

UNIVERSIDADE FEDERAL DE MINAS GERAIS
ESCOLA DE CIÊNCIA DA INFORMAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO

Arthur Christian Huamaní Cuba

**PERSPECTIVA COMPARADA DAS POLÍTICAS E ESTRATÉGIAS EM
SEGURANÇA CIBERNÉTICA NO MARCO DO PANORAMA DE SUAS
CONFIGURAÇÕES DOS PAÍSES DA ARGENTINA, BRASIL E PERU**

Belo Horizonte
2024

Arthur Christian Huamaní Cuba

**PERSPECTIVA COMPARADA DAS POLÍTICAS E ESTRATÉGIAS EM
SEGURANÇA CIBERNÉTICA NO MARCO DO PANORAMA DE SUAS
CONFIGURAÇÕES DOS PAÍSES DA ARGENTINA, BRASIL E PERU**

Tese apresentada ao Programa de Pós-graduação em Ciência da Informação da Universidade Federal de Minas Gerais (PPGCI-UFMG) como requisito parcial para a obtenção do grau de Doutor em Ciência da Informação.

Área de concentração: Informação, mediações e cultura.

Linha de pesquisa: Memória social, patrimônio e produção do conhecimento.

Orientadora: Profa. Dra. Maria Aparecida Moura

Belo Horizonte

2024

C962p

Cuba, Arthur Christian Huamani.

Perspectiva comparada das políticas e estratégias em segurança cibernética no marco do panorama de suas configurações dos países da Argentina, Brasil e Peru [recurso eletrônico] / Arthur Christian Huamani Cuba. - 2024.

1 recurso online (340 f. : il., color.) : pdf.

Orientadora: Maria Aparecida Moura.

Tese (doutorado)– Universidade Federal de Minas Gerais, Escola de Ciência da Informação.

Referências: f. 303-312.

Apêndice: f. 313-340.

Exigência do sistema: Adobe Acrobat Reader.

1. Ciência da informação – Teses. 2. Cibernética – Teses. 3. Cibernética – Sistemas de segurança – Teses. 4. Computadores – Medidas de segurança – Teses. I. Moura, Maria Aparecida. II. Universidade Federal de Minas Gerais. Escola de Ciência da Informação. III. Título.

CDU 007

Ficha catalográfica. Vanessa Marta de Jesus - CRB/6-2419

Biblioteca Profª Etelvina Lima, Escola de Ciência da Informação da UFMG



UNIVERSIDADE FEDERAL DE MINAS GERAIS
ECI - COLEGIADO DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO

ATA DE DEFESA DE TESE

Às 14:00 horas do dia 24 de maio de 2024, Plataforma Microsoft Teams, realizou-se a sessão pública para a defesa da Tese de ARTHUR CHRISTIAN HUAMANI CUBA, número de registro 2018663857. A presidência da sessão coube a Profa. Maria Aparecida Moura - orientadora. Inicialmente, a presidente fez a apresentação da Comissão Examinadora assim constituída: Dr. Rodrigo Benjamin Gesteira (DPF), Dr. Vladimir de Paula Brito (DPF/INASIS), Profa. Lorena Tavares de Paula (ECI/UFMG), Prof. Rodrigo Moreno Marques (ECI/UFMG), e Profa. Maria Aparecida Moura - orientadora (ECI/UFMG). Em seguida, o candidato fez a apresentação do trabalho que constitui sua tese de doutorado, intitulada: "*Perspectiva comparada das políticas e estratégias em segurança cibernética no marco de suas configurações nos países Argentina, Brasil e Peru*". Seguiu-se a arguição pelos examinadores e logo após, a Comissão reuniu-se, sem a presença do candidato e do público e decidiu considerar aprovada a Tese de Doutorado. O resultado final foi comunicado publicamente ao candidato pela presidente da Comissão. Nada mais havendo a tratar, a presidente encerrou a sessão e lavrou a presente ata que, depois de lida, e aprovada, foi assinada pela Comissão Examinadora.

Belo Horizonte, 24 de maio de 2024.

Assinatura dos membros da banca examinadora:



Documento assinado eletronicamente por **Maria Aparecida Moura, Professora do Magistério Superior**, em 27/05/2024, às 14:50, conforme horário oficial de Brasília, com fundamento no art. 5º do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Rodrigo Moreno Marques, Professor do Magistério Superior**, em 28/05/2024, às 12:05, conforme horário oficial de Brasília, com fundamento no art. 5º do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Rodrigo Benjamin Gesteira, Usuário Externo**, em 11/07/2024, às 16:23, conforme horário oficial de Brasília, com fundamento no art. 5º do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Lorena Tavares de Paula, Professora do Magistério Superior**, em 13/08/2024, às 08:08, conforme horário oficial de Brasília, com fundamento no art. 5º do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Vladimir de Paula Brito, Usuário Externo**, em 03/09/2024, às 17:16, conforme horário oficial de Brasília, com fundamento no art. 5º do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site

[https://sei.ufmg.br/sei/controlador_externo.php?](https://sei.ufmg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0)

[acao=documento_conferir&id_orgao_acesso_externo=0](https://sei.ufmg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador 3259912 e o código CRC 55C2C8C3.

Referência: Processo nº 23072.227905/2024-62

SEI nº 3259912

Aos meus anjos Emilio, Maura, Melquiades e Julia por serem minha proteção e guia.

Aos meus pais amados: Susana e Arturo, por serem minha fortaleza e exemplo de luta. A minha amada Alessandra e Lola, por terem me proporcionado amor, alegria e conforto nos momentos difíceis, ao longo das várias etapas deste projeto de vida.

A Susan, Jhon, Simone, Juci, Juninho, Protasio, minha família, pela paciência, conselhos e motivações.

Às novas gerações sul-americanas que serão atores viventes da nova ordem mundial desejando que a força da prosperidade esteja com vocês.

AGRADECIMENTOS

A Dra. Maria Aparecida Moura agradeço a orientação, paciência e ensinamentos que contribuíram para meu crescimento acadêmico. Aos professores Casal, Claudio Paixão, Cristina Dotta, Maria Guiomar e Eduardo Valadares pelos ensinamentos. Aos professores, membros da banca examinadora pelo olhar criterioso e valiosas recomendações sobre a pesquisa realizada.

A Organização de Estados Americanos (OEA), ao Grupo Coimbra de Universidades Brasileiras (GCUB) e ao CAPES, instituições que agradeço a concessão da bolsa de doutorado que permitiu minha dedicação integral aos estudos e pesquisa.

Aos especialistas que participaram como entrevistados e respondentes expresso minha gratidão pela rica contribuição em experiências, profissionalismo e conhecimento. Componentes importantes que fortaleceram os resultados da minha tese de doutorado.

Aos meus colegas do doutorado expresso minha sincera gratidão pela parceria, amizade, diálogos, debates e por compartilharmos juntos as alegrias e angústias ao longo do processo de estudos e pesquisa. Em particular, gostaria de agradecer ao meu amigo, o Dr. Tadeus Mucelli pela amizade sincera.

Agradeço aos meus familiares e amigos pelo apoio incondicional, por me ajudarem a construir meus sonhos e objetivos. Graças a todos vocês, que alcancei um dos meus maiores objetivos de vida.

RESUMO

A presente tese busca compreender, a partir de uma perspectiva comparada, as políticas e estratégias em segurança cibernética adotadas pela Argentina, Peru e Brasil. Por meio da metodologia aplicada, foi possível identificar, sistematizar e analisar os elementos que estão influenciando a consolidação dessas políticas de segurança cibernética, bem como considerar como esses elementos são tratados dentro das especificidades geopolíticas dos países da América do Sul, visando consolidar um modelo integrado para os países sul-americanos. Este estudo apresenta um contexto relevante e contemporâneo dentro de dois modelos: social e pragmático. Portanto, optou-se por abordá-lo sob as diretrizes da investigação qualitativa, do tipo explicativa. Com a finalidade de compreender o papel do Estado na segurança cibernética e as implicações geradas na sociedade contemporânea, procurou-se analisar a lógica das diferentes formas de interação entre o Estado e a sociedade, por meio das relações existentes entre os agentes e a dinâmica da ação pública na segurança cibernética. Para isso, foi adotado o método de análise de conteúdo computacional, que contemplou um total de 108 documentos digitais, 06 entrevistas e 28 questionários individuais, conformando assim nosso projeto de casos múltiplos contexto. Dada a complexidade multifacetada do tema de pesquisa, foi elaborado um Estado da Arte, com o desenvolvimento do caso protótipo norte-americano, contribuindo para os conceitos e principais conclusões da defesa e segurança cibernética norte-americana, contudo, afirmamos que o caso protótipo serviu de nosso laboratório. Esta etapa permitiu a identificação da historicidade, dos elementos e dos agentes envolvidos na concepção da política e estratégia norte-americana, destacando o Aspecto de Poder e Dominação como relevante para a segurança cibernética dos Estados Unidos. Na segunda fase, foram elaborados os estudos de casos da Argentina, Brasil e Peru. Devido à escassa produção de textos eletrônicos oficiais em segurança e defesa cibernética nesses países, outras áreas de conhecimento foram envolvidas para obtenção dos relatórios individuais de cada caso esses relatórios foram agrupados e comparados com base em sete aspectos: Ameaças e riscos, capacidades e resposta, poder e dominação, geopolítico e diplomático, sociocultural e organizacional, socioeconômico e comercial, e tecnológico e industrial. Na terceira fase, realizou-se uma análise comparativa apoiada nas especificidades geopolíticas da região, visando examinar as repercussões existentes na consolidação dessas políticas e estratégias desses três países sul-americanos. Observou-se que o Aspecto Sociocultural e Organizacional é relevante para os objetivos da segurança cibernética, enquanto o Aspecto Geopolítico e Diplomático é menos relevante para esses três países. Portanto, recomenda-se que os 7 aspectos estudados sejam aderidos no desenvolvimento das capacidades cibernéticas nacionais, buscando sua implementação nas estratégias multissetoriais da segurança cibernética dos países da América do Sul. O presente estudo buscou fortalecer nossas inferências, enriquecendo e inovando a pesquisa como um todo. Por fim, serão apresentadas as implicações teóricas, visando fornecer um panorama das configurações políticas e estratégicas no âmbito da segurança cibernética dos países de Argentina, Peru e Brasil.

Palavras-chave: Segurança cibernética; cibercapacidades; ciberpoder; geopolítica no ciberespaço; ciberindustrialização.

RESUMEN

La presente tesis busca comprender, desde una perspectiva comparativa, las políticas y estrategias en seguridad cibernética adoptadas por Argentina, Perú y Brasil. A través de la metodología aplicada, se logró identificar, sistematizar y analizar los elementos que están influyendo en la consolidación de las políticas de seguridad cibernética, así como considerar cómo estos elementos son tratados dentro de las especificidades geopolíticas de los países de América del Sur, con el objetivo de consolidar un modelo integrado para los países sudamericanos. Este estudio presenta un contexto relevante y contemporáneo dentro de dos modelos: social y pragmático. Por lo tanto, se optó por abordar bajo las directrices de la investigación cualitativa, de tipo explicativa. Con el fin de comprender el papel del Estado en la seguridad cibernética y las implicaciones generadas en la sociedad contemporánea, se procuró analizar la lógica de las diferentes formas de interacción entre el Estado y la sociedad, a través de las relaciones existentes entre los agentes y la dinámica de la acción pública en la seguridad cibernética. Para ello, se adoptó el método de análisis de contenido computacional, que incluyó un total de 108 documentos digitales, 06 entrevistas y 28 cuestionarios individuales, conformando así nuestro proyecto de casos múltiples contexto. Dada la complejidad multifacética del tema de investigación, se elaboró un Estado del Arte, con el desarrollo del caso prototipo estadounidense, contribuyendo a los conceptos y conclusiones principales de la defensa y seguridad cibernética estadounidenses, aunque afirmamos que el caso prototipo sirvió como nuestro laboratorio. Esta etapa permitió la identificación de la historicidad, los elementos y los agentes involucrados en la concepción de la política y estrategia estadounidenses, destacando el Aspecto de Poder y Dominación como relevante para la seguridad cibernética de los Estados Unidos. En la segunda fase, se elaboraron los estudios de casos de Argentina, Brasil y Perú. Debido a la escasa producción de textos electrónicos oficiales en seguridad y defensa cibernética en estos países, se involucraron otras áreas de conocimiento para la obtención de los informes individuales de cada caso. Estos informes se agruparon y compararon en base a siete aspectos: Amenazas y riesgos, capacidades y respuesta, poder y dominación, geopolítico y diplomático, sociocultural y organizacional, socioeconómico y comercial, y tecnológico e industrial. En la tercera fase, se realizó un análisis comparativo apoyado en las especificidades geopolíticas de la región, con el fin de examinar las repercusiones existentes en la consolidación de estas políticas y estrategias de estos tres países sudamericanos. Se observó que el Aspecto Sociocultural y Organizacional es relevante para los objetivos de la seguridad cibernética, mientras que el Aspecto Geopolítico y Diplomático es menos relevante para estos tres países. Por tanto, se recomienda que los 7 aspectos estudiados estén adheridos en la elaboración de las capacidades cibernéticas nacionales, buscando su implementación en las estrategias multisectoriales de la seguridad cibernética de los países sudamericanos. El presente estudio buscó fortalecer nuestras inferencias, enriqueciendo e innovando la investigación como un todo. Por último, se presentarán las implicaciones teóricas, con el objetivo de proporcionar un panorama de las configuraciones políticas y estratégicas en el ámbito de la seguridad cibernética de los países de Argentina, Perú y Brasil.

Palabras clave: Ciberseguridad; cibercapacidades; ciberpoder; geopolítica en el ciberespacio; ciber-industrialización.

ABSTRACT

This thesis seeks to understand, from a comparative perspective, the cybersecurity policies and strategies adopted by Argentina, Peru and Brazil. Through the methodology applied, it was possible to identify, systematize and analyze the elements that are influencing the consolidation of cybersecurity policies, as well as to consider how these elements are treated within the geopolitical specificities of the countries of South America, with the aim of consolidating an integrated model for South American countries. This study presents a relevant and contemporary context within two models: social and pragmatic. Therefore, it was decided to approach it under the guidelines of qualitative research, of an explanatory type. To understand the role of the State in cybersecurity and the implications generated in contemporary society, it was sought to analyze the logic of the different forms of interaction between the State and society, through the existing relationships between agents and the dynamics of public action in cybersecurity. To this end, the computational content analysis method was adopted, which included a total of 108 digital documents, 06 interviews and 28 individual questionnaires, thus forming our multiple context case project. Given the multifaceted complexity of the research topic, a State of the Art was elaborated, with the development of the American prototype case, contributing to the main concepts and conclusions of American defense and cybersecurity, although we affirm that the prototype case served as our laboratory. This stage allowed for the identification of the historicity, elements, and agents involved in the conception of U.S. policy and strategy, highlighting the Power and Domination Aspect as relevant to U.S. cybersecurity. In the second phase, case studies from Argentina, Brazil and Peru were developed. Due to the scarce production of official electronic texts on cybersecurity and cyber defense in these countries, other areas of knowledge were involved in obtaining the individual reports of each case. These reports were grouped and compared based on seven aspects: Threats and risks, capabilities and response, power and domination, geopolitical and diplomatic, sociocultural and organizational, socioeconomic and commercial, and technological and industrial. In the third phase, a comparative analysis was carried out based on the geopolitical specificities of the region, to examine the existing repercussions on the consolidation of these policies and strategies of these three South American countries. It was noted that the Sociocultural and Organizational Aspect is relevant to cybersecurity objectives, while the Geopolitical and Diplomatic Aspect is less relevant for these three countries. Therefore, it is recommended that the 7 aspects studied be adhered to in the development of national cyber capacities, seeking their implementation in the multisectoral cybersecurity strategies of South American countries. The present study sought to strengthen our inferences, enriching and innovating the research. Finally, the theoretical implications will be presented, with the aim of providing an overview of the political and strategic configurations in the field of cybersecurity in the countries of Argentina, Peru and Brazil.

Keywords: Cybersecurity; Cyber Capabilities; Cyber Power; Geopolitics in Cyberspace; Cyber Industrialization.

LISTA DE ACRÔNIMOS E ABREVIATURAS

AECID - Agência Espanhola de Cooperação Internacional para o Desenvolvimento

AFI - Agência Federal de Inteligência

AFP - Administração Pública Federal

ARPANET - Advanced Research Projects Agency Network

ATM - Automatic Teller Machine

BRICS - Brasil, Rússia, Índia, China e África do Sul

BID - Banco Interamericano de Desenvolvimento

CAEM - Centro de Altos Estudos Militares

CAEN - Centro de Altos Estudos Nacionais

CCDCOE - Centro de Excelência em Defesa Cibernética Cooperativa da OTAN

CDCiber - Centro de Defesa Cibernética

CDMC - Corpus da Doutrina Militar Conjunta

CDS - Conselho de Defesa Sul-americano

CEO – Chief Executive Officer

CFR - Council on Foreign Relations

CICTE - Comitê Interamericano Contra o Terrorismo

CIGE - Comando de Comunicações e Guerra Eletrônica do Exército

CMM - Capability Maturity Model

CNO - Computer Network Operations

CONCYTEC - Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica

CoE - Council of Europe

COST - The Cost Shutdown Tool

CPI - Comissão Parlamentar de Inquérito

CSDN - Corpus da Segurança e Defesa Nacional

CSPMD - Conselho Sobre o Problema Mundial da Drogas

CSS - Central Security Agency

C2 - Command and Control

DARPA - Defense Advanced Research Projects Agency

DIVINDAT - Divisão de Investigação de Delitos de Alta Tecnologia

DoD - Departamento da Defesa dos Estados Unidos

DSIC - Departamento de Segurança da Informação e Comunicações
DSN - Doutrina da Segurança Nacional
EB – Exército Brasileiro
EU – União Europeia
EUA – Estados Unidos da América
FBI - Federal Bureau of Investigation
FEBRABAN - Federação Brasileira de Bancos
FEM - Fórum Econômico Mundial
FIRST - Forum of Incident Response and Security Teams
GCSCC - Global Cyber Security Capacity Centre
GIE - Global Information Environment
GII - Global Information Infrastructure
GPS - Global Position System
GSIPR - Gabinete de Segurança Institucional da Presidência da República
G7 – Grupo dos 7
G8 - Grupo dos 8
G20 – Grupo dos 20
HIIP - Harvard Information Infrastructure Project
IA – Inteligência Artificial
IANA - Autoridade para Atribuição de Números de Internet
IC - Infraestruturas Críticas
ICANN - Corporação da Internet para Atribuição de Nomes e Números
ICCC - International Computer Communication Conference
IDEP - Infraestrutura de dados espaciais do Peru
IEEE - Institute of Electrical and Electronics Engineers
IETF - Internet Engineering Task Force
INCIBE - Instituto Nacional de Cibersegurança da Espanha
IO - Information Operations
ISOC – Internet Society
JFC - Joint force Commander
JP – Joint Publication
MERCO - Monitor Empresarial de Reputação Corporativa
MIE - Military Information Environment
MIT - Massachusetts Institute of Technology

NCA - National Command Authorities
NCP - Network Control Protocol
NWG - Network Working Group
NSA - National Security Agency
NSS - National Security Strategy
OEA - Organização dos Estados Americanos
OCDE - Organização para a Cooperação e Desenvolvimento Econômico
OIT – Organização Mundial do Trabalho
OMC – Organização Mundial do Comércio
ONGEI - Escritório de Governo Eletrônico e Informática
ONU – Organização das Nações Unidas
ONTI - Oficina Nacional de Tecnologias de Informação
OSCE – Organismo para a Segurança e Cooperação Europeia
OTAN – Organização do Tratado do Atlântico Norte
PDD - Diretiva de Política Presidencial
PF - Polícia Federal
PIB - Produto Interno Bruto
PIDE - Plataforma de interoperabilidade do Estado
PNP – Polícia Nacional do Peru
RCP - Rede Científica Peruana
RIR - Regional Internet Registry
SEDENA - Secretaria da Defesa Nacional
SEGDI - Secretaria de Governo Digital
SSAs - Sector Specific Agencies
SSIG - Escola Sul da Governança da Internet
SUNAT - Superintendencia Nacional de Aduanas y de Administración Tributaria
TIAR - Tratado Interamericano de Assistência Recíproca
TIC – Tecnologias da Informação e da Comunicação
UIT - União Internacional das Telecomunicações
UNASUR - União das Nações Sul-Americanas
UNGA - UN General Assembly
UNIDIR - United Nations Institute for Disarmament Research
URSS - União de Repúblicas Socialistas Soviéticas
USAFRICOM - United States África Command

USC - Códigos dos Estados Unidos

USCENTCOM - United States Central Command

USCyberComm - United States Cyber Command

USEUCOM - United States European Command

USINDOPACOM - United States Indo-Pacific Command

USNORTHCOM - United States Northern Command

USSOUTHCOM - United States Southern Command

WAN - Wide Area Network

WSIS - World Summit on the Information Society

WWW - World Wide Web

W3C - World Wide Web Consortium

3GPP - 3rd Generation Partnership Project

LISTA DE FIGURAS

Figura 1 - Países membros do TIAR (cor azul)	55
Figura 2 - Domínio físico versus domínio da política.....	69
Figura 3 - Distribuição geográfica dos comandos dos Estados Unidos.....	71
Figura 4 - Construção organizacional do Comando e Controle (C2), nas operações do ciberespaço.	73
Figura 5 - As três áreas de tensão política da segurança cibernética	81
Figura 6 - Criticidade do risco (Impacto x Probabilidade).....	85
Figura 7 - Principais sistemas de controle e observação do espaço cibernético.....	91
Figura 8 - Mapeamento mundial dos Data Centers certificados TIER.....	94
Figura 9 - Mapeamento do cabeamento de fibra óptica da Internet mundial.	96
Figura 10 - As cinco dimensões segundo o CMM	119
Figura 11 - Dimensão, fator, aspecto e indicadores por camadas	120
Figura 12 - Foco multidimensional da segurança nacional	125
Figura 13 - A CPI dos crimes cibernéticos: projetos de leis	134
Figura 14 - Organização da análise de conteúdo.....	148
Figura 15 - Diagrama de fluxo metodológico.....	151
Figura 16 - Organização dos documentos no software MAXQDA.....	155
Figura 17 - Código e subcódigos.....	157
Figura 18 - Nuvem de palavras: frequências de palavras	158
Figura 19 - Nuvem de palavras: combinações de palavras.....	159
Figura 20 - Frequência de códigos (unidade: segmentos com códigos)	159
Figura 21 - Mapa de códigos corpus: CDMC	161
Figura 22 - Mapa de códigos corpus: CSDN.....	161
Figura 23 - Mapa de códigos conjunto	162
Figura 24 - Visualizador das conexões entre códigos	163
Figura 25 - Visualizador das conexões entre os códigos	163
Figura 26 - Nuvem de códigos conjuntos	164
Figura 27 - Visualizador da matriz de códigos norte-americano.....	168
Figura 28 - Estrutura de palavras interativas do CDMC	169
Figura 29 - Organização dos documentos do caso argentino	173
Figura 30 - Organização dos documentos do caso peruano.....	173
Figura 31 - Nuvem de palavras do caso argentino.....	174

Figura 32 - Combinações de palavras caso argentino	175
Figura 33 - Frequência de códigos caso argentino	175
Figura 34 - Mapa de códigos corpus caso argentino.....	176
Figura 35 - Visualizador das conexões entre códigos	177
Figura 36 - Nuvem de códigos caso argentino	178
Figura 37 – Frequência das categorias com tabela cruzada do caso argentino.....	178
Figura 38 - Visão geral dos códigos no primer nível dos questionários analisados do caso argentino (categorias)	179
Figura 39 - Nuvem de palavras do caso peruano.....	180
Figura 40 - Combinações de palavras caso peruano	181
Figura 41 - Frequência de códigos caso peruano (unidade: segmentos com códigos)	182
Figura 42 - Mapa de códigos corpus caso peruano	183
Figura 43 - Visualizador das conexões entre códigos caso peruano	184
Figura 44 - Nuvem de códigos caso peruano.....	184
Figura 45 - Comparar frequências de categorias com tabela cruzada do caso peruano	185
Figura 46 - Visão geral dos códigos no primer nível dos questionários analisados do caso peruano (categorias).....	185
Figura 47 - Nuvem de palavras do caso brasileiro	186
Figura 48 - Combinações de palavras caso brasileiro.....	187
Figura 49 - Frequência de códigos caso brasileiro	187
Figura 50 - Mapa de códigos corpus caso brasileiro	188
Figura 51 - Visualizador das conexões entre códigos caso brasileiro	189
Figura 52 - Nuvem de códigos caso brasileiro	190
Figura 53 - Comparar frequências de categorias com tabela cruzada do caso brasileiro.....	190
Figura 54 - Visão geral dos códigos no primer nível dos questionários analisados do caso brasileiro (categorias)	191
Figura 55 - Árvore de palavras interativas do estudo de caso argentino (KWIC: “personas y organizaciones”)	199
Figura 56 - Árvore de palavras interativas do estudo de caso argentino (KWIC: “seguridad de la información”).....	199
Figura 57 - Visualizador da matriz de códigos caso argentino	201

Figura 58 - Visualizador da matriz de códigos nos questionários do caso argentino	202
Figura 59 - Subcódigos e códigos não identificados: Argentina e Peru	222
Figura 60 - Árvore de palavras interativas do estudo de caso peruano (KWIC: “capacidades”).....	224
Figura 61 - Visualizador da matriz de códigos caso peruano	226
Figura 62 - Matriz de códigos dos respondentes, caso peruano	226
Figura 63 - Árvore de palavras interativas do caso brasileiro (KWIC: Internet)	253
Figura 64 - Árvore de palavras interativas do caso brasileiro (KWIC: Segurança Cibernética).....	254
Figura 65 - Visualizador da matriz de códigos caso brasileiro	256
Figura 66 - Matriz de códigos dos respondentes, caso brasileiro.....	256
Figura 67 - Cronologia dos eventos mais importantes da história da Internet, desde as 4 dimensões chaves	333
Figura 68 - Os ambientes da informação: Global e Militar	333
Figura 69 - Missões, ações e forças nas operações do ciberespaço.....	334
Figura 70 - A influência do espectro ciber-eletromagnético nos outros 4 domínios da batalha.	334
Figura 71 - Políticas nacionais e documentos legais em segurança cibernética (OTAN-CCDCOE)	335
Figura 72 - Ano de publicação Vs quantidade de publicações (OTAN-CCDCOE) ..	335
Figura 73 - Proliferação das unidades militares de CNO	335
Figura 74 - Países por continente que pertencem a um organismo internacional...	336
Figura 75 - Linha de tempo, das ações realizadas pela ONGEI.....	336
Figura 76 - Formulação das políticas no Peru.....	337
Figura 77 - Mudanças estruturais na PCM.....	337
Figura 78 - Hierarquia de documentos da segurança e defesa nacional	338
Figura 79 - Secretaria de segurança - Argentina.....	338
Figura 80 - Subsecretaria de tecnologia e cibersegurança – Argentina	339
Figura 81 - Subsecretaria de tecnologia e cibersegurança – Brasil	339

LISTA DE QUADROS

Quadro 1 - A Doutrina de Segurança Nacional na América do Sul	55
Quadro 2 - As quatro dimensões chaves da história da Internet.....	63
Quadro 3 - Linha de mando dos documentos no planejamento da segurança nacional	68
Quadro 4 - Histórico papel do estado na política de segurança cibernética.....	79
Quadro 5 - Riscos do Fórum Econômico Mundial (FEM) 2017-2018	84
Quadro 6 - Evolução das principais teorias internacionais da geopolíticas	88
Quadro 7 - Esquema da visão global dos níveis envolvidos no ciberespaço	99
Quadro 8 - Tipos de transtornos de informações	108
Quadro 9 - Objetivos e diretrizes da SEDENA, com a segurança cibernética	123
Quadro 10 - Cooperação bilateral e multilateral em cybersecurity - Peru	124
Quadro 11 - Cooperação bilateral e multilateral em cybersecurity - Argentina.....	127
Quadro 12 - Os princípios e objetivos da estratégia nacional em segurança cibernética - Argentina	130
Quadro 13 - Base legal de defesa brasileira	131
Quadro 14 - Cooperação bilateral e multilateral em cybersecurity - Brasil.....	134
Quadro 15 - Síntese dos principais reflexos observados no referencial teórico	136
Quadro 16 - Entrevistas aos especialistas governamentais dos países estudados	149
Quadro 17 - Questionário aos especialistas dos países estudados	149
Quadro 18 – Questionário aos especialistas latino-americanos.....	150
Quadro 19 - Funções básicas do MAXQDA na análise qualitativo.....	155
Quadro 20 - Categorias e explicações provisórias do Estado da Arte	165
Quadro 21 - Síntese quantitativa dos reflexos observados na Argentina, Peru e Brasil	191
Quadro 22 - Categorias do caso argentino	196
Quadro 23 - Categorias do caso brasileiro	249
Quadro 24 - Síntese qualitativa dos reflexos observados: Argentina, Peru e Brasil.	279
Quadro 25 - Autoridades com responsabilidade no ciberespaço, segundo o código dos Estados Unidos	340

LISTA DE TABELAS

Tabela 1 - The cost shutdown tool (cost)	40
Tabela 2 - Dados do relatório da cibersegurança 2020- Peru	125
Tabela 3 - Dados do relatório da cibersegurança 2020- Argentina	128
Tabela 4 - Dados do relatório da cibersegurança 2020 - Brasil.....	135
Tabela 5 - Organização e características dos corpus estudados	172
Tabela 6 - Resumo do visualizador da matriz de códigos	223
Tabela 7 - Comparativo numérico de data centers certificados por TIER II, III e IV por continentes	341
Tabela 8 - Países com maior PIB (Produto Interno Bruto, 2019) por continentes ...	341
Tabela 9 - Data centers certificados por TIER, nos países do G-8	341
Tabela 10 - Data centers certificados por TIER dos países tratados na pesquisa ..	341

SUMÁRIO

1 INTRODUÇÃO	21
2 PROBLEMÁTICA E CONTEXTO DA PESQUISA.....	29
2.1 Problema da pesquisa.....	35
2.2 Objetivos	35
2.2.1 Objetivo geral	35
2.2.2 Objetivos específicos.....	35
2.3 Justificativa da pesquisa no âmbito da Ciência da Informação	36
2.4 Perspectivas teóricas que conduzem o contexto da pesquisa	43
2.5 Estrutura da tese	50
3 REFERENCIAL TEÓRICO.....	52
3.1 Historicidade da segurança e defesa nacional sul-americana.....	52
3.2 Historicidade do ciberespaço através da <i>Internet</i>	60
3.3 A Doutrina da Segurança Nacional (DSN) dos Estados Unidos, no âmbito do ciberespaço	67
3.4 Inferências iniciais da DSN cibernética dos Estados Unidos	74
3.5 A política de segurança cibernética, nos diferentes papéis do Estado.....	78
3.6 A geopolítica contemporânea: as disputas do poder mundial são econômicas? ..	83
3.7 O ciberespaço, é um <i>Global Common</i> ?.....	89
3.8 Os elementos estruturais para a construção do ciberespaço	93
3.8.1 O ciberespaço, elementos de construção: infraestrutura	93
3.8.2 O ciberespaço, elementos de construção: dados, informação e conhecimento	100
3.8.3 O ciberespaço, elementos de construção: automação e inteligência	109
3.8.4 O ciberespaço, elementos de construção: conectividade global e controle ...	113
3.9 As capacidades cibernéticas e os modelos de maturidade	117
3.10 Historicidade da política em segurança cibernética no Peru	120
3.11 Historicidade da política em segurança cibernética na Argentina	126
3.12 Historicidade da política em segurança cibernética no Brasil	130
3.13 Síntese dos reflexos observados no referencial teórico	136

4 METODOLOGIA	140
4.1 Tipologia da pesquisa	140
4.2 Delimitação da pesquisa	142
4.3 Técnicas de coleta de dados.....	145
 5 CASO PROTÓTIPO NORTE-AMERICANO	 154
5.1 Organização da análise.....	154
5.2 Análise e tratamento quantitativo dos corpus norte-americano.....	157
5.3 Análise qualitativa dos corpus: protótipo norte-americano	164
5.4 Conclusões do protótipo norte-americano.....	169
 6 APRESENTAÇÃO DOS DADOS DA PESQUISA QUANTITATIVA	 172
6.1 Organização e características dos corpus dos países estudados.....	172
6.2 Análise e tratamento quantitativo: estudo de caso argentino	173
6.3 Análise e tratamento quantitativo: estudo de caso peruano	179
6.4 Análise e tratamento quantitativo: estudo de caso brasileiro.....	186
6.5 Síntese quantitativa dos reflexos observados na Argentina, Peru e Brasil	191
 7 ANÁLISE QUALITATIVA DOS ESTUDOS DE CASOS PESQUISADOS	 194
7.1 Análise qualitativa do estudo de caso argentino	196
7.1.1 Aspecto das ameaças e riscos, segundo os especialistas argentinos	202
7.1.2 Aspecto das capacidades e resposta, segundo os especialistas argentinos	205
7.1.3 Aspecto do poder e dominação, segundo os especialistas argentinos	207
7.1.4 Aspecto geopolítico e diplomático, segundo os especialistas argentinos.....	209
7.1.5 Aspecto sociocultural e organizacional, segundo os especialistas argentinos	210
7.1.6 Aspecto socioeconômico e de mercado, segundo os especialistas argentinos	212
7.1.7 Aspecto tecnológico e industrial, segundo os especialistas argentinos	215
7.8 Relatório do estudo de caso argentino	217
7.2 Análise qualitativa do estudo de caso peruano	222
7.2.1 Aspecto das ameaças e riscos, segundo os especialistas peruanos	227
7.2.2 Aspecto das capacidades e resposta, segundo os especialistas peruanos	231
7.2.3 Aspecto do poder e dominação, segundo os especialistas peruanos	233

7.2.4 Aspecto geopolítico e diplomático, segundo os especialistas peruanos	235
7.2.5 Aspecto sociocultural e organizacional, segundo os especialistas peruanos	237
7.2.6 Aspecto socioeconômico e de mercado, segundo os especialistas peruanos	239
7.2.7 Aspecto tecnológico e industrial, segundo os especialistas peruanos	241
7.2.8 Relatório do estudo de caso peruano	244
7.3 Análise qualitativa do estudo de caso brasileiro	249
7.3.1 Aspecto das ameaças e riscos, segundo os especialistas brasileiros.....	256
7.3.2 Aspecto das capacidades e resposta, segundo os especialistas brasileiros	260
7.3.3 Aspecto do poder e dominação, segundo os especialistas brasileiros	263
7.3.4 Aspecto geopolítico e diplomático, segundo os especialistas brasileiros	266
7.3.5 Aspecto sociocultural e organizacional, segundo os especialistas brasileiros	268
7.3.6 Aspecto socioeconômico e de mercado, segundo os especialistas brasileiros	269
7.3.7 Aspecto tecnológico e industrial, segundo os especialistas brasileiros	272
7.3.8 Relatório do estudo de caso brasileiro	274
7.4 Síntese qualitativa dos reflexos observados na Argentina, Peru e Brasil	279

8 ANÁLISES E CONCLUSÕES FINAIS ENTRE OS ESTUDOS DE CASOS

PESQUISADOS	285
8.1 Conclusões do relatório de casos cruzados	286
8.2 Modificando a teoria e desenvolvendo as implicações teóricas	293

9 CONCLUSÕES FINAIS E PROPOSTAS PARA TRABALHOS FUTUROS

REFERÊNCIAS	304

APÊNDICES	315

“No sé con qué armas se luchará en la III Guerra Mundial, pero la IV Guerra Mundial será luchada con palos y piedras”

Albert Einstein

1 INTRODUÇÃO

Nesta última década, temos testemunhado mudanças imprevistas e transformações no âmbito tecnológico, geoeconômico e social. Esses acontecimentos têm repercutido na ordem, como na cadeia global, nos levando da luz às trevas, entre outras coisas, em um mundo atual de incertezas associadas ao paradoxo do progresso. É aí, onde cabe o conjunto de forças atuantes do bloco Sul-americano: governos, sociedade civil, organismos internacionais e regionais, instituições, empresas privadas e estatais; ajustar e controlar o leme da segurança, a fim de conduzir a um equilíbrio sociopolítico, de inclusão social e de redução de injustiças, desigualdades e violência em seus países integrantes.

A presente tese de doutorado, intitulada: **“Perspectiva comparada das políticas e estratégias em segurança cibernética no marco do panorama de suas configurações nos países da Argentina, Brasil e Peru”**, tem como objetivo identificar, sistematizar e analisar as políticas e estratégias aplicadas à segurança cibernética¹ dos países estudados. Busca-se auxiliar os países sul-americanos na formulação da política nacional em segurança cibernética, analisando a historicidade, os elementos e agentes envolvidos na concepção das políticas em segurança cibernética, levando em consideração as repercussões geopolíticas. Assim, serve de auxílio, como base teórica e de conhecimento para a comunidade acadêmica e *policy-markers* em sua busca de modelos de políticas em segurança cibernética no contexto da América Latina.

Hoje, podemos afirmar que o investimento na segurança do ciberespaço afeta na taxa de sucesso de outras iniciativas políticas de um país. No caso dos países sul-americanos, a capacidade dos recursos é limitada, como a falta de tecnologia para a

¹ Para a presente investigação, os termos de cibersegurança, segurança do ciberespaço e segurança cibernética serão citados dentro de uma mesma definição, nos limitando nesta tese aos aspectos etimológicos desses termos.

enfrentar seus principais problemas², ligados principalmente ao desenvolvimento socioeconômico. Por exemplo: corrupção, insegurança, educação precária, desemprego, pobreza, tráfico de drogas, insuficiência dos serviços básicos de saúde, entre outros. Dando origem a um primeiro pressuposto: As necessidades e ameaças da segurança e defesa nacional nos países sul-americanos são distintas em relação aos países desenvolvidos, especialmente daqueles países que possuem hegemonia político-tecnológica. Se conhece que os países sul-americanos enfrentam ameaças complexas, indefinidas e desestruturadas com problemas desordenados, ausência de uma identidade e dependência no âmbito do ciberespaço e da Internet. Sendo o ciberespaço uma parte intrínseca no desenvolvimento de qualquer país, a capacidade cibernética é crucial para os Estados progredirem e se desenvolverem nos âmbitos social, cultural, econômico e político. A necessidade de integrar capacidades cibernéticas na construção e desenvolvimento das políticas públicas tem sido discutida, estudada e documentada pela comunidade científico-acadêmica e pelos responsáveis no desenho e elaboração das políticas públicas.

A maioria dos países sul-americanos têm expectativas na chamada "Onda Digital³". Identificando-a como uma oportunidade sem prestar atenção suficiente às ameaças e riscos que ela pode implicar em seus interesses e identidades nacionais. Além disso, outros países mostram crescente ceticismo nas medidas necessárias para proteger e garantir seu espaço digital, sendo observado como uma "imposição ocidental" em seus governos. Como resultado, os países sul-americanos estão aumentando exponencialmente seu acesso ao ciberespaço, provavelmente, sem medidas de segurança adequadas, o que pode trazer danos ao Estado e à economia local, estando o progresso indissolivelmente ligado às Tecnologias da Informação e da Comunicação (TIC), necessitando de um aparato de suporte e de uma compreensão correta.

Ao longo da história, os avanços nas TIC, energia e tecnologias de transporte, biotecnologia e ciências da vida, agricultura e indústria, armas tecnológicas e outras áreas científico-técnicas têm desempenhado papéis importantes na

² Há uma listagem dos principais problemas da América Latina, tendo como referência, a pesquisa feita pelo *Ipsos Public Affairs*, dirigida à imprensa e líderes de opinião do ano 2016. Disponível em <https://www.ipsos.com/sites/default/files/publication/2016-03/6300415INF_V7_17Mar16.pdf>. Acesso em 15 de abril de 2020.

³ O rápido avanço da era digital, a confluência das redes sociais, dispositivos inteligentes, *Big Data* e *Cloud Computing*, representam uma grande oportunidade para as empresas. Os dados estão no centro desta oportunidade. Mas à medida que o digital amadurece, também vemos novas oportunidades emergentes para os consumidores aproveitarem seus dados. Para descrever essas oportunidades, devemos primeiro considerar as "três ondas" da era digital: Primeira onda digital: comércio. Segunda onda digital: resultado. Terceira Onda Digital: Poder do Consumidor. Disponível em <<https://www.mca.org.uk/news/updates/the-three-waves-of-the-digital-age>>. Acesso em 15 de abril de 2020.

condução de mudanças no caminho em que homens e mulheres dirigem seus negócios. Isso tem sido verdade em praticamente todas as áreas da atividade humana, incluindo negócios e bancos, indústria e manufatura, políticas governamentais e assuntos militares, relações internacionais, educação e pesquisa, relações sociais e culturais, assuntos políticos, entretenimento e notícias e em outro lugar. Dada a magnitude da mudança que a revolução em ciência e tecnologia tem o potencial de induzir, é de vital importância que compreendamos como esta revolução mudou, está mudando e continuará a mudar nosso mundo (Alberts, 1997, p. ii).

É vasta a literatura sobre mudanças nos modelos socioeconômicos. Segundo Dalio (2022) as criações tecnológicas e o desenvolvimento nos têm aperfeiçoado e levado a contínuas evoluções que caracterizam uma ordem mundial cambiante.

Avanços tecnológicos nas comunicações e nos transportes tornaram todo o mundo mais próximo, o que modificou profundamente a natureza dos relacionamentos das pessoas e impérios. Observamos tais aperfeiçoamentos evolucionários em quase tudo – maior expectativa de vida, melhores produtos, melhores formas de fazer as coisas etc. (Dalio, 2022, p.39).

Os mais recentes estudos tratam das evoluções na sociedade da informação e do conhecimento. Esta nova sociedade contempla a evolução da sociedade industrial com uma característica marcante. O acesso à informação considerada a matéria-prima fundamental para o desenvolvimento, dando origem a tensões entre o “desejo de um governo em manter secretas as informações por razões de segurança nacional e o direito do público à informação detida pelas autoridades públicas” (OSJI, 2013, p.ii). Segundo estudos de Masuda (1982), Dertouzos (1997) e Castells (1999), a sociedade da informação seria a próxima fase da evolução econômica da sociedade pós-industrial (Araújo, Melo, 2012, p.291). No entanto, não existe uma linha que defina os limites da sociedade da informação e da sociedade do conhecimento. Segundo Takahashi (2000, p.11) a sociedade da informação deve ser resultado da colaboração entre diferentes parceiros, nos níveis local, nacional e internacional. O compartilhamento das responsabilidades entre governantes, organizações privadas e a sociedade civil é um modelo básico de apoio na sociedade da informação.

O setor privado é o que dispõe da maior capacidade de investimento e de inovação, do dinamismo e das condições de ação abrangente e ao mesmo tempo capilarizada, que são necessários para converter a proposta do Programa Sociedade da Informação em realidade. [...]

O governo, nos níveis federal, estadual e municipal, tem o papel de assegurar o acesso universal às tecnologias de informação e da comunicação e a seus benefícios, independentemente da localização geográfica e da situação social do cidadão, garantindo níveis básicos de serviços, estimulando a interoperabilidade de tecnologias e de redes (Takahashi, 2000, p.11).

Porém, o modelo idealizado no livro verde da sociedade da informação no Brasil (Takahashi, 2000) apesar dos avanços significativos, problematizamos que nas duas décadas seguidas, ainda se evidenciam preocupações vigentes, como são:

- A desigualdade social na falta de inclusão digital.
- Não se tem alcançado um nível ideal na educação digital, principalmente, nas escolas públicas, sendo comprometida a inserção da população ao mercado digital.
- A elevada dependência estrangeira da infraestrutura de telecomunicações brasileira, sendo ainda insuficiente nas regiões mais vulneráveis.
- A resposta tardia na proteção e privacidade dos dados pessoais.
- Empresas nacionais, principalmente as pequenas e médias, enfrentam desafios na adoção de tecnologias avançadas, limitando sua competitividade frente às multinacionais e concorrência mundial.
- Mudança de paradigma do Estado com a sociedade brasileira, onde o Estado não é um intruso nem um mero facilitador do crescimento econômico. Sendo um investidor muito mais ousado em relação ao setor privado. O Estado não pode se curvar aos grupos de interesse que buscam dele doações, privatizações, rendas e privilégios desnecessários (Mazzucato, 2021).

Na denominada Era da Informação, complexidade e mudança são duas características definidoras do sucesso dos indivíduos, famílias, organizações, comunidades e sociedades. Dependendo da capacidade de adaptação, quase em tempo real, diante de situações complexas e dinâmicas. Ao longo da história, seres humanos precisaram se comunicar e trocar informações. No entanto, estas habilidades sempre foram complicadas pela distância e pelo tempo. O desejo de privacidade, segurança e conexão tem influenciado na forma como as comunicações foram utilizadas, muitas vezes impulsionando a "tecnologia" das comunicações.

Há 20 anos, a governança da Internet era uma questão técnica com algumas implicações políticas. Hoje, a governança da Internet é uma questão política fundamental com alguns componentes técnicos. Essa mudança está desafiando o equilíbrio institucional dentro do ecossistema global de governança da Internet e seus mecanismos de negociação governamentais e não-governamentais. Redes intergovernamentais como o G20, G7 e BRICS, ou organizações como a OTAN, OMC, OIT e OSCE, que no passado não tiveram nada ou pouco a ver com a governança da Internet, estão se tornando atores-chaves. Isso não significa que organizações técnicas como ICANN, IETF, ISOC, RIR, W3C, IEEE, 3GPP etc., que dominaram as discussões sobre governança da Internet nas últimas duas décadas, perderão seus papéis. O que vemos é uma nova "complexidade de

governança da Internet⁴". O reequilíbrio de poder dentro do ecossistema de governança da Internet impulsiona abordagens inovadoras para a formulação de políticas públicas relacionadas à Internet global e para maior cooperação entre partes interessadas governamentais e não governamentais, bem como para uma colaboração mais próxima entre os criadores de códigos e legisladores, tanto nacionalmente quanto globalmente (Wolfgang, 2018, p.6).

Uma das implicações da Era da informação tem sido transferir valor econômico significativo para longe dos recursos naturais e do trabalho físico, onde fontes substanciais de riqueza econômica são agora geradas por meio de informações e comunicação efetiva, predito por alguns para "se tornar a força dominante na definição e configuração das ações humanas, suas interações, atividades e instituições".

Podemos afirmar que a Internet e as tecnologias digitais estão transformando o mundo, em várias áreas da vida humana e de negócios. Assim, em maio de 2015, a Comissão Europeia, entre suas principais prioridades, apresentou os planos para a criação de um mercado único digital⁵. A estratégia para o mercado único digital inclui um conjunto de ações planejadas em três pilares: 1. Melhorar na Europa o acesso dos consumidores e empresas aos bens e serviços digitais; 2. Criar as condições e garantir a igualdade para que as redes digitais e os serviços inovadores possam prosperar; e 3. Maximizar o potencial de crescimento da economia digital. Segundo o Comissário da Economia e Sociedade digitais, Günther H. Oettinger (Comisión Europea, 2015), afirmou:

"Nossas economias e sociedades estão se tornando digitais. A prosperidade futura dependerá, em grande medida, de fazermos essa transição corretamente. A Europa, tem pontos fortes sobre os quais construir, mas também trabalho a ser feito, em particular para garantir que as indústrias se adaptem e os cidadãos aproveitem plenamente o potencial dos novos bens e serviços digitais. Temos que nos preparar para uma sociedade moderna, e vamos apresentar propostas que equilibrem os interesses dos consumidores e da indústria" (Comisión Europea, 2015).

⁴ O termo "governança da Internet" foi cunhado pelo *Harvard Information Infrastructure Project* (HIIP) em meados da década de 1990. Foi usado para esclarecer que a Internet não é gerenciada pelos governos. A Cúpula Mundial da ONU na Sociedade da Informação (WSIS) reconheceu o papel das partes interessadas não governamentais e adotou em Tunis (2005) uma definição de trabalho: "Governança da Internet é o desenvolvimento e aplicação por governos, setor privado e sociedade civil, em seus respectivos papéis, princípios compartilhados, normas, regras, procedimentos de tomada de decisão e programas que moldam a evolução e uso da Internet". A Agenda de Túnis também reafirmou quem "a autoridade política para questões de políticas públicas relacionadas à Internet é o direito soberano de "quando a Internet se tornou mais relevante para a segurança internacional e a economia global, foi introduzida a nova linguagem da "cibernética" (usada principalmente pelos ministérios das relações exteriores, defesa e interior) ou "digital" (usada principalmente pelos ministérios da economia) e assuntos de tecnologia e desenvolvimento).

⁵ Mercado único digital, a Internet e as tecnologias digitais estão transformando o mundo em que vivemos. Contudo, existem obstáculos em linha que impedem os cidadãos de se beneficiar totalmente dos bens e serviços disponíveis e as empresas e os governos de tirar pleno partido pleno das ferramentas digitais, para além de limitarem o espaço de manobra das empresas do setor da Internet e das *start-ups*. É necessário adequar o mercado único europeu à era digital eliminando barreiras regulamentares e passando dos atuais 28 mercados nacionais a um mercado único. Tal fato poderá representar uma contribuição de 415 mil milhões de euros por ano para a nossa economia e criar centenas de milhares de novos empregos. Disponível em <https://ec.europa.eu/commission/priorities/digital-single-market_es>. Acesso em 15 de abril de 2020.

O crescente uso de sistemas integrados nos serviços essenciais de uma nação tem facilitado o desenvolvimento, sem precedentes, na troca de dados e informações, mas ao mesmo tempo representam o aumento do risco e da dependência nas TIC. Perante este cenário, é vital ter consciência da segurança da informação, sendo uma preocupação antiga e pouco explorada como objeto de pesquisa sob a ótica da Ciência da Informação. Sendo um dos interesses da Ciência da Informação permitir que a informação seja um elemento de inclusão social, que conceda oportunidades de desenvolvimento à sociedade e aos sujeitos. diante um mundo conectado em rede e onde a informação flui, organizações privadas e governamentais necessitam de processos e controles de segurança para garantir e preservar suas informações diante uma gama de novas ameaças (Wagner, 2009).

