ESCOLA DE COMANDO E ESTADO-MAIOR DO EXÉRCITO

ESCOLA MARECHAL CASTELLO BRANCO

TC Com SANTIAGO **AGUAYO** MOYA

A EVOLUÇÃO DA POLÍTICA PUBLICA DE SEGURANÇA CIBERNÉTICA DO CHILE E A INCLUSÃO DA DEFESA NACIONAL NA COOPERAÇÃO REGIONAL NO CIBERESPAÇO

Rio de Janeiro

2020

TC Com SANTIAGO **AGUAYO** MOYA

A EVOLUÇÃO DA POLÍTICA PUBLICA DE SEGURANÇA CIBERNÉTICA DO CHILE E A INCLUSÃO DA DEFESA NACIONAL NA COOPERAÇÃO REGIONAL NO CIBERESPAÇO

(PROJETO DE PESQUISA - TCC)

Texto apresentado como Projeto de Pesquisa de Dissertação de Mestrado do Programa de Pós-Graduação em Ciências Militares do Instituto Meira Mattos da Escola de Comando e Estado-Maior do Exército, como requisito para a obtenção do título de Mestre em Ciências Militares.

Orientador: Prof. Dr Carlos Eduardo Franco Azevedo

Rio de Janeiro

2020

TC Com SANTIAGO **AGUAYO** MOYA

A EVOLUÇÃO DA POLÍTICA PUBLICA DE SEGURANÇA CIBERNÉTICA DO CHILE E A INCLUSÃO DA DEFESA NACIONAL NA COOPERAÇÃO REGIONAL NO CIBERESPAÇO

(PROJETO DE PESQUISA - TCC)

Texto apresentado como Projeto de Pesquisa de Dissertação de Mestrado do Programa de Pós-Graduação em Ciências Militares do Instituto Meira Mattos da Escola de Comando e Estado-Maior do Exército, como requisito para a obtenção do título de Mestre em Ciências Militares

Aprovado em _26__ de _Outubro de 2020.

COMISSÃO DE AVALIAÇÃO

Carlos Eduardo Franco Azevedo – Professor Doutor – Presidente
Escola de Comando e Estado Maior do Exército

Orlando Mattos Sparta de Souza – Ten Cel Inf – Membro
Escola de Comando e Estado Maior do Exército

Felipe Araújo Barros – Maj Eng– Membro
Escola de Comando e Estado Maior do Exército

(Dedicatória Omitida).

AGRADECIMENTOS

(Omitido)

“Epígrafe omitido”.

RESUMO

A cooperação em defesa com abrangência ao ciberespaço é um âmbito de desenvolvimento inédito para a Defesa Nacional do Chile. Assim, em 2017 a Política nacional de Segurança cibernética determinou sua contribuição em duas áreas: cooperação e assistência militar, como parte de um esforço encaminhado para fortalecer sua presença internacional e incrementar os relacionamentos baseados nas relações internacionais com outros estados e organizações internacionais em torno à Segurança cibernética de nível global. A tese apresentada tenta analisar desde uma perspectiva qualitativa, baseada no process-tracing e estudo de caso, os principais fatos das ações estratégicas desenvolvidas pelo Estado do Chile e sua relação com as políticas públicas feitas para o ciberespaço que permitam identificar os caminhos causais que justificam à incorporação da Defesa Nacional para cooperar com outras Forças armadas e instituições estrangeras como uma resposta sinérgica para lidar contra os riscos e ameaças que o uso intensivo do ciberespaço gera na sociedade nacional.

Palavras-chave: Cooperação em Defesa – Segurança cibernética – Ciberespaço – Políticas públicas.

ABSTRACT

Defense cooperation covering cyberspace is an unprecedented development area for the National Defense of Chile. Thus, in 2017, the national Cybersecurity Policy determined its contribution in two areas: cooperation and military assistance, as part of an effort aimed at strengthening its international presence and increasing relationships based on international relations with other states and international organizations around the World-class cybersecurity. The presented thesis tries to analyze from a qualitative perspective, based on process-tracing and case study, the main facts of the strategic actions developed by the State of Chile and its relation with the public policies made for cyberspace that allow to identify the causal paths that justify the incorporation of National Defense to cooperate with other armed forces and foreign institutions as a synergistic response to deal with the risks and threats that the intensive use of cyberspace generates in the national society.

Keywords: Defense Cooperation - Cybersecurity - Cyberspace - Public Policies.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE ABREVIATURAS

Forças Armadas	FA
Junta Interamericana de Defensa	JID
Organização das Nações Unidas	ONU
Política Nacional de Defesa Cibernética	PNCD
Política Nacional de Segurança Cibernética	PNCS
União Internacional de Telecomunicações	UIT

SUMÁRIO

INTRODUÇÃO

No 2015, Chile lançou um roteiro para avançar em direção ao desenvolvimento digital do país por meio da definição de objetivos de médio prazo, linhas de ação e medidas concretas a traves do plano denominado “Agenda Digital 2020”. Assim, buscando acompanhar a evolução tecnológica, o Chile possui uma Política Nacional de Segurança Cibernética (PNCS) desde o 2017 que busca proteger usuários e organizações privadas e públicas, contendo diretrizes políticas do Estado nesta matéria. Essa perspectiva aponta, para o 2022, alcançar o objetivo de ter um ciberespaço livre, democrático, aberto, seguro e resiliente que seja principalmente orientado para: salvaguardar a segurança das pessoas no ciberespaço; proteger a segurança do país; promover a colaboração e coordenação entre instituições; e gerenciar os riscos do ciberespaço.

A ideia de elaborar a estratégia nasceu da necessidade do País para modificar, com a maior urgência possível, o cenário de Segurança Cibernética, caracterizado pelos seguintes aspectos: ciberataques e atividades de espionagem nas diferentes redes, a interceptação massiva de redes de telecomunicações, a desativação do serviço de Internet, casos de espionagem contra governos e empresas, bem como ataques contra infraestruturas críticas, como serviços básicos, instituições financeiras e entidades governamentais, entre outros.

Daí que as propostas iniciais e as sucessivas políticas para o ciberespaço, o país estabeleceu que “uma transformação desta magnitude não pode deixar de implicar desafios importantes para o Estado, pois é imprescindível colocar este potencial tecnológico a serviço das pessoas e da convivência social”. (CHILE, Govierno de Chile, 2017, p. 5) No mesmo sentido, evidenciam-se uma acentuada preocupação do Estado chileno com aprofundar os relacionamentos baseados na cooperação e as relações internacionais em torno a Segurança cibernética no contexto global através de diferentes instâncias de comunicação, coordenação e colaboração que fomentem a construção de confianças e a capacidade para fornecer uma resposta comum aos riscos do ciberespaço.

Por esta razão, a política de segurança cibernética não somente constitui uma ferramenta que abrange fatores de natureza doméstica tais, como os políticos, econômicos e estratégicos setoriais, senão, faz parte das ideias, visões de mundo e interesses do Chile como um ator no sistema internacional e por outro lado, demostra sua posição na região em relação a aportar e colaborar no âmbito da segurança cibernética.

Desse modo, a partir da publicação, em 2018, da Política Nacional de Defesa Cibernética (PNDC), como planejamento subsidiário da PNCS, a Defesa Nacional complementa a Segurança Cibernética naqueles aspectos diretamente relacionados à defesa da soberania através de redes digitais, protegendo a infraestrutura crítica de informações e com a proteção dos direitos humanos de todas as pessoas que vivem no território nacional, igualmente preceitua as Forças Armadas (FA) uma responsabilidade no cenário exterior principalmente em duas áreas: cooperação e assistência militar.

Assim, a Defesa Nacional já está abrangida pelo mandato da política pública para desenvolver seu planejamento e ações estratégicas para atingir os objetivos atinentes. Neste contexto, é valido estabelecer questões sobre a pertinência e idoneidade de incorporar às FA para cumprir esse tipo de tarefas, as quais tinham uma perspectiva de desenvolvimento de menor escopo em relação a cooperação em defesa, limitadas aos âmbitos tradicionais de emprego.

Consequentemente, a pesquisa apresentada, a partir de um método da análise de diferente fontes documentais relacionadas com as políticas concebidas como resposta estatal no ciberespaço, as mudanças da estrutura e funções da Defesa nacional e o estudo do processo de formulação de políticas públicas ao interior da institucionalidade chilena, tentará demostrar os caminhos causais para estabelecer as justificativas que proporcionem uma resposta em relação as razoes que tive o Estado de Chile para tomar a escolha política - estratégica de incorporar à Defesa Nacional como parte de um processo de cooperação internacional de tipo-regional.

1. PROBLEMA DE PESQUISA

A “Cooperação em Defesa” cumpre um papel inédito no âmbito da Segurança Cibernética no ciberespaço sob a responsabilidade das FA, pela esta razão, se apresenta como um campo de desenvolvimento ainda em uma etapa de evolução inicial. Daí, existe uma falta de antecedentes documentais que estabeleçam diferentes análises e estudos sobre a origem da incorporação deste imperativo estratégico e os processos de tomada de decisões das diferentes ações estratégicas definidas nas respetivas políticas públicas de Segurança cibernética e subsidiárias no contexto do cenário político nacional e com repercussões sobre as relações internacionais do país que fundamentem a escolha estratégica.

Além disso, este âmbito setorial da Defesa é um campo escassamente desenvolvido em términos de número de pesquisas por instituições acadêmicas, bem como, evidencia-se a carência de desenhos de pesquisas que incorporem uma perspectiva multifatorial de análise em relação as variáveis que compõe o fenômeno. Mas ainda, a política referida foi publicada de modo recente no 2018, assim como também, pode se observar que o caso da “Cooperação em Defesa” é oportuno ser avaliado desde diferentes perspectivas teóricas como as Relações internacionais, a Ciência política, da Segurança e Defesa, entre outros.

Por conseguinte, a referida incorporação da escolha estratégica da “Cooperação em Defesa” no contexto da Segurança cibernética e seu evidente aprimoramento não tem explicações satisfatórias, por tanto, surgem possíveis interpretações para justificar o fato, dentro das quais é viável assumir que seria o resultado de um processo de mudanças na formulação das políticas públicas sob estímulos externos; o resultado dos diferentes processos de mudanças ao interior da Defesa nacional ou como parte de um alinhamento com outras políticas públicas como a Política exterior e de Segurança pública.

Então, surge uma problemática inicial, sobre definir os fundamentos políticos - estratégicos que determinaram a incorporação da “Cooperação em Defesa nacional” no âmbito regional como preceito nas respetivas políticas públicas de

Segurança cibernética e subsidiárias do Chile a fim de justificar os futuros resultados além de 2022 e seus efeitos a partir de um processo histórico que começou no ano 2015 com a difusão da “agenda 2020”.

Consequentemente, se determinou como questão a investigar:

¿Quais são as razões que levaram incorporar na promulgação de políticas públicas de Segurança Cibernética do Chile a inclusão de princípios que sustentam a participação da Defensa nacional no âmbito da cooperação militar[1] de tipo regional?

2. OBJETIVOS

Segundo Vergara (1998, p. 25) “o objetivo é um resultado a alcançar” e seu valor pratico radica de acordo com Hernandez-Sampieri et al. (2014) no fato de “estabelecer que se pretende com a pesquisa” para atingir objetivo final, se é alcançado, dá resposta ao problema. (HERNÁNDEZ-SAMPIERI, FERNÁNDEZ, & BAPTISTA, 2014, p. 37). Neste sentido, a existência de objetivos intermediários se justifica já que são as metas de cujo atingimento depende o alcance do objetivo final. Por isso, estabeleceu-se, para o presente estudo, os seguintes objetivos:

2.1 Objetivo Principal

Explicar as razões que levaram incorporar na promulgação de políticas públicas de Segurança Cibernética do Chile a inclusão de princípios que sustentam a participação da Defensa nacional no âmbito da cooperação militar de tipo regional.

2.2 Objetivos Específicos

Seguidamente, de acordo a sequencialidade e coerência com a desenho da pesquisa foram esboçados os objetivos específicos apresentados:

[1] Para os fines desta pesquisa se entenderá da mesma forma o termo de “cooperação militar” com “cooperação em defesa”.

- Objetivo Específico n°1: Identificar os recentes critérios, definições e estratégias que permitiram o desenvolvimento de políticas públicas dentro do quadro político nacional do Chile com foco na Segurança Cibernética que colaboraram com o fortalecimento da participação da Defesa Nacional no contexto regional.

- Objetivo Específico n°2: Identificar as mudanças nas estruturas e concepção da Defesa Nacional do Chile a partir do ano 2000 para o incremento de sua participação nos processos de cooperação internacional do tipo regional.

- Objetivo Específico n°3: Analisar os conceitos e ferramentas relacionados ao processo de elaboração, implementação e integração de políticas públicas setoriais no Chile em relação a segurança pública e Defesa.

3. HIPÓTESES OU SUPOSIÇÃO

De acordo com Hernandez-Sampieri (2014) as hipóteses se derivam da teoria existente e constituem os lineamentos para uma investigação. Sua função principal indica o que estamos tentando testar e são definidos como explicações provisórias do fenômeno investigado. (HERNÁNDEZ-SAMPIERI, FERNÁNDEZ, & BAPTISTA, 2014, p. 104). Em vista disso e conjuntamente com os reflexos feitos a partir das análises iniciais do fenômeno que orientam o processo analítico, devemos estabelecer a seguinte hipótese: “O processo de aperfeiçoamento das políticas públicas que se relacionam com a Segurança cibernética nacional fomentam a incorporação da atitude estratégica de “cooperar em defesa” no âmbito do ciberespaço regional”.

Consequentemente, tem sido definido as variáveis iniciais para a pesquisa, de acordo ao quadro metodológico proposto por Gil (2002) para o conceito de variável, refere-se a “tudo aquilo que pode assumir diferentes valores ou diferentes aspectos, segundo os casos particulares ou as circunstâncias” (GIL, 2002, p. 32). Assim, as variáveis serão:

QUADRO 1 – Variáveis de Pesquisa.

Variáveis	Tipo de variáveis
o aperfeiçoamento das Políticas públicas de Segurança cibernética	Independente
A cooperação em Defesa no âmbito da Segurança Cibernética de tipo regional	Dependente
Mudanças políticas – estratégicas no cenário interno e externo do país.	Interveniente

Fonte: Elaborado pelo autor.

4. DELIMITAÇÃO DO ESTUDO

A pesquisa em relação a sua temporalidade possui um recorte flexível desde a década de 2010, que se caracteriza por o surgimento de ciberespaço como um cenário de interação político-estratégico para os Estados. Neste contexto surgem oportunidades, ameaças de segurança e desafios em termos de definir a resposta estatal frente a um entorno complexo, de dimensões não físicas e de interações ilimitadas. A partir disso, aparecem nas agendas dos Estados as demandas sociais e de necessidade pública para a adopção de medidas que garantam um espaço seguro e de livre acesso para seus habitantes. No caso do Chile, as primeiras políticas e estratégias setoriais surgem a partir de 2015 com a política denominada “Agenda 2020”, balizando-se a partir desse marco histórico, um processo de rápido de desenvolvimento de díspares e sucessivas políticas públicas, por esta razão, se analisará com maior profundidade esse período.

Entretanto, nos aspeitos que estão relacionados diretamente com a cooperação em defesa, serão estudadas as diferentes mudanças nas faculdades, estruturas e composição da Defesa nacional que permitiram a inserção deste conceito a partir de 2000. Assim, apesar de estabelecer explicações em um período definido, os dados poderão ser obtidos de outros segmentos de tempos, ainda não declarados, para cumprir com o propósito da pesquisa que se guia para estabelecer

caminhos causais e mecanismos que levaram a inclusão da atitude estratégica da cooperação em defesa nas políticas públicas para o ciberespaço.

