em outros existe uma divisão entre militares e civis.

A Colômbia por exemplo trata tanto segurança quanto a defesa cibernética em como algo único. O que dificulta a integração dos planos de defesa regionais. Isso de alguma forma

este associado ao papel que as forças armadas colombianas desempenharam no passado recente na esfera da segurança pública, assumindo no campo físico também os dois papeis. Uma postura um pouco diferente é a da Argentina, na qual a defesa cibernética está sob a tutela da organização militar, que realiza apoio também suporte à segurança cibernética e juntamente a órgãos civis.

No Brasil, as questões de defesa são norteadas pelo Centro de Defesa Cibernética, que está dentro da estrutura do Exército. O Centro de Defesa Cibernética foi criado em 2010, em fruto da sua designação para essa área de interesse na Estratégia Nacional de Defesa. as atuações em termos de segurança cibernética são geridas por sua vez pelo Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República, o qual visa tutelar a segurança dos sistemas destinados à infraestrutura nacional de energia, como a eletricidade, o petróleo e o gás, do sistema financeiro e da infraestrutura social, abastecimento de demais serviços públicos.

Em relação ao desenvolvimento de acordos e declarações de cooperação sobre o tema de defesa cibernética na região, pode se dizer que ainda estão em uma fase embrionária. A colaboração é vista no nível de troca de conhecimento e intercâmbio de agentes de defesa cibernética, com exceção da Colômbia que apresenta uma cooperação um pouco mais robusta ainda que pontual com a Coreia do Sul. Desta maneira, a cibernética é considerada dentro de um espectro amplo da defesa nacional e é utilizada ainda ora como uma forma de aproximação ou ainda como um aparato político.

### 4.3.2 Estados Unidos

A organização com a responsabilidade de nortear a política nacional de segurança da informação dos Estados Unidos é a *National Security Agency*, que faz parte a estrutura do Departamento de Defesa. Ela é a organização responsável pelo monitoramento, coleta e processamento mundial de informações e dados com finalidade de inteligência e de contra inteligência. O U.S. Cyber Command é o centro de defesa cibernética, criado em 2010 como uma subunidade subordinada ao Comando Estratégico norte-americano. Sendo assim, ele tem como finalidade apoiar as forças armadas e outras agencias que fazem parte da comunidade de inteligência.

Em 2011, os Estados Unidos lançaram a sua Estratégia Internacional para o Espaço Cibernético. Essa salienta a importância do setor para o progresso da humanidade, destacando a importância de parcerias e abertura comercial, assim como reconhece posturas associadas ao estímulo da liberdade de expressão, da privacidade e da movimentação livre de informações.

Algo igualmente relevante é a consideração que o documento tem sobre o direito de defesa, o qual poderá não adotar meios diplomáticos. O espaço cibernético não é limitado ao virtual quando se trata de respostas a ataques desse tipo, ou seja, retaliações com forças militares podem ser empregadas como consequência de ofensivas cibernéticas

### 4.3.3 China

A China é notavelmente um estado que vem se desenvolvendo nas esferas econômica, militar e diplomática, este crescimento a posicionou como alvo de vários ataques. Na ótica dos especialistas chineses, os Estados Unidos são o grande agressor global no ciberespaço, o que para a China justifica os seus altos investimentos na área de defesa cyber. A organização militar chinesa que conduz a sua defesa é o Centro de Computadores Norte de Pequim, considerado como análogo chinês do Comando Cibernético americano.

A capacidade de ataque da China é mais avançada que a sua defesa. Suas principais estratégias estão em desgastar a capacidade de decisão e as operações do adversário por meio do controle de fluxo de dados. Além disso, o estado chinês busca nivelar o seu potencial com a sua estrutura, mitigando suas deficiências em defesa cyber como desenvolvimento de software e hardware mais avançados.

A China reconheceu a muito tempo a relevância estratégica do espaço virtual ao constatar que a superioridade de meios militares convencionais de um adversário pode ser contrabalançada por meio de investimentos em recursos cibernéticos. Sendo impossível alcançar a superioridade militar americana em relação a capacidade técnica e militar, a China tem visto o espaço cibernético como um novo domínio de combate e compensado sua vulnerabilidade convencional modernizando suas Forças Armadas.

## 5 CONCLUSÃO

Com o desenvolvimento tecnológico, especialmente por ocasião da propagação civil da Internet a nível global na década de 1990, os meios de controle das infraestruturas críticas e os meios militares se modernizaram de forma que passaram a depender demasiadamente das redes computacionais e de telecomunicações. Diante deste cenário toda a distribuição de energia elétrica, o abastecimento de água, as telecomunicações e algumas atividades militares, se tornaram vulneráveis as ameaças cibernéticas. Ameaças essas que têm capacidade de executar ataques através desse novo domínio e podem afetar a segurança e defesa nacional de um Estado, uma vez que possuem a capacidade de parar e neutralizar o funcionamento dessas estruturas essências para a sociedade.

O cenário global do qual fazemos parte, se apresenta de maneira complexa. Um número cada vez maior de pessoas e entidades utilizam e demandam por conectividade. A velocidade, quantidade de fluxo e flexibilidade requerida pela sociedade atual exige um sistema de redes a sua altura. Com esses benefícios vieram muitas incertezas, os países que desejam preservar seus interesses e proteger suas riquezas bem como áreas críticas, devem investir nesse tipo de tecnologia de maneira contundente, de forma que se adaptem rapidamente e estejam em condições de se posicionarem frente aos diversos níveis de ameaças.