Luís Alberto Moreno, Presidente do Banco Interamericano de Desenvolvimento, no relatório de cibersegurança de 2016, intitulado: "Cibersegurança, estamos preparados na América Latina e no Caribe?". Ele afirma que as vantagens da conectividade são inegáveis, e os latino-americanos e caribenhos adotam essas novas tecnologias com entusiasmo:

Hoje somos o quarto maior mercado móvel do mundo, a metade de nossa população usa a Internet e nossos governos utilizam cada vez mais mídia digital para se comunicar e prestar serviços aos cidadãos. [...] Uma análise de 49 indicadores mostra que muitos países da região são vulneráveis aos ataques cibernéticos potencialmente devastadores. Quatro de cada cinco países não têm estratégias de cibersegurança ou planos de proteção de infraestrutura crítica. Dois de cada três não possuem um centro de comando e controle de segurança cibernética. A grande maioria dos promotores não tem capacidade para processar cibercrimes (BID; OEA, 2016, p.IX).

O acesso à Internet, devido a sua natureza multidimensional e interativa, sua velocidade e alcance global com custos relativamente baixos, uma vez que, seus princípios de design descentralizado e aberto têm um potencial sem precedentes. Na efetiva aplicação do direito de buscar, receber e disseminar informações em sua dupla dimensão: individual e coletiva. A Internet, também serve de plataforma para a realização de outros direitos humanos como o direito de participar da vida cultural, bem como usufruir dos benefícios do progresso científico e tecnológico, o direito à educação (Artigo 14 do Protocolo de São Salvador), direito de reunião e associação (Artigos 15 e 16 da Convenção Americana), direitos políticos (Artigo 23 da Convenção Americana) e direito à saúde (Artigo 10 do Protocolo de São Salvador).

O crescimento irrefreável da Internet no mundo e a integração dos vários sistemas e serviços de informação conectados no ciberespaço tornaram a segurança cibernética como um fator importante. Por essa razão, na Assembleia Geral da Organização dos Estados Americanos (OEA), em 2004, os Estados membros aprovaram a Estratégia Interamericana Integral de Combate às Ameaças à Segurança Cibernética, na resolução AG/RES. 2004 (XXXIV-O/04), sendo estabelecido o mandato que permite à Secretaria do Comitê Interamericano Contra o Terrorismo (CICTE) trabalhar nas questões de segurança cibernética. A Secretaria do CICTE usa uma abordagem integrada na construção de capacidades em segurança cibernética entre os Estados membros, reconhecendo que a responsabilidade nacional e regional para a segurança cibernética recai sobre uma ampla gama de organizações públicas, como do setor privado, trabalhando nos aspectos políticos e técnicos para garantir um ciberespaço seguro (Assembleia Geral da OEA, 2004).

Os governos mais desenvolvidos têm implementado políticas e estratégias para a proteção e backup de suas informações, em três níveis: político-estratégico, operacional e tático. Por isso, no governo do presidente Obama foi aprovada a "Diretiva de Política Presidencial (PDD)-21: Segurança e resiliência da Infraestrutura Crítica e Substituição da Diretriz Presidencial de Segurança Interna 7", dirigido ao ramo executivo do governo dos EUA para tomar medidas em infraestruturas americanas críticas (IC).

O Programa de Segurança Cibernética do Comitê Interamericano Contra o Terrorismo (CICTE) da Organização dos Estados Americanos (OEA) até meados de 2018, conseguiu fornecer apoio a 10 países da região em suas Estratégias Nacionais de Segurança Cibernética. Sendo esses países: Colômbia, Chile, Costa Rica, Jamaica, México, Paraguai, Trinidad e Tobago, Panamá, Guatemala e República Dominicana.

No ano 2015, o Conselho da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) adotou e publicou a recomendação sobre a gestão do risco de segurança digital, para a prosperidade econômica e social da OCDE. Sendo instruído o desenvolvimento de estratégias nacionais destinadas à gestão da segurança digital e à otimização dos benefícios no desenvolvimento econômico e social desejados na abertura digital. Este marco encoraja os países a adotarem um enfoque baseado na gestão dos riscos e alinhados aos oito princípios de alto nível inter-relacionados, independentes e complementares:

- Sensibilização, aquisição de habilidades e empoderamento.
- Responsabilidade dos interessados.
- Direitos humanos e valores fundamentais.
- Cooperação.
- Avaliação do risco e ciclo de tratamento.
- Medidas de segurança apropriadas de acordo com o risco e a atividade econômica e social em jogo.
- Inovação.
- Planejamento da preparação e continuidade.

A OCDE defende a implementação desses oito princípios junto a outros marcos internacionais, a fim de os países possam desenvolver melhores políticas e estratégias, desde a gestão digital do risco de segurança. Estes oito princípios não são um marco per se, mas sim componentes-chaves onde é possível estabelecer ou melhorar os mecanismos de coordenação dentro do governo e com as partes interessadas não governamentais. A OCDE reconhece que a cooperação público-privada é essencial para a redução do risco cibernético (Hathaway, 2018).

Portanto, através desta pesquisa, queremos compreender quais elementos e categorias se influenciam na consolidação de uma política em segurança cibernética, tendo em consideração as especificidades geopolíticas na América do Sul.

“Precisamos resolver nossos monstros secretos, nossas feridas clandestinas, nossa insanidade oculta. Não podemos nunca esquecer que os sonhos, a motivação, o desejo de ser livre nos ajudam a superar esses monstros, vencê-los e utilizá-los como servos da nossa inteligência. Não tenha medo da dor, tenha medo de não a enfrentar, criticá-la, usá-la”

Michael Foucault

2 PROBLEMÁTICA E CONTEXTO DA PESQUISA

O domínio cibernético está passando por mudanças extraordinárias, as quais geram oportunidades excepcionais para o sujeito do ciberespaço. A evolução é evidente, seja no crescente número de participantes no ciberespaço, como na qualidade da participação técnica e social. Porém, as tendências no ciberespaço, também representam grandes desafios. Estes desafios surgem a partir da utilização do ciberespaço por atores maliciosos, como terroristas, criminosos etc. A partir das inúmeras vulnerabilidades que afligem o ciberespaço, por exemplo, os desafios na atribuição, a indisponibilidade dos serviços públicos online e a infiltração ou corrupção de dados sigilosos e sensíveis. Estes desafios incluem o aumento da capacidade humana na resolução dos problemas cibernéticos, o equilibrar as liberdades civis com considerações de segurança nacional e o desenvolver a parceria internacional necessária para enfrentar os desafios cibernéticos (Kramer, Starr, Wentz, 2009, tradução nossa).

Podemos afirmar que na Internet existe o potencial de facilitar melhorias sociais: nos direitos humanos e das minorias, nas condições de vida, da economia etc., mas, na realidade paralela, observa-se que a Internet é utilizada para corroer a privacidade e aumentar a concentração do poder econômico, gerando uma imensa bolha de desigualdades e questionamentos socioeconômicos. Esta perspectiva da problemática é utilizada a serviço dos interesses de alguns indivíduos muito ricos, ou de certos interesses geoeconômicos e geopolíticos (Hill, 2014, tradução nossa).

De acordo com as pesquisas da empresa norte-americana Verizon, no relatório de 2018, mais do 60% dos casos de violação de dados, os invasores demoraram segundos a minutos em ingressar nos sistemas das organizações. Em 60% desses

casos, estas organizações demoraram meses em descobrir os ataques. Verificou-se ainda que 76% das violações foram motivadas por interesses financeiros. Nos países Sul-americanos foram encontrados casos de infiltrações de informações nas esferas dos altos funcionários do governo, de empresas privadas de interesse estratégico e político, no tratamento não autorizado dos dados pessoais, no monitoramento dos cidadãos, roubos cibernéticos a bancos e caixas eletrônicas ATM⁶ (que aconteceu durante o período de investigação desta tese, no dia 24 de maio de 2018, sendo afetado o Banco de Chile⁷).

Segundo Kuehl (2009, p.42, tradução nossa), a estratégia de segurança nacional norte-americana de 1980 faz referência explícita às ligações entre a informação e o poder econômico. Desde o ano de 1990, quase ao final do mandato do governo de Clinton, o rol das informações foi explicitamente reconhecido e explorado no diplomático, militar e econômico. No ano 2009, com o governo de Obama, foi declarado o ano da conscientização nacional no desenvolvimento das competências em informação. Consequentemente, foi aprovada no ano de 2013 a Diretiva da Política Presidencial (PDD-21⁸), que faz referência à segurança e resiliência das IC norte-americanas; sendo dirigida ao ramo Executivo do governo para providenciar medidas nas IC, tanto nas públicas quanto nas privadas. Com a responsabilidade de coordenar e fortalecer a segurança e resiliência das IC para a continuidade das funções essenciais nacionais e dos esforços conjuntos a serem feitos pelas Agências Setoriais Específicas (SSAs – *Sector Specific Agencies*) de conformidade com a orientação estratégica do Secretário da Segurança Nacional. Portanto, na historicidade da segurança cibernética norte-americana foram-se adotando decisões no nível das políticas públicas, estando as atenções do governo norte-americano, além de seu território e de suas fronteiras, centradas mais no intangível que é a informação e o conhecimento.

Os Estados Unidos, estavam na vanguarda do desenvolvimento de forma específica em compreender os benefícios e os riscos emergentes da “Era da Informação”. Enquanto outros países começaram a pensar na Era da

⁶ Conhecido como *ATMJackpot*, o novo malware ATM foi identificado por pesquisadores de segurança da informação no *Netskope Threat Research Labs*. A investigação inicial revelou que o malware se originou em Hong Kong, enquanto o binário com data e hora é identificado como o 28 março de 2018. Em janeiro de 2018, EUA testemunhou o primeiro ataque de *jackpot* contra caixas eletrônicos. O Serviço Secreto emitiu um alerta de segurança e lançou uma operação global contra membros do notório grupo *Carbanak*, que se acredita estar envolvido em ataques a caixas eletrônicos e roubo de mais de US \$ 1,24 milhão.

⁷ Disponível em: < <https://ww3.bancochile.cl/wps/wcm/connect/nuestro-banco/porta/sala-de-prensa/noticias-y-comunicados/declaracion-publica2> >. Acesso em 15 abril de 2020.

⁸ Disponível em < <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil> >. Acesso em 11 abril de 2020.

Informação e na política, especialmente nas necessidades de proteção das infraestruturas de críticas de informações no final dos anos 1990, muitos dos conceitos de políticas e percepções de ameaças foram adotados dos Estados Unidos, pelo menos em seus traços gerais (Dunn, Egloff, 2019, p. 44, tradução nossa).

Segundo Camati (2015), o governo moderno não está mais preocupado com o território; sua preocupação se dirige à população, logo há uma mudança na ação governamental. Para Foucault (2009, p.126-127), a meta essencial do governo é a introdução da economia no seio do exercício político, onde governar um Estado seria, portanto, aplicar a economia. É neste ponto que McChesney (2014) na perspectiva da economia política da comunicação, comenta da maximização do *Laissez-Faire*⁹ na Internet, frequentemente citado como Neoliberalismo. Esta maximização traz como consequência a concentração do poder e riqueza, perturbando os meios de comunicação tradicionais, reduzindo a concorrência e a escolha, minando as ideais da democracia em benefício de uma concentração natural dos monopólios.

Em consequência, as políticas públicas estariam ligadas não somente aos projetos ideológicos, sendo projetos mais amplos, como o controle dos comportamentos, a construção da passividade, da docilidade dos indivíduos, o governo de condutas, a padronização de comportamentos e a restrição de possibilidades de contraposições, sendo possível e evidente, através do ciberespaço. Portanto, essas políticas deverão prestar mais atenção à ecologia social digital (Huamani, Moura, 2024a) onde acontecem as relações de produção e de poder entre os sujeitos e o ambiente informacional. Nela é tratada a interdependência dos sujeitos, dispositivos, coletivos e instituições. Contudo, buscar uma compreensão na perspectiva do regime de informação poderia trazer certas dificuldades, devido que a preocupação primária dos fenômenos imersos na segurança cibernética dos três países em questão, não radica integralmente na política dos corpos. Inferimos que a produção do capitalismo contemporâneo está determinado no imaterial e incorpóreo, contrastando desta forma com a biopolítica disciplinar como força produtiva. Para o capitalismo contemporâneo a força produtiva desejada é a psique. Assim, os limites do regime panóptico e escópico são superados desde desenho e integração entre os dispositivos e artefatos digitais, como a inteligência artificial, *Distributed Ledger*

⁹ Lê-se o artigo *Making Laissez-Faire* do Jamie Peck, Disponível em: https://www.researchgate.net/publication/242161198_Making_laissez-faire. Acesso em 21 Set 2020.

*Technology*¹⁰ (DLT), *Smart contracts*¹¹, *tokenização*¹², *web 3.0*¹³ e *mecanismos de consenso*¹⁴.

“Regímenes da vigilância: “O regime panóptico, o regime escópico e o regime de rastreamento. O primeiro refere-se à vigilância disciplinar que se exerce em ambientes circunscritos. O regime escópico corresponde à distribuição proliferante, com propósitos variados, de câmeras de registro e visualização de imagens, em lugares estratégicos de ambientes fechados e abertos. O terceiro regime brotou do universo digital e a complexa malha do seu tecido torna-se cada vez mais fina” (Santaella, 2010, p. 154).

Em resumo, é necessária a interlocução das teorias de regime de informação e ecologia social digital, a través da análise crítica das inovações e tecnologias disruptivas. Nesta pesquisa abordamos o regime de informação como instrumento que subsidia a compreensão dos atores, dispositivos, artefatos e ações informacionais condicionadas pelo regime. E a ecologia social digital para explorar as relações e dinâmicas no ecossistema informacional e midiático. Portanto, nossa proposta é a junção de ambas as teorias, vistas como uma dinâmica do microcosmo (regime de informação) e macrocosmo (ecologia social digital).

Outra ideia relevante, é que nunca se governa um Estado, um território, uma estrutura política, mas quem é governado são sempre pessoas, homens, indivíduos ou coletividades (Foucault, 2009, p.164).

A razão de Estado sempre esteve à serviço da manutenção e ampliação do Estado, claro que com o advento do liberalismo essa relação sofreu algumas transformações, o que de certa forma enfraqueceu o Estado e fortaleceu as grandes corporações que dominam o poder econômico no mundo contemporâneo (Camati, 2015, p.183).

Nesse sentido, as políticas públicas compõem a intervenção do Estado em resposta a uma situação problemática presente na sociedade. Então, no âmbito informacional, o Estado é o agente da elaboração e implementação da política, porém o domínio de seu exercício são a ciência e a tecnologia. Contudo, “apesar de muitos e importantes esforços, a formulação das políticas de informação não consegue o sucesso esperado nos países de desenvolvimento” (González de Gómez, 2002, p.28).

¹⁰ Distributed Ledger Technology (DLT): “é um sistema digital para registrar transações de ativos nos quais as transações e seus detalhes são registrados em vários lugares ao mesmo tempo” (CUNHA, 2024, p.22).

¹¹ Contratos inteligentes (Smart contracts): “entendo os smart contracts como um mecanismo condicional que determina se avançarmos ou não em certas operações” (CUNHA, 2024, p.19).

¹² Tokenização: “é o processo de converter direitos sobre um ativo em um token digital de uma blockchain” (CUNHA, 2024, p.32).

¹³ Web 3.0: “que será o próximo passo de desenvolvimento da Internet, que terá, entre outros aspectos, a função de dinheiro implícita a ela. Tudo isso via tokens e redes de blockchain” (CUNHA, 2024, p.30).

¹⁴ Mecanismos de consenso: “é por meio deles que são colocados os incentivos para que as redes de Blockchain sigam funcionando da forma como foram projetadas” (CUNHA, 2024, p.26).

Então, é possível inferir que as políticas e estratégias sobre segurança cibernética dos países desenvolvidos¹⁵ exercem influência na concepção das políticas nacionais de segurança cibernética dos países na América do Sul¹⁶.

No pressuposto, que as políticas e estratégias em segurança cibernética não estão de acordo com a realidade problemática, nem do contexto das necessidades e interesses nacionais dos países na América do Sul, a influência sofrida, levanta a possibilidade de que compreendemos mal os pontos fortes e fracos das políticas, sendo necessária uma perspectiva alternativa. Os encarregados de criar e propor as políticas públicas têm buscado explicações sobre o suposto, onde o problema da insegurança no ciberespaço deve ser tratado sob a natureza do pensamento sistêmico, na interação de homens e máquinas, dando maior importância à parte tecnológica, em contraste com a parte social e política. Isso leva a uma compreensão frágil e pouco estudada da historicidade, geopolítica, ameaças e riscos que se relacionam com a segurança cibernética sul-americana.

A necessidade de analisar e sistematizar, com vista a um modelo integrado entre as comunidades de desenvolvimento tecnológico, incubadas principalmente nos países desenvolvidos e nas empresas multinacionais, como nos países que recebem e acolhem essas tecnologias, nos conduz a buscar uma teoria abrangente, robusta e articulada no âmbito da cibernética. Essa teoria deve ser capaz de descrever, explicar e prever como os países podem fazer um melhor uso do poder cibernético, apoiando os interesses nacionais e alinhando a compreensão das necessidades na segurança nacional, especialmente nos países sul-americanos.

Atualmente, o debate político e estratégico sobre a criação das capacidades cibernéticas tem estimulado o impacto do desenvolvimento cultural, geopolítico e socioeconômico nas estratégias de segurança e defesa nacional nos países. No grupo dos países que possuem um elevado nível de maturidade de sua capacidade cibernética, têm-se reportado casos¹⁷ de exigência do governo às empresas tecnológicas multinacionais em revelar ou fornecer suas informações e chaves criptográficas, justificados na segurança e defesa nacional. Esses projetos de segurança foram inseridos nos produtos tecnológicos, como software e hardware,

¹⁵ Basicamente são os líderes das tecnologias da informação e da comunicação.

¹⁶ Basicamente são os consumidores dessa tecnologia.

¹⁷ Por exemplo, o caso entre o FBI e a empresa Apple. Disponível em < <https://epoca.globo.com/vida/experiencias-digitais/noticia/2016/03/fbi-e-apple-apanas-o-fim-de-uma-batalha.html> >. Acesso em 13 de maio de 2020.

sendo subsequentemente introduzidos nos novos mercados¹⁸ para sua comercialização em massa. No caso citado, os produtos tecnológicos tornam-se vulneráveis, como aconteceu na República Popular da China¹⁹, cujo governo é suscetível à possibilidade de que novos produtos tecnológicos enfraquecerão a capacidade de monitoramento das comunicações de seus cidadãos, especialmente aqueles produtos tecnológicos que incorporam criptografia de seus dados. O acesso a esse código permite ao governo chinês exercer controle estrito sobre seus usuários na Internet, como no ciberespaço. Ao mesmo tempo, são incrementadas as capacidades chinesas na ciberguerra e ciberespionagem contra outros Estados que usam esses mesmos produtos.

Desde 1998, a Rússia propôs pela primeira vez um tratado de controle de armas cibernéticas para ser estabelecido entre os países membros da Organização das Nações Unidas (ONU). No ano 2004, foram constituídos seis grupos de trabalho de especialistas, com 3 pilares: (1) reconhecimento da aplicabilidade do direito internacional, (2) normas não vinculativas do comportamento do Estado em tempos de paz e (3) medidas de fortalecimento da confiança cibernética. Porém, na atualidade, persistem essas discrepâncias e falta de interesse em alguns Estados, especialmente nos mais desenvolvidos, para unificar esforços. O objetivo seria aprovar em maioria um contrato social que possa incluir novas normas nacionais e supranacionais, sanções e penas de prisão para os cibercriminosos. Estas são algumas das situações que estão em debate e estudo para uma solução nos diversos fóruns, organizações mundiais, Estados etc., apresentando desafios no desenho, elaboração e implementação na política e estratégias nacionais de segurança cibernética.

Os procedimentos para a implementação de uma estrutura em segurança cibernética, como a classificação dos ativos de infraestrutura crítica, de ameaças e riscos de acordo com uma determinada realidade que surge para a segurança cibernética nos países como os Estados Unidos, Inglaterra, Canadá, França, China e outros países desenvolvidos não foram uma questão de meses ou anos. Foram

¹⁸ O autor refere-se a casos públicos relatados, como Apple, Microsoft, Huawei, Google e outras multinacionais. Além das queixas feitas no site "Wikileaks" para os governos que estão realizando ciberespionagem em grandes escalas. Disponível em <https://search.wikileaks.org/?query=cyber+spy&exact_phrase=&any_of=&exclude_words=&document_date_start=&document_date_end=&released_date_start=&released_date_end=&publication_type%5B%5D=6&publication_type%5B%5D=50&new_search=False&order_by=most_relevant#results>. Acesso em 11 de abril de 2020.

¹⁹ Por exemplo o caso do bloqueio feito pela República Popular China com os serviços da empresa multinacional Google Inc. Disponível em <<https://extra.globo.com/noticias/saude-e-ciencia/servicos-da-google-na-china-como-os-de-celular-sao-alvo-de-bloqueios-106949.html>>. Acesso em 13 de maio de 2020.

necessárias várias décadas de experimentos e modelos de maturidade, sendo um modelo que aponta para o estabelecimento de indicadores que possibilitem comparações no desempenho, no nível de maturidade e no desenvolvimento organizacional. Buscando serem aperfeiçoados para estabelecer as bases de um desenvolvimento sustentado da segurança cibernética para seus cidadãos e para a nação em geral.

A complexidade está sempre aumentando em nosso ambiente informacional e organizacional, nas relações dinâmicas interdependentes com sistemas sócio-tecnológicos e produtivos, resultando em uma ampla variedade, incertezas, assimetrias e falta de informação e controle.

Nos países sul-americanos, há uma necessidade urgente para que as políticas e estratégias na segurança cibernética sejam adaptáveis a nossa realidade, para que suas informações estejam tratadas com medidas adequadas de proteção. Apoiados em soluções tecnológicas que facilitem e disponibilizem ao cidadão digital os serviços públicos vitais de uma nação: serviço energético, de água e saneamento, saúde, transporte etc. No hipotético cenário em que esses serviços fiquem indisponíveis e sem controle, isso produziria uma crise nacional, afetando até vidas humanas.

2.1 Problema de pesquisa

Que elementos e categorias são influenciadas na política de segurança cibernética e como a análise comparada pode ser considerada nas especificidades dos três países estudados?

2.2 Objetivos

2.2.1 Objetivo geral

Identificar, sistematizar e analisar em uma perspectiva comparada as políticas e estratégias de segurança cibernética implementadas notadamente na Argentina, Peru e Brasil, com vista em dispor do panorama das configurações políticas e estratégicas no âmbito da segurança cibernética.

2.2.2 Objetivos específicos

a. Identificar a historicidade da política e das estratégias da segurança cibernética na Argentina, Peru e Brasil.

- b. Constatar, sistematizar e analisar os elementos que constituem uma política de segurança cibernética.
- c. Reconhecer os agentes envolvidos na concepção das políticas e estratégias em segurança cibernética na Argentina, Peru e Brasil.
- d. Analisar a geopolítica da América do Sul com foco na Argentina, Peru e Brasil; e suas repercussões para a consolidação das políticas e estratégias em segurança cibernética.
- e. Elencar sugestões com base nos reflexos observados em cada um dos países estudados, no que tange às políticas e estratégias em segurança cibernética.

2.3 Justificativa da pesquisa no âmbito da Ciência da Informação

A problemática explicitada traz à discussão o contexto atual da segurança cibernética dos países da Argentina, Peru e Brasil; sendo de relevância no âmbito da Ciência da Informação desde o modelo social e pragmático. Como modelo social²⁰, devido ao anseio da sociedade de participar ativamente do governo, não somente como administradora, mas apoiando na administração dos objetivos nacionais da segurança cibernética. E como modelo pragmático²¹, é concretizado na ação, pesquisando as propriedades e os comportamentos relacionados com a segurança cibernética, bem como das forças que regem no fluxo informacional, os meios e as relações de poder influenciadas na segurança cibernética. Assim, inferimos que ambos os modelos remete às relações informação-poder, como atribuição do regime de informação (González de Gomez, 2012, p. 44). Portanto, apoiados nesses dois modelos e sobre os alicerces da teoria crítica, esta investigação buscar ir além das explicações culturais (visão de mundo, identidade, religião etc.), analisando em termos de diagnósticos e soluções os fatores geopolíticos, sociais e econômicos envolvidos na segurança cibernética, desde a perspectiva da ecologia social digital.

Como lembram os estudos de ecologia social, a presente crise não pode ser compreendida e superada sem os seres humanos mudarem a forma com que tratam uns aos outros, sem que se deixe de identificar “progresso” e “desenvolvimento” com os interesses muito particulares das corporações de negócios, sem a mudança do conceito de homem, como espécie “dominante”, para espécie coadjutora (Pilon, 2007).

²⁰ Serviços da Google na China, como os de celular, são alvo de bloqueios. Disponível em < <https://extra.globo.com/noticias/saude-e-ciencia/servicos-da-google-na-china-como-os-de-celular-sao-alvo-de-bloqueios-106949.html>>. Acesso em 14 de maio de 2020.

²¹ O modelo pragmático é oposto ao modelo tecnocrático no qual os especialistas são chamados em apoio às decisões e ocultam seus verdadeiros retos, motivações e consequências.

Nas áreas da segurança da cibernética e da informação, cujo objeto de pesquisa também é a informação, o desenvolvimento do papel do Estado historicamente foi se incrementando na complexidade da política na segurança cibernética e da informação. Segundo Dunn e Egloff (2019, p. 47-48), as fases dos papéis do Estado foram se adicionando em:

- De ser o “proprietário” da informação e das redes (1ª Fase, nos anos 1980).
- Para logo ser o “proprietário do problema”, um Estado que resolve e melhora a segurança do sistema e do coletivo (2ª Fase, nos anos 1990).
- Para finalmente ser o “originador do problema”, onde a corrida armamentista e guerra cibernética têm seu esplendor (3ª Fase, nos anos 2000).

Para um adequado entendimento do papel do Estado no âmbito da segurança cibernética e das implicações geradas na sociedade contemporânea, vamos estudar as políticas e estratégias adotadas, analisando a lógica que existem nas diferentes formas de interação entre o Estado e a sociedade. Buscando identificar as relações existentes entre os elementos, agentes e a dinâmica da ação pública na segurança cibernética. É nesse contexto, a ciência da informação assume relevância, pois vamos estudar os fenômenos envolvidos na dimensão política-estratégica das políticas em segurança cibernética e da informação de forma profunda e detalhada, com o intuito de observar os variados pontos sociais que se manifestam nas políticas de informação. Os estudos de caso apresentados nos capítulos seguintes têm como objetivo oferecer uma forma alternativa de análise, preocupada não apenas com a eficiência dos fluxos informacionais, mas também em considerar as implicações e dependências entre manifestações, relações sociais, ciência e tecnologia. Em suma, nossa abordagem na pesquisa foi aplicada a partir do regime da informação:

Um modo de produção informacional dominante em uma formação social, conforme o qual serão definidos sujeitos, instituições, regras e autoridades informacionais, os meios e os recursos preferenciais de informação, os padrões de excelência e os arranjos organizacionais de seu processamento seletivo, seus dispositivos de preservação e distribuição (Gómez, 2002, p.34).

Nesse sentido, o pesquisador, apoiado nos estudos do regime de informação e das teorias implicadas, demarcou nosso objetivo de pesquisa. Nas observações realizadas, articulamos as complexas relações existentes entre política e informação, permitindo-nos compreender as entrelaçadas políticas das TIC, segurança, defesa,

cultura e informação. Sem dúvida, a Ciência da Informação, com seus estudos nas políticas públicas, proporciona uma perspectiva de mudança significativa, tanto de forma quanto conexão, na abordagem da política em segurança cibernética. Segundo Muller e Surel (2004, p.11), essa tendência afasta-se da orientação operacional para se aproximar de uma abordagem cognitiva. As políticas públicas são entendidas como a “ação do Estado”, abordando-se novos elementos de análise dentro de um conflito complexo de relações, em busca do consenso. À medida que a sociedade, ou parte dela, por meio da informação e do conhecimento, se apropria de novas formas de manifestação e de influência nas decisões e ações públicas (Jardim *et al.*, 2009, p.10). Segundo Gómez (2002, p.28), o Estado é esse “agente privilegiado de sua elaboração e implantação, e a ciência e a tecnologia como domínio de seu exercício”, mas a elaboração das políticas de informação nos países em desenvolvimento não atinge o mesmo sucesso que nos países desenvolvidos.

Num mundo em que os benefícios são repartidos apenas entre os que detêm o poder político e econômico e os custos, “democraticamente” divididos entre os demais, a injustiça prevalece e a ciência e a tecnologia, nas mãos dos setores acadêmicos convencionais, passam a servir aos interesses oligopolísticos, sem que ocorram mudanças substanciais no conjunto do ambiente e das populações marginalizadas (Pilon, 2007).

Os países desenvolvidos, como Estados Unidos, China, Rússia, Reino Unido e Israel, possuem uma resiliência econômica e uma hegemonia política e tecnológica. Isso foi evidenciado no caso envolvendo a Huawei – ZTE da china, e a Google, dos Estados Unidos. O governo do presidente Donald Trump tentou restringir a comercialização dos produtos das empresas chinesas nos Estados Unidos, resultando em vetos que afetaram as operações da Huawei e ZTE. A Google, como parte dessa disputa, restringiu o uso do sistema operacional Android e da loja de aplicativos Google Play Store nos smartphones da Huawei. No entanto, esse evento não teve um impacto significativo nos interesses comerciais da Huawei, levando-os nos poucos meses, ao desenvolvimento do próprio sistema operacional, chamado HarmonyOS. Além disso, com a grande vantagem que os chineses são pioneiros nos dispositivos de Telecom 5G, foram apresentados ao mercado mundial seus novos produtos que incluem essas tecnologias. Ao ponto que Donald Trump busca negociar a possibilidade de permitir novamente o ingresso do produto Chinês nos Estados Unidos. Segundo os dados apresentados no jornal *El País*²², publicado no ano 2019:

²² Disponível em < https://brasil.elpais.com/brasil/2019/05/25/economia/1558795538_036562.html>. Acesso em 26 de maio de 2020.

A Huawei detém 35% do mercado na Europa nas redes de nova geração. Mais de 2.500 patentes relativas ao 5G levam seu nome. A empresa também tem contratos com cerca de 40 operadoras. Se estas, incluindo as espanholas (Telefónica, Vodafone e Orange) se unirem ao bloqueio à Huawei, não poderão lançar a tempo uma rede 5G. De fato, a Europa já está atrasada em relação a países como EUA, Japão, China e Coreia do Sul. Somente a Nokia e a Ericsson podem fazer frente nessa disputa, mas a tecnologia e o posicionamento da empresa chinesa são mais avançados e baratos.

A reflexão sobre o caso Huawei vs. Google, permite observar que a hegemonia político-tecnológica de seus países se sobrepõe à coerção, indisponibilidade e interrupção dos serviços das multinacionais tecnológicas. Diante do impacto econômico dessas ações comerciais, esses países são resilientes, o que significa que possuem a capacidade de se recuperar diante qualquer perturbação ou degradação a que possam estar submetidos. Produto dessa reflexão, chegou-se às seguintes questões: os países na América do Sul teriam mecanismos necessários para mitigar esses impactos econômicos frente a uma indisponibilidade e interrupção dos serviços das multinacionais tecnológicas? Seria um caso complexo, estrutural e uma micromecânica do poder que vem sendo exercida pelos países desenvolvidos na América do Sul?

Desde o pensamento de Foucault (2019), a dominação global não se multiplica; são os fenômenos gerais que agem por investimento e anexação dos micropoderes, os quais estão presentes nas relações privadas e públicas, nos relacionamentos de familiares, de vizinhança etc. A micromecânica do poder produz “um lucro econômico, certa utilidade política e por essa razão, se viram naturalmente colonizados e sustentados por mecanismos globais e, finalmente pelo sistema do Estado inteiro” (Foucault, 2019, p.29). Por exemplo, a micromecânica do poder está constituída de mecanismos de exclusão, de aparelhos de vigilância, entre outros.

Para ter uma referência de quanto seria o impacto econômico diante uma interrupção, indisponibilidade, restrição, bloqueio da Internet e dos serviços tecnológicos das empresas multinacionais norte-americanas: *WhatsApp*, *Facebook*, *Twitter*, *Youtube* e *Instagram*, a ISOC e *NetBlocs*²³, em parceria, desenvolveram uma ferramenta online chamada *The Cost Shutdown Tool*²⁴ (COST) para medir o custo dos desligamentos da Internet e desses serviços em relação à localização e duração, sendo elaborada a seguinte Tabela:

²³ Disponível em < <https://netblocks.org/projects/cost> >. Acesso em 10 de junho de 2020.

²⁴ Disponível em < <https://netblocks.org/cost/> >. Acesso em 10 de junho de 2020.

Tabela 1 - The cost shutdown tool (cost)

Custo Total do Impacto estimado em dólares Americanos (US \$) produzido por um (01) dia de indisponibilidade.						
País	Impacto no custo total	WhatsApp	Facebook	Twitter	Youtube	Instagram
Estados Unidos	\$ 1.675.475.196	X	x	x	x	x
China (*)	\$ 49.341	X	x	x	x	x
Rússia	\$ 118.720.404	X	x	x	x	x
Argentina	\$ 30.655.781	X	x	x	x	x
Brasil	\$ 115.618.231	X	x	x	x	x
Peru	\$ 16.166.702	X	x	x	x	x

Fonte: (<https://netblocks.org/cost/>, laboração própria).

Nota: Os dados foram extraídos no dia 28/09/2024.

(*) Los modelos por aplicación no son aplicables debido a las restricciones de la plataforma en China.

Assim, podemos inferir que o anseio dos governos sul-americanos de melhores condições de segurança cibernética, inicia com a seguinte questão: em benefício ao desenvolvimento de seus cidadãos e instituições, como na sociedade digital de um país desenvolvido é evidenciada a eficiência, o progresso e a disponibilidade? Contudo, temos que entender que a hegemonia político-tecnológica é a supremacia de um Estado sobre outro, tornando-o em um Estado soberano, dado por sua força política e de produção tecnológica. Existindo um mecanismo invisível de influência na sociedade e de dominação consentida pelos países menos desenvolvidos que possuem dependência econômica e tecnológica. Assim, episódios recentes evidenciam a preocupação dos Estados em reafirmar sua autoridade sobre a Internet, a proteção informacional da sociedade e de suas empresas, portanto, a soberania digital possui maior relevância, não só afetando aos sujeitos que interajam com o meio digital, também é parte da disputa pelo controle dos dados, fluxos, objetos, dispositivos e de todo que se relaciona no ecossistema informacional.

Seja por uma abordagem propositiva como a de Floridi, pela qual o desafio da soberania digital envolve disputa entre poderes privados e públicos, seja por uma abordagem mais teórica, como a de Campos, pela qual a soberania digital é um fim a ser alcançado pelo Direito, ou seja por uma abordagem crítica, como a de Zuboff ou de Morozov, pela qual a soberania digital está já em estado de violação pelas Big Tech, é possível observar que trata-se de um tema relevante e atual para estudiosos do Direito, sendo inegável o impacto das empresas apelidadas Big Tech e das novas tecnologias sobre a questão da soberania (Pereira, Faleiros Junior, 2024, p. 7)

É evidente que os modelos contemporâneos propostos de uma sociedade da informação e do conhecimento nos países sul-americanos estão orientados a ser consumidores e dependentes tecnológicos da informação e da comunicação, em

relação aos países desenvolvidos. Uma visão alternativa, seria examiná-los de forma mais profunda e aproximada à ciência da informação, como um problema complexo e estrutural que confronta sujeitos, informação e conhecimento dentro de sua ecologia social digital. Incentivando a troca de experiências e pesquisas com as outras áreas. Na tentativa de confrontá-las com disciplinas diferentes, a fim de relacionar as teorias e perspectivas no âmbito da geopolítica, segurança nacional e das ciências sociais.

A preocupação com a temática dos elementos que se influenciaram na consolidação de uma Política em Segurança Cibernética que considere as especificidades geopolíticas dos países sul-americanos, se estende desde os anos em que o autor trabalhou como Oficial do Exército no Peru, sendo percebida a incerteza e enviesada compreensão dos responsáveis pelo planejamento e elaboração da doutrina militar para a defesa cibernética. Posteriormente, no ano 2016, como docente no Centro de Altos Estudos Nacionais (CAEN) e com o apoio da Secretaria da Defesa Nacional (SEDENA), foi estruturado um projeto que tinha como objetivo a conscientização em segurança e defesa cibernética aos funcionários públicos e ao setor privado de interesse. Sendo ampliadas as minhas preocupações em não ter uma Política em Segurança Cibernética devido à pouca visão na construção das capacidades cibernéticas desejadas e aos insuficientes esforços conjuntos com os demais setores. Por exemplo, com a entidade responsável pela ciência e tecnologia do País (CONCYTEC). Compartilhando estas preocupações com os colegas nacionais e internacionais nos diversos momentos e ambientes acadêmicos onde participei, na Escola Sul da Governança da Internet²⁵ (SSIG), no Instituto Nacional de Cibersegurança da Espanha²⁶ (INCIBE), na Agência Espanhola de Cooperação Internacional para o Desenvolvimento²⁷ (AECID), no 1º Estágio Internacional de Defesa Cibernética para Oficiais de Nações Amigas²⁸ (CDCiber - CIGE) e nos programas de cibersegurança promovidos pela Organização de Estados Americanos²⁹ (OEA- CICTE), passei a procurar bibliografia que respondesse a essas questões naqueles anos.

Foi optada como estratégia de investigação trabalhar inicialmente com a política, os programas e a doutrina militar da segurança e defesa cibernética dos

²⁵ Disponível em < <http://www.gobernanzainternet.org/ssig2016/>>. Acesso em 11 de abril de 2020.

²⁶ Disponível em < <https://www.incibe.es/summer-bootcamp>>. Acesso em 11 de abril de 2020.

²⁷ Disponível em < <https://www.aecid.es>>. Acesso em 11 de abril de 2020.

²⁸ Disponível em < <http://folhamilitaronline.com.br/estagio-internacional-de-defesa-cibernetica-para-nacoes-amigas/>>. Acesso em 11 de abril de 2020.

²⁹ Disponível em: < http://www.oas.org/en/topics/cyber_security.asp >. Acesso em 11 de abril de 2020.

Estados Unidos. Por existir, presumivelmente, maior *expertise* e análise documental do tema investigado, sendo mais factível a instrumentalização para a coleta de dados. Além disso, existiam mais estudos, e o material coletado estava em um idioma conhecido. A escolha na segurança cibernética norte-americana, foi feita pelas seguintes razões:

- É uma das potências mundiais, que na atualidade tem o maior exército cibernético atuando em todos os continentes do planeta.
- Observou-se que durante seus primeiros anos, a Internet foi desenvolvida com o esforço mais independente de pessoas desde o setor do governo e acadêmico dos Estados Unidos, narrado por Vinton Cerf na *Internet Society* (ISOC).
- A influência geopolítica e tecnológica³⁰ que os Estados Unidos exercem na América do Sul, notadamente na Argentina, Brasil e Peru.
- Aprofundei meus conhecimentos com a doutrina militar em segurança e defesa cibernética norte-americana, nos níveis de planejamento estratégico, operacional e tático.

Segundo Bickman (1987, p. 5-18), os analistas confundem, com frequência, a teoria do programa (como tornar a segurança cibernética mais eficaz) com a teoria de implementação do programa (como instalar um programa eficaz). Existem muitas discussões abordadas na mesma estrutura, onde é assumida a existência de um problema fixo, para posteriormente ser adotada como uma solução generalizada.

Sendo conscientes dos erros que são cometidos ao se realizar estudos de caso de conceber a generalização estatística como o método de se generalizar os resultados do caso. Os casos que serão analisados nesta pesquisa não são unidades de amostragem e não foram escolhidos por essa razão. O método de generalização a ser praticado é a “Generalização analítica”, fazendo uso de uma teoria previamente desenvolvida como modelo com o qual se deve comparar os resultados empíricos do estudo de caso.

Se dois ou mais casos são utilizados para sustentar a mesma teoria, pode-se solicitar uma replicação. Os resultados empíricos podem ser considerados ainda mais fortes se dois ou mais casos sustentam a mesma teoria, mas não sustentam uma teoria concorrente igualmente plausível (Yin, 2001, p. 54).

³⁰ Se observou no Merco (Monitor Empresarial de Reputação Corporativa), que os primeiros lugares do ranking das empresas no setor de tecnologia, no ano 2019, é liderada por empresas privadas norte-americanas. Disponível em < <https://www.merco.info/ar/que-es-merco>>. Acesso em 13 de abril de 2020.

Nesse contexto, a presente tese pretende contribuir com reflexões e análises dos elementos e agentes que constituem a política em segurança cibernética e da informação, investigando desde uma perspectiva comparada com as políticas e estratégias de segurança cibernética implementadas nos países sul-americanos, notadamente na Argentina, Brasil e Peru. As teorias e conceitos nesta pesquisa buscam servir de diretrizes, com a difícil tarefa de estar longe de sua generalização, por tanto, buscamos compreender o contexto, as ameaças e relações existentes em suas políticas. As pretensões deste estudo são teóricas e documentais; consequentemente, não pretendemos deduzir soluções práticas, embora esse escopo pudesse também ser alcançado no final desta pesquisa.

2.4 Perspectivas teóricas que conduzem o contexto da pesquisa

Em seguida apresentamos as diversas perspectivas teóricas que servem de insumos na limitação e direcionamento para a compreensão dos fenômenos e questionamentos teóricos que serão abordados na análise documental, bem como, nos casos estudados. Uma primeira perspectiva teórica, se apropria da teoria apresentada pelo cientista político Samuel P. Huntington, na qual “a política local é a política da etnia e a política mundial é a política das civilizações. [...] o que quer dizer que a política mundial está sendo reconfigurada seguindo linhas culturais e civilizacionais” (Huntington, 2010, p.24). Apoiados em Huntington, compreendemos que a segurança do mundo requer a aceitação da multiculturalidade global e está sendo ameaçada pela crise global da governabilidade. No contexto em que foi escrita esta investigação, estamos vivenciando uma pandemia, uma crise global financeira e mudanças na ordem mundial, estando acelerada com a atual guerra de Ucrânia e Rússia. Estas crises podem ser explicadas desde a perspectiva do poder que um Estado ou grupo possui, por meio dos recursos que dispõe em relação a outros Estados ou grupos que ele busca controlar e influenciar, através da indução, coerção e exortação. Assim, temos observado no século XX, como os Estados ocidentais hegemônicos e grupos imperialistas transnacionais tem alcançado seu maior ápice. Ademais, temos testemunhado a ascensão de outras civilizações promovendo processos globais de indigenização e ressurgimento de culturas não ocidentais, devido à modernização e às TIC. De onde, inferimos que a modernização tem reforçado as outras culturas e reduzido o poder ocidental. Segundo Huntington (2010,

p.125) “Ocidente é a única civilização que tem interesses substanciais em todas as outras civilizações”, dispondo das capacidades de influência na política, economia e segurança das outras civilizações ou regiões. Por exemplo, nas últimas três décadas, desde a queda do Muro de Berlim, a civilização Ocidental como a Islâmica têm expressado suas intenções expansionistas e universalistas, dando origem aos contínuos confrontos no âmbito militar, político, cultural e ideológico. Para a tese de Huntington, os conflitos no futuro serão por critérios culturais e religiosos. Além disso, Huntington nos incita em que os países da América Latina deverão definir uma identidade, que pode ser da civilização ocidental ou atuar como autônomos, definidos por ele como Estados-Núcleos. Para os interesses da pesquisa, nós iremos interessar no critério cultural e não no religioso. Para Huntington, a definição de um Estado-núcleos é:

Os Estados-núcleos tentam congregiar suas legiões civilizacionais, fazer alianças com Estados de terceiras civilizações, promover a divisão e defecções nas civilizações adversárias e empregar a combinação apropriada de ações diplomáticas, políticas, econômicas e clandestinas, bem como instigações por propaganda e forma de coerção, para atingir seus objetivos (Huntington, 2010, p.350).

Assim, a primeira perspectiva foi abordada neste estudo como uma provocação sob a ótica de quais são os princípios para as mudanças na ordem mundial. Por esse motivo, a tese faz um diálogo e complementa as teorias de Huntington (2010) com as de Dalio (2022), conduzindo nossa investigação, principalmente, na observação dos padrões e relações de poder existentes, que resumidos em um arquétipo, poderemos possuir dos insumos justificativos do porquê as nações prosperam e fracassam. É assim, que nosso método se apoia na análise computacional apresentado pelo Dalio (2022), influenciando na organização das categorias temáticas e dos sete aspectos que serão apresentados nos capítulos finais desta tese.

A segunda perspectiva se relaciona com os conceitos da engenharia social parcelar e a utópica, linha de pensamento, apresentada nos ensaios de Karl Popper (2018). No prefácio de João Carlos Espada, a “engenharia social parcelar ensaia soluções parcelares para problemas parcelares. A engenharia social utópica, pelo contrário, supõe que todos os problemas parcelares somente podem ser enfrentados com o redesenhar da sociedade no seu conjunto” (Popper, 2018, p. XVI). O redesenhar da engenharia social utópica busca ser materializado na base da formulação de planos globais. Apresentando erros fundamentais, ao desconhecer que nas ações humanas existem efeitos inatos, não intencionais, sendo eles conhecidos

por meio dos ensaios e erros, o que conduz às constantes e graduais reformulações das políticas públicas. Segundo Popper (2018), desde a visão da engenharia social parcelar, os mecanismos do mercado ou da propriedade privada devem ser protegidos adequadamente pelo Estado e a intervenção deste quando seja necessária, criticando nesse sentido o “não intervencionismo universal”. Para Popper, o próprio livre mercado requer de uma proteção adequada do Estado e, por vezes, a sua intervenção. Uma intervenção adequada, quando necessária, deve ser de tipo indireto e institucional e não direto e pessoal” (Popper, 2018, p. XVII-XVIII).

Para uma apresentação mais clara da perspectiva de Popper, o pesquisador encoraja ao leitor ao uso da linguagem das exigências ou propostas políticas. Ou seja, não se busca uma resposta essencialista nem historicista, sem embargo, busca responder o seguinte: o que exigimos do Estado no âmbito da segurança cibernética e da informação? Que propósitos consideramos como objetivo dessa atividade ao Estado? Por que preferimos ter uma política em segurança e defesa cibernética, a não dispor dela? Nesse sentido, como tecnólogos, devemos saber o que se quer, devemos buscar as respostas a essas perguntas antes de apresentar propostas de construção ou de reconstrução das instituições políticas e se elas são ou não adaptadas à sua função. No marco do contexto político atual sul-americano, a visão do Estado em relação às políticas em segurança cibernética e da informação podem ser categorizadas como protecionismo, relacionando o termo com tendências opostas à liberdade. Esta tese se adapta à posição em que o liberalismo como a intervenção do Estado não é oposto, sendo necessária a garantia imposta do controle pelo Estado. Em suma, liberdade e segurança não são uma utopia, pois não se teria liberdade se não fosse assegurada pelo Estado, se caracterizando como um fator estratégico para o desenvolvimento científico e tecnológico, como um novo modelo de soberania. Para González de Gómez (2002, p.27) “o nexos da informação com a política seria então estabelecido por sua inclusão na esfera de intervenção do Estado” e de soberania:

O Estado age como agente privilegiado de geração, recepção e agregação das informações, gerando um “duplo” representacional de seus domínios de intervenção territorial, social e simbólica (González de Gómez, 2002, p.27).

A seguinte perspectiva teórica traz o pensamento de Foucault. Segundo ele, em toda sociedade são múltiplas as relações de poder que irão constituir o corpo social: “elas não podem dissociar-se, nem se estabelecer, nem funcionar sem uma produção, uma acumulação, uma circulação, um funcionamento do discurso

verdadeiro” (Foucault, 2019, p.22). O problema da soberania nas sociedades ocidentais, ligado ao discurso e a técnica do direito, teve a função de dissolver o núcleo do poder, o fato da dominação, reduzindo ou mascarando os direitos legítimos da soberania e a obrigação legal da obediência. Neste sentido, ao falar do direito, não somente estamos nos expressando da lei, mas nos dispositivos, instituições, diretivas, normas e regulamentos. Ademais, o filósofo francês comenta que “o sistema do direito e o campo judiciário são o veículo permanente de relações de dominação, de técnicas de sujeição polimorfos” (Foucault, 2019, p.24). A dominação global não se pluraliza e repercute do nível mais alto até chegar ao mais baixo. Sugere-se analisar os fenômenos, as técnicas, os procedimentos de poder desde o nível inferior, “como eles são investidos, anexados por fenômenos globais e como poderes mais gerais ou lucros de economia podem introduzir-se no jogo dessas tecnologias, ao mesmo tempo relativamente autônomas e infinitesimais, de poder” (Foucault, 2019, p.27).

Conforme exploramos as relações de um modo sistemático, um dos aspectos que precisa de nossa atenção é a compreensão da economia política, expressada nas políticas e linhas de ação do Estado – Nação. Segundo Foucault, a economia política é um sistema de pensamento que nos permite entender tudo. Ele discute “como a economia política e as instituições do mercado nos permitem determinar o valor de bens e serviços, a estrutura essencial do Estado e a sociedade” (Foucault, 2020, p. XIV). Desde essa lógica, podemos afirmar que as ações governamentais e o governo, em si mesmo, são integralmente definidos pela economia de mercado. Sendo assim, não se teria lugar a uma crítica do intervencionismo estatal. Se os governos conhecem os mecanismos econômicos na natureza íntima e complexa, eles deverão respeitá-los. O respeito aos mecanismos não quer dizer o aprovisionar de uma estrutura jurídica em respeito às liberdades e direitos fundamentais. Respeitar os mecanismos é dotar a sua política de conhecimento rigoroso, constante, claro e diferenciado, limitado pela evidência e não da liberdade dos indivíduos.

O liberalismo não é aquilo que aceita a liberdade. O liberalismo é aquilo que propõe fabricá-la a cada instante, suscitá-la e produzi-la, certamente com [todo o conjunto] (*) de limitações, de problemas de custo criados por esse fabrico. Qual vai ser então o princípio de cálculo desse custo de fabrico da liberdade? O princípio de cálculo é, evidentemente, aquilo a que se chama segurança” (Foucault, 2020, p.95).