Por outro lado, a abordagem territorial está delimitada ao espaço geográfico do Chile, mas durante a diferentes explanações poderão ser analisadas antecedentes de diferentes índoles que façam referência ao cenário regional, entendendo-se sua abrangência ao continente sul-americano onde foca-se nossa análise e pudessem identificar-se algumas influências sobre a posição do país.

Seguidamente, os antecedentes documentais e bibliográficos que serão analisados poderão ser de diferente procedência e idioma, destacando-se aqueles aspeitos que permitam balizar avanços no desenvolvimento das políticas estatais no ciberespaço, reconstruir contextos políticos e sociais de acordo ao recorte temporal, e outros relacionados com argumentos técnicos e multidisciplinares que acrescentem o estúdio do fenômeno. Igualmente, como parte de nosso estudo, serão incluídas as abordagens de diferentes disciplinas como parte da estratégia de pesquisa para observar o fenômeno sob prismas teóricos que procuram dar "explicações concorrentes das evidências em foco e a análise de sua plausibilidade" (YIN, 1994, p. vii), e assim, cumprir com os objetivos da investigação.

5. RELEVÂNCIA DO ESTUDO

A crescente utilização das tecnologias de informação e comunicação representa o surgimento de novos riscos e ameaças para a segurança do país, seus habitantes e suas infraestruturas, aspeitos que devem ser analisados de forma integral e numa perspectiva de tipo multifatorial. Logo, uma transformação desta magnitude só pode implicar desafios importantes para o Estado, em especial para a Defesa, pois é imprescindível colocar este potencial tecnológico ao serviço das pessoas e da convivência social.

Certamente, a participação da Defesa Nacional nesta área é emblemática porque incorpora suas capacidades para enfrentar o problema, assim mesmo

contribui nos processos de aprofundamento das relações internacionais baseados na “Cooperação em Defesa”.

Neste contexto, gerar análises multifatoriais para compreender as origens e justificativas dos processos de planejamento político - estratégico, especialmente os associados à Defesa Nacional em um contexto de recente evolução, constituem um desafio, pois a partir deles surgirão a construção de admissíveis explicações teóricas que fundamentam as escolhas estratégicas do Estado Chileno, trazendo consigo plausíveis contribuições para futuras análises neste âmbito.

Além disso, o tipo de estudo proposto contribui a conhecer e ponderar o funcionamento institucional de um país desde a dimensão Política – estratégica e seu relacionamento com decisões e políticas governamentais. Do mesmo modo, verificar empiricamente o desenho das políticas públicas que estabeleceram as interações funcionais entre os órgãos institucionais e a incorporação das mudanças políticas – estratégicas adotadas pelo Estado Chileno durante a década de 2000 – 2020 aspeitos que permitiram assentar as bases da participação da Defesa Nacional no âmbito da Segurança cibernética com ênfase na cooperação internacional.

Enfim, construir desde a abordagem acadêmica uma instancia que permita dar resposta satisfatória respeito dos fundamentos do Estado Chileno para incorporaram nas políticas públicas de Segurança cibernética os princípios da “Cooperação em Defesa” e a partir disso, formular uma teoria que respalde as evidências estabelecidas ou para gerar novas questões para futuras pesquisas (HERNÁNDEZ-SAMPIERI, FERNÁNDEZ, & BAPTISTA, 2014, p. 40).

6. METODOLOGIA DA PESQUISA

No meio de das diferentes fontes bibliográficas consultadas, destaque-se a posição das autoras Martins & Leitao (2018) quem orientam algumas das funções que deve cumprir a metodologia; neste sentido, observamos que:

> É garantir que as informações obtidas na pesquisa permitam respostas às perguntas iniciais o menos equivocamente possível. Isso sugere, portanto, um maior interesse em relação à estrutura lógica da pesquisa, que apontará a melhor estratégia e o método mais adequado para responder à questão e menos o modo de coleta dos dados. (MARTINS & LEITAO, 2018, p. 17).

Em seguida, segundo Yin (1994) cada tipo de pesquisa empírica possui um projeto de pesquisa implícito, se não explícito. Neste sentido, entenderemos como o propósito desta atividade:

> Conduz o pesquisador através do processo de coletar, analisar e interpretar observações. E um modelo lógico de provas que lhe permite fazer inferências relativas às relações causais entre as variáveis sob investigação. O projeto de pesquisa também define o domínio da generalização, isto é, se as interpretações obtidas podem ser generalizadas a uma população maior ou a situações diferentes. (YIN, 1994, p. 41 apud NACHMIAS & NACHMIAS, 1992, p. 77-78)

Então permanecemos em frente de um processo analítico que tenta obter evidências para a construção de inferências causais que proporcionem uma "teoria" que explique o fenômeno em estudo baseado principalmente na produção de conhecimento científico[2].

Gil (2002) sugere que como toda atividade racional e sistemática, a pesquisa exige que as "ações desenvolvidas ao longo de seu processo sejam efetivamente planejadas" (GIL, 2002, p.19). Desta asseveração, podemos entender segundo Martins & Leitao (2018):

> Objetivo da pesquisa é a inferência, seja descritiva ou causal, baseada em informações empíricas sobre o mundo, de preferência a partir de evidências sistematicamente coletadas, que ajudem o pesquisador a concluir sobre o que não é diretamente observado. (MARTINS & LEITAO, 2018, p. 10)

Do mesmo modo, Hernandez-Sampieri (2014), argumenta que quando se manifesta um processo lógico e indutivo orientado a explorar e descrever para gerar perspectivas teóricas, se pode observar o desenvolvimento de uma pesquisa qualitativa em termos de seu "enfoque o aproximación cualitativa" (HERNÁNDEZ-

[2] "A busca pela produção de conhecimento científico gerou um conjunto de critérios que caracterizam sua especificidade em relação aos demais conhecimentos, como a racionalidade, a objetividade, a verificabilidade e a sistematicidade". (MARTINS & LEITAO, 2018, p. 10).

SAMPIERI, FERNÁNDEZ, & BAPTISTA, 2014, p. 8). Para Martins & Leitao (2018) a indução constitui um “processo mental que parte da observação de fatos particulares para se produzir conclusões sobre casos ou acontecimentos não observados, transpondo-se proposições e juízos sobre eventos ou fatos com os quais se teve experiência, para outros com os quais não se teve experiência”. (MARTINS & LEITAO, 2018, p. 12 apud HUME 2004).

Daí devido as peculiaridades do estúdio em discussão, se utilizará uma abordagem de tipo “qualitativa” pela razão que se encontra mais alinhado com o propósito da pesquisa e que se fundamenta sobre as argumentações de Martins & Leitao (2018)

> Sobre a pesquisa qualitativa colabora no estudo da dinâmica interna do fenômeno e no contexto em que ocorrem, de modo a buscar uma compreensão mais acurada por meio do exame em profundidade de um caso específico. (MARTINS & LEITAO, 2018, p. 14 apud RAGIN, 1994; GERRING, 2007; BYRNE, 2013).

Se retomarmos ao objetivo da pesquisa que consiste em explicar as razões que levaram incorporar a participação da Defensa nacional no âmbito da cooperação militar de tipo regional para o espaço cibernético a partir da publicação da PNCS em 2017, se pode evidenciar que acontece um fato de tipo – histórico, já que obedece a uma temporalidade definida em relação a um contexto político – estratégico. Assim é importante analisar desde diferentes perspectivas porque aconteceu esse fato e daí, identificar as justificativas que se deduzem das decisões executadas pelo Estado chileno neste âmbito.

Desde essa perspectiva, Van Evera (1997) existem sete tipos de tese. Devidos aos antecedentes já apresentados em relação a seus objetivos, o trabalho se enquadra no que o autor classifica como “histórico-explanatório”, cujo objetivo central está em explicar causas, padrões ou consequências de eventos históricos. (VAN EVERA, 1997, p. 89-91). A seguir, respeito das pesquisas explicativas segundo Gil (2002) nos explica:

> Essas pesquisas têm como preocupação central identificar os fatores que determinam ou que contribuem para a ocorrência dos fenômenos. Esse é o

> tipo de pesquisa que mais aprofunda o conhecimento da realidade, porque explica a razão, o porquê das coisas. (GIL, 2002, p. 41-42).

De modo que, a incorporação inicial de uma abordagem de tipo “histórico-explanatório” pudesse aprofundar o desenho teórico para esclarecer as causas potenciais e consequências de eventos históricos, como foi a criação de um cenário estratégico inédito para o ciberespaço, e a reconstrução histórica de um ambiente político-estratégico a partir de 2010 no Chile que incentivaram a formulação de diferentes políticas públicas, bem como as mudanças na concepção da Defesa Nacional para adaptá-la aos desafios do século XXI.

Por conseguinte, ao pretende-se que o fenômeno seja estudado em seu próprio contexto “terá incidência sobre os mecanismos causais e desta interação determinará os resultados” (MARTINS & LEITAO, 2018, p. 46).

Deste jeito, se seguirá a argumentação de Martins & Leitao (2018) sobre a importância teórica da definição do “contexto” em relação a nossa pesquisa, bem como sua definição e importância de cada um deles, será dada pela teoria que nos guia:

> Os aspectos relevantes de uma configuração ou cenário (analítico, temporal, espacial, institucional) nos quais um conjunto de condições iniciais conduz (probabilisticamente) a um resultado de escopo e significado definido via um mecanismo causal específico ou conjunto de mecanismos causais. (MARTINS & LEITAO, 2018, p. 47 apud FALETTI e LYNCH, 2009, p. 1152).

Em particular, se fará uma descrição dos acontecimentos e ações desenvolvidas através de um Timeline para estruturar uma possível explicação para guiar a pesquisa em direção de determinar os caminhos causais admissíveis que são necessários para fornecer o objetivo da pesquisa, com foco inicial, nas interações socias que conformaram a agenda política na década de 2010; e ainda, os processos de toma de decisões por parte do Governo do Chile para a adopção de preferencias respeito da promulgação de políticas públicas para o ciberespaço com o fortalecimento de ação da Defesa.

Tal fato, reforça nossa escolha metodológica em termos da “causação” e nos aproxima ao conceito de “multifinalidade”, segundo Martins & Leitao (2018):

> Se entende que, apesar de um conjunto de condições iniciais comuns, um mesmo mecanismo (ou um conjunto deles) gera diferentes resultados, em razão da dependência do contexto, ainda que o mecanismo opere da mesma maneira (apud FALETTI; LYNCH, 2009; KAY; BAKER, 2015). Ou seja, “a causação reside na interação entre o mecanismo e o contexto dentro do qual ele opera” (apud FALLETI; LYNCH, 2009, p. 1145). (MARTINS & LEITAO, 2018, p. 46)

Logo, nossa análise das condições do entorno nos processos descritos, podem ser justificados desde a perspectiva de Martins & Leitao (2018):

> Em relação ao tipo social de nexo causal, considerando o tempo e a ordem dos eventos (apud BYRNE, 2013). Aliás, sendo o mundo social complexo, para atribuir um efeito causal (ou seja, o valor esperado da mudança no resultado quando uma ou mais variáveis independentes mudam) a qualquer intervenção, é necessário considerar o contexto e a ação dos agentes (ideias, interesses, preferências), algo improvável a partir de métodos estatísticos (apud BENNETT; GEORGE, 2005; BYRNE, 2013). (MARTINS & LEITAO, 2018, p. 46).

Supondo que é relevante para os propósitos da pesquisa, entender melhor os efeitos causais e as definições de causalidade a partir de uma base observacional que permita obter adequadas inferências para nosso estúdio, é indispensável a adopção de método de “Process Tracing” (Rastreamento de processos, PT). Segundo Martins & Leitao (2018) se define: “Método que tenta identificar o processo causal interativo – a cadeia causal e o mecanismo causal – entre uma variável independente (ou variáveis) e o resultado da variável dependente”. (MARTINS & LEITAO, 2018, p. 37 apud BENNETT; GEORGE, 2005, p. 206).

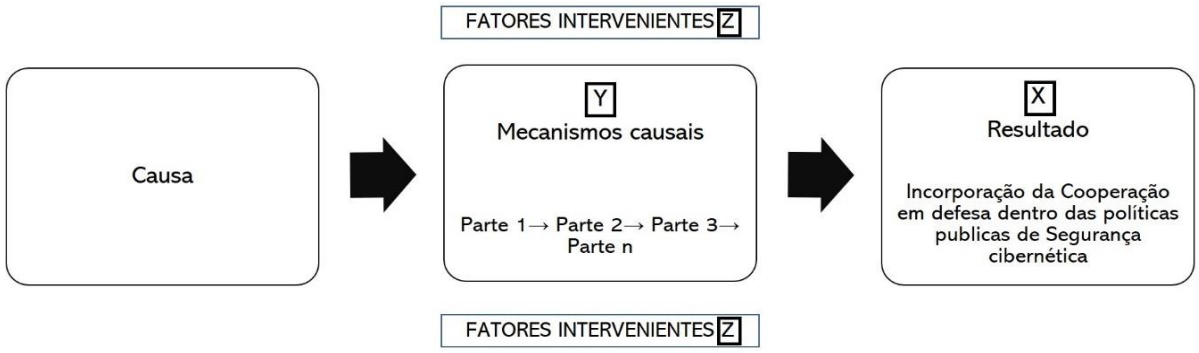
Certamente, é importante conceituar que um mecanismo causal está constituído de acordo a Martins & Leitao (2018) por:

> Conjunto de partes interconectadas e compostas de “agentes ou entidades que têm a capacidade de alterar seu ambiente porque possui uma propriedade invariante, que, num contexto específico, transmite força física ou informação que influencia o comportamento de outros agentes ou entidades. (MARTINS & LEITAO, 2018, p. 37 apud WALDNER, 2012, p.75).

Assim, nas palavras das autoras Martins & Leitao (2018) o process tracing “constitui um caminho intermediário entre as explicações históricas e às complexidades da teorização dos eventos históricos de acordo de cientistas sociais e políticos”. (MARTINS & LEITAO, 2018 p. 37, apud BENNETT E GEORGE, 2005). Além disso, as mesmas autoras estabelecem que teoricamente o Rastreamento de processos apresenta vantagens respeito de outros métodos, nos estudos que envolvem “processos de decisão, preferências, expectativas, intenções, motivações, crenças ou aprendizado nos níveis individual e organizacional” (MARTINS & LEITAO, 2018, p. 41 apud BENNETT; GEORGE, 1997; BATES et al., 1998); seu uso volta-se para a produção de inferências causais baseadas em informações empíricas, evidências selecionadas que contribuem para identificar e analisar os mecanismos causais presentes no caso estudado.

Consequentemente, os fatores procedentes das análises realizadas determinaram a relação de causalidade do tipo Y (variável(eis) Independiente(s))→X (variável dependente – resultado) e ↓ Z (variável interveniente). (HERNÁNDEZ-SAMPIERI, FERNÁNDEZ, & BAPTISTA, 2014, p. 109-115).

FIGURA 1 – Relação de causalidade entre variáveis.



Fonte: Elaboração própria a partir de modelo feito pelo Martins & Leitao (2018) p. 87.