Nesse sentido, diversos estados optaram por uma maneira de desenvolverem suas defesas cibernéticas, com base em pesquisa e desenvolvimento. Fica claro que o domínio da tecnologia cibernética é o caminho para a estruturação de uma defesa cibernética adequada. E o ponto focal do esforço nesse sentido é o recrutamento e a habilitação de pessoal qualificado em primeiro plano, seguido pelo desenvolvimento de uma estrutura de rede com relativa autonomia e criação de *hardware* e *software* adaptados para o uso e a realidade de cada estado.

Desta forma, o domínio da tecnologia cibernética se apresenta como uma meta a ser alcançada pelos Estados no século atual, cabendo a estes aceitarem a importância da questão cibernética para o presente e para o futuro, gerando uma consciência situacional para os diversos segmentos da sociedade. Com base nas informações presentes nesse trabalho, nota-se que essas inovações, geram um clima de incerteza e insegurança e têm se tornado cada vez mais relevantes na relação entre as nações, instigando-os a se planejarem e se organizarem no que tange a segurança e a defesa cibernética, tanto em atividades ofensivas quanto em defensiva. Desta maneira, o fenômeno cibernético impôs uma nova realidade no sistema internacional, visto que tal campo de atuação tem angariado relevância nas estratégias e questões de estado, desta maneira o incremento nos investimentos em tecnologia cibernética com foco em geração

de recursos de poder cibernético é a chave para a adaptação neste cenário global que se apresenta.

## REFERÊNCIAS


AGOSTINI, Marcos Tocchetto et al. A CIBERNÉTICA SOB A ÓTICA DO FENÔMENO DA GUERRA E DA AGENDA DE SEGURANÇA. 2014.

ÁLVARES, João Gabriel. Territorialidade e Guerra Cibernética. **Segurança e Defesa Cibernética: Da Fronteira Física aos Muros Virtuais. Org. Oscar Medeiros Filho et al. Recife: Ed. UFPE**, p. 101-102, 2014.

BUZAN, Barry; HANSEN, Lene. A evolução dos estudos de segurança internacional. **São Paulo: UNESP**, 2012.

BUZAN, Barry et al. **Security: A new framework for analysis**. Lynne Rienner Publishers, 1998.

CANONGIA, Claudia; MANDARINO JUNIOR, Raphael. Segurança cibernética: o desafio da nova Sociedade da Informação. **Parcerias Estratégicas**, v. 14, n. 29, p. 21-46, 2010.

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

CERVO, Amado Luiz; BERVIAN, Pedro A; SILVA, Roberto da. **Metodologia científica**. 6. ed. São Paulo: Pearson Prentice Hall, 2007. 162 p.

CLARKE, Richard A.; KNAKE, Robert K. **Guerra cibernética: a próxima ameaça à segurança e o que fazer a respeito**. Brasport, 2015.

DA CRUZ JÚNIOR, Samuel César. **A segurança e defesa cibernética no Brasil e uma revisão das estratégias dos Estados Unidos, Rússia e Índia para o espaço virtual**. Texto para Discussão, Instituto de Pesquisa Econômica Aplicada (IPEA), 2013.

DE BOGOTÁ, Cámara de Comercio et al. Documento Conpes 3854, Política nacional de seguridad digital. 2016.

DEFESA, M. D. Doutrina Militar Da Defesa Cibernética. **MD Defensa**, 2014.

DUTRA, André Melo Carvalhais. Introdução à Guerra Cibernética: a necessidade de um despertar brasileiro para o assunto. **IX Simpósio de Guerra Eletrônica**, 2007.

GEERS, Kenneth. **Strategic cyber security**. Kenneth Geers, 2011.

MANDARINO JR, Raphael. Um estudo sobre a segurança do espaço cibernético brasileiro. **Brasília: Cubzac**, 2009.

MARIANO, Marcelo Passini; PIGATTO, Jaqueline Trevisan; DE ALMEIDA, Rafael Augusto Ribeiro. Atores internacionais e poder cibernético: o papel das transnacionais de tecnologia na era digital. **Monções: Revista de Relações Internacionais da UFGD**, v. 7, n. 13, p. 199-229, 2018.

NYE, Joseph S. O futuro do poder. **São Paulo: Benvirá**, v. 333, 2012.

NYE JR, Joseph S. **Cyber power**. HARVARD UNIV CAMBRIDGE MA BELFER CENTER FOR SCIENCE AND INTERNATIONAL AFFAIRS, 2010.

OLIVEIRA NETTO, Alvim Antônio de. **Metodologia da pesquisa científica:** guia prático para apresentação de trabalhos acadêmicos. Florianópolis: Visual Books, 2006. 160 p.

PORTELA, Lucas Soares. Geopolítica do espaço cibernético e o poder: o exercício da soberania por meio do controle. **Revista Brasileira de Estudos de Defesa**, v. 5, n. 1, 2019.

SANTOS, José Carlos dos. G**eneral José Carlos dos Santos: Podemos recrutar "hackers"**. Revista Época. 2011. Disponível em? http://revistaepoca.globo.com/Revista/Epoca/0,,EMI249428-15223,00-GENERAL+JOSE+CARLOS+DOS+SANTOS+PODEMOS+RECRUTAR+HACKERS.html .Acesso em 19 out. 2019.

UNITED STATES. DEPARTMENT OF DEFENSE. **Department of Defense Strategy for Operating in Cyberspace**. DIANE Publishing, 2012.