Então, vigiar para que a mecânica dos interesses não seja um perigo deverá responder às estratégias de segurança, que em algumas condições se tornam o reverso à própria condição do liberalismo. Desde essa linha de pensamento de

Foucault, fica evidente que o liberalismo se envolve em mecanismos de arbitragem entre a liberdade e a segurança, sendo ele uma arte de como governar e de manipulação dos interesses. Não existe um liberalismo sem uma cultura do medo, sem processos de controle, de coerção e condicionamento que constituem um contrapeso às liberdades (Foucault, 2020, p.97).

Outra perspectiva teórica que auxiliará nossa análise de pesquisa parte do argumento de Castells, segundo o qual “as sociedades são moldadas pelos atores sociais, com base nos interesses, ideias e valores, em um processo aberto e conflitivo. A mudança social e política é o que em definitiva determina o destino e a estrutura das sociedades” (Castells, 2018, p.89-90, tradução nossa). Para Castells, a reestruturação do capitalismo tem evidenciado sua versatilidade nas regras de funcionamento e a capacidade do uso com eficácia, da lógica das redes se tem induzido às forças produtivas e de crescimento econômico (Castells, 2018, p.26-27, tradução nossa). Porém, surge o aumento da desigualdade e a falta de inclusão nos benefícios do informacionalismo, seja nos países em vias de desenvolvimento e desenvolvidos. Para Castells o informacionalismo é entendido como “um modo de desenvolvimento em que a principal fonte da produtividade é a capacidade qualitativa para otimizar a combinação e o uso dos fatores de produção baseado no conhecimento e a informação” (Castells, 2018, p.32, tradução nossa). Deve-se entender que exclusão social é um processo e não uma condição. Consequentemente, o processo da exclusão social na sociedade em rede, segundo Castells, afeta os sujeitos e seu espaço territorial. Isso significa que esses espaços que não são do interesse do capitalismo informacional e político para os poderes existentes não serão considerados pela riqueza, poder e informação, sendo despossuídos da infraestrutura tecnológica que permite a comunicação, inovação, produção e o consumo. Além disso, devem ser entendidas as relações sistêmicas do capitalismo informacional, a reestruturação do capitalismo, as tendências das relações de produção e as novas relações de distribuição. O capitalismo informacional deve ser entendido não como uma entidade, uma vez que é uma estrutura social específica, com suas regras e sua dinâmica. Observa-se que Castells busca demonstrar a complexidade dos vínculos existentes entre alguns dos problemas sociais nos países menos desenvolvidos, como a desigualdade, a polarização, a pobreza e a miséria, com as características do capitalismo informacional, sendo as tecnologias da informação os condutores globais de acumulação da riqueza e difusão da pobreza.

Portanto, é importante analisar e compreender a dependência e o subdesenvolvimento tecnológico nos três países pesquisados em uma era de aceleração mundial das mudanças tecnológicas. Como consequências, há a falta de conhecimento e preparação das pessoas nos países menos desenvolvidos. Na maioria desses países, as organizações contratam profissionais estrangeiros, que também carecem dos conhecimentos locais dessas organizações e, conseqüentemente, desenham estruturas e sistemas deficientes. Castells ao abordar os assuntos de desenvolvimento e dependência, afirma que “a globalização e identidade interagem na economia criminal da América Latina” (Castells, 2018, p.238, tradução nossa). Na mesma linha de pensamento de Castells, outro argumento interessante é a “importância da identidade cultural na constituição, funcionamento e estratégias das redes criminais” (Castells, 2018, p.234, tradução nossa). Evidentemente, nos últimos anos nos três países estudados, tem-se experimentado um número crescente de convulsões políticas, geopolíticas e de reestruturações tecnológicas. Se tem constatado nos países sul-americanos o crime transnacional organizado, que possui capacidades de se estender na segurança e nas economias dos países, com conexões flexíveis em redes interacionais. Essa ameaça busca ser tratada pelos governos da região com a promessa de garantir uma estabilidade, segurança interna e desenvolvimento econômico da sociedade. Quase todos os países sul-americanos se têm envolvido em “agitações e crises causados pela conexão direta e indireta entre o crime organizado e a política” (Castells, 2018, p.241, tradução nossa), e por vias mais tênues tem sido alcançado o âmbito cultural, sendo os meios das tecnologias da informação e da comunicação difusores da cultura do crime organizado. Neste sentido, a perspectiva de Castells traz insumos na investigação, constituindo um traço essencial da nova economia global e da dinâmica sociopolítica da era da informação (Castells, 2018, p.200, tradução nossa).

Devido às diversas concepções da sociedade da informação, nosso entendimento na pesquisa aborda uma sociedade que não apenas utiliza a tecnologia da informação. A sociedade da informação é uma estrutura social específica, aliada ao paradigma informacional, mas não determinada por ele, buscando navegar entre os traços estruturais das mudanças histórico-culturais desta sociedade. Esta perspectiva também é defendida por Castells, que a denomina como uma sociedade em rede.

A seguinte perspectiva, refere-se ao pensamento da Zuboff sobre o fenômeno que ela nomeia como capitalismo de vigilância. A pesquisadora realiza uma crítica aos interesses do capital de vigilância e da construção de um poder inédito determinado pela imensa acumulação de conhecimento que não é supervisionado pela democracia. Segundo Zuboff, “o capitalismo de vigilância reivindica de maneira unilateral a experiência humana como matéria-prima gratuita para a tradução em dados comportamentais” (Zuboff, 2020, p.18). Desde esta perspectiva, busca-se demonstrar como os capitalistas de vigilância têm concentrado vastas riquezas em produtos de predição, os quais são comercializados em mercados de comportamento futuros. Assim, Zuboff (2020, p.19) busca evidenciar nesse tipo de capitalismo um meio de geração da nova espécie de poder que denomina de instrumentalismo. Nesta linha de pensamento, nós somos as fontes do superávit crucial do capitalismo de vigilância, esses objetos de extração tecnologicamente avançada, matéria-prima, sendo as empresas os verdadeiros clientes deste fenômeno. Para Zuboff, a Internet é essencial para a participação na sociedade, porém, está subordinada a este tipo de capitalismo, que é assimétrico em relação ao conhecimento e ao poder que dele resulta, desconsiderando as normas sociais, anulando os direitos de autonomia individual e ameaçando a essência de uma sociedade democrática. Segundo Zuboff (2020, p. 26), “o capitalismo de vigilância não é tecnologia; é uma lógica que permeia a tecnologia e a direciona numa ação. O capitalismo de vigilância é uma forma de mercado que é inimaginável fora do meio digital, mas não é a mesma coisa que digital”. O questionamento que faz Zuboff (2020, p.27) em relação à inevitabilidade tecnológica nos ajuda a estabelecer os parâmetros da pesquisa, em que se busca deixar em evidência que a tecnologia não é e nem deve ser um fim em si mesma. O sociólogo Max Weber observou na tecnologia como uma orientação econômica, sendo uma expressão dos objetos econômicos que a dirigem para a ação, pois, “o capitalismo de vigilância emprega muitas tecnologias, mas não pode ser igualado a uma específica” (Zuboff, 2020, p.27).

Portanto, apoiados nas teorias e perspectivas que foram descritas, a presente tese de doutorado, busca transitar nas configurações e modos de configuração da ordem sociocultural e política-tecnológica, caracterizadas nas relações e agências dos regimes informacionais dos países da Argentina, Brasil e Peru, no âmbito da segurança cibernética. Para González de Gómez (2012, p.43-44):

O conceito de regime de informação pareceria ser uma ferramenta interessante para situar e analisar as relações de uma pluralidade de atores, práticas e recursos, à luz da transversalidade específica das ações, meios e efeitos de informação; *transversalidade* que se estabelece na medida em que tais relações e interações perpassam uma ou mais esferas da cultura, da economia, da educação, da comunicação, da pesquisa científica e da vida cotidiana, e *especificidade* que se constitui na medida em que o envio e a direção dessa *transversalidade* pertencem as configurações contemporâneas da informação, e são reconhecidas como tais (e não como sendo da esfera da saúde, do transporte ou da mídia).

2.5 Estrutura da tese

No capítulo primeiro, descreve-se a introdução da tese, com uma breve apresentação do cenário atual da segurança cibernética nos países Sul-americanos. Sendo descritas as ameaças complexas do ciberespaço e de seu impacto no contexto mundial desde diversas perspectivas.

No capítulo segundo é apresentada a problemática e contexto da pesquisa, sendo consideradas as questões e pressupostos, em relação, às políticas e estratégias em segurança cibernética, que divergem da realidade problemática e das necessidades dos países Sul-americanos. Sustentados nas informações publicadas pelas diversas organizações e revistas especializadas que conversam com o tema. Ato contínuo, é descrito o problema de pesquisa e seus objetivos, os quais, para serem justificados no âmbito da ciência da informação. Após, serão apresentadas as perspectivas teóricas, que serviram de insumos, para limitar e direcionar a compreensão dos fenômenos e questionamentos teóricos abordados nos posteriores capítulos.

No capítulo terceiro, desde o questionamento: o ciberespaço pode ser considerado um *Global Common*? Foram descritos o referencial teórico, estudando a historicidade da segurança e da defesa nacional Sul-americana. A historicidade do ciberespaço foi descrita através da Internet, utilizando como referências as publicações públicas de Vint Cerf no ISOC. Neste capítulo, foram apresentados os tópicos relacionados à doutrina da segurança cibernética norte-americana, subsidiando as inferências iniciais e os papéis do Estado neste âmbito. Em seguida, na perspectiva da geopolítica contemporânea são questionadas as disputas do poder mundial no fator econômico, sendo apresentados os elementos estruturais para a construção do ciberespaço, como parte dos aportes da pesquisa. Comparecendo à teoria para tratar as capacidades cibernéticas e os modelos de maturidade de relevância na elaboração das estratégias de segurança cibernética. Além disso, são

tratados a historicidade da segurança cibernética na Argentina, Peru e Brasil, sobre as diretrizes do referencial teórico, sendo construída uma síntese dos reflexos observados.

No capítulo quatro, são apresentados os aspectos metodológicos que constituem a elaboração da tese, dando detalhes das regras e procedimentos sistemáticos utilizados. A fim de dar uma explicação aos fenômenos de interesse ao nosso objeto de estudo. Os itens deste capítulo são: a tipologia, as delimitações e as técnicas de coleta dos dados.

Em seu capítulo quinto, é apresentada a análise documental para a elaboração do caso protótipo norte-americano, na perspectiva quantitativa, para depois ser reforçada qualitativamente. Assim, constituindo desta forma nosso “Estado da Arte”, sendo trazidas as conclusões do capítulo.

No capítulo sexto e sétimo são tratados os dados do estudo de caso múltiplo: constituído pelos países de Argentina, Peru e Brasil; apoiados no método quantitativo e qualitativo, respectivamente. O processo de exploração e o método estatístico realizado nos corpus dos países pesquisados, busca-se obter dados descritivos com o intuito de reforçar, posteriormente, nossa análise qualitativa. Nestes dois capítulos foram gerados a síntese quantitativa e qualitativa dos reflexos observados na segurança cibernética da Argentina, Peru e Brasil.

O capítulo oitavo apresenta as considerações finais dos resultados da tese, realizando a comparação entre os relatórios dos estudos de casos estudados. A seguir são elaboradas as implicações teóricas dos estudos de casos cruzados, para finalmente, elaborar as conclusões finais da investigação, como as propostas dos trabalhos futuros de pesquisa.

“Cuánto más lejos hacia atrás mires, más lejos hacia adelante verás”

Winston Churchill

3 REFERENCIAL TEÓRICO

No presente capítulo, serão tratados resumidamente a historicidade dos eventos que definiram a segurança e defesa nacional na América do Sul, desde os primórdios do ciberespaço, através da Internet. Ao realizar uma retrospectiva nos trabalhos dos pioneiros da Internet, podemos afirmar que existem quatro dimensões-chaves que nos proporcionarão uma melhor compreensão da Internet: tecnologia, gestão, comunidade e comercialização. Existem diversos tipos de interesses ligados no político, econômico, psicosocial e territorial. Os obstáculos que surgem na realização desses interesses constituem ameaças que serão categorizadas como riscos e desafios. Por esse motivo, serão abordados alguns tópicos da atual doutrina militar no âmbito do ciberespaço dos Estados Unidos, como parte de nossa busca pelo “Estado da Arte”, como um caso protótipo dos estudos posteriores a serem realizados nos países da Argentina, Brasil e Peru. Neste capítulo, foi elaborado um questionamento inicial: o ciberespaço é um *Global Common*? Posteriormente, analisaremos a construção do ciberespaço através de quatro elementos propostos pelo autor: (1) Infraestrutura, (2) Dados, informação e conhecimento, (3) Automação e inteligência e (4) Conectividade global. Assim, buscaremos compreender como a segurança nacional se articula com a segurança cibernética nos países da América do Sul.

3.1 Historicidade da segurança e defesa nacional sul-americana

Posteriormente com a criação dos novos Estados, ex-colônias espanholas no continente americano, foram feitas diversas tentativas de unificar esses países em uma “Pátria Latino-americana-Caribenha”, mas foram fracassos, principalmente devido às ambições locais e à oposição do poder hegemônico da Grã-Bretanha, seguido posteriormente pelos Estados Unidos³¹.

Em 1826, com Simón Bolívar, houve uma tentativa de estabelecer uma visão de Confederação das ex-colônias espanholas, visando uma defesa e ofensiva comum

³¹ Disponível em <<http://www.cemida.com.ar/conversiondocumentos/LADOCTRINADELASEGURIDADNACIONAL.pdf>>. Acesso em 09 de novembro de 2020.

desses países contra qualquer dominação estrangeira. No entanto, não evoluiu, e houve tentativas fracassadas de acordos de confederação, comércio e navegação em Lima, nos anos 1847 e 1848, que não foram ratificados pelos países da Bolívia, Chile, Colômbia e Equador.

Em 1856, Equador, Peru e Chile assinaram o chamado Tratado Tripartite em Santiago de Chile, posteriormente conhecido como Tratado Continental, com o desejo de cimentar a união entre esses países, considerando suas origens e interesses comuns, bem como os laços e relações entre seus povos. Mais tarde, outros governos aderiram a este acordo, incluindo Bolívia, Costa Rica, Nicarágua, Honduras, México e Paraguai. Este tratado surgiu como uma resposta aos corsários na América Central. Os países signatários declararam-se obrigados a não ceder ou alienar seus territórios a outro Estado, limitando-se em participar de atos de hostilidade mútua, sem antes esgotar os meios pacíficos de resolução de conflitos e garantir a independência mútua. Diante da ameaça representada pelos interesses europeus no chamado “Novo Mundo”, o governo peruano buscou integrar a Argentina ao tratado, mas foi rejeitado pelas autoridades argentinas, argumentando que a ação da Europa sempre foi de “protetor e civilizador”, provocando o distanciamento das relações peruano-argentina. Pouco depois, as consequências dessa situação foram observadas quando o Peru decidiu excluir a Argentina da convocação para o Congresso Americano realizado em Lima.

Em 1865, durante o segundo Congresso de Lima, países como Argentina, Bolívia, Colômbia, Chile, Equador, Guatemala, Peru, Salvador e Venezuela participaram de tentativas infrutíferas de unificação. Mais tarde, em 1890, por iniciativa dos Estados Unidos foi criada a União Internacional das Repúblicas Americanas, cujas funções iniciais incluíam a compilação e distribuição de informações comerciais. Posteriormente, em 1948, essa união evoluiu para a Organização dos Estados Americanos (OEA).

No final da Segunda Guerra Mundial e no início da Guerra Fria, os Estados Unidos desenvolveram vários projetos políticos para a América Latina, com o objetivo de conter a expansão do comunismo liderada pela União de Repúblicas Socialistas Soviéticas (URSS). Isso visava preservar a hegemonia do poder mundial e da segurança nacional dos Estados Unidos. Em 1947, foram estabelecidos dois programas principais: O Plano *Marshall*, para reconstruir uma economia europeia pós-guerra e conter o avanço comunista no continente europeu, por meio de reformas

sociais e econômicas; o outro programa, seria a doutrina *Truman*³² que consiste no envio das forças militares norte-americanas a qualquer país do mundo que solicitasse ajuda, assim enfrentar e impedir o comunismo e sua influência ideológica. Sob a lógica do conflito bipolar, se influenciou no pacto da defesa mútua³³, denominado, como o Tratado Interamericano de Assistência Recíproca (TIAR), em 1947, no Rio de Janeiro. Para os interesses norte-americanos, era crucial manter a América Latina alinhada ao bloco capitalista, para a proteção do Atlântico Sul contra o tráfego marítimo soviético e manter a ordem na região. Segundo o citado anteriormente³⁴, com o tratado do TIAR, os países membros se comprometeram no cenário de uma potência extracontinental ataque algum país membro, o ataque seria considerado um ataque contra todos os países do tratado, estabelecendo um sistema de segurança coletiva. Isso significava que os países signatários seriam automaticamente aliados dos EUA, representando formalmente a América Latina dentro do bloco capitalista ocidental, especialmente considerando o início da Guerra Fria. No entanto, durante a guerra das Malvinas, em 1982, Chile, Colômbia e os Estados Unidos não assinaram dar apoio à Argentina. Apenas Chile e Estados Unidos demonstraram apoio aberto à Grã-Bretanha, revelando que o TIAR poderia funcionar apenas no caso de uma agressão externa a partir de um País do bloco antagônico ao capitalismo.

Naquela conjuntura histórica e contexto da nova ordem geopolítica mundial daquele tempo, com as dinâmicas de poder e força entre os Estados Nacionais, foram estabelecidos os elementos e fundamentos que possibilitaram o desenvolvimento da Doutrina da Segurança Nacional (DSN) nos Estados Unidos, baseando-se nos conceitos da geopolítica. Essa doutrina refletia as condições geográficas, situacionais e as ações políticas, sendo disseminada nas escolas militares da América Latina. Conforme Filho (1999, p.69), a aceitação das forças armadas da América Latina à hegemonia norte-americana nessa nova ordem estrutural, tem como interesse a busca por assessoria militar e aquisição de armamentos norte-americanos. Além disso, historiadores afirmam que os preceitos da DSN foram utilizados como sustento

³² Não é coincidência que a política de contenção de kennan transformou-se em doutrina Truman. Leia-se *The Sources of Soviet Conduct from Foreign Affairs* (July 1947). Disponível em <<https://www.cvce.eu/obj/the-sources-of-soviet-conduct-from-foreign-affairs-july-1947-en-a0f03730-dde8-4f06-a6ed-d740770dc423.html>>

³³ Segundo o artigo 3.1 Em caso de [...] um ataque armado por qualquer Estado contra um país Americano, será considerado como um ataque contra todos os países Americanos e em consequência, cada uma das partes contratantes se compromete na ajuda, para fazer frente ao ataque exercido no direito imaneente da legítima defesa individual ou coletiva. Reconhecida no Artigo 51 da Carta das Nações Unidas.

³⁴ Olhasse o parágrafo 2.1. HISTORICIDADE DA SEGURANÇA E DEFESA NACIONAL NA AMÉRICA DO SUL

ideológico pelas ditaduras instaladas na América do Sul. Segundo Duhalde (1999), é na Declaração de Caracas de 1954 que se encontra a origem embrionária da DSN para a América Latina.

A criação da doutrina foi uma obra de uns poucos países da América do Sul, especialmente Argentina e Brasil, e em menor grau e com posterioridade, Chile, Peru e Equador criaram versões diferentes, com tendências de desenvolvimento (Garcia, 1995, p. 103-116, tradução nossa).

Figura 1 - Países membros do TIAR (cor azul)



Fonte: Wikipedia Commons. Disponível em <https://commons.wikimedia.org/wiki/File:Rio_Pact_member_s.png>. Acesso em 10 Set 2020.

Quadro 1 - A Doutrina de Segurança Nacional na América do Sul

PAÍS	CONTEXTO
Brasil (Primeiro golpe militar exitoso promovido pela DSN)	A DSN serviu de base e justificativa do golpe militar de 1964, contra o governo populista de João Goulart.
Argentina	Ao igual no Brasil, a doutrina serviu de justificativa para derrubar o governo radical (1966) e ao peronista (1976), servindo também, para dar frente a guerrilha urbana dos “Montoneros”.
Chile	A DSN ajudou a legitimar o golpe de 1973, sob o pressuposto de evitar a revolução socialista do Presidente Salvador Allende.
Uruguai	A DSN serviu para estabelecer a necessidade de enfrentar a guerrilha urbana dos “Tupamaros”.
Peru (Caso particular. Naquela época o Centro de Altos Estudos Militares – CAEM, elaborou uma variante de perfil desenvolvimentista da DSN)	A doutrina legitimou o primeiro intento de golpe da segurança nacional em 1962, e depois do fracasso, em 1968. O governo militar instaurado, limitou o poder instaurado pela oligarquia no Peru. Fato paradoxo aos acontecimentos das demais ditaduras da região. O primeiro governo militar promoveu o projeto de cambio social combinado com a eliminação prática da ideologia anticomunista, contando com o apoio de intelectuais da esquerda, sendo Independiente da tutela dos Estados Unidos.
Equador	Desenvolveu uma variante doutrinária similar ao Peru.
Outros países de América do Sul	A influência da DSN foi mais ideológica que operativa.

Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

Segundo Huntington (2010, p.258), “durante a Guerra Fria, a ordem que possa ter existido era fruto de dominação pelas superpotências de seus respectivos blocos e da influência das superpotências no Terceiro Mundo”. Desde uma visão da política mundial, Huntington (2010) também nos diz que “as duas superpotências da Guerra Fria, estão sendo suplantadas pelo surgimento dos Estados-Núcleos³⁵”.

Os países tendem a atrelar-se a países de cultura semelhante e a manter um equilíbrio com os países com os quais não têm aspectos culturais em comum. Isso é especialmente verdadeiro com relação aos Estados-núcleos. Seu poderio atrai aqueles que são culturalmente semelhantes a eles e repele aqueles que são culturalmente diferentes. Por motivos de segurança os Estados-núcleos, podem tentar incorporar ou dominar alguns povos de outras civilizações, os quais, por sua vez, tentam resistir ou escapar a tal controle. Os relacionamentos históricos e considerações de equilíbrio de poder também levam alguns países a resistirem à influência de seu Estado-Núcleo (Huntington, 2010, p.258).

Com o fim da Guerra Fria se acreditava que se daria início a uma era de estabilidade, cooperação e de menos ameaças à segurança mundial, também se pensou que a tendência de diminuir a importância dos estados nacionais e sua maior interdependência fortaleceria as decisões multilaterais para benefício da humanidade. Sendo uma utopia na América do Sul devido à existência de uma marcada instabilidade de suas sociedades, voltando antigos conflitos do tipo regional, étnicos, religiosos, nacionalistas e intervenções nos países mais instáveis, com respaldo legitimador das Nações Unidas.

No mundo que está surgindo, o poder global tornou-se obsoleto, a comunidade global, um sonho longínquo. Nenhum país, inclusive os Estados Unidos, tem importantes interesses globais de segurança. Os componentes da ordem no mundo atual, mais complexo e heterogêneo, se encontram dentro das civilizações e entre elas. O mundo será ordenado com base nas civilizações ou não será ordenado de forma alguma. Nesse mundo, os Estados-Núcleos das civilizações assumem o lugar das superpotências (Huntington, 2010, p.258).

Segundo a descrição realizada neste capítulo, observamos que a participação do Brasil nos acontecimentos citados não tem sido reflexo de uma política externa intermediadora nos desinteresses relacionados com a segurança dos países sul-americanos. Dessa forma, entre o século XIX até os finais da Guerra Fria, o Brasil adotou uma posição de intermediador na Guerra entre Peru e Colômbia, em 1932.

³⁵ Os países tendem a atrelar-se a países de cultura semelhante e a manter um equilíbrio com os países com os quais não tem aspectos culturais em comum (HUNTINGTON, 2010, p.257).

Sem embargo, nos conflitos do Pacífico, do Chaco e das Malvinas, o Brasil não participou. Nos anos de 1990, na guerra do Cenepa entre Peru e Equador, o Brasil, intermédio novamente em uma solução negociada para esse conflito, sendo assinado o acordo de paz de 1995.

Um breve análise comparativo, com as outras regiões do planeta, se observa, principalmente desde os inícios do século XX que a América do Sul é apontado como uma região com baixa incidência de conflitos internacionais. Segundo Desiderá (2013, p.9), são dois pontos que se deve ter em consideração, o primeiro é que nenhum país sul-americano possui armas nucleares, químicas ou biológicas, sendo países secundários na distribuição de poder militar global. Como segundo ponto, existe pouca evidência de uma corrida armamentista na América do Sul, apesar de alguns países sul-americanos fizeram aquisições de reposição de seus armamentos obsoletos.

Para além das ameaças tradicionais, desde os anos 1980 novas ameaças, originadas por novos atores, têm ganhado força na região sul-Americana, as quais possuem naturezas doméstica ou transnacional. A associação de guerrilhas com o crime organizado (narcotráfico, tráfico de armas e lavagem de dinheiro) em determinados países andinos tem se caracterizado como a principal delas, uma vez que registra elevado índice de violência e transborda externalidades negativas para o território dos países circunvizinhos (Desiderá, 2013, p.9).

Desde finais dos anos de 1990, com a declaração política do Mercosul, a Carta Andina para a Paz e Segurança, a Declaração da Zona de Paz, observamos iniciativas que buscam a integração regional, como de mecanismo que garantem a paz e a construção da confiança entre os países sul-americanos, “de forma a possibilitar a estabilidade democrática e o desenvolvimento na região” (Desiderá, 2013, p.12).

No ano de 2008, os países da América do Sul inspirados pela união do modelo europeu (União Europeia), foi criada a União das Nações Sul-Americanas (UNASUR), sendo México e Panamá, países observadores. No ano 2014, na UNASUR, se elabora um plano de ação no Conselho de Defesa Sul-americano (CDS), com a finalidade do avanço técnico e acadêmico na convergência de delimitar as capacidades dos países membros no âmbito da ciberdefesa, para o desenvolvimento de ferramentas que permitam enfrentar as ameaças do ciberespaço, marcando assim um precedente da inclusão do ciberespaço na agenda política e estratégica dos países membros.

A iniciativa sul-americana, no sentido de dispor de mecanismos próprios para uma governança de segurança, sem interferência dos Estados Unidos foi expressa na

abordagem holística tomada pelo Conselho Sobre o Problema Mundial da Drogas (CSPMD), ao estar em clara discordância com os métodos repressivos patrocinados pelos Estados Unidos no Plano Colômbia (Desiderá, 2013, p.13).

No contexto contemporâneo, as ameaças à segurança nacional têm um perfil de problema social de ordem transnacional, por exemplo: narcotráfico, corrupção, terrorismo, violação dos direitos humanos, cambio climático etc. Deixando de ser primordialmente um conflito entre os Estados. Das ideologias e expressões redesenhadas, nasce a segurança multidimensional³⁶, com novas motivações nas atuais doutrinas de segurança nacional nos países da América do Sul. Outro fator que deve ser abordado na segurança nacional da Sul América é a instabilidade política dos países membros, existindo a dificuldade de consolidar seus sistemas democráticos, estando considerados como novas formas de ameaças à segurança nacional dos países sul-americanos.

Segundo Nasser (2019, p.37), são sete as tendências globais³⁷ que vão convergir e que dificultariam na governança e cooperação, mudando assim a natureza do poder, alterando em consequência a paisagem global de maneira fundamental.

As tendências econômicas, tecnológicas e de segurança, especialmente, aumentarão o número de Estados, organizações e indivíduos capazes atuar de maneiras influente internamente nos Estados, a ordem política permanecerá evasiva e as tensões, elevadas até que as sociedades e governos renegociem suas expectativas um com relação ao outro. Entre os Estados, o período Pós-Guerra Fria, o momento unipolar de hegemonia estado-unidense; já passou, e a ordem internacional baseada em regras, como tem sido desde 1945, pode também estar desaparecendo. Alguns grandes poderes e agressores regionais procuraram afirmar seus interesses por meio da força, mas obterão resultados fugazes à medida que as formas de poder tradicionais e materiais deverão ser menos capazes de garantir e sustentar resultados em um contexto de proliferação de agentes com poder de veto (Nasser, 2019, p. 39).

Um Estado moderno em suas atribuições fundamentais possui na segurança nacional a prerrogativa exclusiva do monopólio no uso da força, assim como o estabelecimento e manutenção da ordem e paz social, lançando mão de seu poder econômico, militar e político. Com o exercício da diplomacia, pode orientar ao

³⁶ Garantir a segurança dos povos das Américas é um dos principais pilares da Organização dos Estados Americanos. A través de sua Secretaria de Segurança Multidimensional, a OEA tem avançado para reforçar a cooperação em várias frentes de segurança e de desenvolver políticas e estratégias regionais para abordar uma série de ameaças. A OEA também trabalha através de caminhos diferentes, a fim de fornecer auxílio de segurança que é o mais abrangente e eficiente possível. A Comissão de Segurança Hemisférica é a principal responsável pela formulação e implementação das estratégias da OEA e das políticas relativas à segurança da região. Disponível <https://www.oas.org/pt/topicos/seguranca_multidimensional.asp>

³⁷ Nasser (2019, p.37-39), cita as seguintes tendências globais: 1. Os ricos estão envelhecendo, os pobres não; 2. A economia global está mudando. O baixo crescimento econômico persistirá no curto prazo; 3. A tecnologia está acelerando o progresso, mas causa rupturas; 4. Ideias e identidades estão gerando uma onda de exclusão; 5. Será cada vez mais difícil governar; 6. A natureza do conflito está se transformando; 7. A mudança climática, o meio ambiente e as questões de saúde exigirão atenção.

estabelecimento de alianças, tratados e acordos internacionais para a conservação da integridade da soberania territorial, a proteção da sociedade, dos interesses³⁸ nacionais e conquista dos objetivos³⁹ nacionais frente a todo tipo de ameaça e agressão externa ou interna. Em consequência, a estratégia para uma segurança nacional tem um caráter multidisciplinar, a mudança militar contemporânea de maior importância no nível profissional foi substituir o profissionalismo da “defesa externa” pelo novo profissionalismo da “segurança interna e de desenvolvimento nacional” (Leal, 2003, p.84).

A segurança como a defesa nacional, eles são dois aspectos que não só é matéria de preocupação do Governo, mas também dos cidadãos e pela garantia delas, embora possa ser um desafio para o Estado, sendo prioridade para qualquer País. (Blesa, 2018, p. 3, tradução nossa).

Apontamos que no contexto contemporâneo latino-americano a militarização da segurança nacional, como legado da influência norte-americana, tem trazido discursos incongruentes aos interesses e necessidades de segurança de seus países. Desta forma a DSN norte-americana está presente na função ideológica dos três países estudados, fundamentando a sociabilidade conservadora desses países, onde a segurança nacional pode ser compreendida como “um instrumento utilizado pelos setores dominantes, associados ao capital estrangeiro, para justificar e legitimar a perpetuação por meios não democráticos de um modelo altamente explorador de desenvolvimento dependente” (Alves, 1989, p.27 apud Bruziguessi, 2014, p.63). Esta ideologia mantém como estratégia fundamental a luta contra o inimigo externo e interno, descaracterizando o amplo sentido da segurança nacional, que não se limita apenas a armas e tropas. Portanto, nosso foco nesta tese é que a segurança nacional é o grau de garantia e bem-estar, a través das ações políticas, económicas, militares e psicossociais (Arruda, 2017, p.77-78), sempre orientando-se pelos interesses e objetivos nacionais.

Podemos afirmar que as estratégias de segurança nacional são de caráter multidisciplinar trazendo tópicos como: a mudança climática, as doenças pandêmicas,

³⁸ Os “interesses nacionais” são intangíveis, permanentes e inquebráveis do termo sobrevivência. Sobrevivência é entendida como a conservação da nação fisicamente como tal; do território em sua integridade e recursos; assim como a cultura, como valores qualitativos e quantitativos que unem à sociedade e preservam suas instituições por meio da ordem jurídico-política. Nos interesses nacionais, a unidade e a soberania do Estado são fundadas e são as únicas que têm caráter permanente.

³⁹ Os “objetivos nacionais” são a expressão dos interesses e aspirações vitais que a nação procura satisfazer em um certo período de sua existência, constituem um guia de referência para os governantes, pois indicam onde a ação política deve ser orientada e para os governados, como eles coletam e expressam sua visão do futuro; estabelece também o compromisso de participar ativamente nas tarefas que devem ser realizadas para cumpri-las.

as ameaças e desafios do ciberespaço, entre outros. Portanto é inegável e não menos importante a relevância da historicidade na análise contextual, nas ações do planejamento e na adequação das políticas e ações estratégicas na segurança e defesa cibernética. Esta análise realizada é importante para nós inserirmos nas políticas da segurança nacional, diante uma instável, vulnerável e cambiante realidade geopolítica, econômica, territorial, sanitária e social dos países que serão foco do presente estudo.

3.2 Historicidade do ciberespaço através da *Internet*

São diversas as definições que se tem do ciberespaço, desde a mais histórica e simples, sendo esse espaço onde acontecem conversações telefônicas. Até uma interdisciplinar, que é o espaço ou realidade virtual onde estão agrupados usuários, sites, grupos de chat, redes sociais e blogs digitais e demais serviços da *World Wide Web* (*www*⁴⁰) e da Internet. Mas podemos afirmar que o ciberespaço é uma nova dimensão, onde estão grande parte das nossas vidas, os mais de 3,9 bilhões de pessoas no mundo que estão conectadas à Internet, o equivalente a 51% da população mundial, segundo a União Internacional de Telecomunicações. Esta dimensão social e global onde interagimos, trabalhamos, pensamos, vivemos, sentimos, disfrutamos etc. Foi declarado por *The Economist* (2010, p.22, tradução nossa) com o “quinto domínio”, depois da terra, o mar, o ar e o espaço. Segundo William J. Lynn III quando exercia as funções de *Deputy Secretary of Defense*, publicou na revista *Foreign Affairs* os cinco princípios básicos da estratégia da guerra do futuro:

1. O ciberespaço tem que ser reconhecido como um território de domínio semelhante à terra, mar e ar no relativo à guerra.
2. Qualquer posição de defesa tem que ir além de uma manutenção do ciberespaço “limpo de inimigos”, onde possa se incluir operações sofisticadas e precisas que permitam uma resposta imediata.
3. A defesa do ciberespaço tem que ir além do âmbito das redes militares-domínios .mil e .gov do Departamento da Defesa para ir até as redes comerciais (domínios .com, .net, .info, .edu etc.) e que tem que estar subordinados à concepção de segurança nacional.
4. A estratégia da defesa do ciberespaço tem que ser feita em conjunto com os aliados internacionais para uma política efetiva “de alerta compartilhada” diante as ameaças mediante o estabelecimento da ciberdefesa com os países aliados.
5. O departamento da Defesa tem que contribuir para a manutenção e incremento do domínio tecnológico dos Estados Unidos de Norte América e melhorar o processo de aquisições e estar ao dia com a agilidade da evolução

⁴⁰ Faz referência a todo um sistema de documentos (em diversos formatos: vídeos, sons, hipertextos e imagens) em hipermídia que estão interligados e executados na Internet.

das indústrias das tecnologias da informação (Lynn, 2010, pp. 97-108, tradução nossa).

Segundo Bejarano (2011, p.46), existe uma dificuldade na compreensão e explicação do que é o ciberespaço por uma parte, vai depender da perspectiva e outra, se cai no erro de fazer uma definição com conceitos antigos. Frequentemente, vai se identificar o Internet com o ciberespaço, embora o ciberespaço seja um conceito muito mais amplo. Por esse sentido, nesta pesquisa vamos nos referir à *Cybersecurity* com expressões como cibersegurança, segurança por meios informáticos, segurança digital ou segurança cibernética, desde a perspectiva das políticas e estratégias de segurança e defesa nacional no domínio do ciberespaço.

A impossibilidade de identificar claramente um Heartland⁴¹, Rimland⁴² ou Mittlepunkt no ciberespaço não significa que o objeto de estudo da geopolítica seja quase inexistente. Pelo contrário, um deve ter em mente que estamos no início de um período crescente de domínio do ciberespaço nas relações internacionais, sendo no futuro próximo, altamente provável seu “Cybernetocracy” ainda esteja relativamente longe do primeiro plano da “Telurocracy” e, respectivamente, da “Thalassocracy” (Popa, 2014, p.413, tradução nossa).

A doutrina militar nas operações do ciberespaço do Departamento da Defesa dos Estados Unidos (DoD) define ao ciberespaço como um domínio que atinge fronteiras geográficas e geopolíticas, e em grande parte, residem fora do controle norte-americano. Estando integrado com o funcionamento de suas infraestruturas críticas (IC), bem como, com a conduta do comércio, governança e segurança nacional. É nesse ponto, a importância de repassar a historicidade da Internet⁴³, que vai nos permitir, uma base de discussão com a base doutrinária militar norte-americana e adequada compreensão da Internet no futuro.

Observando que nos primeiros anos da Internet, este foi desenvolvido com o esforço, mas independente de pessoas no setor de governo e acadêmico norte-americano. Desde então, segundo a Internet Society⁴⁴, o Internet evoluciona convertido em um mecanismo para a difusão da informação e um meio para a colaboração e a interação entre as pessoas e seus computadores, sem ter importância

⁴¹ O geógrafo inglês Halford J. Mackinder, conhecido como o pai da teoria da geoestratégia, desenvolveu a teoria do Heartland que significa, literalmente, coração da terra. Mackinder situou o Heartland na zona territorial que abrange os continentes europeu e asiático, recebendo a denominação de Eurásia ou Ilha Mundial.

⁴² Foi com base na teoria do Heartland que o estrategista americano Nicholas J. Spykman (1893-1943) desenvolveu a teoria do Rimland, também denominada de Estratégia da Contenção, que serviu de base para o desenvolvimento da doutrina de segurança dos Estados Unidos após a Segunda Guerra Mundial.

⁴³ Disponível em <<https://www.internetsociety.org/es/internet/history-internet/brief-history-internet/#LK76>>. Acesso em 10 abril de 2020.

⁴⁴ Disponível em <<https://www.internetsociety.org/es/tutorials/shaping-the-internet/module-1-history-of-the-internet/>>. Acesso em 10 abril de 2020.

a localização geográfica, representando um dos maiores exemplos de êxito de benefícios produto do investimento sustentável e o compromisso com a pesquisa e o desenvolvimento da infraestrutura da informação. Portanto, a questão crítica de Mazzucato (2021) no investimento sustentável e de compromisso, está na relação da inovação e os riscos assumidos pelos agentes do sistema: estatal e privado, do caso da Internet:

Para cada investimento bem-sucedido, capaz de levar a uma nova tecnologia como a Internet, existem muitos investimentos fracassados – precisamente porque a inovação é incerta. Mas reduzir a capacidade do Estado de cobrar impostos ou receber sua parte dos rendimentos compromete sua capacidade futura de assumir esses riscos [...]. A identificação de quem arca com os riscos não pode ser feita a simples afirmações de que os acionistas são os únicos que contribuem com a economia sem garantia de retorno – pressuposto central e falacioso de economia financeira baseado na teoria de agência (Mazzucato, 2021, p. 246 -247)

O notável crescimento da Internet desde ARPANET, a rede de pesquisa criada por quatro⁴⁵ universidades conectadas entre si em 1969, até a rede onipresente e global que conhecemos na atualidade, é resultado dos princípios de desenho e modelo de desenvolvimento estabelecidos pelos fundadores do Internet: Vint Cerf, Robert Kahn, Paul Baran, Marc Andreessen e Tim Berners-Lee, conhecidos, hoje em dia, como os pais da Internet. Eles tiveram como foco a criação de tecnologias padronizadas e interoperáveis, fazendo-o em um entorno aberto e participativo.

O modelo da Internet, encarna um conjunto comum de valores operacionais compartilhados entre muitas das comunidades e organizações chave que foram fundamentais para o desenvolvimento e a evolução contínua da Internet. Estes valores incluem: padronizações técnicas abertas, processos de livre acesso para o desenvolvimento da tecnologia e políticas, uma governança transparente e colaborativa, e responsabilidade distribuída para as funções técnicas, de gestão e administrativas (Lynn, 2010, p. 105 tradução nossa).

Fazendo uma retrospectiva no tempo, podemos encontrar que nos primeiros trabalhos da Internet, existem quatro dimensões chaves, que nos permitirá uma melhor compreensão da Internet:

⁴⁵ Refere-se às universidades norte-americanas UCLA, Universidade de Stanford, a UC em Santa Bárbara e a Universidade de Utah.

Quadro 2 - As quatro dimensões chaves da história da Internet

Dimensão	Definição
Tecnologia (a princípios de 1960)	A evolução tecnológica da Internet deu início com pesquisas sobre computação de pacotes e <i>ARPANET</i> ⁴⁶ , a rede que logo vai se converter na base da Internet. A invenção da comutação de pacotes, o protocolo <i>TCP/IP</i> e a <i>World Wide Web</i> foram passos importantes na evolução da tecnologia da Internet.
Gestão dos recursos da Internet (a princípios de 1980)	As primeiras abordagens adotadas na gestão e operação da infraestrutura da Internet constituem aspectos históricos importantes do desenvolvimento e ajudam a explicar como evoluiu o ecossistema da governança da Internet até se converter no que se sabe hoje em dia.
Comunidade técnica da Internet (em 1992)	Também está o aspecto social, que tem relação com a comunidade mais ampla de pessoas e partes interessadas que trabalharam juntos na criação e avanço do Internet e suas tecnologias.
Comercialização (em 1985)	Ela fez com que a Internet fosse uma rede de uso simples para compartilhar os resultados de algumas pesquisas até ser a infraestrutura de informações e comunicações de grande implantação e amplamente acessível, que hoje dependem grande parte da sociedade.

Fonte: Internet Society (ISOC), tradução nossa.

Nota: Mais detalhes, olha-se o Apêndice VIII – Figura 67

Na Internet, a primeira descrição que fora registrada nas interações sociais habilitadas através de uma rede foram diversos memorandos, escritos por Joseph Carl Robnett Licklider, conhecido como “*Lick*”, cientista da computação e psicólogo norte-americano do *Massachusetts Institute of Technology* (MIT) em agosto de 1962. Ele faz uma descrição do conceito de uma “rede galáctica”. Ele imaginou um conjunto de computadores interconectados globalmente, acessando todo o mundo rapidamente a dados e programas de qualquer parte do mundo. Esse espírito é um conceito muito similar ao que hoje em dia é a Internet. Licklider foi o diretor do programa de pesquisa informática da DARPA, que teve seus inícios em outubro de 1962. Sendo os próximos diretores daquela agência: Ivan Sutherland, Bob Taylor e Lawrence G. Roberts, conscientes da importância do conceito de rede defendido pelo “*Lick*”.

Leonard Kleinrock do MIT, publicou o primeiro documento da teoria da “comutação de pacotes”, em julho de 1961 e o primeiro livro daquele tema em 1964. Kleinrock convenceu a Roberts da factibilidade teórica de se comunicar fazendo uso de pacotes em lugar dos circuitos, sendo um grande passo na viagem das redes informáticas. Já em 1965, Thomas Merrill, Roberts e Cerf alcançaram um segundo passo importante que foi que os computadores se comunicaram entre si. Eles conectaram o ordenador TX-2, em *Massachusetts*, com o Q-32, na *California*, fazendo uso de uma rede comutada de baixa velocidade, criando assim a primeira, ainda pequena, rede ampla do mundo (*Wide Area Network* - WAN). Segundo o dito pelo

⁴⁶ *The Advanced Research Projects Agency Network* (ARPANET), foi a rede de computadores criada por encomenda do Departamento de Defesa dos Estados Unidos (DOD) como meio de comunicação entre as instituições estatais e acadêmicas. Hoje em dia, o ARPANET é o organismo conhecido como a Agência de Projetos de Pesquisas Avançadas da Defesa”.

Cerf na ISOC, o resultado daquele experimento era o constatar que os computadores com tempo compartilhado poderiam trabalhar bem juntos, executando programas e recuperando dados de acordo fosse necessário no equipamento remoto, mas que o sistema de “comutação de circuitos” era totalmente inadequado para essa tarefa. Confirmando Kleinrock da necessidade da “comutação de pacotes”.

A finais de 1966, Roberts integrou a *Defense Advanced Research Projects Agency* (DARPA) para desenvolver o conceito de redes informáticas e rapidamente criou seu plano para a Advanced Research Projects Agency Network (ARPANET), publicado em 1967. A conferência onde apresentou seu artigo, também tinha outra pronúncia sobre o conceito de redes de pacotes feito em Reino Unido, pelos pesquisadores Donald Davies e Roger Scantlebury no *National Physical Laboratory* (NPL). Scantlebury comentou a Roberts o trabalho feito com Paul Baran e outros pesquisadores da RAND⁴⁷. O grupo RAND tinha escrito um artigo sobre “redes de comutação de pacotes para cifrar comunicações de voz” no Exército em 1964. A função do MIT (1961 – 1967), da RAND (1962 – 1965) e do NPL (1964 – 1967) foram feitas em paralelo sem que os pesquisadores saibam do trabalho dos demais. Foi adoptado o termo “pacote” do trabalho da NPL e a velocidade de linha proposta no desenho da ARPANET passou de 2,4 kbps a 50 kbps. Nos escritos da comunidade ISOC, Cerf comentou que dos estudos da RAND, foi que se gerou um falso rumor que ARPANET estava relacionada com a criação de uma rede resistente à guerra nuclear. Segundo o pesquisador, foi falso esse rumor, porém a palavra Inter redes enfatiza a robustez e sobrevivência, incluindo a capacidade de suportar a perda de grandes partes das redes subjacentes.

Em agosto de 1968, depois que Roberts e a comunidade financiada por DARPA redefiniu a estrutura geral e as especificações da ARPANET. A DARPA publicou uma solicitação de orçamento para desenvolver um dos componentes chave, os comutadores de pacotes, chamados processadores de mensagens de interfase (IMP). O orçamento foi obtido em dezembro de 1968, por um grupo liderado por Frank Heart, de Bolt, Beranek e Newman (BBN). Quando o time de BBN trabalhava nos IMP com Bob Kahn na realização no desenho arquitetônico geral da ARPANET, Roberts, junto

⁴⁷ Em 14 de maio de 1948, o Projeto RAND - uma organização formada imediatamente após a Segunda Guerra Mundial para conectar o planejamento militar às decisões de pesquisa e desenvolvimento - separou-se da Douglas Aircraft Company de Santa Monica, Califórnia, e se tornou uma organização independente e sem fins lucrativos. Adotando seu nome a partir de uma contração do termo pesquisa e desenvolvimento, a entidade recém-formada foi dedicada a promover propósitos científicos, educacionais e de caridade para o bem-estar e a segurança pública dos Estados Unidos. Disponível em <<https://www.rand.org/about/history.html> >

com Howard Frank e seu time de *Network Analysis Corporation*, desenharam a topologia e a economia da rede. O sistema de medida da rede foi feito pelo time de Kleinrock na *University of California* (UCLA).

Frente ao desenvolvimento inicial de Kleinrock na teoria de “comutação de pacotes” e no trabalho da análise, desenho e medição, sua *Network Measurement Center* da UCLA foi escolhida como o primeiro nodo da ARPANET. Sendo em setembro de 1969, uns dos frutos do esforço quando BBN instalou o primeiro IMP na UCLA e conectou o primeiro host. O projeto de Doug Engelbart: “*Augmentation of Human Intellect*” (aumento do intelecto humano) que incluiu NLS, um antecedente do sistema de hipertexto, no *Stanford Research Institute* (SRI), foi o segundo nodo. O SRI estava detrás do *Network Information Center*, liderado por Elizabeth Feinler (“Jake”) que incluía funções como manutenção de tabelas de nomes de host para atribuir direções, assim com uma diretoria de *Request for comments* (RFC⁴⁸).

Um mês depois, quando SRI foi conectado à ARPANET, foi enviada a primeira mensagem de host a host desde o laboratório de Kleinrock até SRI. Foram adicionados dois nós na Universidade de Califórnia, em Santa Bárbara e na Universidade de Utah. Esses dois últimos nós incluíram projetos de visualização de aplicações, com Glen Culler e Burton Fried da Universidade de Califórnia, pesquisando métodos para amostrar as funções matemáticas usando telas de armazenamento para resolver o problema da atualização na rede, e Robert Taylor e Ivan Sutherland, de Utah, pesquisaram métodos de representação em 3D na rede. Foi assim, que nos finais de 1969, se tinham quatro *hosts* conectados na ARPANET inicial, e como a Internet iniciaria sua trajetória globalizadora. Nesta primeira etapa, devemos destacar que a pesquisa sobre redes, incorporava o trabalho sobre a rede subjacente e sobre como usar a rede, sendo uma tradição que até a atualidade continua.

Nos seguintes anos, foram adicionados rapidamente mais computadores a ARPANET, continuando as pesquisas com a finalidade de dispor de um protocolo de *host a host* funcionalmente completo e outro software de rede. A *Network Working Group* (NWG), em 1970, com a liderança de Steve Crocker foi terminado o protocolo inicial (*host a host*) da ARPANET chamado *Network Control Protocol* (NCP), quando

⁴⁸ Contém documentos técnicos e organizacionais da Internet. Disponível em <https://www.rfc-editor.org/search/rfc_search_detail.php?sortkey=Number&sorting=DESC&page=All&pubstatus%5B%5D=Standards%20Track&std_trk=Internet%20Standard>. Acesso em 20 junho 2021.

foi terminado o NCP, entre os anos 1971 e 1972, os usuários da rede deram início ao desenvolvimento das aplicações. Em outubro de 1972, Kahn organizou uma apresentação da ARPANET, sendo muito exitosa na *International Computer Communication Conference* (ICCC), esta seria a primeira apresentação pública desta nova tecnologia de redes. Em 1972, foi introduzida a aplicação “hot” inicial, o e-mail. Em março, Ray Tomlinson da BBN, escreveu o software básico de envio e leitura de mensagens de e-mail, motivado pela necessidade dos desenvolvedores da ARPANET de um mecanismo simples de coordenação. Em julho, Roberts ampliou a utilidade do e-mail, sendo escrita a primeira listagem de mensagens, lê-los seletivamente, arquivá-los, reenviá-los e responder aos mesmos. Assim, o e-mail será a aplicação mais importante durante mais de uma década, presságio da atividade de hoje em dia da WWW, com um crescimento gigantesco de todo tipo de tráfego de pessoa a pessoa.