Pela mesma razão, o objetivo central do estudo consiste em dar uma explanação em relação a determinar os caminhos causais e esclarecer uma singularidade, respeito da inclusão da “cooperação em defesa” nas políticas de Segurança cibernética mediante o uso de “Process Tracing”. Por isso, opta-se por algumas das ferramentas de desenho de pesquisa de “Estudo de caso” para

complementar os tipos já propostos. Assim, segundo Martins & Leitao (2018) tem sua aplicabilidade mais comum em estudos de caso em profundidade, situados espacial e temporalmente; também, “ser um método robusto para entender a causalidade a partir de relatos internos de mudanças de políticas, ao mesmo tempo em que permite a comparabilidade entre estudos de caso únicos”. (MARTINS & LEITAO, 2018, p. 38-42 apud BENNETT; CHECKEL, 2015, p. 9; apud KAY; BAKER, 2015).

Como resultado, Yin (1994) de acordo com Schramm (1971) argumenta que a essência desde esse tipo de caso, tenta esclarecer uma decisão ou um conjunto de decisões: o motivo pelo qual foram tomadas, como foram implementadas e com quais resultados. Por outro, diversos autores estabelecem que é uma “investigação empírica que investiga um fenômeno contemporâneo localizada temporal e espacialmente em profundidade no seu contexto da vida real, especialmente quando os limites entre o fenômeno e o contexto não estão claramente definidos”. (YIN, 1994, p. 31-32; MARTINS & LEITAO, 2018, p. 38-42 apud VAUS, 2001; CRESWELL, 2007; BENNETT; CHECKEL, 2015; YIN, 2015).

Por outro lado, de acordo com Hernandez-Sampieri (2014), em relação a determinação da amostra argumenta que “na amostragem qualitativa é comum começar com a identificação de ambientes propícios, depois grupos e, finalmente, indivíduos”. (HERNANDEZ-SAMPIERI, 2014, p. 473). Ainda, “a amostra pode ser uma única unidade de análise, como no estudo de um só caso”. (HERNÁNDEZ-SAMPIERI, FERNÁNDEZ, & BAPTISTA, 2014, p. 386 apud MERTENS, 2010, tradução nossa).

Em relação a coleta de dados será feita através de uma pesquisa de tipo “documental”, segundo Gil (2002) “a pesquisa documental vale-se de materiais que não recebem ainda um tratamento analítico, ou que ainda podem ser reelaborados de acordo com os objetos da pesquisa”. (GIL, 2002, p. 45-47). Neste sentido, as fontes são mais diversificadas, abrangentes e acessíveis. A nossa opção metodológica pela análise documental justifica-se como estratégia para obter, com mais clareza e uma posição mais objetiva, as posições de governo, autoridades, instituições e diferentes atores sobre os assuntos estudados neste trabalho.

Como fontes de consulta serão procurados documentos oficiais, registros de arquivos, declarações, discursos, e relatórios técnicos disponíveis nos web sites de Governo do Chile, Congresso Nacional, Ministérios da Defesa, Relações Internacionais e Interior e Segurança Pública. Contudo, as consultas serão ampliadas com algumas fontes bibliográficas que deem suporte aos reflexos obtidos. Desta forma, segundo Martins & Leitao (2018) “o investigador explora um sistema delimitado (um caso) ao longo do tempo, através de uma coleta detalhada de dados envolvendo múltiplas fontes de informação”. (MARTINS & LEITAO, 2018, p. 18 apud BENNETT; GEORGE, 2005, p. 79).

TABELA 1 – Material de Pesquisa por Capítulo.

Tipo de dado	Capítulo	Origem / tipo de dado
Documental	**03**	– Agenda Digital 2020 – Bases para uma Política Nacional de Segurança Cibernética 2015. – Estratégia Nacional de Segurança Cibernética 2017. – Política de Defensa cibernética 2018. – Programa de Governo 2014-2018 “Chile de todos”. – Programa de Governo 2018-2022 “Construamos melhores tempos para Chile”.
	04	– Discursos dos Presidentes de Chile Lagos, Frei e Bachelet; Ministros de Defensa. – Lei nº 20.424, Orgânica do Ministério da Defesa Nacional. – Decreto Supremo 272/1985 Missões e Funções das Forças Armadas. – Decreto Supremo 248/2010, Regulamentos orgânicos e operacionais do Ministério da Defesa Nacional. – Decreto Supremo113/2014, Estabelece Processo de planejamento da Defesa Nacional – Livro da Defesa Nacional 1997, 2002, 2010, 2017.
	05	– Política exterior do Chile. – Decreto 533/2015: Cria Comitê Interministerial Segurança Cibernética – Conta pública presidencial desde 2014 até 2020. – Mensagem presidencial 2014-2018 (Relações internacionais) – Memorias de Ministério de Relações Exteriores do Chile desde 2014 até 2017. – Regulamentos para o funcionamento do Comitê Interministerial de Segurança Cibernética – Padrões e instituições envolvidas em Segurança Cibernética no Chile – Decretos de Segurança Cibernética. – Fundo documental administração presidencial 2014-2018

Fonte: Elaborado pelo autor.

Juntamente, incorporar os sustentos teóricos de diversas disciplinas que justifiquem as evidências descobertas. Assim, se tentará acompanhar os baseamentos de Yin (2015) sobre o processo de coleta de dados e informações em estudos de caso no sentido de assegurar que se cumpram três princípios: a) utilizar múltiplas origens de evidências; b) criar um banco de dados do estudo de caso; c) manter uma cadeia de evidências.

A seguir, para o tratamento dos dados se utilizará a análise sistemático[3]. segundo Hernandez-Sampieri (2014) argumenta que “Este desenho destaca o uso de certas etapas na análise de dados. Inclui os tipos de codificação aberta, axial e seletiva”. (HERNANDEZ-SAMPIERI, 2014, p. 473 apud CORBIN & STRAUSS, 2007).

Assim, segundo Queiroz & Regina (2016) a codificação ou análise é o procedimento através do qual os dados são conceitualizados, categorizados, hierarquizados e as relações entre os dados e as categorias são estabelecidas. O procedimento analítico, neste momento iniciado, tem como objetivos: (1) construir a teoria; (2) dar ao processo científico o rigor metodológico necessário; (3) auxiliar o pesquisador a detectar os vieses da pesquisa; (4) desenvolver o fundamento, a densidade, a sensibilidade e a integração necessária para gerar uma teoria. (QUEIROZ & REGINA, 2016, p. 23 apud CORBIN & STRAUSS, 2008).

7. ESTRUTURA DA PESQUISA

7.1 Estrutura Geral

Esta dissertação será estruturada no formato monográfico, no âmbito de seis capítulos, elaborados de acordo à metodologia apresentada e são coerentes na sua estruturação com os objetivos propostos. Seguidamente, os capítulos serão:

Capítulo 1: Introdução. Neste capítulo serão abordadas, os tópicos referidos à introdução à pesquisa, a questão de estudo, o objetivo principal e os objetivos

[3] Apesar desta teoria utiliza majoritariamente entrevistas como técnica de coleta de dados, ela não exclui outras técnicas, entre elas: conversação informal, observação participante e não-participante, focus groups, análise documental e de literatura. (QUEIROZ & REGINA, 2016, p. 34).

secundários identificados para serem atingidos, a delimitação do estudo, a relevância e estrutura de pesquisa. Além disso, serão apresentados a metodologia da pesquisa, estabelecendo o tipo de pesquisa, a coleta e tratamento dos dados e a análise dele. Deste jeito, para um melhor entendimento da pesquisa se dará a conhecer a estratégia de pesquisa e seus sustentos teóricos que a possibilitam no contexto planteado.

Capítulo 2: Referencial Teórico. Neste capítulo se procurará estabelecer uma abordagem teórico para a definição dos principais conceitos e funções teóricas que serão desenvolvidas e que proporcionam o fundamento acadêmico à pesquisa. Assim, serão analisados inicialmente os conceitos e definições referentes a: ciberespaço, sua evolução e importância para os Estados; a segurança cibernética, a cooperação em defesa e seus efeitos na interação no ciberespaço e as políticas públicas e sua abrangência na solução dos problemas sociais.

Capítulo 3: A evolução da política pública de segurança cibernética: a solução política - estratégica para interagir no ciberespaço. Utilizando uma narrativa descritiva, será detalhado a partir da uma elaboração de um timing, os principais fatos que envolveram a evolução das diferentes políticas públicas para o ciberespaço até a promulgação da PNCS. Bem como, as características do entorno político – estratégico que balizaram seu desenvolvimento. Seu foco, além de definir sua evolução histórica e a reconstrução do ambiente onde se propiciou, será mapear os eventos e precisar os tempos e aportes por diferentes órgãos durante a construção da PNCS, com a finalidade de pesquisar sobre as causas para a incorporação de aspeitos relacionados coma a Defesa Nacional.

Capítulo 4: As mudanças da Defesa nacional do Chile e seu desenvolvimento em direção à cooperação militar de tipo regional. O objetivo desse capítulo será analisar as diferentes mudanças estruturais, de funcionamento, atribuições da pasta da Defesa, para entender como essas inflexões se processam em documentos de política do Estado e encontra-se relacionadas com a maior participação das FA no âmbito da cooperação e assistência militar na região. Desse modo, rastrear os processos de relevância para a configuração de um cenário analítico, temporal, espacial e institucional, nas quais se consiga identificar um conjunto de condições

iniciais que vão a conduzir a um resultado de maior escopo e significado definido através de um mecanismo causal específico ou conjunto deles que forneceu uma decisão estratégica de cooperar em defesa no ambiente cibernético.

Capítulo 5: O processo de elaboração das políticas públicas: O fortalecimento da Institucionalidade pública frente aos desafios estatais no ciberespaço. O capítulo nos apresentará a análise das diferentes políticas públicas que estão relacionadas com as políticas públicas de segurança cibernética. Neste sentido, a través de uma análise sistêmico se determinará as concorrências e integrações entre as diferentes políticas setoriais promovidas pelos diferentes Ministérios, a fim de estabelecer os mecanismos causais que alinham as decisões governamentais no âmbito do ciberespaço com abrangência até a dimensão política-estratégica.

Capítulo 6: Conclusões finais. O objetivo é oferecer as principais descobertas de acordo a metodologia desenvolvida por cada capítulo. Assim, obter as conclusões capitulares para construir o resultado general. A partir desse ponto, poderemos responder quais mecanismos, afinal, estiveram por trás da incorporação da cooperação em defesa como uma política para o ciberespaço, a sua motivação e sentido estratégico.

7.2 Esquema gráfico da pesquisa

Para fins de organizar as ideias, acompanhar o raciocínio e apresentar graficamente a metodologia proposta e seu relacionamento com os objetivos da pesquisa foi desenhado um esquema gráfico que norteou todo o processo de investigação (**APÊNDICE A** – Esquema Gráfico de Pesquisa).

7.3 Cronograma de pesquisa

A fim de estabelecer as coordenações de objetivos e tempos previstos para a realização da pesquisa, se elaborou um cronograma com os principais eventos que serão desenvolvidos.

QUADRO 2 – Cronograma de Pesquisa.

Atividade	2020		2021		
	Dez	Jan/Fev	Mar/Abr	Mai/Jul	Ago/Nov
Pesquisa bibliográfica e documental	X	X			
Especificação dos objetivos da pesquisa	X	X			
Operacionalização dos conceitos		X			
Redação do relatório inicial		X			
Qualificação do projeto pesquisa			X (ABR)		
Revisão da estratégia para o levantamento de dados			X (MAR)		
Coleta de dados			X (ABR)	X (MAY)	
Análise e Consolidação dos dados			X (ABR)	X (MAY)	
Revisão / Confecção dos capítulos				1 (MAY) 2 (JUN) 3 (JUL)	4 (AGO)
Redação do relatório final					X (SEP)
Qualificação					X (OUT)
Avaliação pela banca					X (NOV)
Depósito da Monografia					X (DEZ)

Fonte: Elaborado pelo autor.

8. REFERENCIAL TEÓRICO

A definição de um quadro teórico - referencial da pesquisa em função da natureza do problema de investigação, propõe um plano mínimo para a compreensão do fenômeno analisado para enquadrar as relações que surgem entre as variáveis associadas à pesquisa. Neste sentido, serão apresentadas as conceptualizações iniciais para a construção de uma perspectiva teórica que nos fornece de uma visão sobre o lugar onde se situa a abordagem proposta dentro do campo do conhecimento em que será desenvolvida" (HERNÁNDEZ-SAMPIERI, FERNÁNDEZ, & BAPTISTA, 2014, p. 92), bem como a importância dos conceitos na construção de teorias (BOWDISH, 2013, p. 23) e a posteriori, a relevância dos construtos como básicos unidades de pensamento (SARTORI, 2009, p. 13-43).

8.1 O CIBERESPAÇO, SUA EVOLUÇÃO E IMPORTÂNCIA POLÍTICA

Atualmente, o crescimento vertiginoso do uso das tecnologias de informação e comunicação estabelece um fenômeno sem precedentes onde o uso do ciberespaço constitui o meio pelo qual milhões de redes de computadores se entrelaçam para trocar inúmeros dados de informação instantaneamente. Não há dúvida de que o mundo atual está se transformando em um único ente altamente dependente das tecnologias presentes de forma transversal no cotidiano e nas relações dos Estados, estabelecendo um ambiente digitalizado e virtual que parece mais tangível e próximo, embora repleto de riscos e ameaças cuja real dimensão e alcance são desconhecidos.

Esta discussão apresenta multi-arestas e aqueles mais relevantes é que existe de facto um número crescente de ameaças cibernéticas, que se concentram na infraestrutura de informação civil, gerando a nível regional já em 2013 os países que registaram o maior número de ataques cibernéticos na América Latina foram Brasil, Argentina, Colômbia, México e Chile (PRANDINI & MARGIORE, 2013). Além disso, o acesso ou roubo de informações de um computador infectado, chamado de botnets, predominou na região. Até mesmo um tipo específico deste código malicioso chamado dorkbot gerou mais de 80 mil ações contra o sistema virtual, concentrando-se no Chile (44%), Peru (15%) e Argentina (11%) (BANCO INTERAMERICANO DE DESARROLLO, 2016). Nesse contexto, os tipos de ataques cibernéticos mais frequentes no país são roubo de identidade (phishing), malware e hacking de computador.

Mesmo assim, o relatório de Defesa digital do Microsoft em 2020 (MICROSOFT CORPORATION, 2020) forneceu de uma análise mais profunda de algumas das atividades observadas dos estados-nação, olhamos com frequência setores-alvo e as motivações dos atacantes. Neste sentido, dentro dos setores de alvos de ataques de hackers pode se observar que um 32% correspondem a organizações não - governamentais; 13% organizações governamentais; 7% empresas de desenvolvimento tecnológico; 7% Instituições educacionais; 31% serviços profissionais e 10% em organizações internacionais.

Segundo Caro (2010) e outros, o conceito do ciberespaço vem do termo “ciber”, que evoluiu a partir da obra de Norbert Wiener, que definiu o termo cibernética em seu livro «Controle e comunicação no animal e na máquina». A ideia de que os humanos podem interagir com as máquinas e que o sistema resultante fornece um ambiente alternativo para a interação forma a base do conceito de ciberespaço. (CARO, 2010, p. 48-82).

Após essa conceituação incipiente, existe um certo consenso quanto ao surgimento desse termo, como é o caso de alguns teóricos como Choucri (2012 p. 7); López (2012, p. 119-166) e Czege (2010, p. 85) quem apreciam que tenha sido utilizado pela primeira vez em 1982, na obra “Neuromancer” (GIBSON, 1991), definindo-a como “uma realidade virtual”, onde dados complexos são representados por símbolos, sendo complementado em “Uma Declaração da Independência do Ciberespaço” (PERRY BARLOW, 2021), estabelecendo um espaço virtual de interação, cujo objetivo é a comunicação, que se tornou uma referência atinente no tratamento do termo e seu impacto social desde o seu aparecimento.