Em relação à construção da Internet, a dinâmica do período da Guerra Fria “potencializou o enfrentamento informacional, seja na corrida tecnocientífica ou na disputa político-ideológica” (Brito, Kerr, 2015, p. 155). Portanto, se destacam as contribuições de Bush (1945) na dimensão informacional, preocupado com a explosão informacional pós-guerra ao propor o conceito de *Memex*:

Sendo um termo cunhado da somatória de *memory* e *index*, o *Memex* foi um equipamento visionário, com o intuito de suportar a memória humana, bem como o armazenamento de informações (Brito, Kerr, 2015, p. 155).

Outra contribuição, foi de Norbert Wiener (1965) ao pretender estabelecer a cibernética como uma nova disciplina encarregada do “estudo do tratamento da informação no interior das máquinas”, assim “na acepção de Wiener, sob a égide da transmissão da informação não existiriam diferenças entre máquinas e seres vivos” (Brito, Kerr, 2015, p. 155). Portanto, a cibernética se constitui como um elemento de integração informacional, impactando nas relações produtivas e sociais. Sendo reconhecido no relatório da CIA, o papel fundamental da cibernética.

Os campos no qual o potencial para uma cadeia de “Sputniks” tornaram-se aparentes não se limitam às áreas óbvias de hardware. Eles incluem todo o vasto campo da “engenharia humana”, a aplicação das técnicas de controle cibernéticas, não apenas para as ciências naturais e para a economia, mas para a remodelação da sociedade como um todo (CIA, 1961, p. 8 apud Brito, Kerr, 2015, p. 156).

Então, podemos inferir que a instituição da Internet, inspirada no período da Guerra Fria, foi um projeto cuidadosamente construído que tomou várias décadas

estando gerida por organismos controlados pelo governo norte-americano, sobretudo, “firmemente, alicerçada em tecnologias produzidas neste país, grande parte originadas partir do financiamento do próprio Estado” (Brito, Kerr, 2015, p.160).

Outros aportes de consulta valiosa para esta tese, em relação à historicidade da Internet, como estudo complementar, são seguintes fontes:

- A linha do tempo que detalha os eventos chaves e desenvolvimentos tecnológicos que fizeram a Internet, é a desenvolvida pelo Robert H’obbes’ Zakon⁴⁹.
- O artigo, titulado “*A Brief History of the Internet*”⁵⁰ de Vint Cerf, onde se faz a descrição dos desenvolvimentos formativos da Internet ocorridos entre 1968 e 1996.
- A história do Internet apresentada no Museu de História da Computação⁵¹, onde se descrevem os atores chaves e os desenvolvimentos nas áreas de hardware que aconteceram na década de 90.

3.3 A Doutrina da Segurança Nacional (DSN) dos Estados Unidos, no âmbito do ciberespaço

Passo seguinte foi realizada uma primeira leitura flutuante e intuitiva nos documentos coletados no Apêndice I. Podemos afirmar, que a doutrina conjunta norte-americana tem a finalidade de melhorar a eficácia operativa de suas forças, proporcionando os princípios fundamentais que possam guiar no uso das forças armadas frente a um objetivo comum para a defesa de seus interesses nacionais. A DSN tem uma visão globalizada em seu emprego e se ajusta rapidamente aos cenários e riscos estratégicos. Outro aspecto importante a ser dito, é que a DSN não somente está orientada no desenvolvimento das capacidades militares, mas também fortalece a capacidade dos outros departamentos e agências governamentais.

Segundo a *Joint Publication 1 - Doctrine for the Armed Forces*, ela irá estabelecer uma política para a orientação das demais publicações subordinadas. Além de que a doutrina conjunta irá padronizar a terminologia, treinamentos, as relações, responsabilidades e processos entre as forças armadas, se concentrando nos esforços da busca de uma solução aos problemas dos componentes: estratégico, operacional e tático. Ela faz uso de uma análise histórica do uso dos instrumentos e mecanismos de poder militar nas operações e lições contemporâneas. Segundo a

⁴⁹ Disponível em <<https://www.zakon.org/robert/internet/timeline/>>. Acesso em 20 dezembro de 2019.

⁵⁰ Disponível em <<https://www.internetsociety.org/es/internet/history-internet/brief-history-internet/#PB64>>. Acesso em 20 dezembro de 2019.

⁵¹ Disponível em <<https://www.computerhistory.org/internethistory/>>. Acesso em 20 dezembro de 2019.

DSN, o Presidente dos Estados Unidos, é quem aprova a Estratégia de Segurança Nacional (*National Security Strategy – NSS*), sendo ele a máxima autoridade para o uso das forças armadas e de todos os instrumentos do poder nacional: diplomático, informacional, militar e econômico (JP1, 2017, p.I-1, tradução nossa).

No caso de estudo norte-americano, é importante destacar, que a construção da ação conjunta são atividades integradas e sincronizadas das forças militares com as organizações não militares, agências e o setor privado para o alcance dos interesses e objetivos nacionais. A ação conjunta é planejada e conduzida pelos Comandantes das Forças, de acordo com as diretrizes e orientações recebidas pelo Presidente, Secretário da Defesa e os Comandantes de Combate.

Quadro 3 - Linha de mando dos documentos no planejamento da segurança nacional

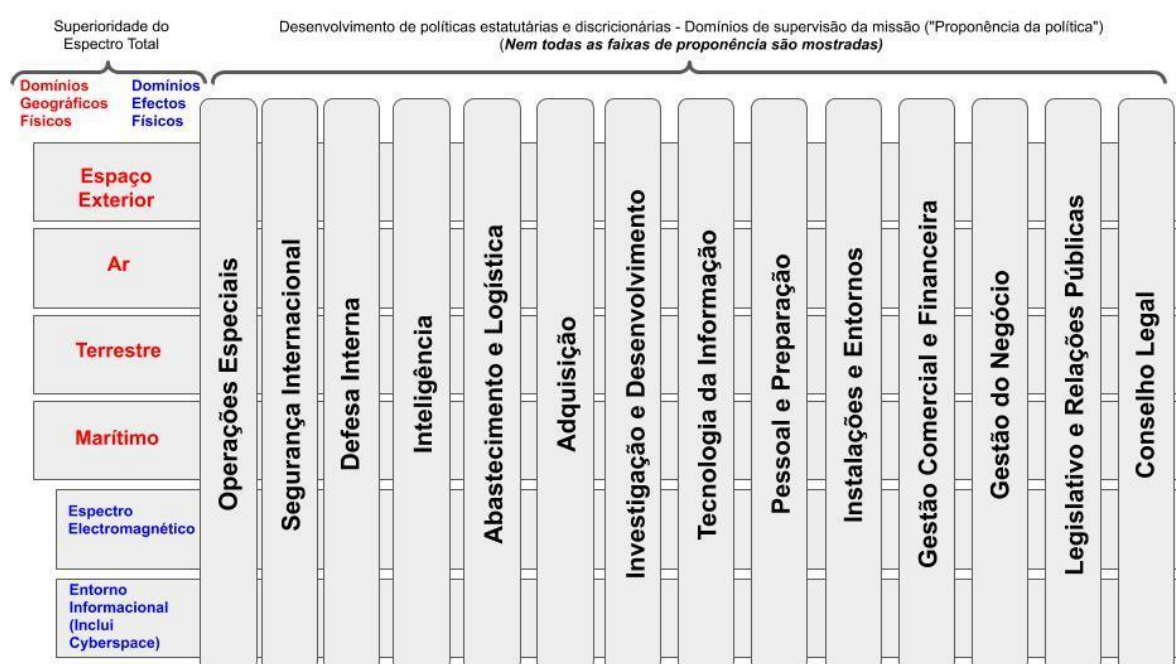
Documentos de Planejamento Nacional	Nível máximo de autoridade que aprova	Observação
Estratégia de Segurança Nacional – <i>National Security Strategy (NSS)</i>	Presidente dos Estados Unidos	Prover os fins (Ends)
Estratégia da Defesa Nacional – <i>National Defense Strategy (NDS)</i>	Secretário da Defesa (SecDef)	Prover as formas (Ways)
Estratégia Militar Nacional - <i>National Military Strategy (NMS)</i>	Presidente Conjunto dos Chefes de Estado Maior (CJCS)	Prover os meios (Means)
Guia do uso da Força – <i>Guidance for Employment of the Force (GEF)</i>	Presidente dos Estados Unidos.	Orientação Político - Militar
Plano Conjunto das Capacidades Estratégicas - <i>Joint Strategic Capabilities Plan (JSCP)</i>	Presidente Conjunto dos Chefes de Estado Maior (CJCS)	Orientação aos níveis de Comandantes de Combate e de Serviços (CCDRs).
Estratégia Nacional para a Segurança Interna – <i>National Strategy Homeland Security (NSHS)</i>	Presidente dos Estados Unidos.	Orientação para organizar os esforços das organizações federais, estaduais, locais, tribais e privadas. Funções primárias que geralmente não estão relacionadas à segurança nacional.
<i>National Response Framework (NRF)</i>	Presidente dos Estados Unidos.	É um guia de como será a resposta frente aos tipos de desastres e emergências.

Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

A DSN tem em consideração que a informação, como as tecnologias da informação, fornece e apoia os elementos cruciais nas atividades operacionais. O ciberespaço é incorporado nos esforços da segurança nacional norte-americana sendo parte dos cálculos estratégicos dos elementos estruturais e geopolíticos. A definição doutrinária da estratégia cibernética (*Cyber Strategy*) é o desenvolvimento e emprego das capacidades estratégicas para operar no ciberespaço, integrando e coordenando com outros domínios operacionais ou também citados como domínios físicos geográficos: espaço exterior, aéreo, terrestre e marítimo. Para alcançar e apoiar na conquista dos objetivos através dos elementos de poder nacional em apoio

à Estratégia de Segurança Nacional. A maior parte da questão da estratégia cibernética diz respeito aos fins para os quais os recursos cibernéticos podem ser usados. Esses fins fazem parte dos objetivos militares, políticos, econômicos, diplomáticos e da segurança nacional. O domínio das políticas geralmente se integra através de todos os domínios físicos, geográficos e dos efeitos, que constituem a superioridade total do espectro. No domínio de efeitos físicos, que são as manifestações físicas de capacidades e efeitos. São incluídos o espectro eletromagnético e o entorno informacional.

Figura 2 - Domínio físico versus domínio da política.



Fonte: (DOD, 2019, p.36, tradução nossa)

Segundo a DSN, o poder cibernético, simplesmente não tem que ser criado para existir. Apoia na realização dos objetivos, servindo como meio na satisfação das necessidades vitais e interesses nacionais da estratégia de segurança nacional.

A estratégia de segurança nacional da administração do presidente norte-americano Reagan em 1980, faz referência explícita às ligações entre informação e poder econômico, incluindo recomendações específicas sobre computadores e tecnologias avançadas de informação. No final do governo de Clinton em 1990, o rol das informações nos assuntos diplomáticos, militares e econômicos foi explicitamente reconhecido e explorado. Enquanto o governo de George Bush não fez essas conexões em seus dois documentos de estratégia de segurança nacional, estratégias de nível inferior, como a Estratégia Nacional de Segurança do Ciberespaço - *National Strategy to Secure Cyberspace* - ou a Estratégia Militar Nacional para Operações do Ciberespaço - *National Military Strategy for Cyberspace Operations*. (Kramer, Starr, Wentz, 2009, p. 42, tradução nossa).

No ano 2009, se criou a *United States Cyber Command* (USCyberComm), como organismo responsável pelas coordenações na prevenção e defesa cibernética norte-americana. Analisando os documentos da APÊNDICE I, observamos que a USCyberComm está subordinada ao Comando Estratégico, devendo buscar a cooperação com as forças armadas e os demais órgãos que conformam a comunidade de inteligência. A autoridade que vem exercendo o comando da USCyberComm, exerce função de Diretor na *National Security Agency* (NSA) e Chefe na *Central Security Agency* (CSS). Portanto, podemos dizer que essa única pessoa é quem tem a responsabilidade da segurança quanto pela defesa nos Estados Unidos, assim as políticas de segurança e defesa cibernética nacional devem estar alinhadas com a diversas frentes de colaboração. Desde a perspectiva, geopolítica global, note-se que a DSN faz menção a seis Comandos: Comando Norte ou *United States Northern Command* (USNORTHCOM), Comando Sul ou *United States Southern Command* (USSOUTHCOM), Comando Africano ou *United States África Command* (USAFRICOM), Comando Europeu ou *United States European Command* (USEUCOM), Comando Central ou *United States Central Command* (USCENTCOM) e Comando Indico-Pacífico ou *United States Indo-Pacific Command* (USINDOPACOM). Sendo delegado a cada um desses Comandos, missões e objetivos específicos, como também, as áreas geográficas de responsabilidade. Além disso, existem outros quatro Comandos, que tem no mundo todo missões e responsabilidades, por sua particular função: *United States Cyber Command*, *United States Special Operations Command*, *United States Strategic Command* e *United States Transportation Command*.

Figura 3 - Distribuição geográfica dos comandos dos Estados Unidos.



Fonte: (DOD, 2019, p.43)

Segundo o Departamento da Defesa (DoD) norte-americano os objetivos do departamento no âmbito do ciberespaço, são:

- Garantir que a Força Conjunta (*Joint Force*) possa alcançar suas missões no ambiente do ciberespaço.
- Fortalecer a Força Conjunta (*Joint Force*) na condução das operações no ciberespaço que aprimoram vantagens militares.
- Defender as Infraestruturas Críticas (IC), das atividades maliciosas que de forma individual ou como parte de uma campanha, poderia causar um incidente cibernético significativo.
- Proteger as informações e sistemas do DoD de atividades cibernéticas maliciosas, incluindo informações das redes não pertencentes ao DoD.
- Expandir a cooperação cibernética do DoD com interagências, indústrias e parceiros internacionais.

Por outro lado, segundo os Códigos dos Estados Unidos (USC) que nomeia e compila a través de códigos oficiais, os estatutos federais gerais e permanentes dos Estados Unidos. Nas operações do ciberespaço a participação das agências e departamentos federais é de acordo ao âmbito de responsabilidade, seja no ordem interno e externo, como garantir os padrões tecnológicos e interesses dos Estados Unidos (Olha-se Apêndice VIII – Quadro 25).

Repare-se que as considerações e desafios presentes no planejamento das capacidades e funções conjuntas no âmbito cibernético são como nos outros domínios

físicos. Os objetivos, as áreas de conflitos e sem conflitos, as intenções do Comandante no exercício da cadeia de comando, a avaliação político-militar e as avaliações dos efeitos colaterais, todas elas, participam no planejamento e cálculo dos esforços nas operações do ciberespaço. Da mesma forma, todos os princípios das operações conjuntas, como manobra e surpresa, são também pertinentes. Como vimos, a doutrina, deixa claro que os efeitos de ordem secundária e superior dentro e através do ciberespaço são mais difíceis de prever, necessitando de mais ramos e sequelas nos planos. Embora, muitos instrumentos do ciberespaço possam ser mapeados geograficamente nos domínios físicos, dispor de uma compreensão completa da postura e das capacidades de um adversário no ciberespaço, envolve a compreensão da infraestrutura de rede subjacente, das forças e capacidades aliadas que podem ser direcionadas, das leis e políticas nacionais, estrangeiras e internacionais aplicáveis.

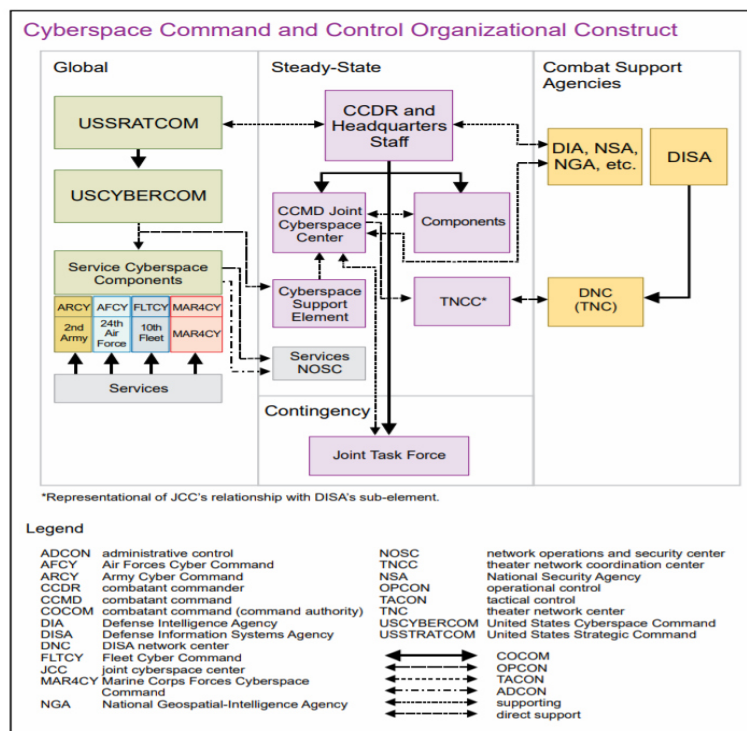
O monopólio ou o garantidor firme da segurança interna atribuída ao território nacional é sensivelmente mais difusa, embora possa se tornado um truísmo. Também não é menos verdade que, apesar de certas realidades da segurança, atores estatais do período pós-moderno estão relativamente longe de manter unilateralmente a hegemonia nos mecanismos de segurança ou, por que não, da segurança do ciberespaço (Popa, 2014, p.414, tradução nossa).

No exercício do controle no ciberespaço, não necessariamente implica estar dentro das fronteiras geográficas associadas à nacionalidade do ator ou proporcional à influência geopolítica do ator. Um elemento criminoso, um grupo politicamente motivado ou mesmo um indivíduo pode ter uma maior presença e capacidade no ciberespaço do que muitas nações fazem hoje. Independentemente da fase operacional em andamento é importante determinar quais autoridades são responsáveis de executar as Operações Cibernéticas.

Os encarregados, do planejamento no ciberespaço, devem levar em consideração o tempo de espera para adquirir das autoridades as necessidades de capacidades desejadas no ciberespaço. O citado, não altera os fundamentos de planejamento do Comandante da Força Conjunta (*Joint force Commander* - JFC), mas enfatiza a importância da coordenação com os parceiros das interações, que podem ter autoridades e mecanismos de poder diferentes do DoD. Além, das considerações e desafios adicionais de integração das operações cibernéticas no planejamento do JFC, os planejadores podem usar muitos dos elementos e

instrumentos presentes, nos processos tradicionais para implementar a intenção e orientação do JFC.

Figura 4 - Construção organizacional do Comando e Controle (C2), nas operações do ciberespaço.



Fonte: (JP 3-12(R), 2013, p. IV-8).

Na ilustração acima, observa-se as linhas de coordenação dos elementos do planejamento do Comando e Controle (*Command and Control* - C2), cuja ação vai depender do tipo e escala da operação, da presença e sofisticação do adversário no ciberespaço, como dos tipos de alvos identificados no ciberespaço. Independentemente de quais elementos são estabelecidas as sobreposições entre as missões globais, o teatro de operações no ciberespaço e as restrições do pessoal que estão conduzindo as operações cibernéticas, se necessita de uma estreita coordenação e sincronização entre os comandos e interagências.

Por outro lado, a preocupação de dominar o Ambiente de Informação Global (*Global Information Environment* - GIE) por meio da condução das Operações de Informação⁵² (*Information Operations* - IO) que basicamente é o uso integrado e global de informações relacionadas a outras linhas de operações, podendo ter como alvo o influenciar, perturbar, corromper ou usurpar as atividades e processos do C2 dos

⁵² A presente pesquisa, as Operações de Informação (IO - Information Operations) parte de uma terminologia usada na doutrina militar norte-americana, o autor quer amostrar seu olhar, desde uma perspectiva do sistema complexo, onde a interação de outros sistemas entre si, exibem propriedades coletivas emergentes. Olha-se o Apêndice VIII- Figura 68.

sujeitos informacionais tendo na segurança da informação, como encarregada de estabelecer os princípios para a proteção da informação.

Os decisórios de todos os níveis encontrarão um domínio de informação em expansão, denominado: “Ambiente de Informação Global” (*Global Information Environment* – GIE), o GIE contém aqueles processos e sistemas de informação que estão além da influência dos militares, chegando até as Autoridades Nacionais de Comando (*National Command Authorities* – NCA). Também, se apresenta o conceito de “dominância da informação” como o elemento chave para operar de forma eficaz dentro deste novo ambiente. Para alcançar o domínio, o decisor deve ser capaz de dominar as manobras tradicionais do campo da batalha e o “Ambiente de Informação Militar” (*Military Information Environment* – MIE).

Devido aos rápidos avanços em tecnologia, especialmente, na área da informação, o ambiente geoestratégico de hoje se tornou cada vez mais complexo e no futuro, se tornará ainda mais. As comunicações globais aceleram e expandem a consciência coletiva de eventos, problemas e preocupações. Eles inflamam paixões, acendem novas perspectivas, cristalizam crenças profundamente arraigadas, e obrigam pessoas, nações, organizações e instituições a examinar, definir e agir de acordo com seus interesses. Enquanto muitos efeitos desse fenômeno podem ser benignos e benéficos, outros criarão turbulência, confusão, caos e conflito. Tal conflito pode estender-se além do tradicional campo de batalha para abranger a espionagem, a sabotagem, o terrorismo, a competição econômica e os esforços para moldar as percepções públicas (FM 100-6, 1996, p. 1-1. Tradução nossa).

Entenda-se que de acordo a uma específica missão as equipes encarregadas das operações no nacional e de proteção, vão coordenar conforme ao tipo de operações, seja na defesa e ofensiva, como na escala do âmbito no ciberespaço interno (defesa e segurança do ciberespaço) ou externa (ataque e exploração do ciberespaço)⁵³. Para o autor, a agrupação de vários GIE define o espectro informacional da ecologia social digital (Huamani, Moura, 2024a).

3.4 Inferências iniciais da DSN cibernética dos Estados Unidos

Observa-se que a DSN cibernética dos Estados Unidos, passou a usar todo seu conhecimento e tecnologia produzida a partir da Internet e do ciberespaço para subsidiar a conquista de seus interesses sociais, militares, geopolíticos e econômicos. O ciberespaço é uma parte intrínseca do desenvolvimento de qualquer país, dispor de uma predominante capacidade cibernética é crucial para os Estados progredirem e se desenvolverem social, cultural, econômico e político. Em soma, países como os Estados Unidos, Rússia, China, Israel, Alemanha, Reino Unido, França e outras potências mundiais dispõem de “Políticas e Estratégias Nacionais em Segurança e

⁵³ Olha-se no Apêndice VIII - Figura 69

Defesa Cibernética” para promover o fortalecimento de seus sistemas, mecanismos e processos no domínio das informações. Como também, de um eficiente e eficaz Comando e Controle (C2) com capacidades de aplicar o poder político, militar e econômico em tempos de paz como de guerra. Em todo tipo de cenários, entenda-se cenários como domínios da batalha⁵⁴: espaço exterior, territorial, marítimo, aéreo e ciberespaço. Sendo o ciberespaço, um domínio que pode gerar influências e efeitos nos outros domínios.

O termo de segurança cibernética ou *Cybersecurity* é relativamente novo, entrando em vigor por volta do ano 2000, com seu origem na ciência da computação, sendo uma história fortemente dominada pelo norte-americanos, devido aos fatores políticos, sociais e econômicos, que moldaram a revolução da informação em seus estágios iniciais.

Os Estados Unidos, estavam na vanguarda do desenvolvimento de forma específica em compreender os benefícios e os riscos emergentes da “Era da Informação”. Enquanto outros países começaram a pensar na Era da Informação e na política, especialmente nas necessidades de proteção das infraestruturas de críticas de informações no final dos anos 1990, muitos dos conceitos de políticas e percepções de ameaças foram adotados dos Estados Unidos, pelo menos em seus traços gerais (Dunn, Egloff, 2019, p. 44, tradução nossa).

Uns dos principais aspectos para a compreensão de como se articulam a segurança nacional, com a segurança cibernética⁵⁵ é que ambas vão contribuir em consolidar os interesses e objetivos nacionais, no exercício do controle para a estabilidade nacional, desenvolvimento integral e justiça social. Possuindo como seu pilar à defesa nacional. A defesa nacional é um conjunto de medidas, previsões e ações que o Estado gera, adota e executa de forma integral e permanente, no interno e externo, de sua soberania no domínio da batalha. Por isso, a segurança cibernética vai se situar e integrar os mecanismos e instrumentos da segurança nacional.

É preciso lembrar que a noção de jurisdição cibernética não se sobrepõe à noção de soberania cibernética, embora a capacidade de exercer jurisdição cibernética constitui o principal vetor da soberania do Estado no ciberespaço. De fato, o direito dos atores estatais de responder firmemente a ameaças cibernéticas específicas pode dificilmente ser contestado da perspectiva da segurança internacional, mesmo que transcenda território nacional. Obviamente, alcançar esse desiderato, como sugiro a seguir, tem certas limitações técnicas e legais (Popa, 2014, p.415, tradução nossa).

⁵⁴ Olha-se o Apêndice VIII - Figura 70.

⁵⁵ Na presente pesquisa os termos de: segurança cibernética, cibersegurança, segurança digital serão relacionados como um mesmo conceito (com foco e escopo na segurança nacional), tendo-se em consideração que muitos países da América Latina, estão usando esses termos em suas políticas, estratégias e programas nacionais aplicadas ao ciberespaço.

Por essa razão, buscar uma definição de segurança cibernética, traz em si, certa dificuldade devido à evolução contínua e mudanças das tecnologias, no cenário geopolítico e do mercado digital. Não faz muito tempo, nas discussões, nos círculos dos tecnólogos e especialistas a relacionavam com proteção da Infraestrutura Crítica das informações ou na segurança da informação, sendo um problema técnico do gerenciamento dos riscos. Na atualidade, tornou-se uma questão tratada nos círculos mais altos do governo, devido ao incremento político-econômico dos interesses nacionais no ciberespaço e que deve ser entendida em suas diversas facetas como uma definição transversal, com as outras políticas do Estado.

A segurança cibernética é um efeito colateral das atuais tensões geopolíticas. Os ciberincidentes de alto nível afetam não apenas indivíduos ou empresas individuais, mas também são vistos como uma ameaça para Estados, sociedades e economias. Consequentemente, os Estados estão revisando suas próprias capacidades ofensivas e defensivas e estão consolidando seu planejamento estratégico quanto ao uso do ciberespaço (Dunn, Egloff, 2019, p.38, tradução nossa).

Na DSN se deixa clara a estratégia nacional de âmbito “cívico-militar-globalizada” e a preocupação do governo dos Estados Unidos, segundo a política nacional de estar sempre à vanguarda na exploração das modernas tecnologias da informação, com a finalidade de aproveitar o potencial da disseminação rápida e uso da informação, como fator determinante de exercer influência e de uma comunicação estratégica globalizada, através de suas indústrias como do uso das mídias digitais.

A economia dos Estados Unidos, as estruturas sociais e civis e os governos federal, estadual e local tornaram-se dependentes do fluxo rápido e preciso de informações. Ao mesmo tempo, os Estados Unidos exercem extraordinária influência em todo o mundo através de suas mídias multinacionais e indústrias comerciais e de entretenimento. Em menor grau, a América é influenciada por fenômenos semelhantes exercidos fora de suas fronteiras. A *Infraestrutura Global de Informação (Global Information Infrastructure – GII)*, conecta eletronicamente organizações e indivíduos em todo o mundo e é caracterizada pela fusão de redes e tecnologias de informação civis e militares (FM 100-6, 1996, p. 1-2. Tradução nossa).

Devido às revelações de Edward Snowden, ex-funcionário da agência Nacional de Segurança (*National Security Agency – NSA*) através da *Wikileaks.org*. Se conhece que os serviços de inteligência norte-americanos são provavelmente os atores mais importantes quando se trata do uso estratégico do ciberespaço. Ao explorar as falhas de segurança não conhecidas e dos instrumentos de poder nas organizações público-

privadas⁵⁶, nos diversos locais operacionais da infraestrutura do Internet⁵⁷, para fins diversos, como: a vigilância, espionagem, ações disruptivas etc. Segundo Dunn e Egloff (2019, p.47), emerge uma situação paradoxal, onde os atores estatais são diretamente responsáveis de pôr em risco a mesma segurança nacional, sendo assim, eles são os responsáveis.

A segurança cibernética e a segurança da informação possuem uma inter-relação íntima tornando-se quase obrigatória, ambas deverão ser atendidas com o devido cuidado de inclinar-se a um relativismo simplista e generalista. A fim de estabelecer adequadas estratégias e linhas de ação aos problemas presentes da segurança cibernética. Segundo Pohle e Thiel (2022, p. 8) “desde as revelações de Snowden em 2013, o foco na autonomia e segurança do Estado tornou-se um elemento central dos discursos sobre soberania digital”. Portanto, para o autor, como um proposta de ação da segurança deverá ela visar a noção da multi-perspectividade:

- Fluxo informacional, frente a necessidade de organizar e compartilhar informações no ambiente organizacional para a tomada de decisões.

A relação entre dados, informação, conhecimento e inteligência resulta na existência de fluxos de informação, que em um ambiente organizacional, dão suporte à tomada de decisão (Cunha *et al.*, p.112).

- Objetos informacionais, desde sua construção “tendo como conceito nuclear a ideia de cultura, como artefato e como processo”. (Marteleto, 1995).
- Sujeitos informacionais, observando o entrelaçamento de duas dimensões: ser humano e informação.

Os sujeitos informacionais não representam apenas uma evidência empírica (seres humanos se relacionando com documentos e informações) mas, sobretudo, se relacionam com um amplo campo de construção de diferentes ‘objetos de pesquisa’, isto é, maneiras distintas de se compreender esses indivíduos e suas relações. Ao mesmo tempo, esses ‘sujeitos informacionais’ acrescentam algo à ideia de ‘sujeito’. Não se trata apenas de se estudar pessoas, sujeitos, em si, ou em seus aspectos sociais (como faz a Sociologia), subjetivos (como faz a Psicologia) ou culturais (como faz a Antropologia). Estudar os indivíduos no campo da Ciência da Informação significa perceber que existem indivíduos usando, buscando, sentindo falta ou disseminando informação, e que essas ações os constituem enquanto um tipo particular de sujeitos – justamente os sujeitos informacionais (Araújo, 2013).

⁵⁶ Disponível em <<https://file.wikileaks.org/file/crs/RS20444.pdf>>. Acesso em 26 de outubro de 2020.

⁵⁷ Disponível em <<https://wikileaks.org/amazon-atlas/>>. Acesso em 26 de outubro de 2020.

- Das relações entre política, informação e poder, para a compreensão dos processos, serviços e produtos informacionais através dos espaços de informação, na sociedade, nas TIC, na economia e no mercado.

Dentro do contexto de ciência da informação, o regime de informação se configura como uma formação social conjunta de elementos em rede como atores sociais (sujeitos, dispositivos e tecnologias), regras de poder, a organização e a gestão política da informação que se operacionalizam em práticas sociais com produtos e serviços (Bezerra *et al.*, 2016, p.61).

3.5 A política de segurança cibernética, nos diferentes papéis do Estado

Com o apoio do estudo dos pesquisadores Dunn e Egloff⁵⁸ (2019), afirmamos que o papel de um Estado democrático, na política de segurança cibernética, tem um espaço político de três dimensões:

Teórico, onde o papel do Estado é ser o ator principal da segurança cibernética. Como as definições existentes vem teorizando o papel do Estado? É um ponto de vista muito limitado, devido que a política de segurança cibernética é olhada exclusivamente como um problema da segurança internacional. Em relação às características internas do Estado, não são contempladas outras questões, onde seja permitida sua articulação com as diferentes políticas existentes no Estado.

Empírico, onde é analisado o desenvolvimento das políticas em segurança cibernética. Qual é o papel do Estado na construção da segurança cibernética no âmbito nacional: passiva e ativa? Que outros papéis o Estado vem desempenhando na atualidade? Que tipo de instituições existem e dão resposta em segurança cibernética? Que tarefas tem e como funcionam? Que impacto tem a segurança cibernética na sociedade? Se destacando os vários papéis do Estado, desejado em parte pelo próprio Estado como exigido desde o exterior. Assim, são apresentados os seis papéis diferentes do Estado:

- Garante da segurança.
- Legislador e regulador.
- Representante e suporte da sociedade.
- Parceiro da segurança.
- Gerador e distribuidor do conhecimento.

⁵⁸ O artigo foi escolhido pelo motivo de conversar com a perspectiva académica que está sendo apresentada na tese. Disponível em < https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Dunn_Cavelty_Egloff_2019%20STAIR%20Issue%2015.1.pdf >. Acesso em 21 novembro de 2019.

- Ator de ameaça.

Normativo, onde é analisado, qual deve ser o papel do Estado? Que papéis o Estado deve ocupar? Sendo descrito as três áreas de tensão entre o Estado, economia e sociedade, em relação à política de segurança cibernética.

Segundo Dunn e Egloff (2019, p. 47-48, tradução nossa), historicamente se olha um desenvolvimento dos papéis do Estado e que é aditivo, onde novos papéis são assumidos, enquanto os antigos permanecem, aumentando a complexidade do campo da política da segurança cibernética. Coincidem três fases, na política de segurança cibernética, onde o Estado aparece como o proprietário das redes ameaçadas (Proprietário). Um segundo papel, o Estado aparece como o ator que deve resolver o problema em termos de política de segurança (Proprietário do Problema). Finalmente, o Estado ou estruturas dentro do Estado (unidades individuais) aparece como criador do problema (Originador do Problema).

Quadro 4 - Histórico papel do estado na política de segurança cibernética

Fase	Área do problema	Papel do Estado
1980	• “<i>Hacking</i>” é reconhecido como um problema na política pública devido aos diferentes incidentes. • A principal preocupação é a prevenção de dados classificados sendo roubados de governos ou das redes governamentais. • As soluções foram principalmente relacionadas ao Estado como proprietário das redes e informações.	Proprietário
1990	• Sistemas cada vez mais em rede e comercialização da internet levam a um problema coletivo maior que diz respeito a partes mais amplas da sociedade e da economia. • Infraestrutura crítica tornar-se um ponto focal (a partir de 1995). • Recursos são feitos ao Estado a partir de atores públicos e privados para melhorar a segurança desses sistemas e do coletivo.	Proprietário Proprietário do Problema
2000	• A quantidade de qualidade de, e atenção dada aos “Alvos de ataque” aumentou. • Os Estados (e serviços de inteligência) são muito mais ativos como atores. • Estados parecem responsáveis pela situação que se torna pior. • A corrida armamentista cibernética se desenvolve.	Proprietário Proprietário do Problema Originador do Problema

Fonte: (Dunn, Egloff, 2019, p.48, tradução nossa)

Um nível satisfatório de segurança cibernética só pode ser alcançado por governo, empresas e sociedades juntos. No entanto, os subgrupos dentro desses setores, muitas vezes têm interesses diferentes. Isto gera pelo menos três áreas de tensão na qual a política de segurança cibernética conscientemente deve estar posicionada. Onde a política de segurança cibernética é prescrita nesses eixos e onde ela se movimenta é resultado dos processos complexos de negociação que são fortemente dependentes a eventos individuais e de percepções de perigo relacionadas (Dunn, Egloff, 2019, p.48, tradução nossa).

Segundo Dunn e Egloff (2019), na primeira área de tensão criada entre o Estado e a economia se tem a necessidade de formular uma política para garantir às IC, que se vem influenciadas pelas consequências negativas da liberalização, privatização e globalização, desde o ponto de vista da política de segurança, sem

impedir os efeitos positivos. Segundo Brito e Kerr (2015, 160) a soberania nacional estaria sendo repassada aos detentores das novas tecnologias.

O Poder Informacional norte-americano foi sendo colocado aos demais atores globais, com um misto de imposição e sedução. Pelo viés da força, a única potência global do planeta exigiu a privatização e desregulamentação das comunicações, sobretudo nos países de terceiro mundo (NRC, 1994; Zittrain, 2008 *apud* Brito, Kerr, 2015, p.161).

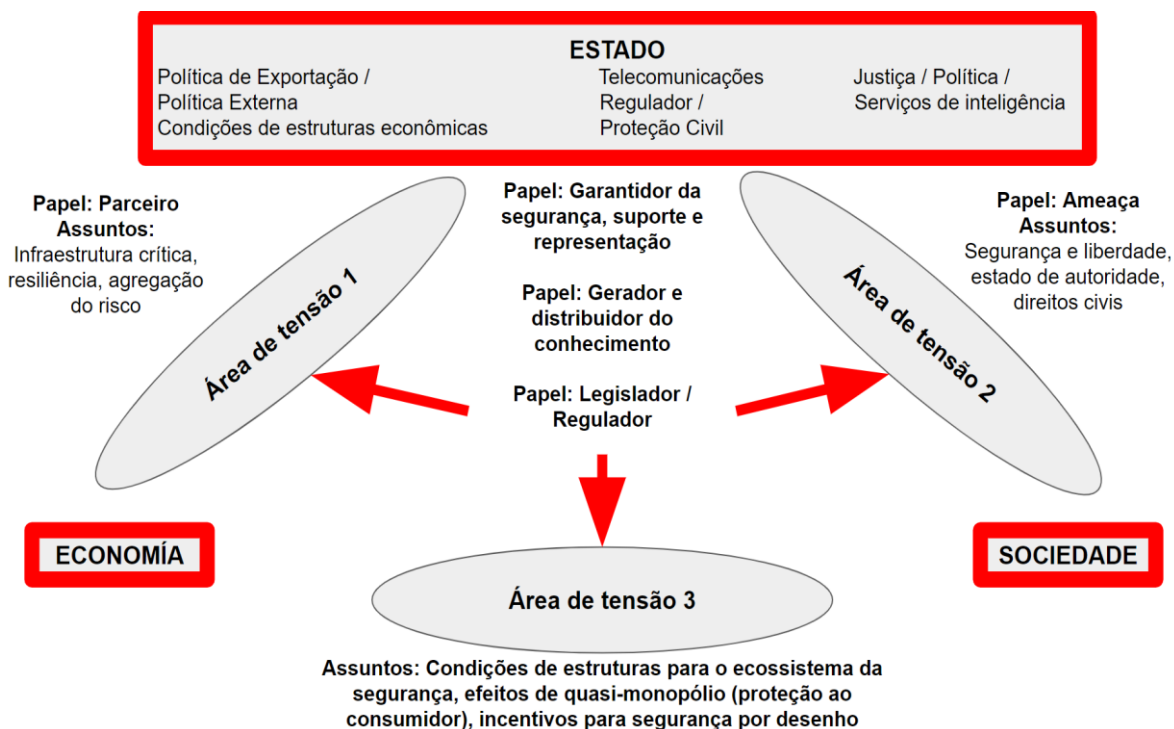
Nesta área de tensão, o Estado deveria estar preocupado com a dependência da ação econômica e a resiliência resultante da sociedade. Os questionamentos do Estado abrangem o como pode ser criada a confiança entre o governo e as empresas, onde deve o Estado intervir para evitar agregações de risco e efeitos colaterais que possam representar uma ameaça à sociedade.

Na segunda linha de tensão, o Estado deverá encontrar um equilíbrio entre a segurança e a liberdade no espaço cibernético. Os poderes da polícia e a inteligência, frequentemente entram em conflito com os direitos civis, especificamente, o direito à autodeterminação ou ao anonimato da informação na Internet. A segurança cibernética é apenas uma das muitas questões intersetoriais complexas que o Estado busca resolver. O dano causado por incidentes cibernéticos passados, pode não ser suficientemente alto ou pode não ter uma experiência diretamente para tornar substancial custos mais altos e cortes nos direitos civis aceitáveis. Ao contrário, o dano percebido em outras questões, como o terrorismo, serve como legitimação para fazer cortes no discurso político dos problemas, na segurança cibernética. Por exemplo: o debate sobre a política da criptografia, onde se autoriza às agências de inteligência e da segurança nacional a ter acesso às chaves criptográficas das empresas tecnológicas.

A terceira área de tensão, conflito entre cidadãos e empresas, é necessário estabelecer as condições estruturais para o desenvolvimento de um ecossistema de segurança bem-sucedido de como estabelecer os processos de diferenciação social. Como pode o mercado, que é também confrontado com o problema dos quase-monopólios, seja regulado de tal maneira alcançar um ótimo equilíbrio entre segurança e funcionalidade? Como podem os incentivos para mais obrigações de segurança ser criado para prestadores de serviços? Como os usuários podem ser sensibilizados em segurança, ao fato de que eles são conscientes das funcionalidades dos produtos tecnológicos que consomem? Como pode o marco jurídico-global ou a diplomacia internacional criar condições para que atividades no ciberespaço sejam

harmonizadas em neutralizar o perigo das brechas e a prioridade de soluções tecnológicas baratas?

Figura 5 - As três áreas de tensão política da segurança cibernética



Fonte: (Dunn, Egloff, 2019, tradução nossa)

Os papéis do Estado na política de segurança cibernética, assumindo uma multidão de papéis, não é de surpreender. Nas questões políticas, o Estado representa ao mesmo tempo, uma ampla variedade de interesses. Consequentemente, são elaboradas nos diferentes departamentos e agências governamentais temáticas similares, mas com diferentes grupos de interesse, principalmente, no político, econômico e social. Cada um desses grupos políticos têm uma visão diferente no papel do Estado. Por esse motivo, os conflitos dos papéis em um Estado democrático são tratados nos níveis político-estratégico e em forma sistemática, sob a influência de novos modelos dando lugar a novos conteúdos e espaços de enunciação. Dando incentivos à reformulação da constituição comunicacional e informacional, nas relações de poder entre um Estado e seus atores econômicos. Segundo Braman (2009) as “mudanças na natureza da sociedade que derivam do processo de informatização, bem como outros fatores, geram problemas adicionais no estudo do poder”, portanto, ao analisar o poder observamos três formas:

instrumental⁵⁹, estrutural⁶⁰ e simbólica⁶¹. Porém, na sociedade contemporânea é identificada uma quarta forma, o poder informacional⁶², como o centro do palco. Desse modo, no paradigma moderno de soberania, o Estado é o agente privilegiado da elaboração e implantação da política de informação, paradoxalmente, nos países em vias de desenvolvimento não se tem alcançado o sucesso esperado.

A convicção no papel causal da informação na modernização e desenvolvimento não se mostraria igualmente eficaz para consolidar, para a informação científico-tecnológica, estruturas institucionais, duradouras e progressivas na formulação de seus parâmetros organizacionais e tecnológicos. Nos fatos, os sistemas nacionais de informação científico-tecnológica não encontram expressão em um domínio estável e transparente de agentes, instituições, espaços e agendas de formulação de políticas públicas, seja porque a informação é objeto de políticas indiretas e tácitas, seja porque o escopo e abrangência das políticas de informação recortadas sobre o grande mapa das políticas públicas são deslocados frequentemente, de acordo com definições de prioridades conjunturais e em constante mudança (González de Gómez, 2002, p.28-29).

Nos países em vias de desenvolvimento é observada a tendência na perda do poder de seus Estados, em relação a outros atores. Dando a impressão que no futuro esses Estados poderiam desaparecer completamente, porém, inferimos que seguem uma transformação na forma. Desde essa perspectiva Braman (2009) comenta o seguinte:

Em processos ainda em andamento, o Estado vem reafirmando sua força de três maneiras. Primeiro, os governos nacionais estão aprendendo a dominar os mesmos tipos de poder informacional que as corporações e outros atores não estatais têm usado com sucesso em seus desafios à força das entidades geopolíticas. A expressão do poder informacional em leis e regulamentos é o assunto da segunda metade deste livro. Em segundo lugar, os estados estão desenvolvendo técnicas para estender o uso de entidades do setor privado como agentes reguladores, transformando centros privados de poder em propósitos estatais. Um exemplo dessa tendência é a exigência de que os provedores de serviços de Internet (ISPs) ajudem os governos nacionais a monitorarem o uso da Internet em busca de abusos de segurança nacional e direitos de propriedade intelectual. Em terceiro lugar, o Estado – como a empresa – é cada vez mais caracterizado como "em rede", devido à multiplicidade de maneiras fundamentais pelas quais os governos estão entrelaçados entre si e com atores não estatais. Os exemplos aqui muitas vezes invertem a direção do apoio que acabamos de descrever, com os governos assumindo a responsabilidade de garantir as condições mais favoráveis possíveis para as atividades corporativas; acordos nacionais com a Organização Mundial do Comércio no âmbito do Acordo Geral sobre o Comércio de Serviços fornecem exemplos desta tendência. O uso de tecnologias de informação e poder informacional é tão importante para todas essas maneiras pelas quais o Estado-nação está evoluindo que a forma

⁵⁹ Poder que formata o comportamento humano pela manipulação do mundo material via força física (Braman, 2009, p.25).

⁶⁰ Poder que formata o comportamento humano pela manipulação do mundo social via regras e instituições (Braman, 2009, p.25).

⁶¹ Poder que formata o comportamento humano pela manipulação dos mundos material, social e simbólico via ideias, palavras e imagens (Braman, 2009, p.25).

⁶² Poder que formata o comportamento humano pela manipulação da base informacional dos poderes instrumental, estrutural e simbólico (Braman, 2009, p.25).

política dominante de hoje é mais bem descrita como o Estado informacional (Braman, 2009, p. 34- 35).

Então, na perspectiva do poder informacional podemos inferir que Braman (2009) não se desvincula sobre a transformação do Estado, desembocando em um novo papel (ou tipo) de Estado, de dimensão informacional.

3.6 A geopolítica contemporânea: as disputas do poder mundial são econômicas?

Embora os países com as economias mais industrializadas do planeta, tais como: Alemanha, Canadá, Estados Unidos, França, Itália, Japão, Reino Unido e Rússia (países do G-8) e organizações internacionais como a União Europeia (UE), a Organização das Nações Unidas (ONU) e a Organização do Tratado do Atlântico Norte (OTAN), dentre outros, estão se preparando diante possíveis consequências de um hipotético "apagão cibernético". Isso faz com que eles estejam conscientes da importância e necessidade de um ciberespaço seguro e das capacidades que devem dispor perante as diversas ameaças e cenários dos riscos cibernéticos.

Existem na atualidade, mais de 81 países no mundo que possuem uma política ou estratégia nacional sobre segurança cibernética⁶³; alguns dos quais estão trabalhando em uma segunda ou terceira versão. No site do Centro de Excelência em Defesa Cibernética Cooperativa (CCDCOE) da OTAN, referenciado como um centro multinacional e interdisciplinar de defesa cibernética. Portanto, foram publicados 229 documentos eletrônicos relacionados com a segurança cibernética de 81 países⁶⁴, observando que o maior número das publicações estão relacionadas diretamente com a Estratégia Nacional em Cibersegurança. Esses documentos foram categorizados em:

- Estratégia de Segurança Nacional.
- Estratégia de Segurança e Defesa Nacional.
- Estratégia Nacional em Cibersegurança.
- Legislação Nacional.
- Declarações sobre direito internacional.

⁶³ Os links incluem estratégias nacionais de segurança e defesa que abordam a cibernética, estratégias nacionais de segurança cibernética, informativa e atos jurídicos. Disponível em <<https://ccdcoe.org/library/strategy-and-governance/>>. Acesso em 12 de maio de 2020. Disponível em <<https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/>>. Acesso em 12 de maio de 2020. Disponível em <<https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies.aspx>>. Acesso em 12 de maio de 2020.

⁶⁴ Maiores detalhes, olha-se o Apêndice VIII – Figura 71.

Também, podemos identificar que dos 229 documentos eletrônicos⁶⁵ disponibilizados pela CCDCOE a maioria deles foram publicados entre os anos 2000 e 2020, só a partir do ano 2011, se observa um incremento dessas publicações. Sem dúvida nos últimos dez anos, a proliferação das capacidades cibernéticas tem sido de especial interesse nos países desenvolvidos. Segundo Antony Craig (2018) de 95 países que foram listados como vítimas pelo Conselho de Relações Exteriores⁶⁶ (*Council on Foreign Relations – CFR*), as unidades militares responsáveis das operações em rede (*Computer Network Operations - CNO*) têm se incrementado notavelmente de 05 a 63 unidades militares de CNO, entre os anos 2000 e 2017.

Observamos também, que dos 81 países analisados pelo CCDCOE, 39 são da Europa, 12 da África, 11 das Américas, 19 da Ásia e Oceania, sendo agrupados pela organização internacional que são membros⁶⁷: *North Atlantic Treaty Organization* (NATO), *Organization for Security and Co-operation in Europe* (OSCE), *European Union* (EU) e *Organization for Economic Co-operation and Development* (OCDE) e da *Council of Europe* (CoE); observando que o maior número de países pertencem à OSCE (incluindo aos Estados Unidos e Canadá) e CoE.

Em 2018, o Fórum Econômico Mundial (FEM) publicou o caderno de resiliência cibernética para a colaboração público-privada⁶⁸. Uma ferramenta destinada a guiar a colaboração público-privada dentro do Estado, no desenvolvimento de políticas de segurança cibernética. Dessa forma, o risco cibernético atingiu degraus, no ranking dos riscos mais prováveis em que as organizações públicas e privadas estariam expostas. Naquele relatório, foram apresentados dez (10) riscos em termos de probabilidade e impacto:

Quadro 5 - Riscos do Fórum Econômico Mundial (FEM) 2017-2018

Risco em termos de probabilidade	Risco em termos de impacto
Eventos climáticos extremos	Armas de destruição em massa
desastres naturais	Eventos climáticos extremos
Ataques cibernéticos	desastres naturais
Fraude ou roubo de dados	Falha na mitigação e adaptação às mudanças climáticas
Falha na mitigação e adaptação às mudanças climáticas	Crises de água
Migração involuntária em larga escala	Ataques cibernéticos
desastres ambientais provocados pelo homem	Crises alimentares
Ataques terroristas	Perda de biodiversidade e ecossistema colapso
Comércio ilícito	Migração involuntária em larga escala

⁶⁵ Maiores detalhes, olha-se o Apêndice VIII – Figura 72.