A partir do exposto, inicia-se um progressivo desenvolvimento conceitual, sendo esse conceito relacionado ao surgimento de computadores e redes que utilizam um espaço virtual para interagir entre si, o que costuma ser denominado como “Internet”, embora na precisão de uso do termo não tinham significados semelhantes.

Mas, após o desenvolvimento tecnológico alcançado na década de 1990, essa relação entre a “internet” e o “ciberespaço” se acrescenta, ao estabelecer-se que ela constitui um nexo entre computadores, redes de telecomunicações e usuários, surgindo assim, um mundo virtual que se interconecta a milhões de usuários, cujo as redes são adequadas para a disseminação de inúmeras informações e, consequentemente, permitiriam o acesso ao controle e domínio da informação, o que valida o que foi afirmado por alguns autores, a respeito da evolução dessa concepção estará condicionada à abordagem de estudo, o tempo e o estado da tecnologia.

Portanto, esse progresso permanente do Ciberespaço pode ser consistente com as noções de Kuehl (2009) que manifesta:

> O Ciberespaço é o conjunto de um domínio global dentro do ambiente de informação cujo caráter único e distinto é dado pelo uso da eletrônica e do espectro eletromagnético criar, armazenar, modificar, trocar e explorar informação por meio de redes interdependentes e interconectadas usando tecnologias de informação e comunicação". (KUEHL, 2009, p. 26-28, tradução nossa).

Embora a definição possa cumprir a função de sintetizar o que está explanado nos parágrafos anteriores, é prudente mencionar que há pontos de vista opostos, como o de Gómez de Ágreda (2012) que questiona o excesso de peso tecnológico nesta abordagem já que não se específica de modo claro e concreto respeito o que e o espaço cibernético, bem como as implicações da sua existência e os efeitos das ações que nele ocorrem. (GÓMEZ DE ÁGREDA, 2012, p. 167-204).

Mesmo assim, o que foi discutido acima constitui uma aproximação às definições atuais que buscam responder a esse problema inicial, de forma que, ao revisá-las, pudesse ser estabelecida uma definição conceitual a ser utilizada nesta pesquisa. TODD (2009) argumenta que "a informação é o elemento central para a existência do Ciberespaço" (TODD, 2009, p. 64, tradução nossa) e, portanto, na atualidade, o domínio e controle desta dimensão, bem como a infraestrutura fornecida para seu propósito que é utilizada por diferentes usuários como governos, organizações e indivíduos, entre outros.

O exposto é demonstrado pela Publicação Conjunta 1-02 dos Estados Unidos, que indica que o ciberespaço é:

> A global domain within the information environment consisting of the interdependent network of IT Infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (UNITED STATES OF AMERICA, Department of Defense, 2010).

A seguir, a expressão é semelhante ao estabelecido pelo Estado-Maior da Defesa da Espanha em termos de estabelecer ao ciberespaço como: "Um domínio global e dinâmico dentro do ambiente de informação, composto por infraestrutura de rede, tecnologia da informação ... junto com seus usuários e operadoras". (FELIU, 2013, p. 4, tradução nossa).

Portanto, de uma perspectiva geral, as noções utilizadas permitem reafirmar uma tendência conceitual que visa estabelecer que o ciberespaço é um espaço onde existem vários recursos, razão pela qual os atores que incluem Estados, organizações, grupos ou indivíduos competirão para controlá-lo e isso vai gerar ameaças e riscos e, portanto, a eclosão de conflitos, como parte de uma contraposição de interesses.

Então, não é de se estranhar que o ciberespaço fosse declarado pelo "The Economist" (THE ECONOMIST REVIEW, 2010); a Junta Interamericana de Defensa (JID) (2020) e autores como Arreola (2020) e Castrillón-Riascos (2015) citado por Cornish (2011); como "quinto domínio" [4] depois da terra, do mar, do ar e do espaço. Pois durante a primeira década do século 21, apareceram novos paradigmas de ataque pelo ciberespaço, que se baseavam em diferentes modos de agressões, variadas motivações, tanto individuais como coletivas, bem como tipos de alvos que tentaram afetar instituições, governos e várias corporações empresariais.

Assim, Clarke, R. e R. Knake (2011) integra na sua argumentação que o "Cyberspace is now a warzone where many of the decisive battles of the 21st century will be fought". (Clarke, R. e R. Knake*,* 2011, p. 192) e por conseguinte, sugere uma visualização de ações coativas dos mais diversos tipos com uma participação dos Estados por assegurar seus objetivos neste ambiente.

Consequentemente, e dada a complementaridade que existe nas várias definições propostas, em relação ao ambiente que enquadra esta investigação, será entendido como ciberespaço em síntese: "O espaço virtual de carácter global e dinâmico dentro do ambiente de informação onde os sistemas informáticos interagir juntos a seus redes e infraestruturas associadas, para além da Internet; aquelas que utilizam meios físicos e o espectro eletromagnético para interligar e desempenhar as

[4] Para que um determinado ambiente seja considerado um domínio de operações, ele deve atender a seis critérios: 1. Requer recursos exclusivos para operar nessa área; 2. Não é totalmente englobado por qualquer outra área (terrestre, marítima, aérea, espacial). 3. É caracterizada por uma presença compartilhada de capacidades aliadas e adversárias. 4. É capaz de exercer controle sobre um oponente por meio de influência e domínio. 5. Oferece oportunidades de sinergia com outras áreas. 6. Oferece oportunidades assimétricas em todas as áreas. (JID, 2020, p.23).

funções de processamento, armazenamento e difusão de informação, tornando-se, em conjunto com outras, uma dimensão a proteger, usar, controlar e dominar a traves de políticas, ações o atividades desenvolvidas por um Estado, qualquer outra organização ou as pessoas".

Em seguida, a crescente dependência das sociedades dos sistemas de informação que utilizam o ciberespaço irá provocar que qualquer intrusão, manipulação, sabotagem ou interrupção de aqueles ou as redes de infraestruturas que os suportam terão efeitos direitos sobre o funcionamento da vida das pessoas, organizações e os Estados.

Nesse contexto, as ameaças adquirem especial relevância e, portanto, sua definição é necessária. Segundo Feliu (2013) é: "A percepção da capacidade de um potencial adversário possui para infligir dano ou detrimento, especialmente se não se atua como ele deseja". (FELIU, 2013, p.40, tradução nossa)

No entanto, essa expressão inicial pode ser insuficiente, o que em parte é resolvido por Buennemeyer (2011) ao fornecer uma definição que consegue relacionar Ciberespaço e ameaça, estabelecendo que:

> Attacks in cyberspace are fast and can simultaneously target an individual or a broad spectrum of systems. Attackers are often anonymous with few concerns regarding attribution. The instantaneous nature and the ability to attack the entire domain simultaneously make cyberspace potentially a much more dangerous and vulnerable environment for the unprepared than the traditional warfighting domains. (BUENNEMEYER, 2011, p. 45)

Da análise desta expressão, pode-se deduzir que há uma caracterização do ciberespaço e de seu entorno, bem como das atividades que devem ser realizadas para evitar que seja afetado por ameaças, o que contemplará uma série de ações destinadas a impedir a divulgação de informações, dados virtuais a pessoas ou sistemas não autorizados, entre outros.

Assim, o desenvolvimento do ciberespaço Segundo Gonzalez (2010) tem facilitado abundantemente a promoção de todos os tipos de atividades, incluindo interações comerciais, sociais e governamentais, constituindo uma dimensão

importante para os Estados, organizações e indivíduos e, consequentemente, a segurança do ciberespaço tem crescido em importância diante das ameaças (GONZÁLEZ, 2010, p. 85-120).

Por outro lado, Acosta (2009) argumenta:

> Como a sociedade atual depende amplamente da tecnologia da informação (TI), isso leva ao surgimento de novas ameaças desconhecidas no passado. Devido à natureza global das redes, os incidentes de segurança de TI que as afetam podem causar interrupções permanentes ou falhas na infraestrutura de informação do país. (ACOSTA, 2009, p.33, tradução nossa).

A citação anterior revela a ligação entre as informações que circulam pelas redes a respeito das ameaças potenciais neste cenário virtual, que, associando-as ao ambiente em que se originam, será denominado: “Ameaças cibernéticas”.

Gonzalez (2010) argumenta que o conceito de ameaças cibernéticas será constituído por ataques perpetrados ou patrocinados por Estados (ataques a infraestruturas críticas), ataques cometidos por grupos terroristas ou por qualquer outra manifestação de extremismo, seja político, ideológico ou religioso. Neste contexto, existem os ataques de crime organizado denominados “Cibercrimes” e, enfim, os ataques discretos, que pela sua natureza muito heterogénea, atingem as pessoas de forma transversal, desde a intrusão em informação pessoal até fraudes de diferente jeito. (GONZALEZ, 2010, p. 93).

Nesse sentido, essa perspectiva já está estipulada nas Tendências Estratégicas Globais do Ministério da Defesa da Grã-Bretanha para o ano de 2050 publicado em 2014, onde se aprecia uma declaração sobre o assunto e que norteia uma visão estratégica nesta política setorial, ao estabelecer: “There could also be an increasing threat of cyber attack from criminals and terrorists as information, communications and critical national infrastructure become more integrated”. (UNITED KINGDOM, Ministry of Defence, 2018).

Contudo, Choucri (2012) manifesta que nas diferentes interações no ciberespaço para os Estados tem criado condições sem claras prescrições sobre as ações relacionadas com a soberania dos Estados, estabilidade e Segurança.

Em suma, o ciberespaço é a expressão de um espaço virtual e vital para a transmissão de informações, razão pela qual se desenvolverão sucessivas ações dos mais diversos tipos para afiançar seu uso, exercer o controle e a proteção das redes de computadores, ocasionando a necessidade de garantir a funcionamento desses sistemas contra várias ameaças, definidas como ameaças cibernéticas, cujos efeitos se sobrepõem do virtual ao físico, gerando consequências múltiplas e insuspeitadas nos Estados e seus habitantes que afetam os direitos das pessoas, as infraestruturas críticas de informação e, portanto, em nível local, os interesses vitais dos países.

8.2 A SEGURANÇA CIBERNÉTICA E A QUESTÃO POLÍTICA - ESTRATÉGICA

Segundo Reardon & Chocri (2012) é razoável esperar que o desenvolvimento do ciberespaço, devido à sua crescente relevância para um número cada vez maior de atividades sociais e políticas, comece a exercer influência no curso da política global. Da mesma forma, as significativas mudanças no ciberespaço terem tido um efeito transformador na política internacional, particularmente com respeito ao empoderamento de grupos anteriormente marginalizados; e a relação dependente entre política internacional e mudança tecnológica. (REARDON & CHOUCRI, 2012, p. 26 apud MANJIKIAN, 2010)

Daí o rápido crescimento da atividade social no ciberespaço e sua crescente importância das múltiplas relações nesse domínio tenha impacto sobre a segurança internacional, a economia global, as organizações políticas e o desenvolvimento social.

Deste modo, a evolução do panorama internacional trouxe consigo, nas últimas duas décadas, o aumento da proeminência do domínio cibernético[5] em todas as expressões do Poder Nacional.

[5] A definição do espaço cibernético como domínio operacional foi adotada pela OTAN em junho de 2016. O secretário geral da OTAN, Jens Stoltenberg, disse que a aliança ocidental decidiu designar o ciberespaço como um domínio operacional, tais como o são a terra, mar, ar e o espaço. Disponível em https://www.nato.int/cps/en/natohq/events_132234.htm.

Como resultado, as ações cibernéticas destinam-se a múltiplos propósitos: servem para a asserção de uma superioridade relativa sobre outros Estados, como uma forma de desafiar e equilibrar a balança de poder no nível mundial para países que tem amplas aspirações geopolíticas ou constituem oportunidades de causar grande prejuízo aos seus oponentes a relativo baixo custo, entre outras.

Segundo Castrillón-Riascos (2015) o advento dessa revolução tecnológica teve uma consequência comum a todos os Estados. De uma forma ou de outra, em grau maior ou menor, todos estamos envolvidos em uma “Ciberguerra”, seja por ações de outros Estados-Nação ou de criminosos comuns, as pessoas e governos encontram cada vez mais riscos à sua segurança digital (CASTRILLÓN-RIASCOS, 2015).

Nesse contexto, desde 2017, pode-se notar um crescente número de ciberataques a órgãos governamentais. Em 2019, os governos foram o terceiro maior alvo de ciberataques no mundo (FIREEYE, 2020).

Devido a isso, segundo a União internacional de telecomunicações (UIT) a Segurança Cibernética se apresenta como uma série de ferramentas para proteger os ativos e usuários de organizações no ambiente cibernético desde os Estados até às pessoas.

> A Segurança cibernética é o conjunto de ferramentas, políticas, conceitos de segurança, salvaguardas de segurança, diretrizes, métodos de gestão de risco, ações, treinamento, melhores práticas, seguros e tecnologias que podem ser usadas para proteger ativos da organização e usuários no ambiente cibernético. Ativos e usuários da organização são dispositivos de computação conectados, usuários, serviços / aplicativos, sistemas de comunicação, comunicações multimídia e todos das informações transmitidas e / ou armazenadas no ambiente cibernético. (UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (UIT), 2010, tradução nossa).

Além disso, apresenta-se como conceito transversal e multifatorial, garantindo que a sua manutenção, em face dos riscos presentes no ciberespaço, seja mantida a partir da estrutura política de um país e, portanto, não venha a

comprometer os direitos das pessoas, segurança pública, infraestrutura crítica e os interesses essenciais de um Estado.

Newmeyer (2015) argumenta que o objetivo de uma estratégia nacional de segurança cibernética “é alinhar todos os esforços do governo para alcançar ou melhorar a segurança cibernética”. Daquele modo as estratégias eficazes definem os “parâmetros para a cooperação do setor público-privado e coordenação dos esforços de segurança cibernética, bem como fornecem uma indicação clara das intenções do país para outros países e partes interessadas”. (NEWMEYER, 2015, p. 10 apud LUIIJF et al., 2013). Porém, “A alocação de responsabilidades de segurança cibernética varia entre os governos” (NEWMEYER, 2015, p. 13, tradução nossa).

Sob esta perspectiva, a Segurança Cibernética garante que as propriedades de segurança das informações da organização e dos usuários são alcançadas e mantidas contra os riscos de segurança correspondentes no ciberespaço desde os níveis superiores de um Estado e, portanto, afeta um amplo espectro de dimensões deste, tais como: política, social, econômica, defesa, entre outras.

Caro (2010) estabelece uma relação entre o ciberespaço e a Segurança nacional, já que argumenta a “segurança do ciberespaço é um objetivo estratégico para a segurança nacional”. (CARO, 2010, p. 76). Além do mais, a “Cybersecurity is now a national security issue that can impact the lives of individuals citizens every day” (NEWMEYER, 2015, p. 10 apud KLIMBERG, 2012). A vista disso, a formulação de estratégias nacionais de segurança cibernética decorre em abordagens que estabelecem um paradigma tradicional do Estado na proteção das fronteiras e de garantia do Estado de direito (NEWMEYER, 2015, p. 10 apud HARKNETT e STEVER, 2009), bem como, em um sentido de proteção sob uma responsabilidade estatal no contexto amplo da Segurança, Reardon & Chocri (2012) estabelece: “That large-scale strategic attacks through cyberspace against “critical infrastructure” pose a grave threat to national security” (REARDON & CHOUCRI, 2012, p. 22 apud CLARKE, 2009; LYNN, 2010; WESLEY K. AND LEVIN, 2010).

A seguir, Newmeyer (2015) reflexa sobre os paradigmas da Segurança cibernética: “A ênfase da segurança nacional na estratégia e na doutrina da segurança cibernética à necessidade de proteger a infraestrutura crítica e à importância dos sistemas públicos e privados nas operações governamentais”. (NEWMEYER, 2015, p. 10 apud AGRESTI, 2010, tradução nossa).

Reardon & Chocri (2012) apresenta uma abordagem que caracteriza à "segurança cibernética": “A term originally reserved for the technical integrity of networks, became a matter of national security and high politics” (REARDON & CHOUCRI, 2012, p. 24 apud HANSEN e NISSENBAUM, 2009).

Desta forma, a Segurança cibernética abrange desde acima das estruturas superiores de um país até os níveis mais baixos conformados pelos usuários das redes, demandando ao Estado uma série de ações que permitam o uso do ciberespaço a traves da definição de políticas, como o caso dos EUA quem se expressa através de seu Departamento de Segurança Interna: “In light of the risk and potential consequences of cyber events, strengthening the security and resilience of cyberspace has become an important homeland security mission” (UNITED STATES OF AMERICA, s.d.).

Por outro lado, a dimensão militar não fica imune às essas ameaças, ao contrário, estão se tornando cada vez mais prováveis, a execução de operações militares de um Estado em relação a outro, a fim de explorar e atacar para obter informações, determinar vulnerabilidades críticas e afetar as capacidades da infraestrutura militar, tais como as sucedidas na Estônia em 2007, na Geórgia em 2008, Ucrânia em 2013 (CONELL & VOGLER, 2016). Também, nos ataques deliberados sobre a estrutura informática dos Estados Unidos por parte da China que incluíam as agências governamentais e corporações em setores da infraestrutura crítica nacional, como financeiro, defesa, tecnologia da informação, transporte e saúde como parte dos prováveis alvos (THEOHARY & HARRINGTON, 2015).

Neste sentido, a Agência de Segurança Cibernética e Infraestrutura dos EUA estabelece a Segurança cibernética: “A Segurança cibernética é a arte de proteger redes, dispositivos e dados contra acesso não autorizado ou uso criminoso e a prática de garantir a confidencialidade, integridade e disponibilidade de informações” (SECURITY, s.d., tradução nossa).

Sob as perspectivas acima mencionadas, todas as ações que forem realizadas com o objetivo de proteger a estrutura de TI a nível nacional respeito às ameaças já ocorridas no ciberespaço estarão inseridas na concepção da Segurança cibernética. Assim, “La ciberseguridad se centra en la protección y recuperación de los sistemas TIC propios”. (JUNTA INTERAMERICANA DE DEFENSA, 2020, p. 41).

Choucri (2012) argumenta que surgem novos desafios para a Segurança Nacional, de fontes de vulnerabilidade sem precedentes, novas dimensões de segurança nacional combinadas com incerteza, medo e ameaças de fontes desconhecidas, ainda assim, a criação de ciberespaço propor oportunidades para o desenvolvimento de políticas para as novas oportunidades e desafios.

Do mesmo modo, em relação a um cenário prospectivo incerto, a incorporação da concepção da Segurança Cibernética de acordo aos preceitos gerais dos Estados, promove a integração do conhecimento como uma forma de mitigar ameaças. Com tal característica, a JID expõe que a segurança cibernética internacional se baseia fundamentalmente na cooperação entre os órgãos responsáveis por cada um dos pilares da segurança cibernética nacional com seus homólogos em outros países e organizações internacionais através de diferentes convenções (JUNTA INTERAMERICANA DE DEFENSA, 2020, p. 87).

Contudo, no âmbito de nossa região, o reporte de Segurança Cibernética 2020 do “Banco Interamericano de Desenvolvimento” pôs em evidência que na Região da América Latina e o Caribe ainda não está suficientemente preparada para afrontar os ataques que são produzidos no ciberespaço. Apenas sete países dos trinta e dos analisados no reporte possuem um plano de proteção de sua

infraestrutura crítica e só vinte tem implementado algum tipo da equipe de resposta a incidentes, então a situação limita a capacidade para identificar ataques e os respondê-los oportunamente. (BANCO INTERAMERICANO DE DESARROLLO, 2020)

Neste novo cenário, segundo Paz y Paz (2017) a Organização dos Estados Americanos (OEA), em seu carácter de foro político hemisférico, através da Secretaria de Segurança Multidimensional, promove e coordena a cooperação entre os Estados membros da organização para avaliar, prevenir, enfrentar e responder efetivamente nas novas ameaças à Segurança regional. Assim, durante 2017 os governos de Chile e Paraguai adotaram os respectivos Planos de Segurança cibernética. Ambos se uniram a países como Colômbia, Trinidad e Tobago, Panamá e Jamaica que de acordo a OEA tem fornecido apoio técnico do "Programa de Segurança cibernética do Comité Interamericano Contra o terrorismo da OEA" (ORGANIZACIÓN DE LOS ESTADOS AMERICANOS, 2017).

Desse momento, Chile possui uma Política Nacional de Segurança Cibernética (PNCS) e definiu seu conceito de Segurança cibernética:

> A Segurança cibernética é uma condição caracterizada por um mínimo de riscos para o ciberespaço, entendido como o conjunto de infraestruturas físicas e lógicas e interações humanas que nesse lugar acontecem. Neste sentido, e seguindo os padrões internacionais, os principais atributos para proteger são a confidencialidade, integridade e disponibilidade das informações, o que por sua vez geram um Ciberespaço robusto e resiliente (CHILE, Govierno de Chile, 2017) (Tradução nossa).

Mas também, evidencia-se uma preocupação do Estado chileno no emprego das capacidades do Ministério da Defesa não restrito só com a perspectiva de Segurança exterior no âmbito das ameaças estatais clássicas, senão assumem uma responsabilidade de contribuição nas relações internacionais, principalmente em duas áreas: cooperação e assistência. Nesse sentido, as ações estratégicas desenvolvidas pela Defesa Nacional e de suas instituições que o compõe, têm um eixo de ação orientado à cooperação internacional, promoção da transparência e confiança entre os estados derivados da natureza transfronteiriça e características dos riscos e ameaças. (CHILE, Govierno de Chile, 2018).

Enfim, segundo Barmpaliou (2020) a Segurança cibernética constitui uma “Un asunto transversal en la política nacional”, (BANCO INTERAMERICANO DE DESARROLLO, 2020, p. 28-32) devido a que a presença dos sistemas digitais estão presentes em todas as áreas de atividade humana, evidenciando-se níveis sem precedentes de inovação tecnológica e interdependência.

Finalmente, a Segurança cibernética não pode analisado desde uma perspectiva isolada, como um assunto técnico ou uma área de política Independiente. A segurança cibernética se localiza na intersecção de múltiplas disciplinas e áreas políticas: acesso digital e conectividade, resiliência, justiça criminal, diplomacia, segurança e defesa internacional e economia e comércio digital, bem como novas tecnologias (BANCO INTERAMERICANO DE DESARROLLO, 2020, p. 28-32) e, portanto, deve ser abordada desde uma perspectiva ampla.

8.3 A COOPERAÇÃO EM DEFESA E OS EFEITOS DA INTERAÇÃO NO CIBERESPAÇO

O conceito da “Cooperação internacional” foi discutido em forma aprofundada por diferentes teóricos, dentro dos quais estiveram engajados neorrealistas e institucionalistas neoliberais durante boa parte das décadas de 1980 e 1990 (TEIXEIRA JÚNIOR, 2013).

Morgenthau (2003) entende que só o poder político será o meio de alcançar os objetivos da Nação. Assim, a política internacional como toda política, consiste em uma “luta pelo poder” (MORGENTHAU, 2003, p. 49). Assim, sempre os fins da política internacional, independente de seus objetivos em termos de procurar um ideal religioso, filosófico, econômico ou social serão o poder.

Dentro da prática da política externa, Morgenthau (1962) ponderava sobre a controvérsia respeito da compreensão e ação da ajuda externa, como um instrumento da política (MORGENTHAU, 1962, p. 301). Sendo assim, Milani (2020) argumenta:

> As visões sobre a ajuda externa variam em um amplo espectro político desde a concepção de que a cooperação seria um fim em si mesmo, justificável do ponto de vista da moral e, portanto, de forma independente da política externa dos Estados, até, no outro extremo, seus opositores ferrenhos, segundo os quais ela não seria passível de justificação política, haja vista que não serviria nem aos interesses do Estado-doador, nem aos dos países beneficiários. (MILANI, 2020, p. 86).

Logo, segundo Milani (2020) reconhecendo a diversidade das políticas existentes, identifica seis tipos de ajuda externa, sendo que todas dizem respeito à transferência de fundos financeiros, bens e serviços de uma Nação para outra: (i) ajuda humanitária; (ii) ajuda para a subsistência; (iii) ajuda militar; (iv) ajuda-suborno (bribery); (v) ajuda para obter prestígio; (vi) ajuda externa para o desenvolvimento econômico (MILANI, 2020, p. 86 apud MORGENTHAU, 1962).

Contudo, segundo Morgenthau (1962) a dimensão da ajuda externa necessária em termos de tipo e quantidade para ser fornecida desde um Estado dador a outro receptor para alcançar o resultado desejado exige:

> Um conhecimento profundo e uma compreensão da situação total de um determinado país. É necessário antecipar a receptividade do país aos diferentes tipos de ajuda externa e seus efeitos sobre ela. É então necessário selecionar, de diversas medidas possíveis de ajuda externa, aquelas que são mais adequadas à situação e, portanto, com maior probabilidade de sucesso". (MORGENTHAU, 1962, p. 308, tradução nossa).

Certamente, as características inerentes do ciberespaço relacionado às relações internacionais na sua forma mais realista, não são capazes de explicar o comportamento dos Estados e outros atores em sua interação neste espaço virtual.

Por outro lado, Teixeira Júnior (2013) argumenta que a cooperação interestatal seria temporária e fadada à dissolução em virtude dos riscos de defecção e da vantagem estratégica adquirida por possíveis contendores (TEIXERA JÚNIOR, 2013, p. 48-49 apud GRIECO, 1993; MEARSHEIMER, 1994; WALTZ, 2000, 2002), não obstante as dificuldades, existe uma "visão otimista" já que se observa ao verificar a existência da premissa "que os agentes (indivíduos, Estados) são racionais e, portanto, capazes de cooperar". (MILANI, 2020, p. 82).

Segundo Morgenthau (2003) dessa apreciação da política internacional decorrem duas conclusões: “A primeira, nem toda ação que um país desenvolva com respeito a outro será de natureza política; a segunda: nem todas as nações estão o tempo todo, em maior ou menor grau, engajadas em atividades de política internacional” (MORGENTHAU, 2003, p. 49-50).

Milani (2020) argumenta que os projetos de cooperação internacional seriam o resultado da falta de capital, de tecnologia e de conhecimento, ou seja, ele seria um acidente de percurso ou uma deficiência e poderia ser superado a partir da injeção dos ingredientes ausentes no contexto nacional. (MILANI, 2020, p. 87). Como se pode ver, esses projetos puderem incorporar-se a aqueles de “nova geração” como o ciberespaço, que surgem de carências de recursos financeiros, de falta de desenvolvimento tecnológico e de conhecimento, entre outras, e, portanto, requerem de uma estreita colaboração entre os Estados que estão dispostos em melhorar a situação descrita através do entendimento e apoio.

Moravcsik (1997) explica como a partir da construção das relações do Estado com a sociedade, as quais estão condicionadas pelas diferentes perspectivas internas e externas no contexto social em que estão inseridos, têm um impacto fundamental no comportamento estatal na política mundial. Assim, as Ideias, interesses e instituições sociais influenciam o comportamento do Estado vão conformando as preferências do Estado, ou seja, os propósitos sociais fundamentais subjacentes guiam aos cálculos estratégicos de governos.

Vale observar que Bull (2002) aporta uma visão complementaria e colabora na compreensão das influências das políticas desenvolvidas por os Estados no âmbito internacional, além de uma posição “Estado centrista”. Estabelece que: “existe uma "sociedade de estados" (ou "sociedade internacional") quando uns grupos de estados, conscientes de certos valores e interesses comuns, formam uma sociedade, no sentido de se considerarem ligados, no seu relacionamento, por um conjunto comum de regras, e participam de instituições comuns” (BULL, 2002, p. 19).

Evidentemente, segundo o Bull (2002) o conceito de uma sociedade pressupõe a existência de um sistema. Neste, as unidades (Estados) produzem relacionamentos mútuos sem, no entanto, terem a concepção de que existem certos valores e interesses compartilhados que são imprescindíveis para a existência de uma sociedade internacional nos termos descritos.

Milani (2020) identifica no Liberalismo institucional alguns ganhos presentes na colaboração externa para os Estados: (i) redução dos custos de transação para negociar e manter acordos; (ii) estabelecimento do ideal da reciprocidade e do princípio da previsibilidade; (iii) circulação de informação para tornar as preferências mais transparentes; (iv) definição de padrões de comportamento e institucionalização de mecanismos de sanção, além da obtenção de vantagens coletivas, os quais podem ser deduzidos das expressões inseridas dentro da política pública com foco no exterior (MILANI, 2020, p. 82).

Por outro lado, Milani (2020) expressa que “a existência de eventuais dificuldades políticas de cooperação (assimetrias, interesses, relações de poder), alguns liberais enfatizaram que a cooperação internacional seria possível em campos técnicos, a exemplo da cooperação em saúde, educação ou desenvolvimento de infraestruturas (MILANI, 2020, p. 82-83), estabelecendo uma figura teórica nomeada de “Cooperação funcional”.

Em seguida, Bull (2002) adiciona que após a “unificação tecnológica do mundo” existiram maiores oportunidades para a integração regional e global, argumentando que isto: “São fatos pouco compatíveis com a teoria clássica da política mundial que focaliza as relações entre os estados”, por tanto, as teorias que pressupõem no foco no Estado seriam insuficientes para dar uma resposta para o atual cenário internacional. Desta forma, Bull comenta: “Nenhuma visão do futuro será realista se não levar em conta a existência de uma interação social, econômica, diplomática e estratégica em escala global”. (BULL, 2002, p. 293).

Castrillón-Riascos (2015) justifica a cooperação entre os Estados devido as características que se manifestam em um espaço virtual como o ciberespaço sem

soberanias efetivas dos Estados e pelos fenômenos que aí se originam (crimes transnacionais, afetação de infraestrutura crítica, entre outros), os quais representam uma ameaça de difícil controle por um Estado no mundo tangível sem a presença de alianças estratégicas e grupos colaborativos tanto nacional como internacionalmente.

> As consequências em termos de distribuição (abrangência das ações além das fronteiras nacionais) e dada a interdependência econômica no sistema internacional e a existência de jurisdições nacionais, cria um interesse comum e incentiva é o início para o desenvolvimento cooperação entre Estados. (CASTRILLÓN-RIASCOS, 2015, p. 120 apud KEOHANE, 1984).

Em particular, ao lado dos processos cooperativos e de interação política nos planos Hemisférico e Regional, as ações de cooperação entre Estados com escopo ao fator militar poderiam se fortalecer a partir das diferentes mudanças nas relações internacionais dos EUA com a região no novo milênio.