⁶⁶ Disponível em <<https://www.cfr.org/cyber-operations/>>. Acesso em 06 novembro de 2020. Maiores detalhes, olha-se o Apêndice VIII – Figura 73.

⁶⁷ Maiores detalhes, olha-se o Apêndice VIII – Figura 74.

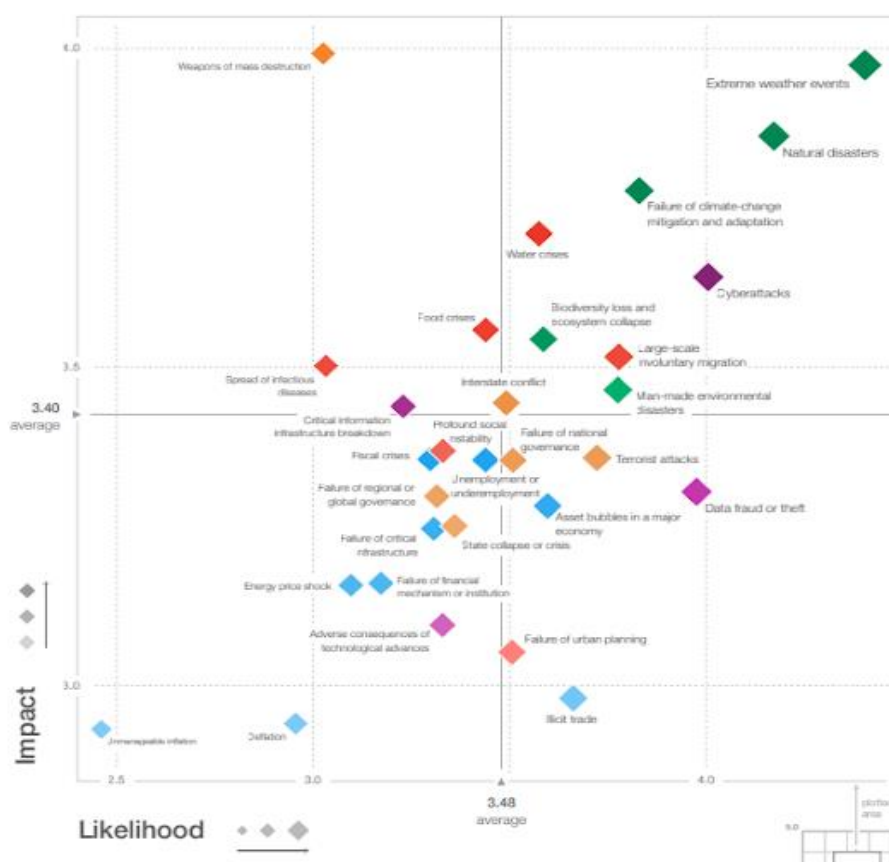
⁶⁸ Disponível em <http://www3.weforum.org/docs/WEF_GRR18_Report.pdf>. Acesso em 12 de maio de 2020.

Bolhas de ativos em uma grande economia	Propagação de doenças infecciosas

Fonte: (http://www3.weforum.org/docs/WEF_GRR18_Report.pdf, elaboração própria).

Sendo agrupados em cinco (05) categorias: Econômico, Ambiental, Geopolítico, Social e Tecnológico. Os riscos de maior criticidade, mantém estreita relação com o ambiental (05 riscos), o social (02 riscos) e o tecnológico (01 risco). Os ataques cibernéticos estão como um dos maiores riscos apresentados pelo FEM:

Figura 6 - Criticidade do risco (Impacto x Probabilidade)



Fonte: (http://www3.weforum.org/docs/WEF_GRR18_Report.pdf).

Na Seção 4.7, do Caderno de resiliência cibernética, em particular, aborda a necessidade de estabelecimento de um marco nacional claro de governança cibernética, que inclua funções, responsabilidades e capacidades dos setores público e privado. O marco de três níveis proposto pelo FEM, tem como objetivo ajudar os governos a designarem responsabilidades e melhorar as funções e responsabilidades específicas com três capacidades em segurança: solidez, resiliência e defesa. Cada uma fortalecendo as demais. A solidez, é definida como a capacidade de prevenir, repelir e conter ameaças. A resiliência, é definida como a capacidade de administrar e solucionar violações bem-sucedidas. A defesa, é definida como a capacidade de

adiantar, interromper e responder a ataques. Este marco está baseado nas iniciativas que datam do Conselho da Agenda Global FEM 2014 sobre Risco e Resiliência e no Livro Branco de 2016, compreendendo o Risco Cibernético Sistêmico. O FEM avançou no diálogo sobre o risco cibernético e fez conexões diretas a impactos econômicos e consequências comerciais da insegurança cibernética (HATHAWAY, 2018).

Temos observado que as potências mundiais contemporâneas têm desenvolvido estratégias interdisciplinares, além do espaço físico. Nas últimas décadas, a correlação de forças e as inúmeras facetas das relações de poder tem gerado uma revalorização dos clássicos estudos geopolíticos.

Já a geopolítica, surgida no início do século XX, tem como preocupação fundamental a questão da correlação de forças - antes vista como militar, mas hoje como econômico-tecnológica, cultural e social – no âmbito territorial, com ênfase no espaço mundial (Vesentini, 2016, p. 10).

Hoje nos países da América do Sul, se vem questionando a guerra militar. Segundo Vesentini (2016, p.11) se tem enfatizado outros tipos de conflitos ou guerras mais do perfil econômico, sociais, culturais e até simbólicos. Teorias trazidas das definições de soberania e defesa dos interesses nacionais de um Estado, onde a "agressão e a insegurança fazem parte da natureza e os conflitos entre Estados" (Vesentini, 2016, p. 65) como algo normal e próprio às relações internacionais, segundo Fukuyama (1989) só aplicariam nos choques ideológicos e de expansionismo, mas com o avanço da tecnologia essas teorias deixariam de estar no contexto da guerra cinética⁶⁹ para se expandir a um contexto de guerra híbrida⁷⁰ e do *soft power*⁷¹. Então, a posição central do Estado como único ator ou agente, na geopolítica contemporânea tem mudado, existindo novos atores e sujeitos, como são as organizações internacionais, empresas multinacionais, blocos de mercados regionais, entre outros.

As novas geopolíticas, não por coincidência surgidas na "era da globalização" e enfraquecimento (relativo) dos Estados nacionais normalmente não são feitas "para o Estado" e tampouco o veem como o único ator na política mundial (Vesentini, 2016, p. 12).

⁶⁹ Se trata das formas tradicionais de um conflito armado, onde as ações militares dependem do impacto físico, explosão e forças mecânicas para a destruição ou neutralização do inimigo.

⁷⁰ Se trata de formas de conflitos que combinam a guerra tradicional ou convencional, a irregular e cibernética, com o uso de estratégias políticas, econômicas, psicologias e informacionais para atingir o objetivo. O confronto neste tipo de guerra não é direta, onde as linhas de ação se tornam difusas.

⁷¹ É um tipo de capacidade que um país ou entidade possui para influenciar e atrair outros sem o uso de força militar ou coerção econômica, mas através de meios não coercitivos, como cultura, valores, ideias, diplomacia e instituições.

Segundo Luttwak (1990), os Estados ou os blocos regionais estão dividindo seu poderio mundial com outros agentes, empresas transnacionais, Internet etc. Por essa razão, falar da geopolítica contemporânea, analogamente seria de uma geoeconomia. Principalmente, porque a competição dos Estados não seria mais a ideológica ou bélica, mas sim a conquista dos mercados e das tecnologias de informação e da comunicação (TIC). Segundo Lester Thurow (1993), “na competição econômica o mundo não está mais dividido em parceiros e inimigos. O jogo será simultaneamente competitivo e cooperativo. É possível ser amigo e aliado e no entanto querer vencer”. Desde essa perspectiva, a crescente interdependência das economias, onde as crises ou expansões tem efeitos sobre os outros, implica “produzir mais e melhores serviços, ampliando a produtividade, o nível tecnológico e educacional, o padrão de consumo da população enfim” (Vesentini, 2016, p. 33).

Segundo Thurow (1993), o capitalismo tem que mudar para sobreviver, o qual implica que os países devem tomar consciência e adotar estratégias adequadas para evitar os perigos do descontentamento gerado pela desigualdade e as injustiças que muitas vezes o mercado tem gerado.

Outro aspecto a considerar, é que nos países sul-americanos tem-se observado diversas iniciativas de mercados regionais, também denominados megablocos, por exemplo: Mercosul, Apec, Alca, entre outros. Existindo a interpretação que os megablocos são os que vem exercendo domínio e poder no cenário mundial, uma vez que, os Estados têm perdido essa autonomia. A União Europeia tem servido de exemplo de integração, desde o ponto de vista geopolítico. Nos países da América do Sul está sendo construída uma interpretação errada, como se todas as formas de associação fossem equivalentes. Deixando de lado a análise das diferenças de criação desses mercados regionais, onde sua coesão é voltada no campo político-diplomática, cuja essência é no âmbito comercial. Por exemplo, no campo dos assuntos políticos e militares não atuam conjuntamente como sujeitos (Vesentini, 2016, p.37).

Ademais, os avanços no processo de globalização relativizam esses mercados pretensamente fechados. Existe sem dúvida uma globalização com regionalização (que lhe é complementar e não oposta), ou seja, a expansão da interdependência econômica não se dá por igual em todas as partes do globo e sim por degraus e etapas, primeiramente- e de forma mais acelerada -entre associados em algum mercado regional, em especial se forem economias desenvolvidas. Esses mercados regionais são na realidade a forma pela qual a globalização avança e não uma nova divisão do mundo

ou o fechamento dos continentes em “blocos” alternativos (Vesentini, 2016, p.37).

A estas como em outros questionamentos para entender o sistema global, a chave seria entender as relações de poder, tendo como fundamento a economia capitalista mundializada. Segundo Soares (2018) a evolução evidenciada entre as teorias clássicas da geopolítica em relação às novas teorias, as divisões deixaram de ser territoriais se tornando às dinâmicas de poder existentes no mundo. Em complemento, Dalio (2022, p. 21-26) ressalta a importância de compreender as relações de causa/efeito que fazem mudar a ascensão ou queda dos impérios, a través de três grandes forças:

- a. O ciclo de endividamento de longo prazo e de mercados de capitais.
- b. O ciclo de ordem e desordem interno.
- c. O ciclo de ordem e desordem externo.

Quadro 6 - Evolução das principais teorias internacionais da geopolíticas

NOVAS TEORIAS DA GEOPOLÍTICA (Após Final da Guerra Fria)			
TEORIA	AUTOR	PREMISSA PRINCIPAL	ANO
Teoria dos blocos	Brochard	Divide o mundo em quatro blocos, englobando Estados dos hemisférios norte e sul, cada um deles liderado preferencialmente por um ou mais Estados que compõem o grupo dos sete grandes (G7)	1991
Teoria dos Limes	Rufin	Com o fim da bipolaridade, os Estados ricos não mais necessitam ajudar os Estados pobres do Sul, como parceiros no contexto mundial, priorizando tratar de seus próprios problemas e de seu desenvolvimento (embate Norte-Sul)	1991
Teoria da Incerteza	Lellouche	A “nova ordem mundial” não seria uma ordem Norte-Sul, tampouco uma ordem, mas uma desordem mundial.	1992
Teoria da Tríade	Clube de Roma	O mundo está dividido em três centros de poder, e por isso não há riscos de conflitos. O mundo se encontra mais “harmônico”.	1961- 1992
Teoria do Choque de Civilizações	Huntington	O mundo é dividido conforme a civilização e por isso os conflitos futuros serão sobre questões étnicas e religiosas, não mais por motivos clássicos.	1993- 1996
Teoria do Quaternio	Mafrá	O mundo em quatro blocos: Bloco Norte Americano, Bloco Sul-Americano, Bloco Europeu, Bloco Asiático.	1996

Fonte: (Soares, 2018, p.150).

Daí a nova postura da geopolítica contemporânea, em relação à clássica, de aprofundar seus estudos nos âmbitos da dominação e competição econômica. Em um mundo globalizado, onde vem surgindo a expansão de problemas comuns entre os Estados, levando de fato a perda relativa das soberanias nacionais. Nesse sentido, surgem as potências hegemônicas que vão comandar as mudanças e a lógica do sistema global.

3.7 O ciberespaço, é um *Global Common*?

Um grupo de especialistas tem categorizado o ciberespaço como um *Global Commons*. “Um *Global Commons*, pode incluir espaços além das jurisdições nacionais, essenciais recursos e preocupações como a conservação da biodiversidade e mudanças climáticas que são o foco do interesse internacional desde a perspectiva da governança” (Ranganathan, 2016, p.693, tradução nossa). Ela nos apresenta em seu artigo dois conceitos, que nos aproximam na compreensão dos *Global Commons*. Um primeiro conceito, delineado pelo Garrett Hardin (1968), onde os recursos comuns são super explorados pela ausência de uma regulamentação, enquanto as preocupações comuns permanecem sem solução (*Tragedy of the Commons* – TOC). O outro, pelo Arvid Pardo (1967)⁷² quem reflete em que alguns recursos pertencem à humanidade, incluídas às gerações futuras, portanto, existe a responsabilidade e o direito de conservação desses recursos (*Common Heritage of Mankind* – CHM). Apesar de ambos os conceitos apresentam certas diferenças, porém eles apontam para a tensão entre a partilha e a preservação dos recursos.

Segundo Ranganathan (2016, p.715, tradução nossa) ambos os autores, tiveram dimensões não liberais e imperiais. O primeiro conceito, busca trazer um sistema de regime de licenciamento centralizado, onde a governança do acesso e do uso é através dos países tecnologicamente avançados, em nome dos demais. Assim, os Estados deveriam renunciar a suas reivindicações continentais de extensão, o qual possibilitava a apropriação e militarização dos Estados tecnologicamente desenvolvidos, solicitando que o benefício das explorações deveria fluir para os Estados em vias de desenvolvimento, deixando esse direito nas mãos dos primeiros, defendendo sua posição, para criar uma agência especial liderada pelos Estados tecnologicamente desenvolvidos. No entanto Hardin, defende não só nas restrições à atividade econômica na área internacional, bem como uma política externa intervencionista rejeitando as escolhas reprodutivas dos países em vias de desenvolvimento, revestido em pressupostos com preocupações ecologistas. Essa integração desenvolvida de combinar fatos e teorias selecionadas de várias disciplinas para o desenvolvimento imaginário dos comuns, enfatizando-os em “teorias baseadas em tecnologia e racionalidade como uma estrutura da qual compreender as questões sociais e econômicas” (Ranganathan, 2016, p.715-716, tradução nossa).

⁷²UN General Assembly (UNGA), *First Committee Debate*, UN Docs A/C.1/PV.1515–1516, 1 November 1967.

Segundo Casar (2012, p.21), “estamos testemunhando uma espécie de “afegunização” do ciberespaço, com bolhas de segurança e insurgência”.

Há espaços sem governo onde os Estados cederam a soberania, voluntária ou involuntariamente, razoavelmente ou não, no todo ou em parte, a outras autoridades. Se entendermos que os espaços não governados são aqueles em que o poder do Estado está ausente, fraco ou contestado, então - além de nos referirmos a territórios de poder tribal ou insurgência persistente, devemos estender essa perspectiva aos domínios da Internet ou aos mercados onde agentes econômicos operam com regulação pública insuficiente (Innerarity, 2011).

As operações militares cibernéticas expõem certos desafios ao direito internacional no âmbito do uso da força, em dois aspectos especialmente: soberania-jurisdição e atribuição-responsabilidade. Apesar das características compartilhadas pelos diferentes espaços comuns, não existe até o dia de hoje nenhum normativo uniforme que regule o acesso e uso deles.

O melhor exemplo desses debates foi na apresentação do projeto do Código Internacional de Conduta para a segurança da informação por parte da China, Rússia, Kazajstão, Quirguistão e Uzbequistão na Organização das Nações Unidas (ONU A/69/723), projeto que reconhece que os Estados estariam obrigados a cumprir com as normas da Carta das Nações Unidas, não se reconhecendo os entendimentos obtidos pelos Grupos de especialistas Governamentais, que refere-se à aplicabilidade das normas do direito internacional do ciberespaço. Desse modo, a posição destes Estados não é clara nesta matéria e tem uma posição oposta dos outros Estados (Estados Unidos da Norte América, Austrália) que se mostram favoráveis à aplicação das normas do “*ius ad bellum*” e das normas do “*ius in bello*” no contexto do ciberespaço. Sobre esse assunto ademais de ter consultado o relatório do segundo Grupo de especialistas Governamentais (A/68/98) pode-se olhar o trabalho feito pelo Eichendehr, K., op. cit., nota 13, pp.361-366, quem desenvolve em extenso esta questão (Llorens, 2016, p.791).

Segundo Alexander Kutt (2015) a hegemonia dos Estados Unidos, se materializou traz a Guerra Fria em seu poder militar, chegando ao ponto mais álgido com a presidência de Bush, mas esta hegemonia é refletida, também, nos espaços comuns: mar, ar, espaço exterior e ciberespaço. Segundo Rattray (2009, p.259, tradução nossa) “a teoria do poder marítimo trata explicitamente de como controlar o entorno permitindo as manobras globais e o impacto da mudança tecnológica”, sendo de importância a compreensão do exercício dos mecanismos de dominação e poder sobre os *Global Commons*, neste século XXI. O posicionamento, de uma parte do direito internacional sobre os *Global Commons*, é que são definidos como o espaço que não é parte concreta de um Estado e nenhum Estado pode exercer direitos soberanos. Sem embargo, pelo que foi descrito até o momento nesta tese, podemos

afirmar que os elementos que estruturam a construção do ciberespaço estão financiados por empresas multinacionais, governos com hegemonia político-tecnológica e grupos de poder. Aliás, nos há permitido ter uma observação menos ingênua, em comparação com os outros *Global Commons* que tem uma origem evolutiva e de mundo natural. O Ciberespaço é artificial e nasce com um interesse de dominação e de poder, que nos próximos parágrafos iremos descrever e justificar.

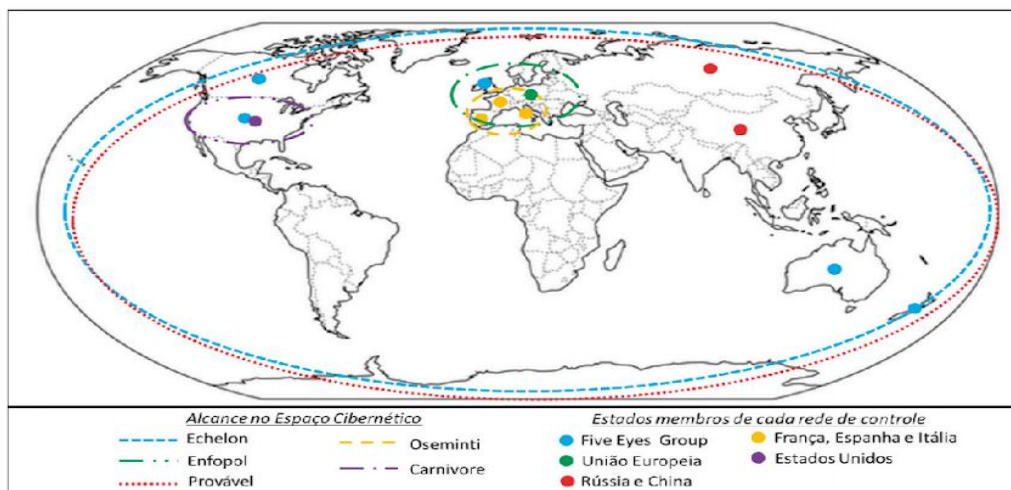
Segundo Soares (2018, p.155) “o espaço cibernético surge de uma criação dos Estados Unidos, sediando as principais empresas detentoras do domínio e abrangência desse ambiente”.

com a vitória sobre os soviéticos e a primazia informacional e ideológica da aldeia global, o governo norte-americano conseguiu edificar o modelo neoliberal vigente na atualidade, a partir da década de 1990, mediante o consenso de Washington e a submissão dos demais países ao modelo do livre mercado (Brito, 2011, p.183).

Assim, a existência de um controle público e por empresas, principalmente norte-americanas têm gerado no cenário internacional contrapontos por outros atores internacionais. A existência de iniciativas no âmbito cibernético para o controle e observação por meio do emprego das redes, estão vinculados com Estados que dispõem das capacidades e do potencial cibernético:

- Echelon: Five Eyes Group, liderados por Estados Unidos (NSA) e Reino Unido;
- Enfopol: União Europeia;
- Oseminti: França, Espanha e Itália;
- Carnivore: Estados Unidos (FBI);
- Rússia e China.

Figura 7 - Principais sistemas de controle e observação do espaço cibernético.



Fonte: (Soares, 2018, p.158).

Assim inferimos, que a hegemonia política-tecnológica e do poder informacional norte-americano permeia diversos setores da sociedade da informação e do conhecimento, estando vinculados aos interesses estratégicos de segurança nacional (Brito, 2011, p. 192).

Atualmente, o maior sistema de inteligência entre as nações é o norte-americano (CEPIK, 2003). Com um grande aparato na área, possuem diversas organizações voltadas para as distintas disciplinas de coleta de inteligência, tendo também organizações especializadas na centralização das informações obtidas e na produção analítica tática, além da confecção das estimativas nacionais. Como única superpotência restante dos enfrentamentos da Guerra Fria, os EUA empregam seus amplos recursos informacionais com poucos rivais, recebendo conhecimento para dar suporte a diversas ações, políticas e militares, dentro de seu contexto de hegemonia global (Brito, 2011, p.126).

Embora, a ideia de querer tratar o ciberespaço como um Global common sustentado no apelo filosófico e moral, não seria suficiente. Porque não abrange realidades políticas, econômicas e tecnológicas estando entre as principais críticas do pesquisador, os seguintes pressupostos:

- O procentaje da administração do ciberespaço é de natureza privada e comercial na sua infraestrutura física da Internet, por exemplo: o cabeamento submarino , servidores e data centers.
- As principais potencias mundiais têm evidenciado uma extensão de sua soberania nacional através do ciberespaço, possuindo controle estatal, ao ponto de restringir e monitorar a Internet.
- A ausência de uma representatividade global, que não esteja influenciada pelos países do Ocidente, conseqüentemente, a inexistência de um quadro jurídico global para governança do ciberespaço e de acordos que normem o comportamento no ciberespaço, respeito às guerras cibernéticas e de proteção às infraestruturas críticas.
- A influência das Big Tech ou grandes *players* tecnologicos, escencialmente, na arquitetura e funcionalidade do ciberespaço, devido a seus interesses comerciais e de regulamentação internacional.

Portanto, buscar uma explicação, que é o ciberespaço? ou ter uma posição etimológica, não é nosso objetivo na tese, mas buscamos analisar como os encarregados das políticas de segurança cibernética dependem da historicidade, perspectiva teórica, contexto e compreensão dos interesses geopolíticos e econômicos. Além disso, a forma como os países vão estabelecendo seus

mecanismos de controle e poder no domínio cibernético e informacional. Portanto, nossa perspectiva e análise do ciberespaço nesta tese, nos situa distante da compreensão do ciberespaço como um *Global Common*⁷³. Esta pesquisa orienta brindar uma visão distinta do ciberespaço desde a perspectiva da hegemonia político-tecnológica, da dominação e controle do capitalismo informacional.

3.8 Os elementos estruturais para a construção do ciberespaço

Segundo Zimet e Skoudis (2009, p.91, tradução nossa), o ciberespaço se constitui em quatro (04) domínios: domínio de sistemas, domínio de conteúdo e aplicações, domínio de pessoas e social, e domínio de governança. Sendo este último aquele que envolve os outros domínios. Em relação aos elementos de construção do ciberespaço, esta tese toma como base conceptual, o afirmado por Zimet e Skoudis, buscando propor os componentes para a constituição e materialização do ciberespaço. Portanto, além de sua natureza artificial, o ciberespaço, possui as seguintes componentes:

1. Infraestrutura.
2. Dados, informação e conhecimento.
3. Automação e inteligência.
4. Conectividade global e controle.

3.8.1 O ciberespaço, elementos de construção: infraestrutura

O Uptime Institute⁷⁴ é uma organização norte-americana, conhecida por seu padrão mundial chamado “*TIER*”, que é o padrão global mais confiável e adotado no setor das Tecnologias da Informação e da Comunicação para o design, construção e operação correta dos *Data Centers*⁷⁵. Partindo dos dados públicos brindados pelo *Uptime Institute Tier Certification (dados avaliados até o dia 18 de maio de 2019)* são 743 data centers espalhados pelo mundo que foram certificados em *Tier IV, III e II*.

⁷³ Se conhece como *Global Common*, aqueles entornos em que nenhuma pessoa ou Estado pode ter sua propriedade o controle que são básicos para a vida. Um *Global Common*, contém um potencial infinito no referente ao conhecimento e avanço da biologia e da sociedade. Incluindo os mares, o ar, o espaço e o ciberespaço. Disponível em <www.twq.com/10july/docs/10jul_Denmark.pdf> («*Managing The Global Commons*», por Abraham M. Denmark). Acesso 30 julho de 2020.

⁷⁴ Disponível em: <<https://uptimeinstitute.com/>>. Acesso em 21 abril de 2020.

⁷⁵ Os *data centers* são ambientes criados para concentrar todo tipo de software (sistemas e serviços de informação públicos ou privados, sites, blogs, redes sociais digitais, foros, base de dados etc.), hardware (servidores, *appliances* de segurança e de *backups* etc.) e networking (sistemas de ativos de rede, switches, roteadores etc.) em condições padrão e critérios altamente técnicos. Pelo que podemos dizer que os *data centers* são os espaços fundamentais para os serviços e atividades de diversos setores da economia: energia, iluminação, telecomunicações, Internet, transportes, tráfego urbano, bancos, sistemas de segurança, saúde pública, entretenimento, e muitos outros. A vida na maioria das cidades depende do bom funcionamento e da disponibilidade de um ou vários *Data Centers*.

Sendo os *Data Centers*, aquelas infraestruturas que constituem a espinha dorsal da economia digital. Considerando que muitas das infraestruturas tecnológicas que brindam o suporte para a criação do ciberespaço e a Internet são os *Data Centers*. Vem existindo a preocupação pelos países mais desenvolvidos de categorizá-los como Infraestruturas Críticas (IC) de interesse nacional. Por exemplo, no governo do presidente norte-americano Obama, foi aprovada a "Diretiva de Política Presidencial (PDD)-21: Segurança da infraestrutura crítica em substituição da Diretriz Presidencial de Segurança Interna 7, onde é dirigido ao ramo executivo do governo dos Estados Unidos para tomar medidas nas infraestruturas críticas". De fato, devemos assumir que nos dados públicos brindados pelo *Uptime Institute*, não estariam relatados os *Data Centers* de interesse para a defesa e segurança nacional dos países. Portanto, nos permite ter uma ideia da infraestrutura mundial, disponível na atualidade. No caso dos países pobres ou menos desenvolvidos, eles vêm fazendo uso de aquelas infraestruturas para a implementação das políticas e programas públicos relacionados ao governo digital, à proteção de dados de seus cidadãos, transparência, cidades digitais e outros.

Figura 8 - Mapeamento mundial dos *Data Centers* certificados TIER



Fonte: (Uptime Institute Tier Certification Map⁷⁶, 2019).

Dos dados da TIER, podemos concluir que a maior infraestrutura de *Data Centers* certificados no mundo estão nos continentes povoados de Ásia e América⁷⁷, sendo um 76.72% dos *Data Centers* existentes no mundo. Devemos ter presente, que os dados extraídos de nossa fonte em menção, o País de Austrália é o único País de Oceania certificado com *TIER*. Ademais, afirmamos que os Estados Unidos e Canada

⁷⁶ Disponível em: <<https://uptimeinstitute.com/TierCertification/certMaps.php>>. Acesso em 2019 abr. 21.

⁷⁷ Maiores detalhes, olha-se o Apêndice IX – Tabela 7.

possuem um 47.37% dos *data centers* certificados com TIER, na América⁷⁸. Ademais, ao considerar os dois países com maior PIB (Produto Interno Bruto) por cada continente povoado (em Oceania, estamos considerando a Austrália) fariam estes 7 países (EUA, Canadá, África do Sul, Egito, Luxemburgo, Suíça, Qatar, Singapura e Austrália) um 26.78% dos *Data Centers* certificados com TIER no mundo. Também, encontramos que os 8 países com economias mais industrializadas constituem um 26.38% dos *Data Centers* no mundo. Destacando os Estados Unidos de Norte América com uma quantidade de 93 *Data Centers* certificados com TIER, possuindo quase a metade dos outros 7 países do G-8⁷⁹. Finalmente, observamos que os países da América do Norte (Canadá, Estados Unidos de Norte América e México) somam um 53.01% do total de *Data Centers* existentes em todo o continente americano⁸⁰, e junto com os países de Colômbia, Chile, Argentina, Peru e Brasil fariam um 84.21% dos *data centers* existentes em toda América.

Sempre falamos de rede de caminhos, rede de trens, rede de telefonia, rede elétrica e rede da Internet. Por conseguinte, podemos deduzir que a infraestrutura frequentemente depende da rede. Uma rede consiste nos pontos de abastecimento ou origem, nas rotas de transporte ou movimento e nos pontos de destino ou consumo.

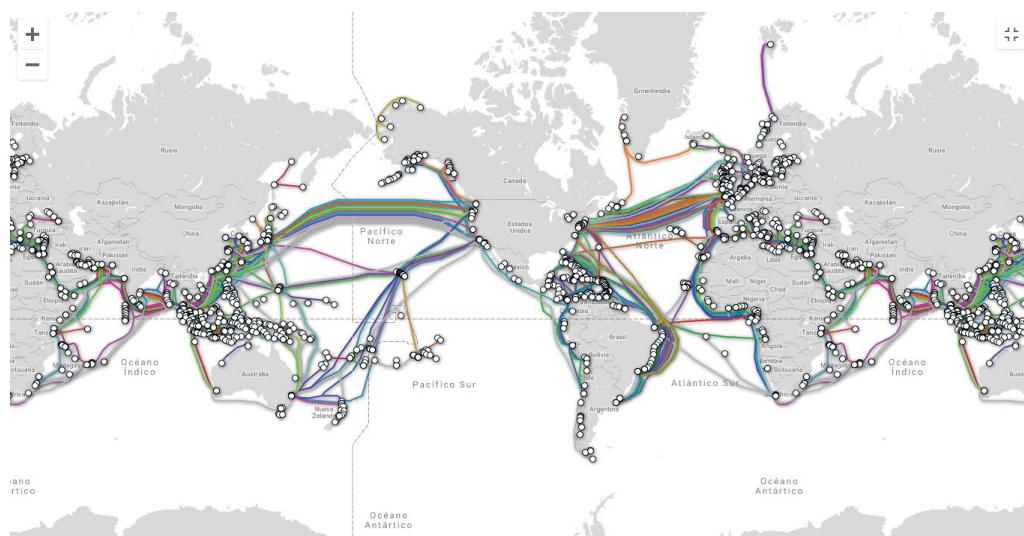
Outras das redes que são de importância na criação da Internet e o ciberespaço é a rede de cabos submarinos de fibra óptica. Segundo a TeleGeography Inc., a partir de 2019, existem mais de 1,2 milhões de quilômetros de cabos submarinos em serviço globalmente. Alguns cabos são bastante curtos, como o cabo CeltixConnect de 131 quilômetros entre a Irlanda e o Reino Unido. Em contraste, outros são incrivelmente longos, como o cabo Ásia América Gateway de 20.000 quilômetros. Aquela conectividade física é possível pelos cabos submarinos modernos que fazem uso da tecnologia de fibra óptica. Basicamente, seu funcionamento se baseia nos lasers, de uma extremidade disparam a velocidades extremamente rápidas em fibras de vidro finas para receptores na outra extremidade do cabo. Estas fibras de vidro são envoltas em camadas de plástico e às vezes fio de aço, para sua proteção. Na Figura 18, observa-se a infraestrutura de cabeamento de fibra óptica mundial que está conectado aos países, sendo em muitos dos casos os *Data Centers* os nós da grande rede denominada Internet.

⁷⁸ Maiores detalhes, olha-se o Apêndice IX – Tabela 8.

⁷⁹ Maiores detalhes, olha-se o Apêndice IX – Figura 9.

⁸⁰ Maiores detalhes, olha-se o Apêndice IX – Figura 10

Figura 9 - Mapeamento do cabeamento de fibra óptica da Internet mundial.



Fonte: TeleGeography⁸¹. Disponível em <<https://www.submarinecablemap.com/>>.

Acesso em 28 abril de 2019.

Os cabos de fibra óptica são colocados diretamente no fundo do oceano, mais perto aos cabos da costa, estão enterrados sob o leito marinho para sua proteção. É claro, que são tomados os cuidados para garantir que os cabos sigam o caminho mais seguro para evitar zonas de falha, zonas de pesca, áreas de ancoragem e outros perigos. Para reduzir danos inadvertidos, a indústria de cabos submarinos, passa muito tempo educando às indústrias navais, sobre a localização dos cabos.

Analisando⁸² o mapeamento de cabeamento de fibra óptica que permite amplamente que o ciberespaço e a Internet mundial funcionar, pode-se observar que não há cabos entre: Rússia e Canadá, Rússia e EUA, Austrália e África, Austrália e América do Sul, Japão e América, China e América. Em resposta a nosso questionamento, TeleGeography Inc., em seu site oficialmente comentou:

Para responder a isso, damos início com a citação de Henry David Thoreau: "Nossas invenções costumam ser lindos brinquedos, que desviam nossa atenção das coisas sérias. Eles são apenas meios aperfeiçoados para um fim não melhorado. Temos muita pressa para construir um telégrafo magnético do Maine ao Texas; mas Maine e Texas, pode ser, não têm nada importante para se comunicar".

Os cabos submarinos são construídos entre locais que têm algo "importante para se comunicar".

A Europa, a Ásia e a América Latina possuem grandes quantidades de dados para enviar e receber da América do Norte. Isso inclui as operadoras de *backbone* da Internet, que garantem a conexão de e-mails e ligações telefônicas, além de fornecedores de conteúdo que precisam vincular seus

⁸¹ A TeleGeography, Inc. fornece serviços de consultoria e pesquisa de mercado de telecomunicações. Oferece serviços de pesquisa nas áreas de redes de telecomunicações e infraestrutura, serviços de Internet, preços de serviços de telecomunicações, redes corporativas e voz internacional, bem como serviços móveis, de banda larga e serviços de telefonia fixa. A empresa foi fundada em 1993 e está localizada em Washington, *District Of Columbia*, com escritórios adicionais em San Diego, Califórnia; Exeter, Reino Unido; e Cingapura. Em 10 de junho de 2003, a TeleGeography, Inc. opera como subsidiária da PriMetrica, Inc.

⁸² Segundo os dados consultados no ano 2019.

centros de dados massivos entre si. Isso explica por que você vê tantos cabos ao longo dessas rotas principais.

Por outro lado, não há muitos dados que precisam ir diretamente entre a Austrália e a América do Sul. Se essa situação mudasse, você poderia ter certeza de que alguém construiria um novo cabo no Pacífico Sul (TeleGeography, c2024, Tradução nossa, [Acesso em 2019 abr. 28]).

Em virtude do manifestado pela TeleGeography Inc., foram gerados mais interrogantes, como são: De que “coisas sérias” estamos falando? Se fala de um fim não melhorado, qual é a finalidade das invenções? Que seria um “algo importante para se comunicar”, África não tem esse “algo importante”? e Como é que se definem ou determinam que países vão a recepcionar e receber as grandes quantidades de dados?. São alguns dos questionamentos que nós poderíamos fazer, sendo de motivação para nossa pesquisa, esperando trazer as respostas nos seguintes capítulos.

Visto que, segundo a informação pública do site da TeleGeography Inc., se sabe que a construção dos cabos de fibra óptica submarinas, recebe investimento das grandes corporações norte-americanas privadas, como: Google, Facebook, Microsoft e Amazon; empresas que fazem o tratamento dos dados pessoais e conteúdo em grande escala mundial. Em razão, se observa uma tendência à monopolização dos serviços que constituem o Internet na América Latina, com capital privado norte-americano:

Eram tradicionalmente propriedade de operadoras de telecomunicações que formariam um consórcio de todas as partes interessadas em usar o cabo. No final dos anos 90 do século XX, um influxo de empresas empreendedoras construiu muitos cabos privados e vendeu a capacidade para os usuários. Os modelos de consórcio e cabo privado ainda existem hoje, mas uma das maiores mudanças nos últimos anos é o tipo de empresas envolvidas na construção de cabos. Provedores de conteúdo como Google, Facebook, Microsoft e Amazon são grandes investidores em novos cabos. A quantidade de capacidade implantada por operadores de redes privadas - como esses provedores de conteúdo - ultrapassou os operadores do *backbone* da Internet nos últimos anos. Diante da perspectiva de crescimento maciço de largura de banda, a propriedade de novos cabos submarinos faz sentido para essas empresas (TeleGeography, c2024, Tradução nossa, [Acesso em 2019 abr. 28]).

William D. O'Neil, em seu artigo: “ciberespaço e infraestrutura”, diz o seguinte:

Uma ampla variedade de sistemas físicos, biológicos e sociais feitos pelo homem e naturais pode ser analisada em termos de rede. Cada infraestrutura é fisicamente distinta, mas, como a terminologia sugere, elas compartilham algo importante no nível da estrutura abstrata.

Embora, as redes de infraestrutura não sejam verdadeiramente aleatórias, elas são complexas e irregulares. Como resultado, muitas das ferramentas aplicáveis da teoria de redes são de natureza estatística. Redes grandes e

irregulares, como a maioria das infraestruturas, podem ser vistas em duas grandes classes. Em um tipo, a maioria de nós tem aproximadamente o mesmo número de links. Apenas alguns nós possuem muitos links. Redes com este tipo de estrutura igualitária são frequentemente chamadas redes exponenciais (*exponential networks* - porque os nós altamente conectados são exponencialmente improváveis) ou, mais descritivamente, redes aleatórias uniformes (*uniform-random-networks*).

Na outra classe principal, a maioria dos nós está conectada a nós que também já possuem muitas conexões (embora ainda exista um elemento aleatório) estas são chamadas de redes de lei do poder (*Power-law-networks* - por razões matemáticas técnicas refletem a abundância relativa de nós altamente conectados) ou, mais comumente, redes livres de escala (*Scale-free-networks*), uma referência à sua falta de uma escala típica ou média dominante no sentido de número de conexões por nó. Um termo mais descritivo pode ser *hub-and-spoke random network*. (Kramer, Starr, Wentz, 2009, p.115, tradução nossa).

Portanto, a natureza física e de localização espacial dos elementos que criam o ciberespaço devem ser de relevância em nossa análise. A infraestrutura não é somente redes, mas também redes sobre redes. Por exemplo: a rede de telefonia, rede elétrica, a rede de fibra óptica submarina etc. Consequentemente, a rede elétrica é fundamental para a existência do ciberespaço e da Internet. Nenhum modelo simples pode captar totalmente a complexidade dessas estruturas, mas em termos gerais, o Ciberespaço e a Internet são:

- a. *Power-law-networks*⁸³, frequentemente usadas para modelar uma ampla gama de redes do mundo real, como redes sociais, redes tecnológicas e redes biológicas (Faloutsos *et al.*, 1999).
- b. *E Scale-free-networks*⁸⁴, que exibem uma robustez incrível contra falhas acidentais, uma propriedade que está enraizada em sua topologia não homogênea (Barabási, Bonabeau, 2003).

Segundo William D. O'Neill, o conteúdo cibernético repousa sobre uma estrutura de elementos físicos que possuem propriedades físicas e locais. Embora sua topologia não seja idêntica à das camadas de rede em que é construída, o próprio ciberespaço, como outras redes de infraestrutura, tem uma geografia e uma topologia, assim ambas afetam sua capacidade de sobrevivência e a tornam vulnerável.

⁸³ Disponível em < <http://snap.stanford.edu/class/cs224w-readings/faloutsos99powerlaw.pdf>>. Acesso em 04 nov. de 2020.

⁸⁴ Disponível em < <https://barabasi.com/f/124.pdf>>. Acesso em 04 nov. de 2020.

Quadro 7 - Esquema da visão global dos níveis envolvidos no ciberespaço

Nível	Descrição	Exemplo
Ciber	Conteúdo intelectual.	Data, comandos, conhecimento, ideias, modelos mentais.
Rede lógica	Serviços que empregam sinais físicos para transportar mensagens lógicas.	Telefones, serviços de transmissão de rádio e TV, serviço de TV a cabo, internet pública, redes baseadas em IP (<i>Internet Private Protocol</i>) transportadas em infraestrutura de operadora comum, redes baseadas em IP de infraestrutura privada, controle supervisão e redes de aquisição de dados.
Rede dura	Infraestrutura formada a partir de elementos de base que transportam sinais elétricos ou eletromagnéticos	Redes de telecomunicações de operadoras comuns, sistemas de rádio tácticos, sistemas dedicados de telefonia fixa, sistemas de cabo comunitários, sistemas de telefones celulares.
Base	Elementos físicos que fundamentam os serviços de telecomunicações.	<i>Headworks</i> de cabo, fibra óptica, cabo coaxial, transmissores e receptores de rádio, caminhos de transmissão de rádio, satélites de comunicações, roteadores de internet, modems.

Fonte: (Kramer, Starr, Wentz, 2009, p. 118, tradução nossa).

O desenvolvimento das TIC deu origem à digitalização das organizações estabelecendo uma ponte com a sociedade da informação. As TIC têm um papel muito importante nos processos dos fluxos informacionais que diminuem ou aumentam os problemas da assimetria da informação. Os avanços relativos às infraestruturas da informação estão sendo determinados pela capacidade de proporcionar o acesso imediato à informação. Para Castells (1999), o Estado-rede é caracterizado pela redistribuição de competências e recursos entre organizações governamentais e não governamentais de onde são exercidos os processos contemporâneos de ação e decisão. Por tanto, a infraestrutura em suas diversas modalidades de complexidade e extensão, fornece os meios para manter ativas relações entre agentes e instituições. A qual pode ser discutida no conjunto dos recursos, instalações e dos meios, como no conjunto das relações da produção e economia. Um entendimento, não longe do relatado é da González de Gómez (2002) que define a infraestrutura de informação como comunicacional e produtiva, “nela acontecem tanto a transmissão como a geração de valor”. Para a pesquisadora, as relações entre política e informação são reconstruídas através de “novas formas de infraestruturas de informação e da sociedade da informação”.

Zurkowski e Porat, nestes textos, põem de manifesto duas tendências que se dissociariam com o andar do tempo: uma indicando a crescente autonomia e importância econômica, política e social dos fenômenos de comunicação e informação que, a partir dos novos modelos econômicos e tecnológicos, ganham uma dimensão estrutural e estruturante das atividades sociais; outra sustentando a constituição de um setor diferenciado das atividades, da indústria e dos mercados de informação, considerados como “o quarto setor”, diferenciado do setor dos serviços (González de Gómez, 2002, p.30).

Temos observado que governos e organismos internacionais, coincidem nos benefícios das iniciativas em infraestrutura das TIC as quais irão oferecer desenvolvimento econômico e social dos países. Esses benefícios são possíveis através da Internet, na criação de espaços comunicativos da política a uma maior quantidade de atores e setores, estando garantida a relação estrutural da informação com a tecnologia e a economia.

O caráter decisional inscrito nas políticas de informação seria recuperado em meados da década do 90, mas circunscrito agora aos programas de institucionalização da Internet e da universalização do acesso a suas aplicações e serviços (González de Gómez, 2002, p.31).

3.8.2 O ciberespaço, elementos de construção: dados, informação e conhecimento

Outros dos elementos essenciais, para a construção do ciberespaço, temos os dados, a informação e o conhecimento. Hoje em dia, em um cabo de fibra óptica submarina podemos transportar na velocidade da luz, um número inimaginável de dados. Por exemplo: o novo cabo submarino batizado com MAREA, construído pela Microsoft e Facebook, é capaz de transportar 208 Tbps. As capacidades dos cabos variam muito, normalmente, os cabos mais novos são capazes de transportar mais dados do que os cabos colocados há 15 anos.

Segundo a empresa TeleGeography Inc., existem duas maneiras principais de medir a capacidade de um cabo de fibra óptica submarina:

1. A capacidade potencial, é a quantidade total de capacidade que seria possível se o proprietário do cabo instalasse todos os equipamentos disponíveis nas extremidades do cabo. Essa é a métrica mais citada na imprensa.
2. A capacidade de iluminação é a quantidade de capacidade que está sendo executada em um cabo. Essa figura simplesmente fornece outra métrica de capacidade. Os proprietários de cabos raramente compram e instalam o equipamento de transmissão para realizar o potencial de um cabo desde o primeiro dia. Como esse equipamento é caro, os proprietários preferem atualizar seu cabo gradualmente, conforme a demanda do cliente exigir (TeleGeography, c2024, Tradução nossa, [Acesso em 2019 abr. 28]).

As ameaças cibernéticas têm sua origem desde a própria criação do ciberespaço. Ao comentar, hoje em dia, que as ameaças cibernéticas surgiram no presente século XXI, estaríamos criando uma falsa perspectiva e expectativa para seu tratamento. Devemos ter em consideração que a ARPANET⁸⁵, projeto que deu impulso à Internet, foi criado a meados do século XX, depois da “Segunda Guerra

⁸⁵ The Advanced Research Projects Agency Network (ARPANET), projeto financiado pelo Departamento da Defesa do Estados Unidos (DoD); foi uma rede de comutação de pacotes e a primeira rede a implementar o conjunto de protocolos TCP/IP, sendo ambas tecnologias as que posteriormente estabeleceram a base da Internet.

Mundial” e entre o período da chamada “Guerra Fria”, onde se tinham como atores principais, aos países dos Estados Unidos e a União das Repúblicas Socialistas Soviéticas (URSS). Ademais, é neste período, que se dão os inícios da Ciência da Informação e que segundo Santos Júnior (2012, p.130):

Outro fator, de consequência mais notável para o surgimento da Ciência da Informação, foi a produção maciça de documentos e o rápido e vertiginoso desenvolvimento de serviços de acumulação e armazenamento de informação, onde pesquisadores e cientistas das mais variadas áreas de estudo repensaram suas práticas de produção e gestão informacional.

Em 1964, a *Science Information* é dissociada de seu conceito, seja no contexto da atividade da informação científica ou na teoria da informação científica. Em 1966, com a publicação dos autores soviéticos Mikhailov, Chernyi e Gilyarevskii se busca encontrar um novo nome da teoria da informação científica dando origem à *informatika*.

Aparecem como objetos de estudo da nova disciplina a atividade da informação científica em todos seus aspectos e os instrumentos de tratamento da informação. Ao mesmo tempo mantém relações interdisciplinares com a Cibernética, a Eletrônica, a Engenharia, a Biblioteconomia e a Lógica e a Linguística Matemática (López Yepes, 1995, p.219, tradução nossa)

Segundo López Yepes (1995), a *informatika* estuda a estrutura e as propriedades da informação científica, não o conteúdo específico. Ela terá sua origem em duas causas: 1) As leis internas do desenvolvimento da própria ciência, e 2) As necessidades da atividade social (López Yepes, 1995, p.222). Também, irá estudar as leis da atividade científica-informativa, teorias, história, metodologia e meios ótimos de apresentação ou registros, recollecção, processamento analítico-sintético, armazenamento, busca e disseminação da informação científica (López Yepes, 1995, p.225, tradução nossa).

Como consequência do exposto, e continuando o dito pelos autores russos, devem ser considerados como fatores de crescimento da ciência, e por consequente de sua bibliografia, as seguintes:

A acumulação ininterrupta de conhecimento científico determina a sucessão e o caráter internacional das ciências.

A diferença e especialização mais profundas e o aumento da produtividade do trabalho científico a que daí lugar.

A intensificação da influência recíproco das ciências.

O regime econômico, político e social que ele pode contribuir ao progresso da ciência que pare com isso.

A aceleração do desenvolvimento das ciências produtivas da sociedade.

O aperfeiçoar dos meios de comunicação.

O incremento dos meios invertidos nas investigações científicas.

O aumento da quantidade de pessoas dedicadas às pesquisas científicas (López Yepes, 1995, p.222, tradução nossa).

Podemos dizer que o tratamento da informação é a principal característica que contribuiu no desenvolvimento e dependência do ciberespaço. Na sociedade informacional, a premissa é que “a informação por si só tem um valor capaz de gerar poder político, econômico e social. Quanto maior seja a eficiência com que é administrada e tratada, maiores serão os benefícios” (Bejarano, 2011, p.52. tradução nossa).

Estamos vivendo em um paradoxo: onde a conquista das idades industriais e da informação estão moldando um mundo futuro que será tanto mais incerto quanto mais rico de oportunidades do que nunca. Uma gama cada vez maior de Estados, organizações e indivíduos capacitados moldará a geopolítica (Nasser, 2019, p.29).

Embora a força material permaneça essencial, para Nasser (2019, p.30), ao garantir o poder geopolítico e estatal, os atores mais poderosos do futuro se baseiam em redes, relacionamentos e informações para competir e cooperar. Em outubro de 2009, o presidente norte-americano Barack Obama, declarou como o mês de conscientização nacional para o desenvolvimento das competências em informação (*National Information Literacy Awareness Month*). Incentivando um conjunto de aptidões em informação frente aos desafios informacionais da atualidade. Em seu discurso, Obama (2009) nos diz que os Americanos estão sendo “inundados” todos os dias por uma vasta quantidade de informações. Às 24 horas por dia pelos meios de imprensa, milhares de redes televisivas e de rádio, somando-se a imensa coleção de fontes da Internet, e que têm desafiado o modo como as informações estão sendo gerenciadas.

Na inteligência de Obama (2009), mais do que a mera posse de dados, necessita-se de novas habilidades para adquirir, coletar e avaliar informações para situações diversas, convergindo para um novo tipo de alfabetização (*Literacy*), as competências em informação (*Information Literacy*), um conjunto de habilidades informacionais, incluindo competências nas tecnologias da comunicação, tais como o uso de computadores e dispositivos móveis que auxiliam o processo diário de tomadas de decisões (Serafim, Freire, 2013, pp, 75).

Segundo o argumentado pelo Lojkin (1999) “a revolução informacional não se limita à estocagem e à circulação de informações codificadas sistematicamente pelos programas de computador ou difundidas pelas diferentes mídias de massas”. Ele comenta que a revolução informacional envolve sobretudo a criação, o acesso e a intervenção sobre as informações estratégicas, de síntese, sejam elas de natureza econômica, política, científica ou ética. Logo depois, Wolton (2004) afirmaria como as numerosas revoluções das tecnologias da comunicação não tiveram o impacto

esperado, mostrando que a técnica não é suficiente para ter uma mudança na comunicação na sociedade.

A informação não é mais suficiente para criar comunicação, mesmo o contrário acontece. Tornando as diferenças culturais visíveis e desigualdades, força um esforço gigantesco de compreensão. É aqui, provavelmente, uma das rupturas mais importantes do século XXI (Wolton, 2004, p.13, tradução nossa).

Neste contexto, Wolton (2004, p.14) aposta na busca da convivência do triângulo da identidade, da cultura e da comunicação, descartando a ideia de que a mundialização da comunicação teria seu foco nos meios massivos de difusão e da lógica econômica. Portanto, para obter um impacto positivo, deveria se estar em sintonia com o movimento da evolução do modelo cultural de comunicação.

Neste meio, é relevante destacar que os aparatos tecnológicos possuem um papel secundário na revolução da informação, mas nunca exclusivamente ferramenta. Koltay (2011, p. 211) afirma que a tecnologia não é apenas uma ferramenta, pois determina as nossas ações, devendo-se refletir sobre as questões ideológicas, econômicas e culturais inerentes ao seu desenvolvimento e uso (Serafim, Freire, 2013, p. 78).

O fundamental para Geertz (1989, p.63) é entender o modo de funcionamento de uma cultura informacional. Não se busca entender o que é a informação em si (a sua essência), mas sim aprofundar na sua funcionalidade no terreno sócio-histórico e da economia informacional.

O que se faz necessário é ampliar a possibilidade de um diálogo inteligente entre pessoas que diferem consideravelmente entre si em interesses, perspectivas e poder, e, no entanto, estão limitadas em um mundo onde, envolvidas em interminável conexão, fica cada vez mais difícil sair uma do caminho da outra (Geertz, 1989, p.63).

Segundo Foskett (1980, p.21), a informação é mais do que simples indicação de percepções sensoriais ou respostas a determinados estímulos: exige processamento da mente humana antes de ser parte de um modelo ou paradigma passível de conformidade. Para Regina Marteleto (1995, p.2), a informação diz respeito não apenas ao modo de relação dos sujeitos com a realidade, mas também aos artefatos criados pelas relações e práticas sociais. Por isso, tentar desligar a própria natureza da informação com a cultura seria difícil no entendimento dos conceitos e dos fenômenos que as embrulham. A cultura, vista como a genoteca⁸⁶ da sociedade humana, os padrões culturais, religioso, fisiológico, estético, científico ou

⁸⁶ O termo “*genoteca*” foi criado por B. Ryback para demonstrar o funcionamento dos sistemas neguentrópicos, ou seja, que têm a capacidade de, pelo menos temporariamente, reduzir, afastar, ultrapassar ou “negar” o aumento da entropia no interior dos sistemas. O termo “*genoteca*” é empregado por Morin quando se refere ao sistema social o qual por meio de uma memória ou repertório cultural (a genoteca) (Marteleto, 1995, p.2).

ideológico, funcionam como programas ou gabaritos para a organização dos processos sociais e psicológicos (Marteleto, 1995, p.2).

Esses padrões representam fontes extrínsecas de informação, em cujos termos a vida humana pode ser padronizada, funcionando como mecanismos extra pessoais para a compreensão, julgamento e manipulação do mundo (Geertz, 1978, p.188).

Segundo Capurro (2003), a ligação existente entre o conhecimento (cognição) à pragmaticidade e à resolução de problemas, o trabalho informativo é um trabalho de contextualizar ou recontextualizar praticamente o conhecimento. O valor da informação precisamente é feito na possibilidade prática de ser aplicado um conhecimento a uma demanda concreta. Por isso, a importância que os encarregados da criação das políticas públicas na América Latina estejam cientes que o conhecimento é informação potencial.

A evolução da hierarquia DICS [dados, informação, conhecimento e sabedoria] segue os passos contrários à sua estrutura natural. Em vez de progredir desde os dados até a sabedoria, tem evoluído desde os conceitos mais abstratos até os mais específicos, informação e dados, que foram obtendo a sua importância em nossa época com o surgimento dos meios de comunicação e da informática (Semidão, 2014, apud García-Marco, 2011).

Segundo Serafim e Freire (2013, p.70), o fenômeno informacional observado nas formações sociais contemporâneas demonstra a informação como matéria-prima para o desenvolvimento e bem-estar social, o qual recém ocorre com o reconhecimento da informação como fator de produção econômica, sendo parte paradigmática de nossa atual sociedade. Por outro lado, não se sustenta como um novo paradigma econômico na medida em que não promoveu mudanças nos grandes problemas sociais da humanidade, por meio de um resultado diferenciado da atividade econômica, fonte de provisão do desenvolvimento das sociedades (Serafim, Freire, 2013, p.72).

Quanto ao próprio processo de transferência da informação, não tem recebido tanta atenção e quando chegamos às aplicações práticas da teoria. Uma vez mais, encontramos uma concentração quase exclusiva sobre a tecnologia de como fazê-la e não um exame do que deve ser feito e por quê. Isto é parte do fenômeno da “informação como mercadoria” em que se presume que informação é uma coisa boa, e o problema é produzir tanto quanto se possa: isso é ou se torna, sua própria justificativa (Foskett, 1980, p.30).

Paradoxalmente, os crescentes volumes de informação não conseguiram reduzir as desigualdades sociais, compreendidas pelos que possuem (ou não) amplo acesso à informação. O enriquecimento entre uma distinção entre a sabedoria e o conhecimento se dá durante o processo da industrialização e a explosão da informação, sendo entendido o conceito de informação, fundamentalmente, como notícia no marco de desenvolvimento dos meios de comunicação coletiva e das massas, tendo inicialmente à imprensa e o cinema, para logo depois a rádio, a televisão e nas redes sociais digitais. O papel do conhecimento desde a ilustração foi evoluindo desde uma perspectiva mais abstrata até uma mais aplicada e contextual, marcando assim uma compreensão pragmática da função do conhecimento, Segundo Garcia-Marco (2011, p.13), nos diz:

Desde os inícios da ilustração, o avanço do conhecimento científico e as profundas mudanças sociais produziram uma demarcação importante no próprio conceito de conhecimento, que durante séculos havia estado mais ligado ao saber teórico e ao saber viver, e agora passava a estar profundamente implicado, inclusive de forma preferencial, na evolução da matéria e na mudança das condições econômicas e sociais.

A informação compreendida desde a perspectiva da economia informacional, analisa as relações dos agentes econômicos em situações, em que existe uma desigual distribuição da informação, conhecida também como assimetria da informação, e apesar de dispor de uma informação incompleta existem processos de tomada de decisão. Os consumidores como os produtores não têm a mesma informação, em relação às variáveis mais importantes para uma eleição, consequentemente, “a existência da assimetria da informação deve ser entendida como um funcionamento errado do mercado perfeito” (Otter, Cortez, 2003, p.4, tradução nossa).

Obter vantagem por ter um conhecimento melhor das tecnologias de informação ou de transporte é visto, por vezes, como algo quase desonesto, embora fazê-lo, explorando as melhores oportunidades disponíveis, seja tão importante para a sociedade quanto utilizar as mais recentes descobertas científicas. Este preconceito tem afetado consideravelmente a atitude em relação ao comércio em geral, se comparada com a atitude em relação à produção (Hayek, 2018, p.156).

O simples ato de que as pessoas conhecem de diferentes coisas, faz à assimetria da informação natural e inevitável. As pessoas, não estão condenadas a situações desvantajosas pela falta de informação, querer encontrar todas as peças de informação não é apenas difícil ao extremo, assim também, deve ser a tarefa de reunir

e organizar essas peças para obter produtos úteis. Segundo Otter e Cortez (2003, p.8, tradução nossa), “se tem incentivos e mecanismos para adquirir informação e o mais potente deles é a educação, que por si mesmo é um processo da aquisição de informação e sua tradução em conhecimento”. Na medida em que os governos permitem operar os mercados, eles tornam a educação acessível e melhor. Então, dispor de informação imperfeita pode ser benéfico para os mercados. Segundo Boudreaux (2018, p.64), o capitalismo de livre mercado seria o sistema que melhor assegura que os recursos sejam usados eficientemente, para ele a raiz da liberdade econômica é a liberdade do consumo. No entanto, existe o problema quando a interferência de um governo protecionista dos produtores e operários, procura protegê-los de ter que competir pelo gosto do consumidor, promovendo um capitalismo clientelista.

Desse modo, a governança da informação e do conhecimento é um elemento chave na compreensão cognitiva (cognição ligada à computação), atuando também na teorização do impacto das tecnologias nas esferas humanas e sociais (em especial as organizacionais). Pelo comentado e de incentivo à crítica, hoje em dia, apesar do crescimento exponencial que se tem com a explosão dos dados e da informação graças às tecnologias da informação e da comunicação. Nos países latino-americanos não se tem a impressão de que estejamos em organizações e sociedades muito mais sábias ou em produção constante de sabedoria. Enquanto, os problemas sociais, econômicos e políticos na região não fazem senão multiplicar-se, por exemplo: a superpopulação, o meio ambiente, a corrupção, o desemprego etc.

Desde a perspectiva da ciência da informação, a informação como um processo cognitivo que parte desde os dados e chegando até o conhecimento (cognitivismo). De modo, para o cognitivismo, a mente tem seu equivalente no computador, em uma máquina, possuindo um repertório de instrumentos, representações do mundo e da linguagem, que lhe permite resolver problemas. Por esse motivo, a cognição seria entendida como a solução aos problemas, ademais podemos dizer que a informação e o conhecimento passam a constituir recursos econômicos fundamentais para os países latino-americanos e aliado ao advento das tecnologias da informação, ré valorou a importância da ciência da informação, como uma ciência social.

O fenômeno da digitalização de tudo o que é resultado das observações feitas por diversos gêneros de tecnologia, pode levar a algum tipo de processamento distorcido, além, da manipulação e transformação dos dados originais processados

pela tecnologia. Por essa razão, ao oferecer a aceitação do conhecimento devemos ser críticos, desde a forma como foi capturado, manipulado e representado pelas tecnologias.

Há alguns anos, os computadores possibilitam uma concentração de poder inimaginável. Essa concentração das informações torna o controle uma tarefa relativamente simples. “A transmissão de um sistema monolítico de valores e pensamento, o que significa exatamente o contrário da liberdade de pensamento, pode levar à produção de uma geração extremamente bem-informada, mas à qual faltam as qualidades essenciais à vida social” (Motta, 1986, p.123).

Segundo Nasser (2019, p.77), o ambiente de informação está dividindo o público e as incontáveis realidades percebidas, prejudicando o entendimento de eventos mundiais, que no passado, facilitaram a cooperação internacional, levando a alguns questionar as ideias democráticas, como a liberdade de expressão e o mercado das ideias. Nessa lógica, uma nova esfera de poder informacional nas relações internacionais seria hegemonizada por algumas potências mundiais, “como consequência, mais do que um destino marcado pela dependência econômica e tecnológica, diversas nações no decorrer dessa jornada também abrem mão inconscientemente de sua própria soberania nacional” (Brito, Kerr, 2015, p. 146). Por essa razão, muitos especialistas acadêmicos e políticos comentam que estamos na era da “pós verdade” ou “pós factual”, existindo múltiplos casos, na tentativa da manipulação das massas em forma fácil e sistemática. Os interesses dos provedores dos serviços de tecnologia e os atores detrás das campanhas de desinformação ou também conhecidas no argot da doutrina militar como operações de informação, estão alinhados. Existindo o interesse de ambos, de poder capturar o recurso escasso da economia da informação que é a atenção dos usuários. Os indivíduos não só são os alvos, também servem de meio de distribuição da desinformação, que tem uma natureza participativa. Segundo Huamani e Moura (2024a, p.25) é necessária a “revisão crítica discursiva da ecologia social das redes sociais digitais, como médio de influência e de instrumento efetivo na comunicação”. Em múltiplas pesquisas, se tem demonstrado que o uso de técnicas de micro segmentação e inteligência artificial como são os robôs sociais, tem sido a chave fundamental da disseminação na desinformação e alterando as regras da rede. As ferramentas de publicidade dependem da coleta e análise dos dados pessoais sobre o público-alvo. Os dados são

coletados diretamente dos indivíduos, observados da atividade do usuário na Internet usando tecnologias de rastreamento e obtidas de terceiros.

Os estudiosos argumentaram que o termo de “*Fake News*” (notícias falsas) é lamentavelmente inadequado para descrever os complexos fenômenos de “*misinformation*” and “*disinformation*”⁸⁷. Problemas semelhantes com o termo “*Fake News*” foram identificados pela *European Commission’s High-Level Expert Group on Fake News and Online Disinformation* (HLEG⁸⁸). Em seu relatório final, o A HLEG considerou o termo “*Fake News*” como inadequado para capturar o complexo problema de “*disinformation*” o que envolve não necessariamente ao “falso”, mas com conteúdo fabricado e práticas que vão além das notícias convencionais. Além disso, é considerado enganoso, devido ao fato de ter sido apropriado por alguns políticos para descartar qualquer conteúdo que eles consideram desagradável. O HLEG preferiu a palavra “*disinformation*” e usou a seguinte definição ao longo do relatório: todas as formas de informações falsas, imprecisas ou enganosas projetadas, apresentadas e promovidas para causar intencionalmente dano público ou com fins lucrativos (EUROPEAN PARLIAMENT, 2019, p. 24-25, tradução nossa).

Quadro 8 - Tipos de transtornos de informações

Tipos	Definição	Exemplo
Misinformation (Informação errada)	Quando a informação falsa é compartilhada, mas nenhum dano se quer denotar.	Durante as eleições presidenciais dos Estados Unidos da Norte América em 2016, um tweet sobre uma máquina de votação “fraudada” na Filadélfia foi compartilhado mais de 11.000 vezes. Mais tarde, foi estabelecido que o tweet original foi um erro cometido por um eleitor que não seguiu as instruções exibidas na máquina de votação ⁸⁹ .
Disinformation (Desinformação)	Quando a informação falsa é compartilhada, mas conscientemente se quer causar dano.	Durante as eleições presidenciais na francesa de 2017, foi criada uma versão duplicada do jornal Belga Le Soir, com um artigo falso alegando que Emmanuel Macron estava sendo financiado pela Arábia Saudita.
Mal-information (má intenção da informação)	Quando a informação genuína é compartilhada para causar prejuízo	O vazamento intencional das informações de um político (e-mails), como aconteceu durante as eleições presidenciais na França.

Fonte: (Wardle, Derakhshan, 2017, p.21, tradução nossa)

Segundo Nasser (2019, p.80), nos diz que a expansão da conectividade global através da informação e de redes está permitindo que atores com menos poder, mas bem conectados, tenham um imenso impacto. Então os Estados, grupos ou indivíduos que disponham dessas capacidades, relacionamentos e informações materiais de forma mais rápida, integrando e dispondo de poder de adaptação, poderiam usar seus recursos materiais para se influenciar e em alguns casos garantir ou evitar resultados. Eles terão o poder de determinar o resultado ao mobilizar o apoio das massas, no uso

⁸⁷ Onde “*misinformation*” se refere a imprecisões decorrentes de erro, e “*disinformation*” é falsidade deliberada promulgada pelo design “*misinformation*” pode ser usada para definir “*disinformation*” quando se sabe que “*misinformation*” é proposital e intencionalmente disseminada.

⁸⁸ Disponível em <<http://www.hleg.de/>>. Acesso em 10 de abril de 2020.

⁸⁹ Electionland, Viral ‘Rigged’ Voting Machine Video Actually User Error, 8 November 2016, <https://projects.propublica.org/electionland/pennsylvania/viral-rigged-voting-machine-actually-user-error/>; <https://www.nytimes.com/2016/11/09/us/politics/debunk-fake-news-election-day.html>

de informações para persuadir ou manipular sociedades e Estados, em favor de suas causas.

A capacidade de criar narrativas e ideologias evocativas, gerará tensão e cultivar a confiança e a credibilidade dependerão de interesses e valores justapostos, mas não idênticos. As entidades poderosas poderão induzir os Estados, bem como corporações, movimentos sociais ou religiosos e alguns indivíduos a criar redes de cooperação em todos os aspectos. Tais entidades apresentarão poder e equilíbrio em termos materiais, relacionais e de informação. Para se manter os resultados será necessária uma tendência constante a desenvolver e conservar relacionamentos (Nasser, 2019, p.80).

Circundados por redes digitais em que os dados fluem para as distintas partes do globo, modificando comportamentos, reorganizando sociedades e afetando modelos econômicos, o entendimento da dimensão de poder informacional é fundamental aos cidadãos, bem como para o conjunto das nações. Sob a égide de um discurso ideológico de uma “aldeia global”, alicerçado por uma “sociedade pós-industrial”, produzidos por uma pretensa “inevitabilidade tecnológica”, diversos setores sociais se conectam às redes de informação mundiais com a crença de que adentram um subproduto do avanço científico, que tal como um templo estaria desvinculado dos interesses políticos e econômicos dos atores estatais (Brito, Kerr, 2015, p. 145-14).

Embora, qualquer que seja a direção política a ser adotada pelos países latino-americanos, seus Estados não devem ser indiferentes em delegar capacidades de Operações de Informação e de Influência aos grupos privados, evitando estar expostos à crise da verdade e da desconfiança de sua sociedade (Huamani, Moura, 2024a, p. 25). Finalmente, é o conteúdo e o propósito que contam: essa organização social dos produtos das mentes individuais de sorte a beneficiar “realmente” à sociedade como um todo, onde possam ser acrescentadas a qualidade e a segurança nos processos de produção e consumo informacional. Por conseguinte, as políticas e estratégias públicas devem estar orientadas no desenvolvimento das habilidades de busca e uso crítico de informação nos cidadãos.

3.8.3 O ciberespaço, elementos de construção: automação e inteligência

A palavra cibernética vem do grego *Kubernêtes*, que significa piloto e o circuito fechado de automação implica, portanto, uma automação das faculdades humanas. Os meios de trabalho, são agora decompostos em execução, supervisão e interface. Com respeito ao conteúdo do trabalho, o autômato implica o desenvolvimento de um tipo novo de competência, que se refere às funções de recepção e emissão de sinais e às funções de programação e otimização. Caracterizam essas funções sua independência crescente em relação ao processo de trabalho (Motta, 1986, p. 96).

O termo Big Data⁹⁰, nos anos noventa foi criado por ciências como a astronomia e a genética, sendo os pioneiros no acúmulo massivo dos dados. Entenda-se que nos encontramos em um momento em que a humanidade está gerando em 15 minutos o triplo da coleção da Biblioteca do Congresso dos Estados Unidos, que é uma das maiores bibliotecas do mundo. Charles Duhigg (2012) em seu livro: "O poder do hábito", nos relata como algumas empresas preveem e manipulam os hábitos de consumo, o vasto acúmulo de dados digitais e sua transformação em valor econômico, que está revolucionando o mundo; citando à empresa privada Target, uma cadeia de lojas de departamento dos Estados Unidos. Eles analisaram os dados de milhões de clientes até encontrar uma correlação entre os hábitos de compra e uma provável gravidez, chegando mesmo a estimar a data do parto com uma estreita margem de erro, oferecendo assim os produtos mais adequados em cada fase da gravidez.

Uma das maiores empresas privadas em termos de acumulação de dados digitais é a Google Inc., em estudos de pesquisas de usuários, a empresa previu em tempo real, a propagação de uma epidemia de gripe desde 2008. Vale ressaltar que, hoje em dia, os algoritmos são a arma secreta das empresas globais e inovadoras, esses algoritmos estão sendo utilizados nas diferentes áreas de negócio. Segundo Carlos Gómez Uribe, ex-vice-presidente de inovação da Netflix⁹¹ existem quinze (15) algoritmos diferentes que, juntos, definem quais filmes serão recomendados ao usuário. Outro conjunto de algoritmos são usados no "streaming", isto é, para decidir em qual qualidade o vídeo será enviado ao usuário, dada a banda larga. Por exemplo, se a banda larga cai durante a reprodução de um filme, ela é passada para um arquivo de vídeo com menos definição sem que o usuário perceba. E quando a banda larga se recupera novamente, ela retorna ao arquivo que tem a melhor resolução. Também se tem algoritmos, que são usados para definir a estratégia de aquisição de conteúdo e escolher quais imagens serão usadas quando as recomendações são mostradas, existindo diferentes imagens e *posts* para cada vídeo, e algoritmicamente é decidido qual representa o melhor vídeo para cada usuário. Há outro conjunto de algoritmos para compactar e codificar os vídeos, e outros, que são usados para decidir quantas cópias de cada episódio serão armazenadas em cada servidor na Internet.

⁹⁰ Big Data é uma palavra que permeia grande parte da discussão sobre o uso da informação digital em empresas e governos. Surpreendentemente, há pouco consenso sobre a definição do termo citado, a definição mais acadêmica vem da descrição de suas três características: "Volume, velocidade e variedade". Disponível em <<https://mitcre.mit.edu/wp-content/uploads/2018/01/URBAN-DATA-AND-REAL-ESTATE-JAN-2018-1.pdf>>. Acesso em 10 de abril de 2020.

⁹¹ Netflix, Disponível em: <<https://www.amexcorporate.com.ar/multitaskers/nota.php?id=462&cat=9>>. Acesso em 20 de março de 2019.

Kai-Fui Lee, fundador e CEO da Sinovation Ventures e presidente do Instituto de Inteligência Artificial da Sinovation Ventures, na entrevista realizada para a MIT Technology Review⁹² comentou que um motorista UBER na China, provavelmente perderá seu emprego entre os próximos 10 a 15 anos, devido à proliferação dos veículos autônomos. Pode parecer surpreendente, mas é óbvio que metade das tarefas executadas pelos humanos, poderia ser feita melhor e quase sem custo por meio da Inteligência Artificial (IA). Esta premonição é sustentada devido, em primeiro lugar, porque a China tem um enorme exército de jovens que estão se inserindo na IA. Na última década, o número de publicações de IA de autores chineses dobrou e nas competições mundiais de IA, eles ocuparam as primeiras posições. Em segundo lugar, a China dispõe de "mais dados" do que os Estados Unidos. Os dados são os insumos que possibilitam o trabalho da IA. Imaginemos um cientista comum, com uma tonelada de dados, em definitiva ele irá superar a um super cientista que dispõe de uma quantidade modesta ou pouco significativa de dados. É de muita importância entender este fenômeno dos dados e da informação, no âmbito do Big Data e da IA. Segundo as estatísticas a China tem o maior número de telefones celulares e usuários de Internet no mundo, quase o triplo que nos Estados Unidos, esta diferença é ainda maior devido à maneira como as pessoas na China usam seus dispositivos. Um cidadão chinês não carrega dinheiro físico, pagando as contas e compras com seus telefones celulares. Na China, as bicicletas compartilhadas (Mobike Technology Co⁹³) geram 30 Terabytes de dados por dia porque suas 8 milhões de bicicletas têm integrado o GPS (*Global Position System*), que é aproximadamente 300 vezes mais do que os dados gerados nos Estados Unidos.

Na tese de que a automação implica uma ruptura tecnológica radical. É o caso de O. Vicent e W. Grossin. Na perspectiva desses pesquisadores é possível ver a questão de duas maneiras: a primeira é aquela normalmente característica da visão do engenheiro, enquanto a segunda é em geral a forma pela qual optou o sociólogo. Frequentemente, o engenheiro interroga-se sobre a natureza da máquina enquanto dispositivo de transformação da matéria e conservação da energia. Nessa visão privilegia-se a substituição do homem pela máquina, encarando o sistema produtivo em termos de continuidade e integração. A maneira de ver típica do cientista social volta-se mais para os efeitos econômicos, sociais, políticos e culturais da introdução e generalização da automação. (Motta, 1986, pp, 97-98).

⁹² Disponível em: <<https://www.technologyreview.com/s/610298/tech-companies-should-stop-pretending-ai-wont-destroy-jobs/>>. Acesso em 20 de março de 2019.

⁹³ Imagine um mundo onde você pode pegar e largar uma bicicleta em sua conveniência. Mobike, é um serviço de bicicletas compartilhadas para viagens urbanas curtas, a qualquer hora, para qualquer destino de estacionamento legal, combinando inovação e tecnologia IoT (Internet das coisas) de hoje. O Mobike é ecológico, reduz o congestionamento e se esforça continuamente para melhorar a qualidade de vida na cidade. Disponível em: <<https://mobike.com/cn/>>. Acesso em 10 de dezembro de 2019.

Pelo dito, a presente tese se apropria na distinção entre automatização e automação. A automatização, vai se caracterizar com a informática centralizada de grandes unidades, mas por formas não integradas de produção. Por outro lado, a automação, caracterizar-se-ia pela informatização das massas e pela integração de grandes sistemas produtivos das máquinas automáticas. Para Motta (1986, p. 98), “na automatização há efeitos organizacionais diretos que afetam quase exclusivamente o conteúdo do trabalho”. Mas os efeitos da automação podem ser menos diretos, porque “apresentam-se em maior amplitude e dimensão, ao ponto de afetar o nível de emprego e a organização do trabalho”. Uma das tendências globais descritas nas reflexões do Nasser (2019, p.37), diz que “o produto de se ter uma aceleração no progresso por meio da tecnologia, ela também vem causando rupturas”. Os rápidos avanços tecnológicos aumentaram o ritmo das mudanças e criaram oportunidades, mas agravaram as divisões entre vencedores e perdedores.

A automação e a inteligência artificial ameaçam transformar as indústrias mais rapidamente do que as economias podem se adaptar, com potencial de tornar trabalhadores redundantes e limitar o câmbio usual de desenvolvimento dos países pobres. As biotecnologias, como a edição do genoma, revolucionaram a medicina e outros campos, ao mesmo tempo em que levantaram questões morais (Nasser, 2019, p. 38).

Se pode observar, que a intensa existência da automação nos países desenvolvidos, como nos Estados Unidos, França, Alemanha, Reino Unido, China etc., está criando um problema sério de desemprego, sobre exploração e exclusão social, nos países latino-americanos. É certo que ainda se concentra a produção nessa região, mas devido a que a mão de obra é mais barata. Os estudos dizem que nas próximas décadas, isso irá diminuir, com o impulso da tecnologia 5G, muitas empresas multinacionais ou gigantes tecnológicos tem impulsionado múltiplos projetos na utilização da automação, porque no plano econômico é muito mais rentável para eles em suas atividades de produção. Segundo Nasser (2019, p. 44), a tendência de demandar mão de obra cada vez menos especializada nos países pobres, à medida que a automação, a inteligência artificial e outros avanços de fabricação serão os mais utilizados. Isto poderá fazer voltar às matrizes essas atividades produtivas; tendo-se pesquisas e simulações, onde as atividades profissionais feitas na atualidade, um grupo delas serão extintos pela automação.

3.8.4 O ciberespaço, elementos de construção: conectividade global e controle

Segundo Bejarano (2011), uma nova dimensão emergiu onde podem se materializar as ameaças no ciberespaço. Tempo atrás no campo da defesa, era claro que os movimentos eram em três dimensões: terrestre, aérea e marítima, logo depois, foi inserido o espaço exterior. Hoje, temos uma dimensão adicional e mais intangível que as anteriores. “Um traço distintivo das sociedades avançadas contemporâneas é a riqueza de informações que a nova tecnologia propicia. Outro traço é o poder imenso que conferem aos que sabem administrar essas informações” (Motta, 1986, p.117). Para enfatizar o expressado por Motta, na citação realizada do Rodrigues da Silveira ao Dizard, comenta o seguinte:

Para a configuração do poder, então, exige-se a existência de uma “vontade”, de uma “capacidade” para fazer valer à vontade, ou seja, a produção dos “efeitos desejados”, e finalmente, da certeza de que é preciso agir, pois os efeitos não aconteceriam “espontaneamente”. Para conhecer, conceber ou divulgar uma “vontade” e avaliar a “capacidade” operacional, o poder demanda informação. Por isso também se afirmar que a informação é poder, ou mais que isso, é fator multiplicador e medida de avaliação do poder (Dizard, 1982, p. 213 apud Rodrigues da Silveira, 2000, p.80).

Na sociedade contemporânea, se tem um condicionamento social na crença dos valores democráticos e da livre iniciativa por meio da manipulação do “mercado” e de influências políticas. Sem embargo, temos que admitir que apesar de aquelas restrições a prática do poder proporciona uma certa “organicidade” à vida social. Segundo Rodrigues da Silveira (2000, p.80) “A simbiose entre o Estado e o poder, então, não é apenas inevitável, como também socialmente necessária, desde que o governo seja “legítimo e democrático”, mesmo com a prevalência das desigualdades no exercício do poder”.

Ideias e identidades estão gerando uma onda de exclusão. A crescente conectividade global, em meio ao baixo crescimento, aumentará as tensões internas das sociedades e entre as nações. O populismo aumentará à direita e à esquerda, ameaçando o liberalismo. Alguns líderes usarão o nacionalismo para reforçar o controle. A influência religiosa será cada vez mais significativa e autoritária do que muitos governos. Quase todos os países verão as forças econômicas impulsionarem o status das mulheres e seu papel de liderança, mas também ocorrerá uma grande reação contrária a isto (Nasser, 2019, p. 38).

Como observado por Göra Therborn, em sua obra *“The World: A Beginner’s Guide”*, nas diferentes ondas históricas da humanidade, sempre estava presente a tendência globalizante, entendida como a aceleração ou intensificação de grandes processos sociais de alcance e impacto, pelo menos, de nível continental. Segundo Osterhammel e Peterson, em *“Globalization, a short history”*, foi precisamente a última dessas ondas que tem dado o seu nome à “globalização” na expressão e no escopo conceitual

que esteve a partir do final dos anos oitenta. O tempo implodiu no espaço e no futuro tornou-se um extenso domínio globalizado, dominado pela espacialidade (Molina, 2014, p.3. tradução nossa).

Segundo Molina (2014, p. 4), “a globalização é uma força supraindividual em que as conexões e o impacto são expandidos sem direção nem sentido concreto e é representativa da mistura de um câmbio rápido com uma paralisação transformadora”. O ascenso do informacionalismo no final do século XX, nos apresenta um ciberespaço “naturalizado” ao processo da globalização devido às diversas vantagens que ele trouxe no processo globalizador, especialmente, como meio de integração e de comunicação global, financeira e comercial. A reestruturação do capitalismo a um capitalismo informacional, tem como lógica fortalecida a competitividade econômica.

Os Estados, governos, sociedades, indivíduos, relações sociais, econômicas e políticas, no domínio cibernético estão mudando rapidamente e inconscientemente, sem serem conhecidos até onde chegarão. Por momento, os efeitos da abertura da globalização e a hiper conectividade, vem superando os obstáculos expressados através de novas formas de vigilância e controle. Frente a esta necessidade, desde o ponto de vista da dimensão informacional e dos episódios pontuais à renacionalização cibernética, vinculada às intenções antidemocráticas de controle político, conformam as fronteiras imaginárias do ciberespaço, que no suposto, seria um freio ao processo globalizador e segundo ao entender do Molina (2014, p.4-5) confirma o seguinte:

Sem esquecer que junto a este processo é destacado diariamente por outros de signo oposto, de diferenciação simbólica e natureza antropológica, manifestada sob a forma de tribalização, particularismo étnico ou processos análogos. O resultado é o ponto crítico de equilíbrio entre esta tendência de globalização supranacional e a redução do espaço para o exercício da ação política que, até hoje, continua a ser incorporada no Estado-Nação.

Outra perspectiva que vai se influenciar na definição, historicidade e compreensão do ciberespaço, é o famoso “manifesto” pelo Jhon Perry Barlow⁹⁴, conhecido como: “A declaração do ciberespaço”. Desde sua publicação se tornou referência forçada a ser estudada no termo do impacto social. Barlow declara um ciberespaço dentro de seus diferentes significados: “alucinação sensual”, “espaço virtual de interação” e “nova casa da mente”.

Os governos obtêm seus justos poderes de consentimento daqueles que são governados. Você não pediu ou recebeu a nossa. Nós não te convidamos. Você não nos conhece, você não conhece o nosso mundo. O ciberespaço não está dentro de suas fronteiras. Não pense que você pode construí-lo,

⁹⁴ Disponível em <<https://www.eff.org/cyberspace-independence>>. Acesso em 14 abril de 2020.

como se fosse um projeto público de construção. Você não pode. É um ato natural que cresce a partir de nossas ações coletivas.

Você não se juntou à nossa grande conversa coletiva, nem criou a riqueza de nossos mercados. Você não conhece nossa cultura, nossa ética ou os códigos não escritos que já fornecem a nossa sociedade com mais ordem do que o que poderia ser obtido por qualquer uma das suas imposições.

Você proclama que existem problemas entre nós que você precisa resolver. Você usa isso como uma desculpa para invadir nossos limites. Muitos desses problemas não existem. Onde existem conflitos reais, onde existem erros, vamos identificá-los e resolvê-los nos nossos próprios meios. Estamos criando nosso próprio Contrato Social. Esta Autoridade será criada de acordo com as condições do nosso mundo, não o seu. Nosso mundo é diferente. O ciberespaço é composto de transações, relações e pensamento em si mesmo, que se estende como uma passiva onda na teia de aranha de nossas comunicações. Nosso mundo está em todas as partes e em nenhum lugar, mas não está onde os corpos vivem.

Estamos criando um mundo no qual todos podem entrar, sem privilégios ou preconceitos devido a raça, poder econômico, força militar ou local de nascimento. Estamos criando um mundo onde qualquer pessoa, em qualquer lugar, pode expressar crenças, por mais originais que sejam, sem medo de serem coagidos a fazer silêncio ou conformismo.

Seus conceitos legais sobre propriedade, expressão, identidade, movimento e contexto não se aplicam a nós. Eles são baseados na matéria.

Cá não tem matéria. Nossas identidades não têm corpo, então, ao contrário de vocês, nós não podemos obter ordem por coerção física (Barlow, 1996, tradução nossa).

Para a adequada compreensão do processo da globalização é importante analisar os processos de produção, distribuição e de consumo. Em soma a esse análise, deve ser considerada a “informação como elemento que permeia as dinâmicas de constituição, objetivação e negociação, em que as representações sociais e os discursos identitários são formulados, aceitos, confrontados e/ou reelaborados” (Perdigão, Nascimento, 2019, p.23).

A interação com teorias e conceitos, como o projeto de modernidade, nos permitirá ter um olhar crítico das consequências geradas pela sociedade ocidental. Onde acontecem as relações de produção, circulação e consumo dos bens culturais, em relação a um modo prevalecente de conhecimento que tinha como fundamento unitário os referenciais simbólicos e de poder (Marteleto, 1995, p.4). Constituindo e fortalecendo campos relativamente autônomos de produção ou reprodução cultural. Por exemplo: artístico, filosófico, científico, educacional etc. E os campos de distribuição e consumo. Por exemplo: editoras, bibliotecas, arquivos, museus, indústria cultural etc. Dando origem a uma forma de consumo dos bens culturais, semelhante aos bens materiais. Sendo esses campos uma situação institucionalizada, segundo Bourdieu (1980, p.113), “os agentes desenvolvem suas ações como

atividades regidas por regras válidas para cada campo”. Serão os *Hábitus*⁹⁵ que vão propiciar a participação ou não dos sujeitos nos campos.

Sendo então forjado no interior de relações sociais exteriores, “necessárias” e “independentes das vontades individuais”, o *Habitus* possui uma dimensão inconsciente para os sujeitos, uma vez que estes não detêm a significação da pluralidade de seus comportamentos e nem dos princípios que estão na gênese da produção de seus esquemas de pensamentos, percepções e ações: “...o *Habitus* tende a assegurar sua própria constância e a sua própria defesa contra a mudança através da seleção que ele opera entre as informações novas, rejeitando, em caso de exposição fortuita ou forçada, as informações capazes de colocar em questão a informação acumulada e sobretudo desfavorecendo a exposição a tais informações...” (Bourdieu, 1980 apud Marteleto, 1995, p. 5).

Podemos observar, que os conceitos associados de campo e *Habitus*, irá nos ajudar a entender o processo da globalização no ciberespaço, como um processo além de uma simples conectividade global, comunicação e interação universal. Por isso, segundo Marteleto (1995, p.5) a “importância de perceber o modo de estruturação dos sentidos produzidos socialmente, agenciados e gerenciados por agências e agentes produtores e reprodutores das informações e do seu fluxo na sociedade”.

É nesse contexto da modernidade cultural, dividida em campos de produção simbólica, que surge e se consolida a ideia de informação como elemento que organiza o que, por natureza, é disperso e conflitam – as relações sociais – e que dá aparência de dispersão e neutralidade ao que é produzido com homogêneo e indivisível – o conhecimento racional (Marteleto, 1995, p.5).

É essencial analisar as práticas informacionais aplicadas no ciberespaço, onde a construção do objeto informacional é complementada com as estruturas materiais e simbólicas de um dado universo cultural. Hoje em dia, faz-se de importância conhecer que para estabelecer as políticas públicas e estratégias em segurança cibernética vai se precisar ter uma noção de informação, frente aos discursos e iniciativas de uma sociedade globalizada, sem fronteiras culturais, políticas e econômicas. Uma sociedade como a peruana, argentina e brasileira estão permeadas por matrizes de significações diferentes, conflitivas e ainda múltiplas, concorrentes e superpostas, sendo afirmado pelo Marteleto o seguinte:

É nessas sociedades que o objeto informação poderá ser construído e se transformar em problema relevante de pesquisa, sobretudo para os países cuja maioria da população encontra-se ainda à beira do caminho das grandes vias cibernéticas, e não em sociedades ditas de massa, informatizadas ou sem história. Afinal, “nossa história nem apenas começou...” (Marteleto, 1995,

⁹⁵ *Habitus* é o conceito que diz algo concreto e dinâmico sobre os agentes sociais, pois representa o esquema de percepção e de ação de cada indivíduo, adquirido e formado pela história social de cada um deles é resultante de um longo processo de aprendizagem formal e informal (Marteleto, 1995, p.5).

p.7).

Na paisagem global emergente, repleta de surpresas e rupturas, os Estados e organizações mais capazes de explorar as oportunidades serão aqueles que resistirem às adversidades inesperadas e tomar ações para a rápida recuperação. Tais atores investem em infraestrutura, conhecimento e relacionamentos que lhes permitirão gerenciar o choque, seja econômico, ambiental, social ou cibernético (Nasser, 2019, p. 33).

Então a compreensão do ciberespaço que iremos trabalhar na presente tese, terá como base teórica esses quatro elementos de construção estudados.

3.9 As capacidades cibernéticas e os modelos de maturidade

Não dispor de uma política nacional que considere a integração transversal do planejamento das capacidades cibernéticas nos componentes: político, estratégico, operacional e tático poderia dificultar nossa compreensão dos retos e benefícios no uso do ciberespaço. A inadequada atenção do contexto geopolítico, das ameaças e riscos cibernéticos associados aos interesses nacionais de um Estado. Especialmente, por aqueles que dispõem limitados recursos, falta de experiência, dependência industrial e tecnológica, devido que os principais problemas socioeconômicos estão ligados com os baixos níveis de vida, pobreza, desemprego, informalidade, corrupção, violência (CEPAL, 2020). Pode despertar nos países em vias de desenvolvimento utopias e enganos na chamada “Onda Digital”. Segundo Castells (2018, p.96, tradução nossa) “o balanço aparentemente desigual do desenvolvimento no alvorecer da era da informação transmite uma perplexidade manipulado ideologicamente na ausência de clareza analítica”.

O crescente ceticismo, às medidas necessárias de dispor de um ciberespaço seguro, de livre acesso e neutralidade na Internet, se mostram como a imposição instaurada pelo capitalismo informacional que “se caracteriza pela formação de uma economia criminal global e por sua crescente interdependência com a economia formal e das instituições políticas” (Castells, 2018, p.100, tradução nossa). Os países sul-americanos, nos últimos anos, estão aumentando rapidamente seu acesso ao ciberespaço, sem ter adequadas estratégias em segurança e defesa nacional, o qual pode trazer mais danos do que beneficiar tanto ao Estado quanto à economia local (Burt, 2014 apud Muller, 2015, p.6). Segundo Nasser (2019, p.34), o problema central que desafiará aos governos e às sociedades é como combinar os talentos individuais,

coletivos e nacionais de forma a produzir segurança, prosperidade e esperança sustentáveis. Desde a perspectiva do capitalismo informacional, as áreas pouco valiosas e que não possuam um interesse político para os grupo de poder, eles “serão esquivados pelos fluxos de informação e riqueza, induzindo a uma geografia desigual de exclusão e inclusão social-territorial que incapacita a amplos segmentos da população” (Castells, 2018, p.99-100, tradução nossa). Em nossa compreensão, as capacidades cibernéticas são um instrumento chave para garantir um adequado nível de segurança cibernética.

A definição das capacidades cibernéticas se relaciona com os recursos e ativos disponíveis que se encontram à disposição de um Estado, para resistir e projetar sua influência e coerção por meio do ciberespaço. Segundo a doutrina militar dos países desenvolvidos, o efeito causado pelo uso do ciberespaço como resultado das operações defensivas e ofensivas é dispor de capacidades cibernéticas. Consequentemente, esse efeito causado, pode ter como finalidade obter ou consolidar os objetivos nacionais, os quais podem incluir os âmbitos econômico, diplomático e da segurança. Além disso, para Biller e Schmitt (2019, p.183, tradução nossa), “as capacidades cibernéticas não podem ser categorizadas logicamente como armas ou meios de guerra cibernética”.

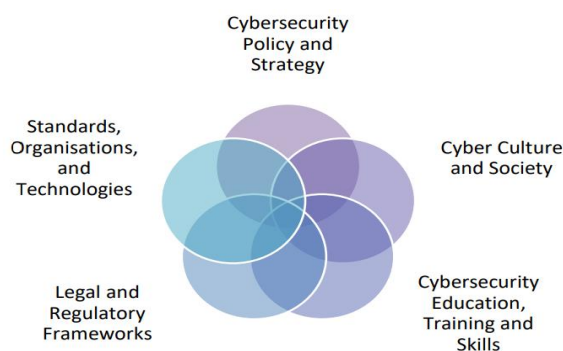
Estudos recentes relacionados às capacidades cibernéticas vem sendo desenvolvido pelo Centro da Capacidade de Segurança Cibernética Global (*Global Cyber Security Capacity Centre – GCSCC*⁹⁶) da universidade de *Oxford*. As pesquisas do GCSCC desenvolvem uma proposta, no sentido de fechar as lacunas na criação de um modelo de maturidade da capacidade de segurança cibernética (*Capability Maturity Model - CMM*). Embora, ainda seja apenas um modelo piloto, ele tem como parte de suas atividades o permitir aos países, uma autoavaliação de seu nível de capacidade cibernética e, em seguida, diretamente receber informações sobre como fazer as melhorias. Eles vêm atuando desde o nível político de Governo, devendo se inserir informações ao modelo por meio de respostas às perguntas diretas e indiretas

⁹⁶ O Modelo de Maturidade da Capacidade Cibernética para as Nações (CMM), foi implantado desde 2015 através da cooperação entre a GSCC e seus parceiros estratégicos: Organização dos Estados Americanos (OEA), Banco Mundial, Organização de Telecomunicações da Commonwealth (CTO) e União Internacional das Telecomunicações (UIT), NDR Cybersecurity, NUPI e o Centro de Cybersecurity de Oceania (OCSC). Por meio dessas parcerias, o CMM foi implantado em mais de 60 países, incluindo Reino Unido, Kosovo, Butão, Uganda, Senegal, Quirguistão, Chipre, Lituânia, Madagascar e Indonésia, e apoiou um estudo regional na América Latina e no Caribe por meio da colaboração com a OEA: Relatório de Cibersegurança 2016: Estamos preparados na América Latina e no Caribe. Disponível em <<https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-assessments-around-world>>. Acesso em 20 abril de 2020.

sobre suas capacidades no ciberespaço. Se o país estiver de acordo com sua autoavaliação, o GCSCC vai propor as ações que necessitarão ser feitas na melhora das capacidades cibernéticas. Segundo o GCSCC, o objetivo do modelo busca dividir em um espaço de análise de cinco pilares da sociedade, sendo as seguintes:

1. Planejamento de uma ciberpolítica e estratégia.
2. Incentivar a responsabilidade de uma cibercultura na sociedade.
3. Construir habilidades cibernéticas na força de trabalho e liderança.
4. Criar estruturas jurídicas e reguladoras eficazes.
5. Controlar os riscos através de organizações, padrões e tecnologia.

Figura 10 - As cinco dimensões segundo o CMM



Fonte: (GCSCC, 2016, p. 5).

Qualquer país, independentemente de seu nível de capacidade, poderia usar a ferramenta do CMM. Em base às respostas, se tem uma pontuação, de forma que os países avaliados são classificados, de acordo com as seguintes níveis:

- Nível 1 - Startup: embrionário.
- Nível 2 - Formativa: 'novo'.
- Nível 3 - Estabelecido: indicadores são funcionais e definidos.
- Nível 4 - Estratégicos: as escolhas têm sido sobre o que priorizar.
- Nível 5 - Dinâmica: tomada rápida de decisão, realocação de recursos e ambiente em constante mudança.

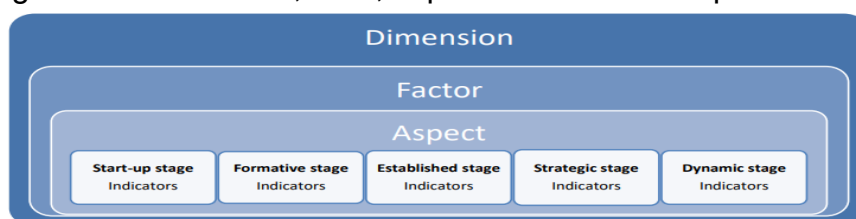
Segundo Muller (2015), os desafios que fazem difíceis na garantia de um ciberespaço seguro, estão relacionados com:

- O acesso ao ciberespaço versus estabilidade institucional.
- Um marco legal, adequado para a construção segura do ciberespaço.
- Acessibilidade, onde a implementação de infraestrutura e arquitetura tecnológica é limitada, ainda sem capacidade de manutenção.

- Construindo conhecimento, compreensão e consciência em relação às ameaças e riscos que vem com o ciberespaço.
- Cooperação público e privada, dando ênfase a que é o setor privado quem concentra a maior infraestrutura e arquitetura tecnológica do Internet.

Na análise crítico desta tese, podemos apreciar que a implementação do CMM na categorização do estado de maturidade da segurança cibernética, não é dinâmico nem transversal às problemáticas vigentes dos países em vias de desenvolvimento. Ela apresenta um diagnóstico relativo desde o ponto de vista estatístico e tecnológico, além de poder ser manipulado desde o nível político de Governo. Nosso contraponto, sustenta-se, que aquele modelo não brinda de maneira adequada uma ação de resposta às nossas necessidades e interesses reais em segurança cibernética, sendo nosso objetivo de análise na presente tese. Principalmente, pela ausência de uma tratativa social e de uma abordagem qualitativa, como um problema complexo e heterogêneo, que possa atender às problemáticas socioeconômicas, geopolíticas e culturais. A generalização das ameaças e riscos cibernéticos, como também, a leveza com que é tratado o contexto geopolítico, social e econômico no CMM, apresenta uma outra posição de que o GCSCC precisa das informações desde o alto nível político governamental, onde muitas dessas informações são privilegiadas e sigilosas para que sejam, neste caso, confiados neles. Posteriormente, com base nos indicadores estabelecidos pelo GCSCC, eles irão propor melhorias desde um parâmetro estabelecido por eles, em dimensões com múltiplos fatores, e onde cada fator é apresentado como um número de aspectos que irá se categorizar em cinco (05) níveis.

Figura 11 - Dimensão, fator, aspecto e indicadores por camadas



Fonte: (GCSCC, 2016, p. 7).

3.10 Historicidade da política em segurança cibernética no Peru

Ao fazer uma breve exploração e análise nos documentos oficiais que guardam relação com a defesa nacional peruana, se observa que desde o ano 1933 a Constituição Política do Peru estabeleceu a obrigação das comunidades indígenas em contribuir na defesa nacional (Valeriano-Ferrer, 2013, p.30), estando em evidência

que não existe uma doutrina integral em segurança e defesa nacional que seja refletida a toda a sociedade civil⁹⁷ peruana, onde estigmatizações do passado segregam ao cidadão civil com o militar. Portanto, se dispõe de uma doutrina de uso exclusivo no âmbito militar. Apesar de existir sinais de aproximar aos civis e militares, em uma única sociedade civil, através do cenário acadêmico entre o Centro de Altos Estudos Nacionais (CAEN) e algumas universidades no Peru (Valeriano-Ferrer, 2013, p.114) a doutrina em segurança e defesa nacional possui limitações em relação aos outros poderes e estruturas do Estado.

Posterior à Segunda Guerra Mundial, se iniciou o desenvolvimento da doutrina da segurança e defesa nacional, a criação do Centro de Altos Estudos Militares (CAEM) e de uma mudança na visão da defesa nacional a qual deveria ser integral e permanente, e que toda pessoa natural e jurídica está na obrigação de participar. Estas iniciativas foram influenciadas pelo destacado e visionário, José del Carmen Marín Arista, que ocupou o cargo de Ministro de Guerra e General do Exército do Peru. Posteriormente, nas próximas Constituições Políticas do Peru (1979 e 1993) é destacado um capítulo, para a segurança e defesa nacional, sendo o cargo de Presidente da República responsável na direção do Sistema da Defesa Nacional. Outro ponto que destacou em nossa análise é que na Constituição Política de 1993, no Artigo 54, o território peruano está constituído pelo solo, subsolo, o domínio marítimo e o espaço aéreo que os cobre, portanto temos observado que o domínio cibernético como a Internet, ainda é incerto e pouco conhecido na constituição peruana. Recém no seguinte ano (1994) por primeira vez, o Peru se conecta ao Internet através de um satélite, sendo a Rede Científica Peruana⁹⁸ (RCP) o primeiro fornecedor do serviço e instalando a "primeira *cabina*" de Internet no país. No ano 1995, o Peru tem acesso aos domínios da *World Wide Web (WWW)*.