> Segundo Buzan e Waever (2003), a mudança do relacionamento com os EUA tem mais a ver com a mudança das próprias prioridades estadunidenses. Com a priorização dos EUA para outras regiões, a política do dividir para governar acaba sendo desvanecida, e os Estados Unidos acabam servindo como pretexto para a cooperação dos países sul-americanos. (FUCCILLE & REZENDE, 2013, p. 82)

Segundo Pereira Rezende (2015) afirma que: “Desde que associados à política externa, arranjos cooperativos em segurança podem contribuir para os objetivos de segurança e estratégicos dos Estados”. (PEREIRA REZENDE, 2015, p. 527 apud MUTHANNA, 2006).

Para mais, Choucri (2012) disse que a “construction of cyberspace creates new complexities for international” (CHOUCRI, 2012, p. 155), neste argumento, novas questões internacionais exigirão de um importante gerenciamento já que novos grupos que estão surgindo, têm novas demandas e disposições diferentes frente os âmbitos de conflito e colaboração. Então, podemos estabelecer que a política exterior dos Estados no âmbito do ciberespaço deverá ser abalizada de acordo com os fundamentos do Milano (2020):

> A política externa reflete não apenas os constrangimentos sistêmicos, provenientes da própria estrutura da ordem internacional, mas também, e

> principalmente, as estratégias estabelecidas pelos atores domésticos no contexto da distribuição de interesses e preferências no interior do Estado. (MILANI, 2020, p. 89 apud LIMA, 2000)

Dado isso, se os Estados incorporam nos processos de formulação de suas políticas a avaliação desses fatores, consequentemente, as decisões neste âmbito contribuirão para conseguir uma estabilidade cibernética global baseada no desenvolvimento de capacidades regionais e nacionais de todos os países para prevenir e reagir frente ante incidentes cibernéticos (BANCO INTERAMERICANO DE DESARROLLO, 2020, p. 23-26).

Por causa disso, segundo Herczynski (2020) a natureza global da ameaça e os desafios que representa para os Estados, no contexto da "Diplomacia cibernética", fomentará a construção e incremento de alianças fortes e parcerias com terceiros países para a prevenção e dissuasão de ataques cibernéticos, que são cada vez mais importante para a estabilidade e segurança internacional. Assim frente ao incremento das ameaças e seus potenciais efeitos no ciberespaço de entorno global, regional e local surge como um bem público a segurança coletiva em termos de proteger as interações e direitos no ciberespaço onde convivem os Estados e os indivíduos (BANCO INTERAMERICANO DE DESARROLLO, 2020) . Deste modo surge como um imperativo para os Estados a necessidade de cooperar. Neste sentido, segundo Choucri (2012) a escolha política de cooperar justifica-se:

> In general, countries collaborate either (1) in the pursuit of common interests or (2) in the management of common aversions. In the first instance, states seek to collaborate as a way to pursue jointly some objective they might not be able to attain individually. In the second, collaboration is driven by the recognition that states face shared adverse conditions that require coordinated action for the most effective management. (CHOUCRI, 2012, p.156)

Contudo, Barmpaliou (2020) nos adverte respeito das tensões existentes ao redor dos valores de governança de uma Internet "aberta e descentralizada", versus o foco em "Cibersoberania", mesmo o uso do ciberespaço como um ambiente para competição estratégica entre os Estados. Em seguida, agrega: "Essa polarização pode prejudicar a segurança no ciberespaço e a confiança para a cooperação global contra desafios comuns de segurança cibernética". (BANCO

INTERAMERICANO DE DESARROLLO, 2020, p. 31, tradução nossa). Apesar disso, Nye (2010) argumenta que o ciberespaço não reduzirá a soberania estatal, mas a difusão do poder no ciberespaço gerará complicações no relacionado com o exercício de poder neste ambiente (NYE, 2010, p. 3).

Não obstante, Barmpaliou (2020) faz um destaque da importância que as organizações regionais têm na promoção da estabilidade regional, segurança e esforços para construir confiança no ciberespaço através de medidas de geração de segurança, ratificando-se a importância da contribuição interestatal com foco na cooperação internacional no âmbito do ciberespaço.

Segundo Choucri (2012) a lógica da cooperação internacional estabelece certos efeitos sobre os Estados. Nos aspeitos favoráveis, os países podem determinar suas preferências e objetivos específicos em relação a suas vulnerabilidades e percepções. Da natureza igual, os estados estabelecem as melhores condicionantes sob quais desenvolverão suas ações nas relações bilaterais. Por outro lado, “a colaboração impõe restrições à soberania nacional, tanto internas, esses devem se abster de realizar ações que tenham consequências nacionais negativas, quanto externas, esses devem se abster de gerar efeitos negativos para outros Estados”. (CHOUCRI, 2012, p. 156, tradução nossa).

Além disso, Newmeyer (2015) adiciona outro efeito sobre os estados, ao adicionar a importância de contar com quadros legais para detectar e prevenir os ilícitos que acontecem no ciberespaço, aspeito que contribui a cooperação internacional e a diminuição de crimes associados neste ambiente (NEWMEYER, 2015, p. 17).

Consequentemente o mesmo autor expressa que o elemento essencial é elaborar e implementar as respectivas estratégias nacionais com “altos níveis de eficácia de segurança cibernética para aumentar as chances de sucesso nos objetivos que contenha” (NEWMEYER, 2015, p. 18), de modo que os governos possam responder eficientemente aos problemas gerados pela “interdependência

complexa” e, nesse sentido, produzir bens públicos globais ou regionais (MILANI, 2020, p. 82) que pudesse ter escopo aos assuntos como a mitigação de riscos e ameaças que têm incidência sobre a segurança cibernética.

Neste sentido, o Chile a partir da publicação da PNCS 2017 tal como já foi comentado, começou a elaboração de uma Política internacional para o ciberespaço, ainda não terminada, onde se estabeleceu como objetivos de alto nível desta política um estreito alinhamento com a cooperação e as relações internacionais em torno da Segurança cibernética no contexto global. (CHILE, Govierno de Chile, 2017).

Por esse motivo para facilitar seu atingimento os Estados empregaram recursos não tão somente políticos, justificando-se o emprego da cooperação militar, “Fundamentalmente porque a política externa e suas agendas de cooperação para o desenvolvimento estão cada vez mais conectadas às demais políticas públicas” (MILANI, 2020, p. 88). Como resultado, será necessário avançar no desenvolvimento de forças cibernéticas nacionais capazes de atuar neste novo ambiente individual e coletivamente em defesa dos objetivos comuns (JUNTA INTERAMERICANA DE DEFENSA, 2020).

Assim, segundo Abdul-Hak (2013) a cooperação em defesa consiste “na coordenação e no ajuste recíproco das políticas de dois ou mais Estados com relação à ameaça, ao uso e ao controle da força nas relações interestatais” (ABDUL-HAK, 2013, p. 25 apud TAMS, 1999, KEOHANE, 1988). Pressupõe que a abrangência das ações de cooperação pode ocorrer entre países que não nutrem relações de antagonismo entre si, mas também pode ocorrer entre rivais e como “collaboration between conflictuous parties”, (TEIXEIRA JÚNIOR, 2013, p. 47-48 apud MÜLLER, 2003).

Então, as relações de cooperação e colaboração no âmbito militar com outros Estados estão orientadas aos cumprimentos de preceitos de tipo político –

estratégico com ênfases sobre ações de Segurança e Defesa[6]. No entanto, Saint Pierre (2011), Abdul-Hak (2013) argumentam que a colaboração em Defesa possui um escopo mais restrito do que a cooperação em segurança, pois a segurança abrange tanto aspectos militares quanto não militares e portanto, a segurança tem uma maior abrangência conceitual e da resposta a questões mais amplas. Então, segundo Pereira Rezende (2015) a cooperação em defesa "inclui os ministérios de defesa, agências associadas e as FA de diferentes Estados, incluindo, mais especificamente, a questão da cooperação militar" (PEREIRA REZENDE, 2015, p. 524).

Além disso, é interessante destacar os aportes de Pereira Rezende (2015) que argumenta em relação dos ganhos da cooperação militar para os estados:

> Pode servir para melhorar a posição estratégica dos Estados de segunda linha frente à potência unipolar sem terem que gastar tanto. Uma vez que o balanceamento não é possível sob a unipolaridade, as parcerias estratégicas são uma forma de alinhamento que contribui para a melhoria da posição estratégica dos seus participantes, aumentando a sua capacidade de sobrevivência via a melhor forma possível de maximização de seus recursos. (PEREIRA REZENDE, 2015, p. 527)

Desse ponto, segundo Abdul-Hak (2013) as modalidades de cooperação incluem exercícios combinados, capacitação de recursos humanos, o desenvolvimento de tecnologia militar e intercambio de inteligência. Mesmo assim, não apenas tem uma finalidade meramente "técnica", mas também, contribui a ação política do Estado em termos de gerar confiança e consolidar as relações entre os participantes, além de "ser um valioso instrumento diplomático, inclusive com efeitos demonstrativos e até dissuasórios para terceiros Estados" (ABDUL-HAK, 2013, p. 26 apud MORAES, 2010).

Além disso, segundo JID (2020) para alcançar uma cooperação internacional sólida da Defesa no ambiente do ciberespaço, é necessário estabelecer acordos

[6] Segundo JID, 2020, para cumprir sua missão de proteger os interesses nacionais, as FA de um país devem ter a capacidade de enfrentar a ameaça onde quer que ela ocorra, seja em terra, no mar, ar, espaço ou ciberespaço. Para isso, devem ter capacidades militares adequadas para lutar em todas as áreas de operação, adaptadas à natureza da área, treinados e preparados para serem usados quando e onde forem necessários e devidamente organizados para realizar suas atividades, funções e operações em coordenação com as demais áreas.

bilaterais com outras forças que utilizam o ciberespaço no ambiente geoestratégico e participar ativamente nos acordos de defesa cibernética coletiva das diferentes alianças multilaterais. De tal forma que, é necessário, em primeiro lugar, criar ambientes de confiança mútua que facilitem uma troca equilibrada de informações para evitar desbalanços em termos de quantidade e qualidade das informações recebidas versus as informações oferecidas. (JUNTA INTERAMERICANA DE DEFENSA, 2020, p. 55)

Como consequência, alguns autores ratificam que umas das maneiras de colaboração no ciberespaço estão baseadas no âmbito da Defensa cibernética. Segundo SANCHO (2020) é explicada: “como el conjunto de capacidades disponibles, relacionándolo directamente con la fuerza o lo estratégico militar” (SANCHO, 2020, p. 64). Igualmente, a JID (2020), o define como: “Capacidad organizada y preparada para combatir en el ciberespacio. Comprende actividades defensivas, ofensivas y de inteligencia”. (JUNTA INTERAMERICANA DE DEFENSA, 2020, p. 55)

Enfim, segundo Abdul-Hak (2013) e como sínteses das diferentes abordagens apresentados devemos reconhecer que os processos de cooperação em defesa dependem das premissas formuladas por líderes políticos e militares sobre a natureza das relações interestatais, as perspectivas duradouras de paz ou de conflito, a possibilidade sistêmica de mitigação ou superação de rivalidades e a importância de instituições, regras, valores e interesses na distribuição de poder entre os atores da ordem internacional.

8.4 AS POLÍTICAS PÚBLICAS COMO ESPAÇO DE AÇÃO DO ESTADO.

O desenvolvimento e análise das diferentes políticas públicas é um elemento chave em uma sociedade civil. Segundo Meny e Thoenig (1992); Doña (2005) o conceito de Políticas Públicas evoluciona no campo das ciências políticas e administrativas nos Estados Unidos. Doña (2005) argumenta que uma primeira conceptualização de acordo ao contexto norte-americano está inserida na solução de problemas dentro de “uma dinâmica democrática e vinculada às etapas do processo decisório” (DOÑA, 2005, p. 34 apud LAHERA, 2002).

Logo, segundo Dona (2005) existe outro entendimento de acordo aos cientistas sociais que forneceram uma abordagem mais “científico” a partir de três enfoques teóricos:

> A teoria administrativa (onde o Estado e suas lógicas de funcionamento ganharam importância no tratamento da questão das políticas públicas); a sociografia dos grupos de pressão (para entender o que está relacionado com a construção das demandas da sociedade e as respostas das autoridades) e o determinismo dos grandes sistemas (isso está relacionado às matrizes político-ideológicas que de alguma forma condicionam o papel do Estado e da sociedade). (DOÑA, 2005, p. 32-35 apud MENY, Y THOENING, CLAUDE, 1992, tradução nossa)

Além disso, Segundo Meny e Thoenig (1992) considera as teorias da política em três grupos com base no papel atribuído ao Estado e à sociedade na produção da ação pública. O primeiro conjunto de teorias enfatiza o papel do indivíduo e dos grupos sociais e o modo como se edificam as demandas desde a sociedade para o Estado baseadas nas teorias pluralistas e racionalistas. O segundo conglomera abordagens que concebem o Estado como um instrumento, seja da classe social dominante (neomarxismo), seja de grupos específicos (neoweberianismo) para focar sua atenção nos funcionários do Estado e aqueles que controlam ao Estado. No terceiro se distingue por rejeitar os dois tipos de determinismos e se posicionar em um ponto intermediário, a partir do qual interpretam as políticas como representações de equilíbrios e desequilíbrios nas relações Estado-sociedade, surgem assim as teorias como neocorporativismo, neoinstitucionalismo e as perspectivas focadas nas comunidades, subsistemas e redes de políticas. (MENY & THOENING, 1992, p. 15-35).

Por otro lado, segundo Doña (2005):

> O estudo das políticas públicas não seria outra cosa que o estudo da ação das autoridades nas atividades da sociedade, ou seja, um estudo do que os governantes produzem em relação aos resultados que eles esperam e pelos meios que possuem. (DOÑA, 2005, p. 32 apud MENY, Y THOENING, CLAUDE, 1992, tradução nossa)

Contudo, segundo Lahera (2004) estabelece que:

> Apesar da frequência de uso do conceito de políticas públicas, existem diferenças significativas ou imprecisões a partir das quais mal-entendidos analíticos e dificuldades podem surgir operacional. [...] Frequentemente a definição de políticas público é disputado. Em última análise, é uma questão de quem "Engloba" quem. (LAHERA, 2004, p. 13, 18, tradução nossa)

Assim, existem diferentes abordagens e elementos constitutivos destas que dificultam sua conceptualização e sua utilização. De acordo aos requerimentos teóricos iniciais que se precisam para nossa pesquisa, as políticas públicas segundo Lahera (2004) são: “cursos de ação e fluxos de informação relacionados a um objetivo público definido democraticamente; aquelas que são desenvolvidas pelo setor público e, frequentemente, com a participação da comunidade e do setor privado” (LAHERA, 2004, p. 8, tradução nossa).

Neste contexto, Segundo Lahera (2004) esta definição vai mais além de um conceito tradicional que considera como o resultado de uma autoridade investida de poder público e legitimidade governamental. (LAHERA, 2004, p. 13-16)

Não obstante, segundo Meny & Thoening (1992) argumenta que:

> “Cada vez mais os estudos de políticas públicas têm destacado a importância das instituições do Estado como organizações por meio das quais os agentes públicos (eleitos ou administrativos) perseguem objetivos que não são exclusivamente respostas às demandas sociais e, ao mesmo tempo, como configuradores de organizações e ações que se estruturam, modelam e influenciam os processos econômicos e classes ou grupos de interesse. (MENY & THOENING, 1992, p. 35, traduçao nossa).