É a partir do ano 2000, onde temos identificado as primeiras iniciativas de interesse ao âmbito da segurança e defesa cibernética. Uma dessas iniciativas é a Lei N° 27291, que modifica o código civil permitindo o uso dos meios eletrônicos para a comunicação da manifestação da vontade e uso da firma eletrônica, olha-se o Apêndice III. Com a criação do Escritório de Governo Eletrônico (ONGEI⁹⁹) no 2003,

⁹⁷ Na nossa concepção de uma sociedade civil, não deveria existir diferenças entre um cidadão militar com o civil.

⁹⁸ Disponível em <<https://rpp.pe/peru/historia/asi-era-la-primera-cabina-de-internet-del-peru-noticia-1051281?ref=rpp>>. Acesso em 05 de novembro de 2020.

⁹⁹ *Oficina Nacional de Gobierno Electrónico e Informática*. Entidade responsável do sistema Nacional de Informática e encarregado da implementação da Política Nacional de Governo eletrônico (norma, promove e articula). Em complemento, olha-se o Apêndice VIII – Figura 75.

segundo os documentos analisados se observou que a segurança da informação é considerada em suas linhas de ação e de atenção na melhoria da qualidade dos serviços públicos:

Linha de Ação 1 – Governo Eletrônico:

- ✓ Políticas, planos e estratégias.
- ✓ Projetos de Governo eletrônico.
- ✓ Segurança da informação.
- ✓ Plataforma de interoperabilidade do Estado (PIDE).
- ✓ Infraestrutura de dados espaciais do Peru (IDEP).
- ✓ Governo móvel.
- ✓ Governo aberto.
- ✓ Normatividade.

Linha de Ação 2 – Sociedade da informação:

- ✓ Acesso inclusivo e participativo.
- ✓ Desenvolvimento das competências digitais.
- ✓ Agenda digital 2.0.
- ✓ Normatividade.

Conforme os peruanos foram se inserindo no uso de serviços pela Internet, se deu origem aos novos delitos, por esse motivo, é criada no ano 2005 uma divisão encarregada de atender os casos de delitos informáticos (Divisão de Investigação de Delitos de Alta Tecnologia - DIVINDAT) na Polícia Nacional do Peru (PNP). Em agosto de 2009, é evidenciada uma maior preocupação em dispor de uma liderança centralizada, na administração pública, em atenção aos incidentes cibernéticos de escala nacional, sendo criado o PeCERT¹⁰⁰. Outrossim, observa-se que desde a publicação oficial da Lei Marco de Modernização da Gestão do Estado Peruano¹⁰¹, como a Lei da transparência e acesso à informação pública, foram elas, as impulsoras para uma maior consciência na segurança da informação e cibernética peruana, se inserindo assim na política de Estado e políticas nacionais. Como por exemplo: a Agenda Digital Peruana 2.0, o uso obrigatório da NTP-ISO/IEC 27001:2008 EDI TI - *Técnicas de seguridad* -SGSI, a implementação da Autoridade Nacional para a

¹⁰⁰ *Equipo de Respuesta ante Incidentes de Seguridad Digital Nacional*, também denominados nas Siglas: CSIRT ou CERT.

¹⁰¹ Olha-se no Apêndice IV, os documentos descritos no parágrafo.

Proteção dos Dados Pessoais e sua regulamentação, a regulação do dinheiro eletrônico, Lei do backbone de fibra óptica peruana e sua regulamentação etc. A finais de dezembro de 2012, com o Decreto Legislativo N°1131¹⁰² é criada a Secretaria de Segurança e Defesa Nacional (SEDENA) como a responsável de articular a Política de Segurança e Defesa Nacional. É nessa Secretaria onde se estabelecem as primeiras definições da segurança cibernética no nível político-estratégico, tendo que articular três objetivos:

Objetivo N°1. Defesa nacional, estruturada por 8 diretrizes;

Objetivo N°2. Ordem interno, estruturado por 7 diretrizes; e

Objetivo N°3. Ações de Desenvolvimento, estruturado por 6 diretrizes.

Quadro 9 - Objetivos e diretrizes da SEDENA, com a segurança cibernética

Objetivo	Descrição	Diretrizes
Defesa Nacional.	Garantir a soberania, independência, integridade territorial e a proteção dos interesses nacionais.	N°08. Implementar o Sistema Nacional de Segurança Cibernética e a Política Nacional de Segurança Cibernética, para fazer frente às ameaças no ciberespaço, que possam afetar a segurança nacional.
Ordem Interno.	Garantir a estabilidade e o normal funcionamento da institucionalidade político-jurídica do Estado.	N°06. Desenvolver tecnologias na prevenção, vigilância e gestão de resposta para a manutenção da ordem interna, ordem pública, segurança do cidadão, proteção da infraestrutura crítica e gestão do risco de desastre, integrando-as em um centro operacional de alcance nacional.
Ações de Desenvolvimento.	Obter níveis sustentados de desenvolvimento, público e privado, em proveito da segurança humana.	N°02. Incentivar a competitividade das empresas na diversidade produtiva na modalidade de <i>clúster</i> , tendo em consideração o setor defeso, incorporando novas tecnologias nas cadeias globais de valor, como consequência de investimentos que possam realizar em pesquisa de ciência e tecnologia. N°03. Incentivar o desenvolvimento em ciência, tecnologia e inovação, prioritariamente nos setores estratégicos da cibernética, energia, alimentação, saúde, ambiental, defesa e interior, com a participação do setor acadêmico.

Fonte: (SEDENA, 2015, tradução nossa, elaborado pelo autor).

Nota: Em relação ao ano 2013.

Outro fator identificado que deu impulso à Política em Segurança e Defesa Nacional, são os compromissos e acordos internacionais assinados no nível *Marco Supranacional* que influenciaram fortemente no *Marco País*, na formulação das políticas no Peru¹⁰³. Entre os principais destacam a Agenda 2030 para o Desenvolvimento sustentável pelas Nações Unidas¹⁰⁴, a OCDE¹⁰⁵ e a Aliança do Pacífico¹⁰⁶.

¹⁰² Disponível em <<https://leyes.congreso.gob.pe/Documentos/DecretosLegislativos/01131.pdf>>. Acesso em 05 de novembro de 2020.

¹⁰³ Olha-se Apêndice VIII – Figura 76.

¹⁰⁴ Disponível em <<https://agenda2030lac.org/en/countries/peru>>. Acesso em 05 de novembro de 2020.

¹⁰⁵ Foi encontrado o Peru em processo de vinculação. Disponível em <<http://www.oecd.org/latin-América/countries/peru/peru-yla-ocde.htm>>. Acesso em 05 de novembro de 2020.

¹⁰⁶ Disponível em <<https://alianzapacifico.net/>>. Acesso em 05 de novembro de 2020.

No âmbito da cooperação bilateral e multilateral da política em segurança cibernética, segundo a *United Nations Institute for Disarmament Research*¹⁰⁷ (UNIDIR), o Peru integrou os seguintes acordos:

Quadro 10 - Cooperação bilateral e multilateral em cybersecurity - Peru

Cooperação Internacional	Descrição	Ano
Resolução do Grupo de Trabalho em cooperação e fortalecimento da Confiança para o Ciberespaço, <i>Inter-American Committee Against Terrorism</i> (CICTE) da OEA.	Apresentado por Chile, Colômbia, Peru, Costa Rica, Canadá, Guatemala e México. Preparar um conjunto de projetos de medidas de fortalecimento da confiança, com base nos relatórios do <i>Group of Governmental Experts</i> (GGE) da ONU para aprimorar a cooperação interestadual, transparência, previsibilidade e estabilidade e para reduzir os riscos de percepção equivocada, escalada e conflito que pode resultar do uso de TICs.	10 Abr 2017
Aliança em cibersegurança para o mútuo progresso - CAMP (Membro)	Comissão nacional de telecomunicações (CONATEL). Plataforma de rede para elevar o nível geral de segurança cibernética dos membros por meio de experiências de desenvolvimento e compartilhamento de tendências.	11 Jul 2016
Memorando de entendimento Peru-Espanha	Cooperação em cibersegurança	08 Jul 2015
Reunião Peru-Estados Unidos	Forças Armadas e Secretaria de Segurança e Defesa Nacional	20-22 Jan 2015
Fórum Global em Cyber Expertise (Membro)	Uma plataforma global para países, organizações internacionais e empresas privadas trocarem as melhores práticas e conhecimentos sobre a construção de capacidade cibernética.	2015

Fonte: (UNIDIR, 2020, tradução nossa).

A partir do ano 2016 aconteceram diversas mudanças organizacionais¹⁰⁸. Por exemplo, a SEDENA foi absorvida pelo MINDEF e incorporaram ao CAEN¹⁰⁹. Em resposta às sugestões do estudo de governança política da OCDE, o desenho estrutural da Presidência do Conselho de Ministros (PCM) foi modificada com a aprovação do Regulamento de Organização e Funções (ROF), criando Secretarias e Subsecretarias.

Segundo o relatório do BID e a OEA (2020, p.142-143) o tema de governo digital, a inovação e a economia digital são do interesse principal no Estado peruano, ressaltando a adesão do Peru na Convenção de Budapeste, que facilitará na cooperação internacional contra a luta do crime informático. Mesmo assim, se ressalta o apoio da OEA no desenvolvimento da política nacional peruana para a segurança cibernética.

¹⁰⁷ Disponível em <<https://unidir.org/cpp/en/states/peru>>. Acesso em 6 de novembro de 2020.

¹⁰⁸ Olha-se Apêndice VIII- Figura 77 e Figura 78.

¹⁰⁹ Em 1950, foi criado o Centro de Altos Estudos do Exército (CAEE), para logo em 1950 ser denominado como o Centro de Altos Estudos Militares (CAEM), é a partir do ano 1997, foi denominado como o Centro de Altos Estudos Nacionais (CAEN), neste centro se capacitam e aperfeiçoam os altos mandos militares das forças armadas no Peru como autoridades e profissionais civis.

Tabela 2 - Dados do relatório da cibersegurança 2020- Peru

Ano 2017	Quantidade Reportada
População	31,444,297
Telefones celulares	38,915,386
Pessoas com acesso à Internet	15,322,061
Porcentagem de penetração da Internet	49%
Número de CIRST	4*

Fonte: (BID, OEA, 2020, p.142, tradução nossa).

Nota: (*) São os seguintes: PeCERT de tipo nacional, o CITELEP, CSTPERU e CSIRT-MGP do tipo militar.

O foco multidimensional da política de segurança e defesa nacional, aprovada em 2017, corresponde a um processo em que foram determinadas as diretrizes gerais para o alcance dos objetivos da segurança e defesa nacional, com base ao estudo da concepção estratégica da segurança e defesa nacional. Também se observa, pela primeira vez, a política busca impulsionar a criação de um sistema nacional de cibersegurança, com participação da sociedade e do setor privado, como o desenvolvimento de tecnologias. Finalmente, esta política comparada às outras do setor, busca orientar a criação de capacidades no âmbito externo, interno e de desenvolvimento humano.

Figura 12 - Foco multidimensional da segurança nacional



Fonte: MINDEF, 2018.

3.11 Historicidade da política em segurança cibernética na Argentina

No caso argentino, observa-se a “ênfase político” da delimitação e diferenciação dos conceitos de segurança e defesa nacional, se deixando de lado definições estabelecidas por organismos internacionais (Por exemplo: OEA e ONU). Por causa da má reputação da Doutrina de Segurança Nacional que conduz à instauração da legitimação do golpe de Estado no ano 1966 e a instauração da ditadura militar. Segundo Míguez (2013, p.65, tradução nossa), “a doutrina de segurança nacional foi utilizada nesse período como argumento contra o comunismo, mas no caso argentino também contra o peronismo, e contra a intervenção do Estado na economia”. No Catálogo dos Documentos do Observatório de Políticas Públicas (OPP) reconhece que em “base na experiência da aplicação da chamada “Doutrina da Segurança Nacional” se prefere delimitar o conceito “segurança”, à segurança da população ou interna e “defesa” à segurança do Estado em relação ao ordem internacional” (OPP, 2005, p.12, tradução nossa).

Conforme às Leis Nº 23554 de Defesa Nacional e Nº 24059 de Segurança Interior, no País se distinguem âmbitos conceituais da defesa nacional relativas às agressões externas de carácter militar (art. 2º, Lei Nº 23554) e da segurança interior (artículos 2º e 4º, Lei Nº 24059) prevenção conjuração e investigação do delito, dentro dos âmbitos terrestres, marítimos e aéreos nos que Argentina exerce jurisdição (UGARTE, 2018, p.67, tradução nossa).

Em base a esse antecedente delimitando o planejamento do emprego da segurança e defesa no ciberespaço, é localizado nos níveis de subsecretaria, diretorias nacionais e coordenações em vários ministérios, estando desintegrada a responsabilidade da cibersegurança nos diversos organismos e instituições.

No ano 1999, se cria o equipe de respostas para incidentes em redes e a coordenação, no âmbito da Subsecretaria de TI, sendo o ArCERT um dos primeiros equipes de respostas nacionais da América Latina e no ano 2004, foi membro do *Forum of Incident Response and Security Teams (FIRST)*¹¹⁰. Os serviços desse time eram para os organismos da administração pública nacional, atuando no nível tático e de suporte técnico, mas não político-estratégica.

A partir dos anos 2000 e 2002, temos identificado as primeiras iniciativas de interesse ao âmbito da segurança e defesa cibernética, as quais estariam relacionadas com a Lei de proteção dos dados pessoais e a assinatura digital (Olhasse

¹¹⁰ Disponível em <<https://www.first.org/about/>>. Acesso em 10 novembro de 2020.

o APÊNDICE II). No ano 2003, a Argentina é declarada pela Comissão Europeia, adequada aos padrões europeus¹¹¹ na proteção dos dados pessoais. Posteriormente, no ano 2004, se estabelece uma Política em Segurança da Informação Modelo, de base para cada organismo do setor público, sendo implementado pela Oficina Nacional de Tecnologias de Informação (ONTI), passando por múltiplas atualizações. Em 2005, é aprovado o Plano Nacional de Governo Eletrônico e os planos setoriais. No ano 2011, se estabelece o Programa Nacional de Infraestrutura de Informação Crítica e *Cybersecurity* (ICIC), adotando um marco regulador na definição e proteção da infraestrutura estratégica e crítica público-privada incluindo às organizações inter-jurisdicionais.

No âmbito da cooperação bilateral e multilateral da política em segurança cibernética, segundo a *United Nations Institute for Disarmament Research*¹¹² (UNIDIR), a Argentina tem sido parte dos seguintes acordos:

Quadro 11 - Cooperação bilateral e multilateral em cybersecurity - Argentina

Cooperação Internacional	Descrição	Ano
Estados Unidos- Argentina. Grupo de trabalho em Ciberpolítica ¹¹³ .	A cargo da Secretaria de Tecnologia e Cibersegurança. Reunião focada nas principais iniciativas em segurança cibernética, incluindo implementação de uma estrutura em política nacional cibernética, proteção de redes, desenvolvimento em capacidades e gerenciamento de incidentes cibernéticos.	23 May 2017
Iniciativa em segurança cibernética OEA (Co-Sponsor)	Aborda questões de segurança cibernética com base em uma abordagem flexível e dinâmica, em políticas de segurança cibernética e a provisão de treinamento adaptado às novas tendências e necessidades em evolução.	16 Abr 2015
Memorando de entendimento Argentina-Espanha	Cooperação em cibersegurança	23 Feb 2015
Ciber cooperação Argentina-Brasil	Acordo sobre reunião bilateral em segurança cibernética, treinamento em guerra cibernética e criação de uma organização bilateral destinada a analisar as ações de cooperação na defesa cibernética.	12-13 Set 2013
Fórum Global em <i>Cyber Expertise (Membro)</i>	Uma plataforma global para países, organizações internacionais e empresas privadas trocarem as melhores práticas e conhecimentos sobre a construção de capacidade cibernética.	2015

Fonte: (UNIDIR, 2020, tradução nossa).

Segundo o relatório do BID e a OEA (2020, p.142-143), a Argentina é uns dos países que têm desenvolvido uma oferta educativa, no público e privado, tendo em consideração a formação especializada em segurança cibernética desde o ponto jurídico e técnico. Também é ressaltado a ratificação de adesão (2018) da Argentina na Convenção de Budapeste, como facilitador na cooperação internacional contra a

¹¹¹ UE 2003/490 da Comissão Europeia do 30 de junho de 2003. Disponível em <<https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32003D0490>>. Acesso em 6 de novembro de 2020

¹¹² Disponível em <<https://unidir.org/cpp/en/states/argentina>>. Acesso em 6 de novembro de 2020.

¹¹³ Disponível em <<https://www.state.gov/joint-statement-on-u-s-argentina-partnership-on-cyber-policy/>>. Acesso em 6 de novembro de 2020.

luta do crime informático, outrossim, é um dos poucos países que participam no Conselho da Europa (CdE), em relação à proteção de dados pessoais automatizado.

Tabela 3 - Dados do relatório da cibersegurança 2020- Argentina

Ano 2017	Quantidade Reportada
População	44,044,811
Telefones celulares	61,897,379
Pessoas com acesso à Internet	32,723,051
Porcentagem de penetração da Internet	74%
Número de CIRST	3*

Fonte: (BID, OEA, 2020, p.50, tradução nossa).

Nota: (*) São as seguintes: MINSEG-CSIRT e BA-CSIRT de tipo Governo, o CERT-UNLP do tipo Acadêmico.

No ano 2010, se cria o Ministério de Segurança tendo na Secretaria de Segurança¹¹⁴, uma Subsecretaria de Investigação do Delito Organizado e Complexo, essa subsecretaria está conformada por três Diretorias, das quais dois atuaram no âmbito cibernético. Sendo a Diretoria Nacional de investigações, responsável primaria das investigações nos *ciberdelitos* e a Diretoria Nacional da Polícia Científica como encarregada das perícias informáticas, estudos científicos e técnicos na descoberta do delito cibernético. Em julho de 2015 com Decreto 1131/2015, é aprovada a Nova Doutrina de Inteligência Nacional, sendo no artigo 8, estabelecida a Comissão responsável da criação do banco de proteção de dados e arquivos de inteligência. Esta doutrina confere que o sistema de inteligência nacional é um observatório dedicado à produção e gestão de conhecimentos das problemáticas relevantes em matéria de defesa e segurança. A Agência Federal de Inteligência (AFI) tem uma estrutura operacional de inteligência, a qual tem uma Diretoria Operacional de Inteligência em Cibersegurança.

Assim, com a criação do Ministério de Modernização¹¹⁵, se busca impulsar uma gestão moderna no desenvolvimento de tecnologias para que sejam aplicadas nos demais setores e de aproximação ao cidadão. O ministério tem uma Subsecretaria de Tecnologia e Cibersegurança, a qual dirige e supervisiona as ações da ONTI, oficina que a partir do 2016, terá uma maior intervenção na formulação das políticas e implementação no marco do Plano da Modernização do Estado. Nesta Subsecretaria

¹¹⁴ Olha-se no Apêndice VIII - Figura 79.

¹¹⁵ Olha-se no Apêndice VIII - Figura 80.

por intermédio de sua Diretoria Nacional de Infraestrutura Críticas de Informação e Cibersegurança, terá a responsabilidade na proteção das infraestruturas críticas e das capacidades de detecção, defesa, resposta e recuperação de incidentes cibernéticos. No 2017, se cria o Comité de Segurança Cibernética agrupado pelos ministérios da Defesa, Ministério de Segurança e o Ministério de Modernização¹¹⁶, com o objetivo de desenvolver a estratégia nacional em segurança cibernética” (BID, OEA, 2020, p.51, tradução nossa). Nesse mesmo ano, é criada a Plataforma Digital com a finalidade que os cidadãos interajam com os serviços do Estado. Logo no ano 2018, com a aprovação da Agenda Digital Argentina, se busca desenvolver capacidades cibernéticas para assim instaurar a confiança nos entornos digitais.

Na Diretiva da Política de Defesa Nacional¹¹⁷, é mostrada a preocupação, de como a desconfiança impacta nas políticas internacionais associadas aos bens globais comuns (*Global Commons*). Para o Estado Argentino a dissuasão tem se recuperado no protagonismo das políticas da defesa dos Estados, mas que é hoje em dia, mais complexa que nos anos da Guerra Fria porque a doutrina militar tem se estendido ao ciberespaço e espaço exterior. A Diretiva em seu Anexo I¹¹⁸ ressalta o uso do ciberespaço argentino com fins militares, onde se expressa a necessidade de adequar as organizações militares, orientando a uma redução das vulnerabilidades emergentes da informatização, devendo ter em consideração a cooperação dos outros setores do Estado, com responsabilidade na política de segurança cibernética. Outro aspecto que merece ser comentado é a permissão que oferece o Estado Argentino aos seus instrumentos militares na priorização em tempo de paz e crises nas operações de vigilância e controle dos espaços soberanos, citando ao ciberespacial dentro deles.

No ano 2019, é aprovada a Estratégia Nacional em Segurança Cibernética onde se declara ao ciberespaço como um domínio que tem de imperar a paz, subtraindo-o dos conflitos armados. A privacidade dos dados das pessoas e das organizações argentinas, e as infraestruturas críticas de informações são citados, como uma preocupação para o exercício de medidas de proteção. Neste mesmo ano é criado o Centro Nacional de Ciberdefesa, que está constituído pela Subsecretaria

¹¹⁶ Hoje em dia é a Secretaria de Governo de Modernização.

¹¹⁷ Decreto 703/2018, DECTO-2018-703-APN-PTE. Disponível em <<https://www.boletinoficial.gob.ar/detalleAviso/primera/189076/20180731>>. Acesso em 09 novembro de 2020.

¹¹⁸ Disponível em <<https://www.boletinoficial.gob.ar/detalleAviso/primera/189076/20180731>>. Acesso em 09 novembro de 2020.

de Ciberdefesa, o Centro de Respostas frente a Emergências Informáticas do Ministério da Defesa (CSIRT Defesa), o Centro Inteligente de Operações em Segurança (iSOC) e o Laboratório de Análise Cibernéticos (CyberLab). Além disso, o BID aprova um empréstimo em respaldo às reformas políticas e mudanças institucionais na “implementação de políticas relacionadas com as infraestruturas críticas, segurança dos dados pessoais, e boas práticas no uso das TIC” (BID, OEA, 2020, p.51, tradução nossa), esses tipos de empréstimos são denominados de *Policy-Based Loans*¹¹⁹ (PBL).

Quadro 12 - Os princípios e objetivos da estratégia nacional em segurança cibernética - Argentina

Princípios Retores	Objetivos
Princípio 1: Respeito pelos direitos e liberdades individuais.	Objetivo 1: Consciência no uso do ciberespaço
Princípio 2: Liderança, construção de capacidades e fortalecimento federal.	Objetivo 2: Capacitação e educação no uso seguro do ciberespaço.
Princípio 3: Integração internacional.	Objetivo 3: Desenvolvimento do marco normativo.
Princípio 4: Cultura em segurança cibernética e responsabilidade. Compartilhada	Objetivo 4: Fortalecimento de capacidades na prevenção, detecção e resposta.
Princípio 5: Fortalecimento do desenvolvimento socioeconômico.	Objetivo 5: Proteção e recuperação dos sistemas de informação do setor público.

Fonte: Estratégia Nacional de Ciberseguridad de la República de Argentina, 2018, tradução nossa.

A Subsecretaria de Ciberdefesa no Ministério da Defesa é responsável da elaboração da política de ciberdefesa, devendo estar constituída por quatro linhas de ação em harmonia aos três eixos da política, bem como, elaborar o Plano de Infraestruturas Críticas Cibernéticas Nacional e o Plano de Adequação das Organizações Militares. Além dessas mudanças organizacionais e administrativas acontecidas nos últimos anos, são criadas a Diretoria do Cibercrime no Ministério de Segurança e as unidades especializadas de fiscais no cibercrime.

3.12 Historicidade da política em segurança cibernética no Brasil

Ao igual que na Argentina, relativamente diferente do Peru¹²⁰, se observa que a aplicação da Doutrina de Segurança Nacional no Brasil, incitou ao golpe militar do 31 de março de 1964, se instaurando uma ditadura militar no Brasil, que conduz uma política totalitarista na procura de ajuste aos moldes da DSN. Ademais, no Artigo N° 91 da Constituição do Brasil, se constitui o Conselho de Defesa Nacional (CDN) que

¹¹⁹ Disponível em <<https://www.iadb.org/en/about-us/public-sector-financing/policy-based-lending-category>>. Acesso em 15 de setembro de 2020.

¹²⁰ Lê-se o parágrafo 2.1. Historicidade da segurança e defesa nacional na América do Sul.

é presidido pelo Presidente da República. Existe também uma base legal de Defesa constituída pela Política Nacional de Defesa, a Estratégia Nacional de Defesa e o Livro Branco de Defesa Nacional. Pela Lei Complementar N° 136/2010, o Poder Executivo a cada quatro (04) anos encaminha aqueles documentos, para a apreciação das devidas atualizações ao Congresso Nacional, estando pela terceira vez, atualizados neste ano 2020.

Quadro 13 - Base legal de defesa brasileira

Base Legal	Descrição
Política Nacional de Defesa (O que fazer)	-Ambiente Nacional e Internacional. -Concepção Política de Defesa. -Oito (08) Objetivos Nacionais de Defesa.
Estratégia Nacional de Defesa (O como fazer)	-Poder Nacional. -Capacidades Nacionais de Defesa. -Base industrial de Defesa. -Dezoito (18) Estratégias de Defesa.
Livro Branco de Defesa	Trata os seguintes tópicos: o ambiente estratégico do século XXI, o Estado brasileiro e a defesa nacional, a defesa e o instrumento militar, defesa e sociedade, a transformação da defesa, economia da defesa.

Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

Em relação ao corpus documental brasileiro se observa que as competências na segurança e defesa nacional, no âmbito cibernético, é descentralizada e tratada por diversos organismos públicos¹²¹. “De fato, os conceitos de segurança e defesa são complementares” (Da Cruz, 2013, p.9). Existindo ações desde os níveis político, estratégico, operacional e tático, se incluindo ao setor privado. No ano 2000, com Decreto N° 3505/2000¹²², se institui a Política de Segurança da Informação nas entidades da Administração Pública Federal. Portanto, no ano 2006, se institui o Departamento de Segurança da Informação e Comunicações (DSIC) no Gabinete de Segurança Institucional da Presidência da República (GSIPR), sendo o DSIC responsável de estabelecer os critérios, procedimentos e aprovações sobre a gestão de Segurança da Informação e Comunicações no âmbito da Administração Pública Federal (AFP). É evidenciado (Olha se o Apêndice IV) que nos anos seguintes, o interesse pela segurança e defesa cibernética vai tomando força no nível político e estratégico do Brasil. Uma dessas ações, por exemplo, é o workshop em parceria com a OEA (2009) sobre o desenvolvimento de uma Estrutura Nacional para a Segurança Cibernética. Nesse mesmo ano são publicadas as diretrizes para a elaboração da

¹²¹ Olha-se Apêndice VIII – Figura 81.

¹²² Disponível em <http://www.planalto.gov.br/ccivil_03/decreto/d3505.htm>. Acesso em 6 de novembro de 2020. Decreto que foi revogado pelo Decreto N° 9637/2018.

política e gestão de riscos de segurança da informação, como também, a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais da AFP.

No ano 2010, o GSIPR faz o lançamento do Livro Verde Segurança Cibernética no Brasil onde se apresentam as potenciais diretrizes estratégicas para o estabelecimento da Política Nacional de Segurança Cibernética, ademais foi apresentada a Guia para a segurança das infraestruturas críticas de informação que dita as melhorias práticas e promove a cultura de segurança das infraestruturas críticas de informação. Em agosto, no mesmo ano, o Exército Brasileiro criou o Centro de Defesa Cibernética (CDCiber), estando em operação a partir do ano 2011, Centro que adquiriu visibilidade e maior participação nos eventos internacionais, atuando na gerência da segurança e defesa cibernética, o que aumentou seu orçamento de 2012 em 20% (Da Cruz, 2013, p.25). Ademais dos acontecimentos citados o Exército Brasileiro tem utilizado a capacidade industrial nacional para desenvolver ferramentas estratégicas dentro do programa de segurança nacional” (Da Cruz, 2013, p.26), se estabelecendo acordos e parcerias locais privadas, no âmbito da segurança cibernética.

Em novembro de 2012, foi publicada a Lei nº 12.737/2012¹²³ (Lei Carolina Dieckmann) sendo um marco inicial que regulamenta os crimes cibernéticos, oferecendo proteção legal contra invasão de dispositivos e crimes associados à manipulação e ao furto de dados digitais. Portanto, em suas limitações tecnológicas os especialistas apontam que a lei não cobre de forma eficaz todos os tipos de crimes cibernéticos que surgiram posteriormente, como golpes complexos envolvendo criptomoedas, *deepfake* ou novos tipos de ataques cibernéticos.

Em maio de 2013, sendo públicos os casos de espionagem internacional protagonizado por Edward Snowden e o governo norte-americano¹²⁴, deram origem a diversas denúncias de infiltrações nas comunicações governamentais brasileiras como nos outros países sul-americanos.

Novos documentos apontaram o Brasil como um dos alvos preferenciais do serviço de inteligência norte-americano. Brasília teria inclusive sediado, pelo menos até 2002, uma das 16 bases de espionagem da NSA ao redor do mundo. A embaixada do Brasil em Washington e a missão do Brasil na Organização das Nações Unidas (ONU) estariam entre os espionados (CPI ESPIONAGEM, 2013, p.13)

¹²³ Lei nº 12.737/2012 - Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm> Acesso em 9 de agosto de 2024.

¹²⁴ Edward Snowden, público documentos secretos vazados, ligados à Agência de Segurança Nacional dos Estados Unidos (*National Security Agency*- NSA) e a Central de Inteligência Americana (*Central Intelligence Agency* - CIA)

No 2014 em consequência desses acontecimentos é sugerido, no relatório final, ao Poder Executivo Federal a criação do Grupo de Trabalho com a finalidade de elaborar uma Política Nacional de Segurança Cibernética. No mesmo ano, é realizado o Acórdão do Tribunal de Contas da União – Plenário, se apontando a necessidade de um planejamento estratégico e de coordenação com os atores responsáveis pela segurança da informação, estando em evidência o interesse, no nível político e estratégico, de uma segurança cibernética nacional. Nesse mesmo ano, o Marco Civil da Internet¹²⁵ (MCI) ou também chamada Constituição da Internet Brasileira foi aprovada, sendo desenvolvidos dez princípios, como a neutralidade da rede, a liberdade de expressão e a privacidade, direitos aos cidadãos - online e offline (Arnaudo, “s.d”).

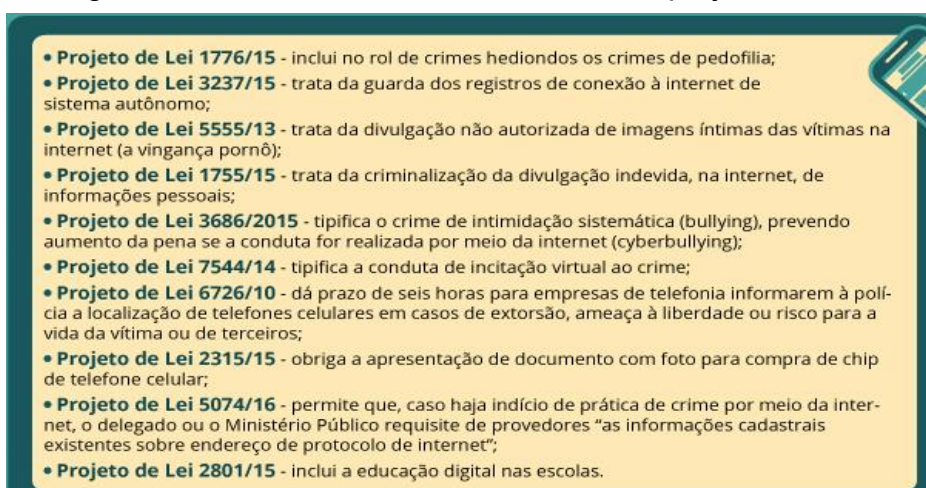
No relatório final da Comissão Parlamentar de Inquérito (CPI) dos Crimes cibernéticos no 2016, são apresentadas diversas indicações as quais são: A melhoria da segurança da infraestrutura de TI da administração pública. O Banco Central regule o combate ao crime cibernético, devendo compartilhar informações com a Polícia Federal (PF) e a Federação Brasileira de Bancos (FEBRABAN). A adoção de medidas regulada pelo Ministério da Justiça no combate ao crime cibernético e de criação de varas especializadas em crimes cibernéticos. A inclusão obrigatória da educação digital em escolas de ensino fundamental e médio. A identificação de usuários da Internet pela Anatel. Consequentemente, observa-se na CPI, a sugestão de diversos projetos de Lei (Figura N° 29). Adicionalmente, é aprovada a investigação de crimes contra a ordem tributária, a três empresas multinacionais norte-americanas com sedes em território brasileiro: Facebook, Twitter e Yahoo, pelo motivo que elas, não recolhem o Imposto Sobre Serviços (ISS) e o Imposto sobre a Circulação de Mercadorias e Prestação de Serviços (ICMS) no Brasil. Depois de múltiplas reuniões pelo grupo de trabalho, congregando a diversos setores do Estado. Em maio de 2017, é feita a entrega da proposta de Política Nacional de Segurança da Informação (PNSI) ao Ministro do GSI/PR, sendo aprovada no ano seguinte. No ano 2018, foi publicada a Lei nº 13.709/2018¹²⁶, conhecida como a Lei Geral de Proteção de Dados (LGPD),

¹²⁵ Lei nº 12.965 de 23 de abril de 2014, estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Disponível em < <https://legislacao.presidencia.gov.br/atos/?tipo=LEI&numero=12965&ano=2014&ato=93eUTRE9ENVpWTdb6> > . Acesso em: 29 agosto de 2024.

¹²⁶ Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em < https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm > . Acesso em: 19 de agosto de 2024.

onde a legislação brasileira regula o tratamento de dados pessoais em qualquer contexto, seja online ou offline, sendo inspirada no Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia. Na LGPD são estabelecidas as diretrizes e regras sobre como dados pessoais devem ser coletados, armazenados, processados e compartilhados, buscando garantir maior transparência e controle para os cidadãos brasileiros sobre suas informações pessoais.

Figura 13 - A CPI dos crimes cibernéticos: projetos de leis



Fonte: Disponível em <<https://www.camara.leg.br/noticias/486622-relatorio-da-cpi-de-crimes-ciberneticos-preve-fiscalizacao-da-anatel/>>. Acesso em 10 de novembro de 2020.

No âmbito da cooperação bilateral e multilateral da política em segurança cibernética, segundo a *United Nations Institute for Disarmament Research*¹²⁷ (UNIDIR), o Brasil tem sido parte dos seguintes acordos:

Quadro 14 - Cooperação bilateral e multilateral em cybersecurity - Brasil

Cooperação Internacional	Descrição	Ano
Cooperação Europol-Brasil	Acordo estratégico para cooperar no combate ao crime cibernético e outras atividades criminosas transfronteiriças.	Abr 2017
Consultas cibernéticas Alemanha-Brasil	Consultas bilaterais entre os representantes dos dois governos. Representantes do nível decisor de empresas, academia e sociedade civil.	22-23 Fev 2016
Declaração Conjunta, Estados Unidos-Brasil. Ministério do Desenvolvimento, Indústria e Comércio Exterior.	Atualização do Memorando de Entendimento, que abordará a colaboração estratégica e os padrões na medição do tempo e frequência, cibersegurança, smart grid, sistemas ciberfísicos.	19 Nov 2015
16ª Reunião da Comissão Conjunta, estrutura do acordo para a cooperação Brasil-Estados Unidos. Ministério das Relações Exteriores.	Versão do comunicado final, no futuro estabelecimento do diálogo Brasil-Estados Unidos sobre política cibernética internacional.	28 Abr 2015
Ciber cooperação Argentina-brasil.	Acordo sobre reunião bilateral de segurança cibernética, treinamento em guerra cibernética e criação de uma organização bilateral destinada a analisar a defesa cibernética nas ações de cooperação.	12-13 Set 2013
Cooperação Brasil-Turquia. Ministério da Defesa.	Criação de cinco grupos de trabalho para o estudo de parcerias nos diferentes setores, incluindo a defesa cibernética.	22 Ago 2013

¹²⁷ Disponível em <<https://unidir.org/cpp/en/states/argentina>>. Acesso em 6 de novembro de 2020.

Fonte: (UNIDIR, 2020, tradução nossa).

Segundo no relatório do BID e a OEA (2020, p.23) no ano 2018, foi efetuada a avaliação seguindo o modelo de maturidade da capacidade, desenvolvido pelo GCSCC¹²⁸. Um dos pontos resultantes do relatório é que as partes interessadas na proteção da infraestrutura crítica pública têm cooperado e coordenando, através dos canais formais de comunicação com o Ministério da Defesa. Outrossim, o CERT Nacional (CERT.br) é o “responsável principal em conduzir os relatórios de incidentes a nível nacional e as atividades nas redes brasileiras” (BID, OEA, 2020, p.71, tradução nossa). No que corresponde, ao crime cibernético, o Brasil participa como observador na Convenção de Budapeste. Na cultura de segurança cibernética, o relatório deixa evidenciado que o setor financeiro e das TIC estão mais avançados em segurança cibernética. Porém, a sociedade em conjunto ainda carece de uma mentalidade em segurança cibernética” (BID, OEA, 2020, p.71, tradução nossa).

Tabela 4 - Dados do relatório da cibersegurança 2020 - Brasil

Ano 2017	Quantidade Reportada
População	207,833,831
Telefones celulares	218,255,041
Pessoas com acesso à Internet	140,228,155
Porcentagem de penetração da Internet	67%
Número de CIRST	2*

Fonte: (BID, OEA, 2020, p.70, tradução nossa).

Nota: (*) São as seguintes: CIRTGov de tipo Governo e o CERT.br do tipo Nacional.

Segundo o analisado o Exército Brasileiro, como coordenador responsável da proteção cibernética, tem buscado articular com os diversos atores públicos-privados. Assim, existe uma segregação entre as ações de segurança da informação e da defesa cibernética. Sendo o GSI/PR quem dirige a Segurança da Informação e o CDCiber/EB/MD a defesa cibernética. Se constituindo, neste caso, dois órgãos autônomos que irão priorizar seus objetivos conforme às necessidades e regulamentações de seus setores. Além disso, se observa uma similitude no caso peruano, em que cada força armada possui sua própria unidade de proteção

¹²⁸ Lê-se o parágrafo: 2.8. As capacidades cibernéticas e os modelos de maturidade.

cibernética, e que poderia ser contraproducente na gestão do conhecimento e de recursos a serem empregados, si não se dispõem de uma integração robusta e canais de comunicação escaláveis e oportunos.

3.13 Síntese dos reflexos observados no referencial teórico

Com o intuito de estreitar as relações entre a segurança nacional e o âmbito cibernético, o referencial teórico trouxe em discussão, a historicidade da doutrina da segurança nacional no contexto da América do Sul e da criação do Internet, trazendo em relevância ao ciberespaço na atual doutrina norte-americana. Para demonstrar os diferentes papéis e responsabilidades assumidos pelos Estados na criação de suas políticas nacionais em segurança cibernética. Desde o papel desempenhado pelos Estados, se trouxe em análise as teorias, conceitos e perspectivas da geopolítica contemporânea (as novas geopolíticas), porém delimitou-se o posicionamento visto no ciberespaço como um Global common. Sendo focalizados os mecanismos de controle e das relações de poder no domínio cibernético, buscando analisar desde a perspectiva da hegemonia político-tecnológica das potências, da dominação e competição econômica e do capitalismo informacional. Por outro lado, da coleta bibliográfica digital, publicada pelos governos de Peru, Argentina e Brasil, limitados entre os anos 2000 e finais de setembro de 2020, foram analisadas e descritas a historicidade das Políticas e Estratégias em Segurança Cibernética dos três países estudados, para depois nos próximos capítulos aprofundar nos objetivos de pesquisa.

Para facilitar a interpretação e construção das ideias, vamos resumir a continuação os principais reflexos observados neste capítulo:

Quadro 15 - Síntese dos principais reflexos observados no referencial teórico

Tópico	Principais Reflexos
2.1. Historicidade da segurança e defesa nacional da América do Sul.	• Posteriormente à criação dos novos Estados, se deram diversos intentos de unificação entre as ex-colônias espanholas. • O Tratado Continental, buscava uma união tendo em consideração a origem, os vínculos e as relações entre seus povos. • No Tratado Continental, se somam novos países, como uma reação aos corsários da América Central, com o objetivo de não ceder ou alienar seus territórios a outro Estado, se limitando, em participar em atos de hostilidade mútua sem ter esgotado os meios pacíficos de resolução de conflitos. • A Argentina não aceitou se aderir ao Tratado Continental, com o argumento, que a ação da Europa tem sido sempre de “protetor e civilizador”. • A iniciativa dos Estados Unidos, se cria a União Internacional das Repúblicas Americanas, a partir de 1948, será a Organização de Estados Americanos (OEA). • No marco inicial da Guerra Fria, foram criados diversos projetos políticos norte-americanos para a América Latina; com os princípios de conter a expansão do comunismo. • O TIAR foi com a finalidade, no caso em que uma potência extracontinental ataca para algum país do acordo, se conformando com um sistema de segurança coletiva. • Na Guerra das Malvinas, os países de Chile, Colômbia e os Estados Unidos não foram assinantes no TIAR, para brindar o apoio à Argentina. • A participação do Brasil não tem sido reflexo de uma política externa intermediária nos

	dissentimentos originados com a segurança dos países Sul-americanos. • países como Brasil e Argentina tinham iniciado entre os anos de 1930, um desenvolvimento industrial militar para a produção de armamento, fuzis, tanques e aviões. Porém o distanciamento tecnológico foi aumentando a partir do ano de 1945. • América do Sul é apontado como uma região com baixa incidência de conflitos internacionais. • Desde 1990, se observam iniciativas que buscam a integração da América do Sul, e de mecanismos que garantem a paz e a construção da confiança, para possibilitar a estabilidade democrática e o desenvolvimento na região. • No sentido de dispor de mecanismos próprios para uma governança da América do Sul de segurança, sem interferência dos Estados Unidos foi expressa na abordagem holística tomada pelo Conselho Sobre o Problema Mundial da Drogas (CSPMD). • No ano de 2008, se criou o Conselho da Defesa Sul-americano (CDS). A partir da iniciativa incentivada pelo Brasil, se cria na região um organismo especializado em defesa para o desenvolvimento de funções múltiplas, buscando encontrar maneiras de articular necessidades comuns aos países da América do Sul. • No Mercosul no 16 de setembro de 2008, é exposta a intenção em construir uma autonomia e integração industrial no âmbito da defesa¹²⁹. A estratégia de desenvolvimento condiciona e motiva a estratégia da defesa, e a estratégia da defesa proporciona um escudo para a estratégia de desenvolvimento¹³⁰. • Outro fator que deve ser abordado na segurança nacional da América do Sul é a instabilidade política dos países membros, existindo a dificuldade de consolidar seus sistemas democráticos.
2.2. Historicidade do ciberespaço através da internet.	• O ciberespaço tem que ser reconhecido como um território de domínio semelhante à terra, mar e ar no relativo à guerra. • A doutrina militar nas operações do ciberespaço do Departamento da Defesa dos Estados Unidos (DoD), define o ciberespaço como um domínio que atinge fronteiras geográficas e geopolíticas. • Nos primeiros anos da Internet, este foi desenvolvido com o esforço, mas independente, de pessoas do setor do governo e acadêmico dos Estados Unidos. • A evolução tecnológica da Internet deu início com pesquisas sobre computação de pacotes e ARPANET. • Também se tinha outra pronúncia sobre o conceito de redes de pacotes, feito no Reino Unido, pelo Donald Davies e Roger Scantlebury no <i>National Physical Laboratory</i> (NPL). • A finais de 1969, se tinham quatro hosts conectados na ARPANET inicial. • Devemos destacar que a pesquisa sobre redes incorporava o trabalho sobre a rede subjacente e sobre como usar a rede, sendo uma tradição que até a atualidade continua. • Em 1972, Kahn organizou uma apresentação da ARPANET, sendo muito exitosa na International Computer Communication Conference (ICCC), seria a primeira apresentação pública desta nova tecnologia de redes. • Em 1972, foi introduzida a aplicação "hot" inicial, o e-mail.
2.3. A Doutrina da Segurança Nacional (DSN) dos Estados Unidos, no âmbito do ciberespaço.	• A DSN tem uma visão globalizada em seu emprego e se ajusta rapidamente aos cenários e riscos estratégicos. • A DSN não só está orientada no desenvolvimento das capacidades militares, mas também fortalece a capacidade dos outros departamentos e agências governamentais. • A <i>Joint Publication 1 - Doctrine for the Armed Forces</i>, faz uso de uma análise histórica do uso dos instrumentos e mecanismos de poder militar nas operações e lições contemporâneas. • O Presidente dos Estados Unidos, é quem aprova a Estratégia de Segurança Nacional (<i>National Security Strategy</i> – NSS), sendo ele a máxima autoridade com as facilidades para o uso das forças armadas e de todos os instrumentos do poder nacional: diplomático, informacional, militar e econômico. • A construção da ação conjunta são atividades integradas e sincronizadas das forças militares com as organizações não militares, agências e o setor privado para o alcance dos interesses e objetivos nacionais. • O ciberespaço é incorporado nos esforços da segurança nacional norte-americana sendo parte dos cálculos estratégicos, dos elementos estruturais e geopolíticos. • A definição doutrinária da estratégia cibernética (Cyber Strategy) é o desenvolvimento e emprego das capacidades estratégicas para operar no ciberespaço, integrando e coordenando com outros domínios operacionais para alcançar e apoiar na conquista de objetivos através dos elementos de poder nacional em apoio à Estratégia de Segurança Nacional. • O poder cibernético é para apoiar a realização dos objetivos; servindo como meio na satisfação das necessidades vitais e interesses nacionais da estratégia de segurança nacional. • Em 2009, se criou a United States Cyber Command (USCyberComm), como organismo responsável pelas coordenações na prevenção e defesa cibernética norte-americana. • A autoridade que vem exercendo o comando da USCyberComm, exerce função de Diretor na National Security Agency (NSA), e Chefe na Central Security Agency (CSS). • Desde uma perspectiva geopolítica global, nota-se que a DSN faz menção a seis Comandos. • Para o exercício do controle no ciberespaço, não necessariamente implica estar dentro das fronteiras geográficas associadas à nacionalidade do ator ou proporcional à influência geopolítica do ator. • Devido aos rápidos avanços em tecnologia, especialmente na área da informação, o ambiente geoestratégico de hoje se tornou cada vez mais complexo e se tornará ainda mais, no futuro.

¹²⁹ Disponível em <<https://nuso.org/articulo/o-brasil-e-a-criacao-do-conselho-de-defesa-sul-americano-uma-convergencia-de-vantagens/>>. Acesso em 6 de novembro de 2020.

¹³⁰ Disponível em <<https://www.gov.br/defesa/pt-br/arquivos/2012/mes07/end.pdf>>. Acesso em 6 de novembro de 2020.