Assim, Rodrigues (2017) caracteriza ao argumento apresentado pelo Meny & Thoening (1992) como “útil para estudar a “ação do Estado” dentro de uma dinâmica contextual que esclarece a análise de impacto sobre o conteúdo e o jeito das políticas”. (RODRIGUES, 2017, p. 187, tradução nossa)

Desta forma, “as políticas são desenhos para ação pública” (LAFUENTE & ROJAS, 2010, p. 4, tradução nossa) bem como, “aquelas que correspondem a soluções específicas de como gerir assuntos públicos” (LAHERA, 2004, p. 7, tradução nossa), cujo âmbito estimula às autoridades e atores da sociedade a participar ativamente sobre sua abrangência e a modernização através da gestão pública, o que tem produzido “mudanças nos modos de gerir o Estado” (OLAVARRÍA, NAVARRETE, & FIGUEROA, 2011, p. 110).

Consequentemente, se as políticas públicas estão associadas à ação das autoridades e de outros atores diante das demandas da sociedade, então é pertinente questionar como essas demandas se originam e como se tornam ações. Segundo Meny & Thoening (1992) o que leva as autoridades públicas a agir é a “agenda”, que pode ser definida como “o conjunto de problemas que apelam a um debate público, incluindo a intervenção (ativa) de autoridades públicas legítimas...são institucionais, sistémicos ou conjunturais” (MENY & THOENING, 1992, p. 114 apud PADIOLEAU, 1982, tradução nossa). Segundo Doña (2005), a definição de uma agenda é importante devido ao “grau de consenso ou conflito que gera; porque este seria o elemento que indicaria a oportunidade da autoridade intervir e como deve fazê-lo” (DOÑA, 2005, p. 34, tradução nossa). Logo, Elder, Cobb, & J. (1993) argumenta que “o processo de preparação da agenda é o momento em que o governo decide se vai ou não decidir sobre determinado assunto, no qual delibera e decide intervir ou decide não intervir, adiar a sua intervenção”. (ELDER, COBB, & J., 1993, p.27-28, tradução nossa).

Meny & Thoening (1992) estabelece que outro aspeito, é distinguir quais são os problemas que originam a intervenção pública. Um diz respeito à fase de definição de um problema, a formulação das demandas; o outro se refere às estratégias de resposta implantadas em relação com as demandas (MENY & THOENING, 1992, p. 118). Elder, Cobb, & J. (1993) estabelece que a definição de um problema se dá em um contexto de limites de plausibilidade por restrições ideológicas e restrições de recursos. Assim, “Um problema será levado a sério em consideração apenas se os custos previstos de sua solução forem realistas e aceitáveis, no contexto dos recursos públicos previsíveis e atualmente acessíveis. (ELDER, COBB, & J., 1993, p.94, tradução nossa). Também, segundo Meny & Thoening (1992) a definição inicial de um problema na maioria dos casos, não permanece estável nem invariável, devido a sua transcendência no contexto político.

Meny & Thoening (1992) expressa certas condições necessárias e suficientes para que um assunto ou problema está incluído na agenda do governo, dentro dos principais, deve ser da responsabilidade das autoridades públicas em geral, ou de

uma determinada autoridade pública; que seja percebido como um assunto de percepções problemáticas, que o definam como merecedor de “atenção pública”; e que o problema possa constituir, deve ser acessível em termos de ação pública. (MENY & THOENING, 1992, p. 124). Além disso, Elder, Cobb, & J. (1993) adiciona que “da mesma forma que os problemas insolúveis são descartados, o surgimento de novas soluções torna possível criar novos problemas”. (ELDER, COBB, & J., 1993, p.95, tradução nossa).

Meny & Thoening (1992) argumenta que uma autoridade pública tem uma multiplicidade de respostas para uma demanda incluída na agenda. Destaque-se que existe uma grande abrangência de ações que poderiam ser feitas.

> Essas respostas variam de rejeitar, desabilitar, bloquear, brincar, evitar; para dar sinais positivos, invoque um imponderável que permite escapar da ação, adiar o exame do problema, estabelecer um procedimento para o tratamento deste sem se comprometer com o conteúdo, regular uma pequena parte do problema com um valor simbólico sem atacar a totalidade dele, levar em consideração a demanda como um todo e antecipar o surgimento de demanda, entre outras fórmulas possíveis (MENY & THOENING, 1992, p. 125-127, tradução nossa).

Em relação a adopção da decisão pública, Meny & Thoening (1992) expressa que “Agir é tomar decisões” (MENY & THOENING, 1992, p. 129, tradução nossa). Segundo Doña (2005):

> Quando a autoridade atua é quando toma uma decisão e, portanto, ocupa um lugar importante no processo de formulação de políticas públicas. A decisão resolve um problema, selecionando alternativas, marcando uma descontinuidade no tempo, há antes e depois da adoção da decisão (DOÑA, 2005, p. 34, tradução nossa).

Meny & Thoening (1992) estabelece que o tomador de decisão é o iniciador para a elaboração das políticas públicas, é ele quem assina e resolve em última instância, mas na prática depende das soluções concretos que nascem de outros especialistas. Segundo Aguilar (1993):

> Quem define é quem decide "é uma máxima que ele quer sublinhar o fato de que os grupos sociais e / ou governamentais que tiveram a capacidade de oferecer a abordagem e definição parte aceitável da questão são aqueles que efetivamente influenciam a decisão. (ELDER, COBB, & J., 1993, p.52, tradução nossa).

Em seguida, Meny & Thoening (1992) existem grupos de terceiros que fornecem essas soluções, elaboram as opções e garantir a sua legitimidade operacional; em síntese, as medidas adotadas não seriam respostas obrigatórias às demandas da sociedade e de seus representantes políticos, mas, se não o produto de atividades feitas por intermediários (MENY & THOENING, 1992, p. 133-135).

Meny & Thoening (1992) o processo de toma de decisões está composto de duas fases principais: a fase de formulação e de legitimação. A primeira corresponde ao trabalho pelo qual uma questão pública está inscrita na agenda do governo ou se transforma em alternativas para a ação (soluções) baseado em três ações iniciais: identificar as causas que originaram o problema, levantar os conhecimentos que o compõe e levantar um diagnóstico. Esta etapa de formulação ou de preparação considera duas fases: análise e seleção. A análise define o trabalho de investigação do problema, busca as opções e alternativas, as consequências, vantagens e desvantagens, os efeitos desejados; concentrando o esforço em saber se é necessário agir ou não. Enquanto a subfase de seleção, corresponde ao processo de redução das opções para apenas uma. Na fase de legitimação se desenvolve quando o responsável formal, o indivíduo ou grupo ao qual institucionalmente corresponde o direito e o dever de resolver, resolver. Neste sentido, corresponde a um ato de poder discricionário por parte das autoridades investidas da capacidade de decisão, segundo o autor: “tem seu valor agregado, o que é política e simbolicamente decisivo: pelo seu voto, pela sua assinatura, você legitimidade a opção e a torna oficial, autorizada e irreversível”. (MENY & THOENING, 1992, p. 138).

Como último aspeito, Meny & Thoening (1992) incorpora dentro do processo de decisão, o “modelo de decisor racional”, baseado em uma análise antecedido de uma decisão baseada em critérios racionais e objetivos. Segundo Doña (2005):

> Há um ator enfrentando um problema que está em uma situação de escolher. Escolhe suas preferências, define metas, define seus valores, seleciona sua vantagem. Em seguida, procura as alternativas disponíveis, faz uma lista delas e pesquisa suas falhas e méritos para responder ao problema. Adota um critério de escolha objetivo que permite determinar a melhor relação entre vantagens e desvantagens de cada alternativa, permitindo que você as explore e adote a solução. (DOÑA, 2005, p. 42, tradução nossa).

Por outro lado, de acordo com nossos objetivos da pesquisa, é importante aprofundar as abordagens teóricos sobre como conceber as políticas públicas e suas respostas em um sistema político. Neste sentido, elas podem ser analisadas desde diferentes prismas, embora, a teoria deve atender satisfatoriamente o requerimento de nosso estudo norteado para avaliar as concorrências e integrações entre as diferentes políticas setoriais promovidas pelos Ministérios chilenos, para assim determinar o número de coordenações estratégicas com outras políticas públicas para alcançar determinados resultados da ação pública em seu conjunto.

Segundo Dye (2011) a ciência política tem como objeto de estúdio as políticas públicas, já que elas são parte das causas e consequências da atividade governamental. Neste sentido, essa abordagem implica:

> Uma descrição do conteúdo das políticas públicas; uma análise do impacto das forças sociais, econômicas e políticas; uma investigação sobre o efeito de vários arranjos internacionais e processos políticos nas políticas públicas; e uma avaliação das consequências das políticas públicas na sociedade, intencionais e não intencionais. (DYE, 2011, p. 6)

Entretanto, Easton (1999) estabelece certas restrições teóricas em relação à ciência política já que argumenta que: “não pode estudar todos os fenômenos; o mundo real precisa ser reduzido e simplificado de alguma forma”. (EASTON, 1999, p. 77)

Deste jeito, Segundo Dye (2009) os modelos que servem para estudar as políticas públicas são modelos conceituais que estão focados ente outros tópicos em: “esclarecer as ideias sobre políticas e políticas públicas; identificar aspectos importantes de questões políticas e problemas sociais; direcionar nosso esforços para compreender melhor as políticas públicas e propor explicações para as políticas públicas e prever suas consequências” (DYE, 2009, p. 100). Logo, o mesmo autor, menciona que as políticas públicas são examinadas desde diferentes óticas e levam à compreensão delas. Se podem observar os modelos: institucional; de processo; de grupo; de elite; racional; incremental; teoria de jogos; de opção pública; sistêmico. (DYE, 2009, p. 100-125).

Desta forma, Dye (2009) estabelece que não existe um método que seja o “melhor” e faz uma crítica respeito de sua origem em termos de argumentar que: “nenhum desses modelos foi desenvolvido especialmente com a finalidade de estudar a política pública” (DYE, 2009, p. 100). Contudo, de SAN ROMÁN (2012), baseado na argumentação das obras de Easton, adverte que:

> A abordagem do analista político não deve ser centrada em regularidades. Que não são as repetições de comportamentos observáveis que permitem diferenciar um sistema político de outro, mas sim aqueles "significados" que tornam um sistema politicamente interessante”. (de SAN ROMÁN, 2012, p. 89, tradução nossa).

Seguidamente, Dye (2011) em relação à análise de políticas argumenta que esta deve ser desenvolvida sem a existência de um padrão rígido por se tratar desde uma visão de arte e ciência, devido que este tipo da análise se encontra ligada a um processo de criatividade por parte do pesquisador e é “estimulada pela teoria e moldada pela prática, que pode ser aprendida, mas não ensinada”. (DYE, 2011, p. 11, tradução nossa). Também, Lindblom (1994) caracteriza o que deveria ser outra regra para uma boa análise política, em relação de “forçar ao analista político a adotar um ponto de vista mais amplo ... minimiza a oportunidade de infiltração dos próprios valores do analista”. (LINDBLOM, 1994, p. 255, tradução nossa).

Por outro lado, quando um pesquisador social formula uma versão do interesse público e faz sua análise sob esse prisma, “estamos pedindo a ele que vá além do conhecimento até chegar à escolha ou ao compromisso” (LINDBLOM, 1994, p. 259, traução nossa).

Da mesma forma, DYE (2009) refere que antes de iniciar o estudo de uma política pública é importante identificar a utilidade do modelo de análise a escolher. Desta forma, ao obter alguns critérios que justifiquem a preferência, se deve compreender que o modelo deve orientar a pesquisa sobre as políticas públicas, a partir de uma análise operacional, vale dizer:

> Referir-se a fenômenos do mundo real, que possam ser observados, medidos e verificados. Um conceito ou uma serie de conceitos interrelacionados (a que chamamos *modelo*) devem sugerir relações no mundo real, que possam ser testadas e verificadas. (DYE, 2009, p. 127)

Bem como, sugerir um esclarecimento da política pública, em termos de identificar causas e as consequências e possíveis explicações e não, apenas em descrições. (DYE, 2009, p. 128-129).

Daí, Easton (1999) aborda que o compromisso ao tentar caracterizar a vida política como um sistema de conduta, estaria validado no valor que tem o conceito do "sistema" além das ciências sociais, devido a sua utilidade e abrangência, dentro do possível, a todo o universo social o qualquer de suas partes.

> O mesmo pode ser dito em relação à função de um sistema como conceito na pesquisa social. Representa uma forma de nos orientarmos, pelo menos, em direção aos nossos dados e, fornece também um guia crucial para a análise do nosso assunto (interação política). (EASTON, 1999, p. 60)

Assim, procurando uma coerência com nosso objetivo de pesquisa, de SAN ROMÁN (2012), estabelece uma valorização de caráter prático da teoria de Easton sobre um "Esquema para a análise político", já que esta orienta-se na "indagação de causas e suas relaciones" (de SAN ROMÁN, 2012, p. 90, tradução nossa).

Easton (1999) argumenta respeito da importância da abordagem sistémica nos estudos de políticas públicas:

> No caso do conceito de sistema, isso significa que ele poderia ser tomado como o núcleo essencial de uma estrutura analítica, construindo em torno dele conceitos secundários apropriados que constituiriam toda uma série de categorias inter-relacionadas. A análise em termos sistêmicos promete facilitar essa estrutura conceitual e é aí que reside sua maior justificativa. (EASTON, 1999, p. 186)

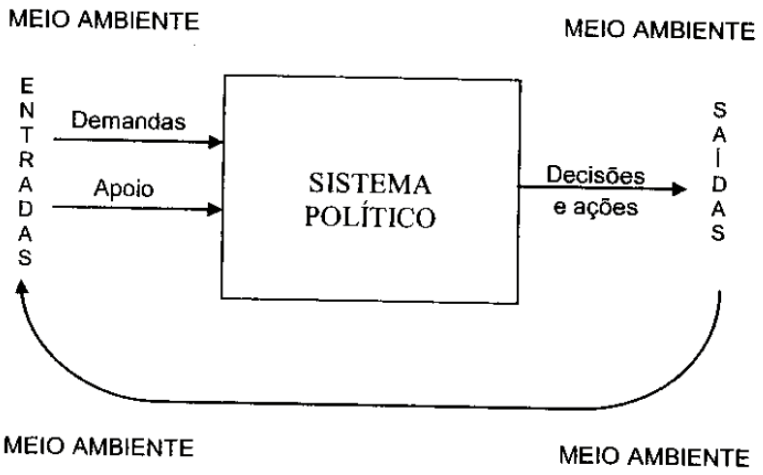
Desse jeito, Dye (2009) em relação do emprego da Teoria sistémica com foco na política como produto do sistema, expressa que a concepção do sistema político tem sido utilizada em diferentes pesquisas, ratificando mais uma vez, com o propósito de "analisar causa e as consequências das políticas públicas". (DYE, 2009, p. 124), bem como, "a formulação e implementação de um processo político-administrativo com foco em interações complexas" (DYE, 2009, p. 130). Igualmente, o valor do modelo sistêmico encontra-se de acordo a nosso interesse em algumas das questões levantados por o autor que permitiram balizar o nosso trabalho. Logo, destaque-se:

De que maneira as características do sistema político influenciam o conteúdo das políticas públicas? e; de que modo os inputs ambientais influenciam o conteúdo das políticas públicas? (DYE, 2009, p. 126)

Consequentemente, Easton (1999) propõe um diagrama de fluxo para analisar as diferentes interações no ambiente e as influências que se exercem sobre o sistema político. “Por meio de suas estruturas e processos, o sistema opera nessas entradas de forma que se tornem produtos, ou seja, decisões autoritárias e sua execução. (EASTON, 1999, p. 155-156)

Easton (1999) conceitualiza de um jeito simplificado, sua visão sobre a atividade política e seu produto, as políticas públicas; deixando apenas as relações dinâmicas que se estabelecem dentro do sistema política, constituindo um ponto de partida para o início de um posterior análise.

FIGURA 2 – O modelo Sistêmico.



Fonte: DYE, Políticas Públicas e Desenvolvimento, 2009, p. 125, de acordo com EASTON, 1999, p. 156.

Dye (2009) fornece uma explicação sobre o diagrama apresentado, em termos de expressar que os inputs estão concebidos em demandas e apoios. As demandas agem para influenciar na política devido às condições do meio ambiente e os apoios

aceitam diferentes resultados e se conformam-se com os resultados das decisões políticas. Assim, para transformar essas demandas em output (políticas públicas), o sistema deve promover acordos e fazê-los cumprir pelas partes interessadas. (DYE, 2009, p. 124-125)

Enfim, a presença de um modelo da análise sistémico utilizado para a análise das políticas públicas, permite avançar teoricamente para cumprir com os objetivos determinados para nossa pesquisa para identificar um conjunto de instituições e atividades que se interrelacionam para a adopção de decisões e ações no contexto político-social.

9. REFERENCIAS BIBLIOGRÁFICAS

ABDUL-HAK, A. P. (2013). *O Conselho de Defesa Sul-Americano (CDS): Objetivos e interesses do Brasil.* Brasília: Funag.

ACOSTA, P. A. (2009). *Cuadernos Catedra ISDEFE-UPM «Seguridad nacional y Ciberdefensa».* Madrid: Fundación Rogelio Segovia para el desarrollo de las Telecomunicaciones.

ARREOLA, A. (Abril de 2020). Ciberespacio: quinto dominio de la guerra. Obtenido de https://www.researchgate.net/publication/340819837_Ciberespacio_quinto_dominio_de_la_guerra

BANCO INTERAMERICANO DE DESARROLLO. (2016). Obtenido de Ciberseguridad, ¿Estamos preparados en América Latina y el Caribe?, Informe Ciberseguridad 2016: https://publications.iadb.org/bitstream/handle/11319/7449/Ciberseguridad-Estamos-preparados-en-America-Latina-y-el-Caribe.pdf?sequence=7

BANCO INTERAMERICANO DE DESARROLLO. (2020). *Ciberseguridad, riesgos, avances y el camino a seguir en América latina y el Caribe.* Obtenido de www.observatoriociberseguridad.com

BOWDISH, R. (2013). *Military Strategy: Theory and Concepts. Tesis (Doctorado en Filosofía).* (D. d. Políticas, Ed.) Nebraska, Estados Unidos de Norteamérica: Universidad de Nebraska.

BUENNEMEYER, T. K. (Parameters 41, no. 3 (Autumn, 2011) de 2011). *"A Strategic Approach to Network Defense: Framing the Cloud."*. Obtenido de ProQuest Military Collection.: https://csl.armywarcollege.edu/SLET/mccd/CyberSpacePubs/Buennemeyer.pdf

BULL, H. (2002). *A Sociedade de Anárquica. Um estudo da ordem na politica mundial.* (S. B. Edição), Trad.) São Paulo: Editora Universidade de Brasília, Instituto de Pesquisa de Relações Internacionais.

CARO Bejarano, M. J. (2010). «Alcance y ámbito de la Seguridad Nacional en el Ciberespacio.». En I. E. Estratégicos, *Cuaderno de Estrategia Nº 149 Ciberseguridad. Retos y Amenazas a la Seguridad nacional en el Ciberespacio* (págs. 48-82). Madrid: Imprenta del Ministerio de Defensa.

CASTRILLÓN-RIASCOS, J. A. (2015). *Nada volverá a ser igual: ciberguerra y ciberpoder.* Memorias, 13(23). doi:http://dx.doi.org/10.16925/me.v13i23.1072

CHILE, Govierno de Chile. (2017). *Política Nacional de Ciberseguridad (PNCS).* Obtenido de https://www.ciberseguridad.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf.

CHILE, Govierno de Chile. (2018). *Política de Ciberdefensa del Estado de Chile.* Obtenido de

https://www.diariooficial.interior.gob.cl/publicaciones/2018/03/09/42003/01/1363153.pdf.

CHOUCRI, N. (2012). *Cyberpolitics in international relations.* Cambridge, Massachusetts: Massachusetts Institute of Technology.

CLARK, R. A. (2011). *Guerra en la Red: Los nuevos campos de Batalla.* Barcelona: Editorial Ariel.

COLÔMBIA. (s.f.). Obtenido de COMANDO CONJUNTO CIBERNÉTICO (CCOCI). Historia, 2017.: <https://www.ccoc.mil.co/quienes_somos_historia>

CONELL, M., & VOGLER, S. (2016). *Russia´s Approach to Cyber Warfare.* Arlington, VA: Center for Naval Analyses.

CZEGE, H. W. (2010). «Warfare by Internet: The Logic of Strategic Deterrence, Defense, and Attack». *Military Review Jul/Aug. ProQuest Military Collection*, 85.

de SAN ROMÁN, P. (2012 de 2012). Fundamentos y tensiones del sistema político moderno, Comentario a la obra de David Easton, Esquema para el análisis político. *Leviathan, Cuadernos de Investigación Política, 5*, 82-93.

DOÑA, M. K. (2005). *Aplicación del concepto de política pública a la política de defensa de Chile, 1990-1999.* Univerdad de Chile. Santiago: Instituto de asuntos públicos.

DYE, T. R. (2009). *Políticas Públicas e Desenvolvimento.* (F. G. Salm, Trad.) Brasília: Editora Universidade de Brasília.

DYE, T. R. (2011). *Understanding public policy.* Boston: Longman.

EASTON, E. (1999). *Esquema para el análisis político.* (A. C. Leal, Trad.) Buenos Aires, Argentina : Amorrortu editores.

ELDER, C. D., COBB, R. W., & J., N. B. (1993). *Problemas públicos y Agenda de Gobierno.* (L. F. VILLANUEVA, Ed.)

FELIU, L. (2013). *«Seguridad nacional y Ciberdefensa» Aproximación conceptual: Ciberseguridad y Ciberdefesa.* Obtenido de Escuela Superior de Ingenieros de Telecomunicaciones: http://catedraisdefe.etsit.upm.es/wp-content/uploads/2013/01/Ponencia-Luis-Feliu.pdf

FIREEYE. (2020). *M-Trends 2020: Insights into Today's Cyber Attacks*. Obtenido de https://content.fireeye.com/m-trends/wbnr-m-trends-2020-insights-into-todays-cyber-attacks

FUCCILLE, A., & REZENDE, L. (Jun de 2013). ARTIGOS Complexo regional de segurança da América do Sul: uma nova perspectiva. *Contexto Internacional, 35*, p.77-104.

GIBSON, W. (1991). *Neuromancer.* São Paulo: Editora Aleph.

GIL, A. C. (2002). *Como elaborar projetos de pesquisa.* Sao Paulo: Atlas.

GÓMEZ de Ágreda, A. (2012). “El ciberespacio como escenario de conflictos. Identificación de amenazas”. En C. S. Nacional, *Monografías del CESEDEN Nº 126 El Ciberespacio. Nuevo Escenario de Confrontación* (págs. 167-204).

GONZÁLEZ, C. J. (2010). «Estrategias legales frente a las Ciberamenazas». En Instituto Español de Estudios Estratégicos, *Cuaderno de Estrategia Nº 149 Ciberseguridad. Retos y Amenazas a la Seguridad Nacional en el Ciberespacio.* Madrid: Imprenta del Ministerio de Defensa.

HERNÁNDEZ-SAMPIERI, R., FERNÁNDEZ, C., & BAPTISTA, M. (2014). *«Metodología de la Investigación»* (Sexta ed.). Distrito Federal, México: McGRAW-HILL/ Interamericana Editores.

JUNTA INTERAMERICANA DE DEFENSA. (2020). *Guía de Ciberdefensa.*

KUEHL, D. T. (2009). From cyberspace to cyberpower: Defining the problem. En N. D. Press, *Cyberpower and National security* (págs. 26-28).

LAFUENTE, M., & ROJAS, F. (2010). *La formulación de políticas en la OCDE, ideas para América Latina.* Banco mundial.

LAHERA, P. E. (2004). *Política y políticas públicas.* Santiago: CEPAL, División de Desarrollo Social.

LINDBLOM, C. E. (Segundo semestre de 1994). La investigación social para la elaboraci6n de politicas: quien la necesita y para que. *Gestión y Politica Pública, III*.

LÓPEZ de Turiso y Sánchez, J. (2012). «La Evolución del conflicto hacia un nuevo escenario bélico». En C. S. Nacional, *Monografías del CESEDEN Nº 126 El Ciberespacio. Nuevo Escenario de Confrontación* (págs. 119-166). Madrid: Imprenta del Ministerio de Defensa.

MARTINS, C. E., & LEITAO, A. C. (2018). *Process tracing nas Ciências Sociais: fundamentos e aplicabilidade.* Brasília: Escola Nacional de Administração Pública.

MENY, I., & THOENING, J.-C. (1992). *Las políticas públicas.* (F. Morata, Ed.) Barcelona: Editorial Ariel.

MICROSOFT CORPORATION. (Setembro de 2020). *Microsoft Digital Defense Report.* Obtenido de file:///C:/Users/funcional/Downloads/Microsoft_Digital_Defense_Report_2020_September.pdf

MILANI, C. R. (2020). *Solidariedade e Interesse. Motivações e estratégias na cooperação internacional para o desenvolvimento.* 1º ed. Curitiba: Appris de CS Mombelli.

MORAVCSIK, A. (1997). *Taking Preferences Seriously: A Liberal Theory of International Politics.* (Vol. 51). International Organization. Obtenido de http://www.jstor.org/stable/2703498

MORGENTHAU, H. (1962). *A Political Theory of Foreign Aid* (Vol. 56). American Political Science Review.

MORGENTHAU, H. (2003). *A Política entre as nações: a luta pelo poder e pela paz.* Brasília: UnB.

NEWMEYER, K. (2015). Elements of national cybersecurity strategy for developing nations. (publications.excelsior.edu, Ed.) *National Cybersecurity Institute Journal, 1*, 9-19.

NYE, J. S. (2010). Cyber Power. (H. K. School, Ed.) *Belfer Center for Science and International Affairs*. Obtenido de http://belfercenter.org

OLAVARRÍA, G. M., NAVARRETE, Y. B., & FIGUEROA, H. V. (1er. semestre de 2011). ¿Cómo se formulan las políticas públicas en Chile? *Política y gobierno, XVIII*, 109-154.

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. (28 de Abril de 2017). *Centro de noticias de la OEA*. Obtenido de http://www.oas.org/es/centro_noticias/fotonoticia.asp?scodigo=fnc-21545

PAZ, P. Y. (2017). OEA COMITÉ INTERAMERICANO CONTRA EL TERRORISMO. *DECIMOSEPTIMO PERÍODO ORDINARIO DE SESIONES.* Washington, D.C., Estados Unidos.

PEREIRA REZENDE, L. (2015). Sobe e Desce: Explicando a Cooperação em Defesa na América do Sul. (U. d. Brasília, Ed.) *Contexto Internacional, 1*.

PERRY BARLOW, J. (2021). *«A Declaration of the Independence of Cyberspace».* Obtenido de https://www.eff.org/cyberspace-independence.

PRANDINI, P., & MARGIORE, M. (2013). *«Ciberdelito en América Latina y El Caribe. Una visión desde la sociedad civil».* Obtenido de LACNIC Registro de Direcciones de Internet para América Latina y Caribe.: https://www.proyectoamparo.net/files/ciberdelito_lac_lacnic_amparo_estudios 2013_completo_vfinal.pdf.

QUEIROZ Campos, A., & REGINA Rech, S. (enero-junio de 2016). Método para pesquisa de tendências: uma revisão do modelo Futuro do Presente. (U. d. Catarina, Ed.) *ModaPalavra e-periódico*(17), pp. 26-47. Obtenido de http://www.redalyc.org/articulo.oa?id=514054174004

REARDON, R., & CHOUCRI, N. (2012). *The Role of Cyberspace in International Relations: A View of the Literature.* San Diego, CA: Department of Political Science, MIT.

RODRIGUES, D. C. (septiembre-diciembre de 2017). Las políticas públicas. YVES MENY y JEAN-CLAUDE THOENIG. (U. C. Venezuela, Ed.) *Cuadernos del CENDES, 34*, 185-192. Obtenido de www.redalyc.org/articulo.oa?id=40354944011

SAINT-PIERRE, H. L. (julho/dezembro de 2011). “Defesa” ou “Segurança”? Reflexões em torno de Conceitos e Ideologias. *33*(2), 432.

SANCHO, H. C. (Julio de 2020). Seguridad y defensa en el ciberespacio: tendencias contemporáneas y desafíos para el caso chileno. *Escenarios Actuales, 2*, 49-72.

SARTORI, G. (2009). *«Guidelines for concept analysis, Concepts and method in social science».* Nueva York, Estados Unidos da America.

SECURITY, A. C. (s.f.). *Security Tip (ST04-001)*. Obtenido de https://us-cert.cisa.gov/ncas/tips/ST04-001: https://us-cert.cisa.gov/ncas/tips/ST04-001

TEIXEIRA JÚNIOR, A. W. (2013). *O Brasil e a Criação do Conselho de Defesa Sul-Americano da Unasul: Cooperação e Balanceamento como Estratégias de Autoajuda.* Recife: Universidade Federal de Pernanbuco.

THE ECONOMIST REVIEW. (July de 2010). Cyberwar, The threat from the internet. *The Economist Review, 396*.

THEOHARY, C. A., & HARRINGTON, A. I. (2015). *Cyber Operations in DOD Policy and Plans.* Congressional Research Service. Obtenido de www.crs.gov

TODD, H. M. (2009). "Armad attack in cyberspace: Deterring asymmetric warfare with an asymmetric definition. *The Air Force Law Review, ProQuest Military Collection.*, 64.

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (UIT). (Noviembre de 2010). *Recomendación UIT–T X.1205*. Obtenido de https://www.itu.int/es/about/Pages/default.aspx

UNITED KINGDOM, Ministry of Defence. (2018). *Ministry of Defence (MOD).* Obtenido de «Strategic Trends Programme Global Strategic Trends - Out to 2050»: https://www.gov.uk/government/publications/global-strategic-trends

UNITED STATES OF AMERICA. (s.f.). *Department of Homeland Security, Cybersecurity Overview*. Obtenido de Official website of the Department of Homeland Security: https://www.dhs.gov/cybersecurity-overview.

UNITED STATES OF AMERICA, DEPARMENT OF DEFENSE. (2010). *Joint Publication 1-02 Dictionary of Military and Associated Terms.*

UNITED STATES OF AMERICA, Department of Defense. (2010). *Joint Publication 1-02 Dictionary of Military and Associated Terms.*

VAN EVERA, S. (1997). *Guide to methods for students of Political science.* New York: Cornell University Press.

VERGARA, S. (1998). *Projetos e relatórios de pesquisa em administração* (2da. ed.). São Paulo: Atlas.

YIN, R. K. (1994). *Estudo de caso: Planejamento e Métodos* (2a. Edição ed.). (D. Grassi, Trad.) São Paulo, SP: Artmed Editora S.A.

APÊNDICE A – Esquema Gráfico de Pesquisa

EVOLUÇÃO DA POLÍTICA PUBLICA DE SEGURANÇA CIBERNÉTICA DO CHILE E A INCLUSÃO DA DEFESA NACIONAL NA COOPERAÇÃO REGIONAL NO CIBERESPAÇO