2.4. Inferências iniciais da DSN cibernética dos Estados Unidos.	• A DSN cibernética dos Estados Unidos, passou a usar todo seu conhecimento e tecnologia produzida a partir da Internet e do ciberespaço para subsidiar a conquista de seus interesses militares, geopolíticos e econômicos. • Dispor de uma predominante capacidade cibernética é crucial para os Estados progredirem e se desenvolverem no social, cultural, econômico e política. • A segurança cibernética vai se situar e integrar nos mecanismos e instrumentos da segurança nacional.
2.5. A política de segurança cibernética nos diferentes papéis do Estado.	• O papel do Estado (nos países democráticos) na política de segurança cibernética, tem um espaço político de três dimensões: teórico, empírico e normativo. • Historicamente se olha um desenvolvimento dos papéis do Estado e que é aditivo. • O Estado aparece como o proprietário das redes ameaçadas (proprietário). • O Estado aparece como o ator que deve resolver o problema em termos de política de segurança (Proprietário do Problema). • O Estado ou estruturas dentro do Estado (unidades individuais) aparecem como criador do problema (Originador do Problema). • Os conflitos de papéis são tratados nas democracias, na esfera dos níveis político-estratégico, devendo ser abordado sistematicamente.
2.6. A geopolítica contemporânea: as disputas do poder mundial são econômicas?	• Nas últimas décadas, a correlação de forças e as inúmeras facetas das relações de poder tem gerado uma revalorização dos clássicos estudos geopolíticos. • A posição central do Estado, como único ator ou agente, na geopolítica contemporânea tem mudado, existindo novos atores ou sujeitos, como são as organizações internacionais, empresas multinacionais, blocos de mercados regionais, entre outros. • A competição dos Estados não seria mais a ideológica ou bélica, mas sim a conquista dos mercados e das tecnologias de informação e da comunicação. • Para entender o sistema global, a chave seria entender as relações de poder, tendo como fundamento a economia capitalista mundializada. • A nova postura da geopolítica contemporânea, em relação à clássica, de aprofundar seus estudos nos âmbitos da dominação e competição econômica.
2.7. O ciberespaço, é um global common?	• Um grupo de especialistas tem categorizado o ciberespaço como um Global Commons. • É demonstrado que ambos os conceitos (Pardo e Hardin), tiveram dimensões não liberais e imperiais. • “Estamos testemunhando uma espécie de “afeganização” do ciberespaço, com bolhas de segurança e insurgência” • É de importância a compreensão do exercício dos mecanismos de dominação e poder sobre os Global Commons, neste século XXI. • A construção do ciberespaço é financiada por empresas multinacionais, governos com hegemonia político-tecnológica ou grupos de poder. • A existência de iniciativas no âmbito cibernético para o controle e observação por meio do emprego das redes, estão vinculadas com Estados que dispõem do potencial e de capacidades cibernéticas.
2.8. Os elementos estruturais para a construção do ciberespaço.	• Além de sua natureza artificial, o ciberespaço requer essencialmente dos seguintes componentes para sua constituição e materialização: infraestrutura; dados, informação e conhecimento; automação e inteligência; conectividade global e controle. • O desenvolvimento das TIC, tem gerado a digitalização das organizações estabelecendo essa ponte com a sociedade da informação. • Observa-se que os governos e organismos internacionais, coincidem nos benefícios que as iniciativas em infraestrutura em TIC irão oferecer desenvolvimento econômico e social nos países. • As ameaças cibernéticas têm sua origem desde a própria criação do ciberespaço. • Na sociedade informacional, a premissa é que “a informação por si só tem um valor capaz de gerar poder político, econômico e social. • A informação compreendida desde a perspectiva da economia informacional, analisa as relações dos agentes econômicos em situações em que existe uma desigual distribuição da informação, conhecida também como assimetria da informação. • Se pode observar, que a intensiva existência da automação nos países desenvolvidos, como nos Estados Unidos, França, Alemanha, Reino Unido, China etc., está criando um problema sério de desemprego, sobre exploração e exclusão social, nos países da América Latina. • O ascenso do informacionalismo no final do século XX, nos apresenta um ciberespaço “naturalizado” ao processo da globalização, devido às diversas vantagens que ele trouxe no processo globalizador, especialmente como meio de integração e de comunicação global, financeira e comercial. • É essencial analisar as práticas informacionais aplicadas no ciberespaço, onde a construção do objeto informacional é complementada com as estruturas materiais e simbólicas de um dado universo cultural.
2.8. As capacidades cibernéticas e os modelos de maturidade	• As capacidades cibernéticas são um instrumento chave, para garantir um adequado nível de segurança cibernética. • A definição das capacidades cibernéticas se relaciona com os recursos e ativos disponíveis que se encontram à disposição de um Estado, para resistir ou projetar sua influência por meio do ciberespaço. • As capacidades cibernéticas não podem ser categorizadas logicamente como armas ou meios de guerra cibernética. • A implementação do CMM na categorização do estado de maturidade da segurança cibernética, não é transversal às problemáticas vigentes dos países em vias de desenvolvimento.
2.9. Historicidade da política em	• O cargo de Presidente da República teria a direção do Sistema da Defesa Nacional. • Em 1994, o Peru se conecta à Internet fazendo uso de um satélite, sendo a Rede Científica

segurança cibernética no Peru.	Peruana. • No ano 1995, o Peru tem acesso aos domínios da World Wide Web (WWW). • Em 2003, foi criado o Escritório de Governo Eletrônico (ONGEI) • Em 2005, se criou a divisão encarregada de atender os casos de delitos informáticos na Polícia Nacional do Peru. • Em 2009, se criou o PeCERT, para a atenção aos incidentes cibernéticos de escala nacional. • Em 2012, foi criada a Secretaria de Segurança e Defesa Nacional (SEDENA) como a responsável de articular a Política de Segurança e Defesa Nacional. • O governo digital, a inovação e a economia digital são do interesse principal no Estado peruano.
2.10. Historicidade da política em segurança cibernética na Argentina.	• A “ênfase político” da delimitação e diferenciação dos conceitos de segurança e defesa nacional, se deixando de lado definições estabelecidas por organismos internacionais. • O planejamento do emprego da segurança e defesa no ciberespaço, é localizado nos níveis de subsecretaria, diretorias nacionais ou coordenações de vários ministérios, estando desintegrada a responsabilidade da cibersegurança nos diversos organismos e instituições. • Em 1999, foi criado o ArCERT, um dos primeiros times de respostas nacionais da América Latina. • Entre os anos 2000 e 2002, foram as primeiras iniciativas de interesse ao âmbito da segurança e defesa cibernética, relacionadas com a Lei de proteção dos dados pessoais e a assinatura digital. • Em 2005, é aprovado o Plano Nacional de Governo Eletrônico e os planos setoriais. • No ano 2011, se estabelece o Programa Nacional de Infraestrutura de Informação Crítica e Cybersecurity (ICIC). • Argentina é uns dos países que têm desenvolvido uma oferta educativa, no público e privado, tendo em consideração a formação especializada em segurança cibernética desde o ponto jurídico e técnico. • No ano 2010, se criou o Ministério de Segurança tendo na Secretaria de Segurança, uma Subsecretaria de Investigação do Delito Organizado e Complexo. • A Agência Federal de Inteligência (AFI) tem uma estrutura operacional de inteligência, a qual tem uma Diretoria Operacional de Inteligência em Cibersegurança. • Em 2017, se criou o Comité de Segurança Cibernética, integrado pelos ministérios da Defesa, Ministério da Segurança e o Ministério da Modernização. • Na Diretiva da Política de Defesa Nacional, é mostrada a preocupação, de como a desconfiança impacta nas políticas internacionais associadas aos bens globais comuns (Global Commons). • No ano 2019, é aprovada a Estratégia Nacional em Segurança Cibernética onde se declara ao ciberespaço como um domínio onde se tem que imperar a paz, subtraindo-o dos conflitos armados. • A Subsecretaria de Ciberdefesa no Ministério da Defesa é responsável pela elaboração da política de ciberdefesa.
2.11. Historicidade da política em segurança cibernética no Brasil.	• Se constitui o Conselho de Defesa Nacional (CDN) que é presidido pelo Presidente da República. • As competências na segurança e defesa nacional, no âmbito cibernético, é descentralizada e tratada por diversos organismos públicos. • No 2000, se institui a Política de Segurança da Informação nas entidades da Administração Pública Federal. • No 2006, se institui o Departamento de Segurança da Informação e Comunicações (DSIC) no Gabinete de Segurança Institucional da Presidência da República (GSIPR). • O interesse pela segurança e defesa cibernética vai tomando força no nível político e estratégico do Brasil. • Em 2010, o GSIPR fez o lançamento do Livro Verde Segurança Cibernética no Brasil. • Em agosto deste mesmo ano, o Exército Brasileiro criou o Centro de Defesa Cibernética (CDCiber). • O Exército Brasileiro tem utilizado da capacidade industrial nacional para desenvolver ferramentas estratégicas para o programa de segurança nacional. • O CERT Nacional (CERT.br) é o responsável principal em conduzir os relatórios de incidentes a nível nacional e as atividades nas redes brasileiras. • Existe uma segregação entre as ações de segurança da informação e de defesa cibernética.

Fonte: Elaboração pelo autor com dados do capítulo, Referencial Teórico.

Assim concluímos nosso referencial teórico, para que no próximo capítulo, podamos descrever os procedimentos metodológicos adotados na confecção da presente tese.

“Las ideas se exponen, no se imponen”

Gral. EP. José del Carmen Marín Arista

4 METODOLOGIA

Este capítulo destina-se a descrever os aspectos metodológicos que constituem a elaboração desta tese. Nas próximas linhas, serão apresentadas as regras e procedimentos sistemáticos na busca de explicar e descrever os mecanismos e relações que sejam do interesse da nossa pesquisa.

Inicialmente, o processo de estruturação da tese se cimentou nas pesquisas e coleta de documentações digitais relacionadas ao tema, buscando identificar o provável “Estado da Arte”. Por essa razão, segundo o Apêndice I, foram coletados e analisados os documentos oficiais digitais da segurança e defesa norte-americana, como também dos documentos relacionados à capacidade cibernética, no âmbito da doutrina militar conjunta norte-americana. Sendo nossa primeira análise o caso protótipo norte-americano.

À vista disso, se fizeram as pesquisas e coleta das documentações que evidenciem a historicidade e os agentes envolvidos nas iniciativas acontecidas dos três países Sul-americanos: Argentina (olhe-se o Apêndice II), Peru (olhe-se o Apêndice III) e Brasil (olhe-se o Apêndice IV) tendo como foco de estudo às políticas e estratégias em segurança cibernética, limitados entre os anos 2000 e finais de setembro de 2020.

4.1 Tipologia da pesquisa

A problemática de nossa investigação é de natureza social, iniciando nosso problema de pesquisa com as seguintes questões: Que elementos influenciam na consolidação de uma Política de Segurança Cibernética? e Como eles são considerados nas especificidades geopolíticas da América do Sul, no âmbito cibernético? Para a análise do problema, considerou-se conveniente que fosse abordada sob as diretrizes de uma investigação qualitativa¹³¹, do tipo de investigação

¹³¹ Alguns pesquisadores vão considerar a análise a partir de uma metodologia quantitativa, insuficiente para recuperar aspectos subjetivos dentro do processo informacional ou que o método limite ao rigor do cálculo a realidade. Uma posição contrária dos pesquisadores, defendem o uso desse método pelas suas características objetivas, distanciando dos valores do pesquisador em face do objeto, como diz Durkheim (1999).

explicativa, porque necessitaremos lidar como os vínculos operacionais que precisam ser traçados ao longo do tempo, mais do que as meras frequências ou incidências (Yin, 2015, p.11), procurando conectar as ideias e teorias para compreender as causas e efeitos.

A tese foi elaborada tendo como suporte o delineamento para um estudo quantitativo e qualitativo. A abordagem quantitativa é confirmada na frequência que aparecem nos determinados elementos da mensagem, obtendo-se dados descritivos por meio de um método estatístico, sendo mais objetiva, fiel e exata. A abordagem qualitativa, corresponde a um processo mais intuitivo, maleável e adaptável aos índices não previstos, envolvendo-se na participação, compreensão e interpretação dos dados coletados na pesquisa, via análise de conteúdo. A característica qualitativa se faz presente e é reforçada, devido à compreensão e interpretação dos dados coletados por meio das entrevistas e questionários com os agentes do governo, tecnólogos, advogados, sociólogos, politólogos e geopolíticos, bem como, à observação pessoal própria. Lidando com uma ampla variedade de evidências, que partem desde documentos eletrônicos, entrevistas em vídeos e informação de natureza pública, extraídas dos sites governamentais dos países da Argentina, Brasil e Peru. Os resultados quantitativos são bastante reveladores e a abordagem qualitativa reforçou esses resultados, deixando o estudo robusto e confiável.

Em termos metodológicos a pesquisa caracteriza-se como um estudo de casos múltiplos devido ao interesse e à necessidade de compreender os fenômenos sociais complexos que podem se manifestar no objeto pesquisado: a Política em Segurança Cibernética nos países da América do Sul, notadamente na Argentina, Brasil e Peru.

O estudo de caso é preferido durante o exame dos eventos contemporâneos, mas quando os comportamentos relevantes não podem ser manipulados. O estudo de caso conta com muitas das mesmas técnicas que a pesquisa histórica, mas adiciona duas fontes de evidência geralmente não disponíveis como parte do repertório do historiador: observação direta dos eventos sendo estudados e entrevistas das pessoas envolvidas nos eventos. Novamente, embora os estudos de caso e as pesquisas históricas possam se sobrepor, a força exclusiva do estudo de caso é a capacidade de lidar com uma ampla variedade de evidências - documentos, artefatos, entrevistas e observações – além do que pode estar disponível em um histórico convencional. Além disso, em algumas situações, como a observação participante, pode ocorrer a manipulação informal (Yin, 2015, p.12-13).

Segundo Yin (2015, p.44), o objetivo de uma generalização analítica ainda é generalizar para essas outras situações concretas, e não apenas contribuir para a construção de teoria abstrata.

Em outras palavras a generalização analítica pode ser baseada tanto em (a) corroboração, modificação, rejeição ou, de outra forma, avançar conceitos

teóricos que você referiu no projeto de seu estudo de caso quanto em (b) novos conceitos que surgiram com a *conclusão* do seu estudo de caso (Yin, 2015, p.44).

Por esse motivo, considerou-se estudar o problema a partir de uma abordagem holística, envolvendo a análise de conteúdo e os estudos de casos múltiplos, utilizando a generalização analítica. O intuito é ir além do cenário para o caso específico de estudo, provocando controvérsias e lições aprendidas para os responsáveis do planejamento governamental das Políticas em Segurança Cibernética nos países da América do Sul. Busca-se, assim auxiliar na compreensão das causas e efeitos relacionados às políticas e estratégias em segurança cibernética, analisando a aplicabilidade do modelo cibernético norte-americano aos outros contextos concretos, como é o caso dos países Sul-americanos ou em vias de desenvolvimento. Dessa forma, a presente pesquisa busca contribuir no âmbito do planejamento e desenho das políticas e estratégias nacionais em segurança cibernética.

Qualquer utilização de projetos de casos múltiplos deve seguir uma lógica de replicação, e não de amostragem, e o pesquisador deve escolher cada caso cuidadosamente. Os casos devem funcionar de uma maneira semelhante aos experimentos múltiplos, com resultados similares (replicação literal) ou contraditórios (replicação teórica) previstos explicitamente no princípio da investigação (Yin, 2001, p.75).

4.2 Delimitação da pesquisa

Desde a perspectiva do autor, optou-se pela conveniência na escolha de uma amostra intencional, devido ao objetivo de pesquisa ser a obtenção de boas ideias e percepções ou “*insights*”, indo além das opiniões críticas experientes e evitando generalizar os resultados. Por essa razão, dentre os 13 países sul-americanos, decidiu-se estudar a Argentina, Peru e Brasil, devido às seguintes características:

1. São países membros da OEA e da ONU, estando envolvidos nos planos, programas e projetos dessas organizações, no âmbito da segurança e delito cibernético¹³².
2. As semelhanças nas ameaças e nos riscos vivenciados, entre os três países em estudo, segundo o Fórum Econômico Mundial¹³³, em comparação a outras regiões do planeta, como Europa e Norte-América. Os ataques cibernéticos, não ocupam as dez primeiras posições dos riscos na região da América do Sul.

¹³² Disponível em <https://www.oas.org/pt/topicos/seguranca_cibernetica.asp>. Acesso em 30 de novembro de 2020.

¹³³ Disponível em <<https://reports.weforum.org/regional-risks-for-doing-business-2019/regional-profiles/latin-America-and-the-caribbean/>>. Acesso em 30 de novembro de 2020.

3. Tiveram uma historicidade em comum, de ex-colônias e dependentes das metrópoles ocidentais europeias.
4. As semelhanças socioculturais entre Peru e a Argentina incluem memórias do império incaico e da descolonização. Esses dois países compartilham um passado em comum, com os outros países sul-americanos não incluídos no estudo, como Equador, Colômbia, Bolívia e Chile.
5. A influência da Guerra Fria em suas Doutrinas de Segurança Nacional, a qual serviu de instrumento para a instauração das ditaduras militares em seus países.
6. A localização central e a influência geopolítica do Brasil pelo Atlântico e de Peru pelo Pacífico são notáveis, ambos países abrangem a totalidade das fronteiras com os outros países Sul-americanos.
7. No Índice de Desempenho Industrial Competitivo (*Competitive Industrial Performance Index* - CIP) das Nações Unidas (UNIDO), a Argentina, Brasil e Peru ocupam o Quintil Médio Superior (*Upper Middle Quintile*) no ranking mundial¹³⁴.
8. Apresentaram crescimento econômico semelhante em seu Produto Interno Bruto (PIB)¹³⁵, antes da pandemia do COVID-19.

O protótipo norte-americano, foi escolhido como o “Estado da Arte”, devido ao fato de que, segundo os estudos, os Estados Unidos é um país que dispõe dos maiores exércitos com capacidades cibernéticas no mundo, possuindo a hegemonia política, militar e tecnológica na região. Assim, o caso protótipo norteará nossa análise e compreensão, em relação aos três países Sul-americanos que representam um estudo de caso múltiplo para a região. Na medida que o Brasil serve de referência, pelas suas dimensões continentais e que tem ocupado nos últimos anos as primeiras posições (6ª posição) na região de América, segundo o ranking do Índice Global de Segurança Cibernética¹³⁶ (CGI) da União Internacional de Telecomunicações (ITU). E nos casos, da Argentina e do Peru, eles ocuparam as posições próximas (11ª e 12ª posições, respectivamente). Dessa forma, nos países estudados existem características, ações e iniciativas de política e estratégias públicas que podem ser analisadas, comparadas e adaptadas adequadamente nos países da região da América do Sul.

¹³⁴ Disponível em <<https://stat.unido.org/cip/>>. Acesso em 02 de janeiro de 2020.

¹³⁵ Disponível em <<https://data.worldbank.org/indicator>>. Acesso em 30 de novembro de 2020.

¹³⁶ Disponível em <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf>. Acesso em 30 de novembro de 2020.

Outrossim, sendo o estudo da Segurança e Defesa Nacional um tópico amplamente estudado e complexo, esta pesquisa delimita-se por estudar a área da segurança cibernética, com destaque no nível político-estratégico, optando-se por delimitar os níveis operacionais e táticos da segurança cibernética. Abordam-se alguns aspectos do nível operacional quando estejam inter-relacionados ao estratégico quando necessário. O principal motivo para esta delimitação é o fato que o setor escolhido para a presente tese, segurança e defesa nacional, é um setor com informações e dados sigilosos, sendo problemático devido a uma série de fatores conjunturais e até mesmo estruturais nos países estudados. Se o pesquisador abordasse todos os níveis, em forma qualitativa e quantitativa, corre-se o risco de que os resultados sejam gerais e superficiais, dando uma falsa noção de unidade e impedindo o tratamento de um problema específico.

No intuito, de ampliar as técnicas interpretativas para decodificar, traduzir, interpretar e analisar a significância dos fenômenos observados a partir da teorização e coleta de dados. Foi realizada a coleta e revisão dos documentos eletrônicos, relacionados com as leis, regulamentações, políticas e estratégias nacionais. Já dito linhas anteriores, o caso protótipo norte-americano, no suposto de ter uma política em segurança cibernética de referência mundial e desejada pelos países sul-americanos. Segundo o Apêndice I, mais de 96% dos documentos eletrônicos coletados e revisados foram publicados entre janeiro do ano 2000 e setembro do ano de 2020. Os documentos consultados, em grande medida, sustentam a base de referência dos programas públicos e a doutrina militar conjunta da defesa e segurança cibernética norte-americana¹³⁷, com o intuito de identificar, sistematizar e analisar os elementos e agentes do “Estado da Arte”.

Para a condução dos casos da Argentina, Peru e Brasil segundo os Apêndices: II, III e IV respectivamente, se optou também, por coletar e revisar os documentos eletrônicos que foram publicados entre janeiro do ano 2000 e setembro do ano 2020, com exceção do Apêndice IV, em que foi considerado um único documento, publicado no ano de 1997, que para os objetivos da pesquisa seria relevante.

¹³⁷ Veja o Anexo I, onde se tem a tabela consolidada que serviu de Estado da Arte para a proposta de um modelo de política de segurança cibernética para a América do Sul.

4.3 Técnicas de coleta dos dados

O passo inicial do projeto de pesquisa, consistiu no desenvolvimento do marco teórico para efetuar uma seleção dos casos e a definição das medidas específicas para nosso processo de coleta de dados, por meio de diversas técnicas de coleta. Nesta fase, foi realizada a coleta dos dados por meio de pesquisa documental. A partir das análises desses documentos, contemporâneos e antigos, foram utilizados para a contextualização histórica, política e geoeconômica da América do Sul em matéria da segurança e defesa nacional, delineada no âmbito do ciberespaço. A partir de então, na construção de nosso caso protótipo: “Estado da Arte”, o modelo de coleta de dados consistiu na identificação e seleção das principais referências documentais da Doutrina Conjunta das Forças Armadas norte-americanas, sustentada no *JP 1, Doctrine for the Armed Forces of the United States, 25 March 2013 Incorporating Change 1, 12 July 2017*¹³⁸. Sendo identificados na citada doutrina o número total de setenta e um (71) documentos oficiais eletrônicos de interesse da Segurança e Defesa Nacional dos Estados Unidos, sendo organizados da seguinte maneira:

1. Leis e Regulações Nacionais nos Estados Unidos, no âmbito da Segurança e Defesa Nacional: 05 documentos.
2. Política e Linhas de Ação Estratégica dos Estados Unidos, no âmbito da Segurança e Defesa Nacional: 15 documentos.
3. Publicações do Departamento da Defesa nos Estados Unidos: 51 documentos.

Outro grupo pertinente e relevante para a seleção dos documentos de nosso projeto de corpus, encontra-se as publicações dos Chefes do Comando Conjunto das Forças Armadas, identificando 35 documentos oficiais eletrônicos que em seu conteúdo citam palavras como: *Internet, Cyber, Cyberspace e Cybersecurity*; estando organizados nas seguintes categorias doutrinárias conjuntas:

1. JP 1-0 *Joint Personnel Support* (Pessoal): 01 documento.
2. JP 2-0 *Joint Intelligence* (Inteligência): 03 documentos.
3. JP 3-0 *Joint Operations* (Operações): 26 documentos.
4. JP 4-0 *Joint Logistics* (Logística): 02 documentos.
5. JP 5-0 *Joint Planning* (Planejamento): 01 documento.

¹³⁸ Considerada, no argot militar, a pedra angular doutrinária. Disponível em <<https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/Capstone-Series/>>. Acesso em 11 de abril de 2020.

6. JP 6-0 Joint Communications System (Sistemas de comunicações): 02 documentos.

A proposta na construção do corpus¹³⁹ é do tipo seletivo e computadorizado, pois os dados devem estar em um formato que possa ser processado por computador. Esse é o princípio alternativo de coleta de dados e de procedimento, para a seleção dos documentos oficiais eletrônicos.

Para o projeto de um corpus computadorizado, devem-se observar um conjunto de requisitos que impactarão na validade e confiabilidade da pesquisa baseada no corpus, incluindo se o corpus de estudo serve ao propósito inicial da pesquisa (Kennedy, 1998; Biber et al., 1998; Renouf, 1998; Sinclair, 2005): autenticidade, representatividade, balanceamento, amostragem, diversidade e tamanho (Aluísio, Barcellos, 2006, p.158).

Segundo Galisson e Coste (1983), o corpus trata-se de:

Uma coleção de documentos quer orais (gravados ou transcritos) e escritos, de acordo com o tipo de investigação pretendido. As dimensões do corpus variam segundo os objetivos do investigador e o volume dos enunciados considerados como característicos do fenômeno a estudar. Um corpus é chamado exaustivo quando compreende todos os enunciados característicos. E é chamado de seletivo quando compreende apenas uma parte desses enunciados.

Para Biber (1993), o processo de elaboração do corpus inicia-se com a escolha dos textos eletrônicos, por exemplo, baseada em critérios externos culturalmente aceitos: tipologia de gêneros e tipos de textos. Para prosseguir com as investigações empíricas do conteúdo desses documentos, chamados de critérios internos e posteriormente proceder com a revisão.

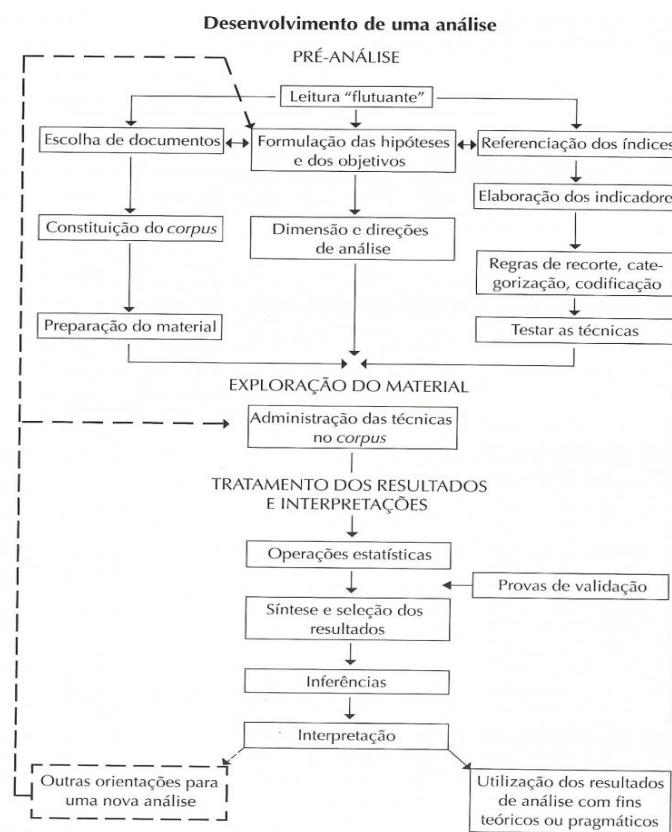
Após a coleta de dados empreendeu-se a técnica de análise de conteúdo nos documentos, com a finalidade de pré-analisá-los, realizando leituras flutuantes com o intuito de apreender e organizar de forma não estruturada aspectos importantes e conhecer o contexto. No intuito de conseguir visualizar primariamente as pistas e indícios não óbvios, tendo como resultado a seleção das unidades de análise ou também denominadas unidades de significado. Para a evidência das unidades de análise temática, será concebido, como um processo dinâmico e indutivo de atenção. Na busca de uma interdependência entre o pesquisador e material pesquisado, são utilizados os objetivos da pesquisa, teorias e questões trazidas no marco teórico, como primeiros norteadores, sendo um constante ir e vir, porém, não se pode

¹³⁹ Pode ser definida como: "Um corpo de uma coleção completa de escritos ou coisas parecidas; ou conjunto completo de literatura sobre algum assunto... vários trabalhos da mesma natureza, coletados e organizados" (*Oxford English Dictionary*, 1989).

dissociar, nem se abster do uso dos recursos mentais e intuitivos necessários, para uma análise deste porte (Gomes, 2004, p.613). Assim, as categorias podem ser caracterizadas como grandes enunciados, abrangendo um número variável de temas e através do análise revelam significados importantes permitindo alcançar os objetivos de pesquisa, bem como, na criação de novos conhecimentos, para dispor de uma visão diferenciada dos temas propostos. Durante o agrupamento das unidades de análise, que compõem nossas categorias, temos pensado fazê-lo por repetição de conteúdos comuns (frequências) e pela importância do tema que não é repetido, mas que guarda uma riqueza e relevância para o estudo (relevância implícita). Porque se acredita que as duas modalidades não são excludentes. No entanto, se tem planejado com um olhar retrospectivo, a modo de auto-observação, com a finalidade de esclarecer e desenrolar o procedimento, tendo em consideração que outros indicadores poderiam se apresentar, deixando assim entrever desde a primeira abordagem a possibilidade de outros índices (Bardin, 2016, p.55).

Conjuntamente na formação das categorias e subcategorias, é prudente a codificação das unidades de análise para evitar que elas se percam na diversidade do material trabalhado. “A codificação é o processo pelo qual os dados brutos são transformados sistematicamente e agregados em unidades, as quais permitem uma descrição exata das características pertinentes do conteúdo” (Bardin, 2016, p. 133). A fase de análise propriamente dita será efetuada pelo computador com o apoio do software MAXQDA, sendo um facilitador eficaz nas operações de codificação indutiva das características interessantes dos dados. Os códigos serão agrupados em temáticas potenciais durante a tratativa dos resultados obtidos e de interpretação. Ao final deste processo com a intenção de evidenciar de forma sistemática a construção progressiva das categorias de análise, será elaborado o relatório inicial do caso protótipo norte-americano. Isso nos permitirá identificar aos elementos e agentes envolvidos na concepção da política e estratégias da segurança cibernética norte-americana e, conseqüentemente, orientar nossas ações na análise do estudo comparativo a ser feito com os países da Argentina, Brasil e Peru.

Figura 14 - Organização da análise de conteúdo



Fonte: (Bardin, 2016, p.132).

Em uma segunda fase de nossa pesquisa, onde trataremos os casos da Argentina, Brasil e Peru, nós iremos deparar com escassa produção de textos eletrônicos oficiais em segurança e defesa cibernética. Remetendo-nos com frequência aos estudos relacionados às outras áreas de conhecimento, porém subsidiam nosso objeto de investigação, sendo adicionada a busca de textos eletrônicos nos sites oficiais-públicos. Em soma, foram realizadas entrevistas semiestruturadas (videoconferência gravadas) e questionários qualitativos individuais (formulário online, perguntas abertas) aos especialistas que participam nas funções e papéis, no âmbito da segurança e defesa cibernética dos três países em estudo, conforme ao seguinte detalhe:

- Seis (06) entrevistas semiestruturadas, aos especialistas do setor público.
- Vinte (20) questionários semiestruturados individuais, aos especialistas do setor privado, público e acadêmico.

- Oito (08) questionários semiestruturados individuais¹⁴⁰, aos especialistas (as) do setor privado, público e acadêmico dos países da Bolívia, Chile, Colômbia, México, Uruguai.

O objetivo principal das entrevistas e dos questionários é aprofundar nas informações, em especial daquelas que não foram visualizadas ou descritas nos documentos estudados. Portanto, esses instrumentos de pesquisa auxiliam na compreensão mais ampla desde a perspectiva dos participantes, tendo eles a condição de fornecê-los, por diversos aspectos: experiências, familiaridade do contexto, cultural e organizacional, entre outros. em relação aos questionários dos países que não são parte do escopo de estudo, basicamente, acodem no fortalecimento do posicionamento das ideias, sugestões e inferências do autor.

Quadro 16 - Entrevistas aos especialistas governamentais dos países estudados

Entrevistados Brasil			
Identificador	Entidade	Departamento	Estado ou Cidade
Entrevistado_Brasil_1	Ministério Público do Estado de Minas Gerais (MPMG)	Gabinete de Segurança e Inteligência	Minas Gerais
Entrevistado_Brasil_2	Ministério Público do Distrito Federal e dos Territórios (MPDFT)	Procuradoria Geral	Brasília
Entrevistados Argentina			
Entrevistado_Argentina_1	Escritório Nacional de Tecnologias da Informação (ONTI)	Padrões Tecnológicos	Buenos Aires
Entrevistado_Argentina_2	Força Aérea Argentina	Direção Geral de Investigação e Desenvolvimento	Buenos Aires
Entrevistados Peru			
Entrevistado_Peru_1	Ministério de Transporte e Comunicações	Regulação e Assuntos Internacionais de Comunicações	Lima
Entrevistado_Peru_2	Ministério de Transporte e Comunicações	Regulação e Assuntos Internacionais de Comunicações	Lima

Fonte: Elaborado pelo autor (2024).

Quadro 17 - Questionário aos especialistas dos países estudados

Identificador	Entidade	Função
Idioma Português		
Respondente_Brasil_1	<i>Global Foundation for cyber-Studies and Research</i>	Pesquisador
Respondente_Brasil_2	Exército Brasileiro	Instrutor de Guerra Cibernética
Respondente_Brasil_3	Universidade de São Paulo	Advogado e Professor
Respondente_Brasil_4	Accenture	Diretor Cybersecurity
Respondente_Brasil_5	Associação Brasileira de Estudos de Defesa (ABED)	Vice President
Respondente_Brasil_6	Instituto de Referência em Internet e Sociedade (IRIS)	Diretor
Respondente_Brasil_7	Exército Brasileiro	Estado Maior Conjunto do Comando de

¹⁴⁰ As evidências trazidas desses questionários servem ao autor para uma compreensão mais ampla em base aos outros especialistas da região. Elas não estão diretamente relacionadas com nossos objetivos da investigação, porém somente validam nossas sugestões finais na pesquisa.

		Defesa Cibernética
Respondente_Brasil_8	Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec)	Diretor
Idioma Espanhol		
Respondente_Argentina_1	CIBERPRISMA	Diretor
Respondente_Argentina_2	Universidade da Defesa Nacional	Professor Gestão da Ciberdefesa
Respondente_Argentina_3	Jefatura de Gabinete de Ministros	Diretor Prevenção em Sistemas e Redes Informáticas
Respondente_Argentina_4	ISACA Buenos Aires Chapter	Vice-presidente
Respondente_Peru_1	<i>Ministerio del interior</i>	Diretor General de inteligência
Respondente_Peru_2	<i>Smart Regulation Peru</i>	<i>Consultor Asociado</i>
Respondente_Peru_3	<i>Organismo supervisor do Investimento em energia e Minería (OSINERGMIN)</i>	<i>Gerente de Sistemas e Tecnologias da Informação</i>
Respondente_Peru_4	Superintendência Nacional de Migrações	Chefe de Plataforma e Segurança Tecnológica
Respondente_Peru_5	Secretaria de Governo e Transformação Digital (SEGDI)	Consultor
Respondente_Peru_6	Presidencia del Consejo de Ministros (PCM)	Especialista em Análise Político
Respondente_Peru_7	Grupo Falabella	Gerente Corporativo de Projetos de Cibersegurança
Respondente_Peru_8	Ministério de Desenvolvimento e Inclusão Social	Consultor Sênior TIC

Fonte: Elaborado pelo autor (2024).

Quadro 18 – Questionário aos especialistas latino-americanos

Identificador	Entidade	Função
Respondente_Bolivia_1	Câmara de Senadores	Assessor Legislativo
Respondente_Chile_1	Controladoria Geral da República	Oficial de Cibersegurança
Respondente_Chile_2	Exército do Chile	Chefe do CSIRT
Respondente_Colombia_1	ECOPETROL	Profissional Sênior de Ciberseguridad
Respondente_Mexico_1	Coletivo de Análise da Segurança com Democracia (CASEDE)	Pesquisador - Segurança Pública e Nacional
Respondente_Mexico_2	Blackstring México	Consultor Sênior de Inteligência Estratégica
Respondente_Mexico_3	MB Consulting	Diretor - Coordenação e Análise
Respondente_Uruguai_1	Krav Maga Hacking	Diretor

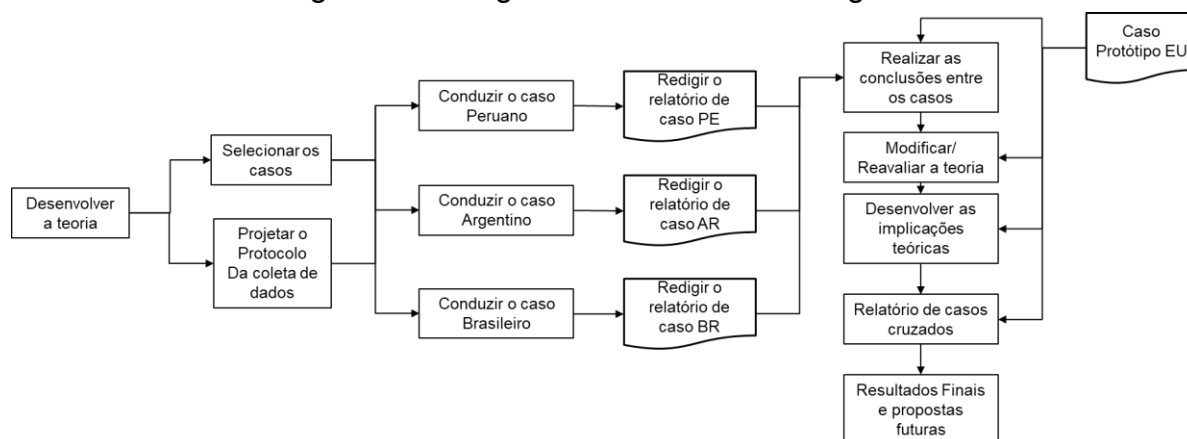
Fonte: Elaborado pelo autor (2024).

Os roteiros das entrevistas realizadas aos participantes estão nos Apêndices VI e VII. Como parte do planejamento foi iniciado um pré-teste a dois (02) entrevistados, com o intuito de identificar imprecisões discursivas, erros gramaticais ou técnicos, complexidade, questões desnecessárias, constrangimento e exaustão do entrevistado. Por se tratar de um estudo transcultural, a pesquisa é um estudo multilíngue que oscila em três (03) idiomas: inglês, espanhol e português. No caso das perguntas aos entrevistados, vão sofrer certas alterações devido ao país estudado, estando o material coletado nos idiomas de português e espanhol.

A coleta de dados nos países em estudo, será realizada de forma similar com o caso protótipo norte-americano e fazendo uso do *software* MAXQDA na análise de conteúdo. O método a ser utilizado é o estudo de casos múltiplos contextos, de modo a deixar em evidência, logo da análise de interpretação, as relações existentes entre Argentina, Brasil e Peru, para afinal obter os relatórios do caso individual desses países.

Em uma terceira fase, ao observar e identificar os padrões, elementos e agentes envolvidos na concepção da política em segurança cibernética desses países. Em uma análise comparativa e apoiados no protótipo norte-americano, vamos analisar as repercussões existentes na consolidação das políticas e estratégias de segurança cibernética, é claro que nossa compreensão se apoiará na análise temático e das especificidades geopolíticas na região de onde teremos as conclusões entre os casos que permitirá trazer insumos e propostas de mudança na teoria, a fim de desenvolver as implicações teóricas e escrever um relatório de casos cruzados.

Figura 15 - Diagrama de fluxo metodológico



Fonte: Adaptado de Yin (2015, p.64).

Segundo Stoecker (1991), o estudo de caso como estratégia de pesquisa, compreende um método que abrange tudo com a lógica de planejamento incorporando abordagens específicas à coleta de dados e à análise de dados. Nesse sentido, o estudo de caso não é nem uma tática para a coleta de dados, nem meramente uma característica do planejamento em si, mas uma estratégia de pesquisa abrangente.

Yin (2001, p. 71-72), sugere que os estudos de caso, em geral, não devem ser utilizados para avaliar a incidência dos fenômenos. Ademais, um estudo de caso, teria que tratar tanto do fenômeno de interesse quanto de seu contexto, produzindo muitas variáveis potencialmente relevantes. Isso acabaria exigindo, sucessivamente, um

número inconcebivelmente grande de casos – grande demais para permitir qualquer avaliação estatística das variáveis relevantes. Por fim, se uma lógica de amostragem tivesse de ser aplicada a todos os tipos de pesquisa, muitos tópicos poderiam não ser empiricamente investigados. Deste modo, a problemática apresentada permitirá pesquisar um fenômeno contemporâneo em seu real contexto, especialmente, quando os limites entre o fenômeno e o contexto não estão claramente definidos. Segundo Laville e Dionne (1999, p.214), o princípio da análise de conteúdo consiste em desmontar a estrutura e os elementos desse conteúdo para esclarecer suas diferentes características e extrair sua significação. Portanto, curiosos pelas mudanças que vão marcando as atuais políticas e estratégias da segurança cibernética nos países Sul-americanos e de estimular nossa compreensão na evolução e do conteúdo nas políticas e estratégias na Argentina, Brasil e Peru. Esta pesquisa busca deixar em evidência as tendências, os elementos, os agentes envolvidos e suas repercussões na consolidação da política. Provocando uma conclusão dos países pesquisados, onde elencaremos sugestões, com base aos reflexos observados para finalmente, apresentar os resultados de nossa pesquisa.

A temática investigada é um estudo pouco explorado, não havendo referências em relação ao grupo social específico¹⁴¹. Portanto, relatamos brevemente a historicidade, no desejo de ir além da etimologia e da descrição dos conceitos teóricos. A tese busca aprofundar e compreender os fenômenos presentes no ciclo de vida da política em segurança cibernética, explorados a partir de uma perspectiva dos participantes, em um ambiente natural e em relação ao contexto social e geopolítico. Uma limitação desta pesquisa, é que não pretendemos aprofundar nos estudos dos fenômenos que visam responder às causas dos eventos sociais que se relacionam com a consolidação das políticas em segurança cibernética, mas sim dos elementos que se vão se influenciar nelas. Portanto, esperamos que esta tese seja de incentivo para próximas pesquisas na busca de respostas para essa limitação.

Metodologicamente, compreender a abordagem da pesquisa, irá nos brindar um conhecimento profundo da natureza dos principais cenários de ameaças, riscos e problemáticas da segurança cibernética. Nessa situação, é essencial para sua avaliação, desenvolver uma teoria de como deveria ser entendido o funcionamento da defesa e segurança cibernética nacional, com foco nos países estudados, dentro do

¹⁴¹ Em relação, principalmente, aos três países de nosso estudo: Argentina, Brasil e Peru.

contexto das políticas, a partir de ações de informação efetivadas pelos atores sociais dentro do fluxo informacional em um espaço social específico.

Assim, o problema da pesquisa será abordado nas ciências sociais, desde uma perspectiva particular das teorias contemporâneas da ciência da informação: regimes de informação, memória e informação.

Dentro do contexto de Ciência da Informação, o regime de informação se configura como uma formação social conjunta de elementos em rede – como atores sociais (sujeitos, dispositivos e tecnologias), regras de poder, a organização e a gestão política da informação que se operacionalizam em práticas sociais com produtos e serviços (Bezerra *et al.*, 2016, p. 61).

A pesquisa social tem a capacidade de lidar com situações complexas, onde não há consenso sobre o problema. Nesses casos, as consequências são conhecidas, mas não sabemos exatamente o que fazer para que o sistema em foco atinja seus objetivos. Este é precisamente o caso da realidade dos países da América do Sul, em relação à elaboração de suas políticas em defesa e segurança cibernética. Adicionalmente, este tipo de pesquisa permitirá introduzir uma percepção da realidade, considerando a sensibilidade de seus elementos nas diferentes faixas das possíveis mudanças, e desenvolver propostas ou linhas razoáveis de ação.

A tese se insere na linha “Memória Social, Patrimônio e Produção do Conhecimento”, compreendendo que a investigação sobre as inter-relações entre o comportamento dos sujeitos e o ambiente informacional contribui para o fortalecimento teórico dos campos da Ciência da Informação. Isso ajuda a encontrar sentido na base teórica que abrange a compreensão das cibercapacidades, o ciberpoder, as e-polis, a ciberindustrialização e as ciberleis exercidas no ciberespaço. Busca-se assim, um benefício factual com interesse social, cultural, econômico e geopolítico para os governos sul-americanos.

“A política é quase tão excitante como a guerra e não menos perigosa. Na guerra a pessoa só pode ser morta uma vez, mas na política diversas vezes”

Winston Churchill

5 CASO PROTÓTIPO NORTE-AMERICANO

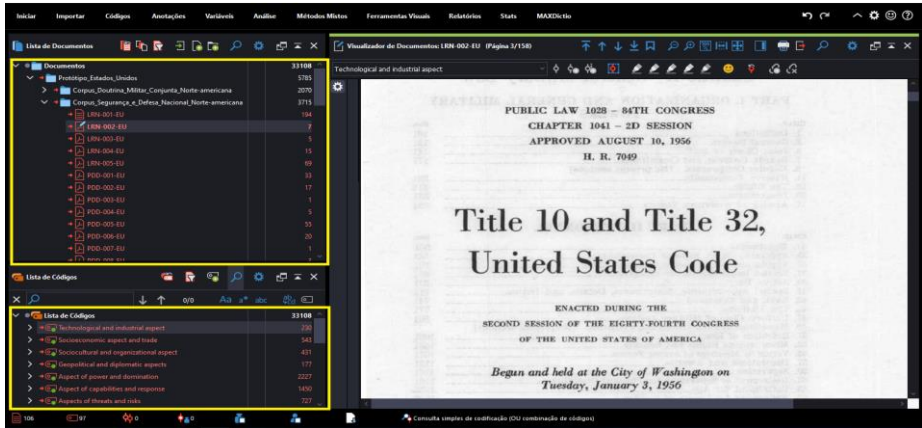
No presente capítulo, vamos desenvolver o caso protótipo norte-americano. Essencialmente, trabalharemos na análise de conteúdo nos documentos do Apêndice I. A análise de conteúdo é um conjunto de técnicas aplicadas aos discursos: conteúdos e continentes, segundo Bardin (2016, p.15) desde o cálculo de frequências até a extração de estruturas traduzíveis em modelos “é uma hermenêutica controlada, baseada na dedução: inferência”. Já na interpretação, a análise de conteúdo irá oscilar entre a objetividade e a subjetividade. Segundo o descrito nos capítulos anteriores, o caso norte-americano foi escolhido como o “Estado da Arte”, com a intenção de nos ajudar na refinação dos planos de coleta de dados, tanto no conteúdo dos dados, quanto nos procedimentos seguidos, entendendo que não se trata de um pré-teste. Segundo Robert K. Yin (2015, p.100), “O caso piloto é mais formativo, ajudando-o a desenvolver linhas relevantes de questões-fornecendo até esclarecimentos conceituais para o projeto de pesquisa”. Neste capítulo, faremos o tratamento e análise documental sob uma perspectiva quantitativa, para posteriormente reforçá-la qualitativamente por meio das entrevistas realizadas com funcionários governamentais e especialistas. Finalmente, elaboraremos um relatório sobre o caso protótipo norte-americano.

5.1 Organização da análise

Após a técnica de coleta de dados para o processo de escolha e organização dos documentos, estes foram agrupados em: Corpus da Doutrina Militar Conjunta (CDMC) e no Corpus da Segurança e Defesa Nacional (CSDN). Em seguida, foram etiquetados e submetidos ao software MAXQDA para a análise na formulação dos pressupostos e objetivos da pesquisa, auxiliando na elaboração dos indicadores e critérios para a fundamentação e interpretação do “Estado da Arte” da Política em segurança cibernética. Foi escolhido o software MAXQDA devido às suas diversas funcionalidades, sendo um facilitador na análise de dados coletados em cada fase do

contexto da pesquisa social empírica. Uma característica central do software é sua capacidade de trabalhar com códigos e categorias, permitindo a atribuição de códigos nas partes selecionadas dos dados, desde palavras, parágrafos de textos até porções de imagens, vídeos ou áudios.

Figura 16 - Organização dos documentos no software MAXQDA



Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

Quadro 19 - Funções básicas do MAXQDA na análise qualitativo

Função de análise	Descrição
Codificação	Atribuir códigos a partes de um documento (passagem de texto, parte de uma imagem, videoclipe). Categorias de forma indutiva a partir do texto, por exemplo, codificação ao vivo, codificação de cores como você faria com um marcador, codificação com símbolos ("smileys"), atribuição de atalhos de código de uso frequente.
Busca de texto e codificação automática	Pesquisa por termos em todos os documentos ou em documentos selecionados de um projeto. Codifica automaticamente seus locais com uma determinação flexível em relação ao contexto a ser codificado (por exemplo, frases completas, parágrafos).
Sistema hierárquico de categorias	Trabalhar com um sistema hierárquico de categorias (sistema de código) – subcategorias até 10 níveis. Organiza o sistema de categorias e suas camadas por meio de arraste e solte. Utiliza os códigos favoritos e um conjunto de códigos como uma compilação de códigos. Função de ponderação e de comentários nos segmentos codificados.
Memorandos e comentários	Anexe memorandos a documentos, códigos ou segmentos de dados com comentários, ideias e hipóteses. Opção de escrever memorandos. Para Organizar os memorandos existem onze tipos diferentes de memorandos e etiquetas disponíveis. Busca e filtra memorandos na visualização de tabela. Pesquisa por termos em todos os documentos ou memorandos de um projeto.
Paráfrase	Selecione parte de um texto e resuma o conteúdo da passagem de texto em suas próprias palavras.
Resumos temáticos	Resuma as passagens de texto às quais o mesmo código foi atribuído, caso por caso, por exemplo, escrever um resumo das afirmações sobre um tópico específico para cada documento.
Pesquisa de código	Pesquise por segmentos de dados codificados selecionando ("ativando") documentos e códigos. Listas interativas com resultados, mostrando os segmentos em seu documento original. Filtragem possível por ativação, variáveis, cores e pesos.
Classificação com variáveis, métodos mistos	Atribuir informações demográficas e outras informações padronizadas como variáveis para documentos. Agrupe e pesquise dados usando valores de variáveis. No âmbito de estudos de métodos mistos, combinam dados quantitativos com dados qualitativos.
Links e referências	Vincula passagens de texto individuais ou porções de imagem entre si e com arquivos externos, páginas da web ou referências geográficas.
Diário	Registrar em um diário de pesquisa informações valiosas sobre o processo de trabalho de um projeto de pesquisa.

Fonte: (Rädiker, Kuckartz, 2019, p.18, tradução nossa).

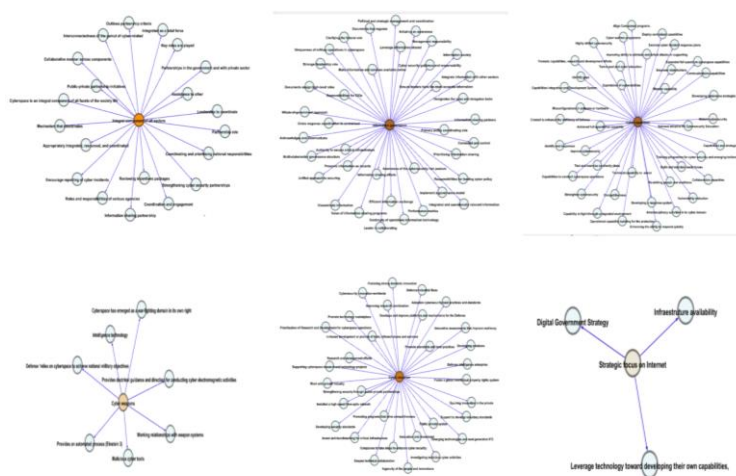
A pré-análise documental desenvolvida proporciona ao pesquisador uma organização, embora, “composta por atividades não estruturadas, “abertas”, por oposição à exploração sistemática dos documentos” (Bardin, 2016, p.126). Em consonância com a justificação da pesquisa a experiência do pesquisador com os documentos da doutrina militar possibilitou que as “leituras flutuantes” se tornassem mais precisas, em função de pressupostos emergentes na projeção de teorias e de possíveis técnicas a serem utilizadas. A formulação dos pressupostos e objetivos, foram direcionados na realização de análises a cegas e sem ideias preconcebidas, prosseguindo para efetuar o mecanismo da indução na busca de deixar os documentos falarem por si só, fazendo uso do recurso computacional disponível para a pesquisa. Uma vez concluídas as operações da pré-análise, importamos todos os documentos coletados no software MAXQDA, iniciando a exploração do material com atividades e operações de codificação indutiva. Os documentos que apresentaram a maior frequência de ocorrência das palavras: *Internet*, *cyber*, *cyberspace* e *cybersecurity* foram selecionados para ser codificados inicialmente, seguindo então para a fase mais longa e tediosa, até atingir à saturação teórica.

Considera-se saturada a coleta de dados quando nenhum novo elemento é encontrado e o acréscimo de novas informações deixa de ser necessário, pois não altera a compreensão do fenômeno estudado (Nascimento *et al.*, 2018, p. 244).

Sendo alcançada a saturação foi adotada a estratégia de realizar a codificação automática nos documentos restantes. O resultado da codificação semiautomatizada, identificaram-se 64 subcódigos os quais foram agrupados em 26 códigos, para logo estruturar nossas categorias temáticas¹⁴².

¹⁴² Maiores detalhes observa-se o Apêndice V.

Figura 17 - Código e subcódigos

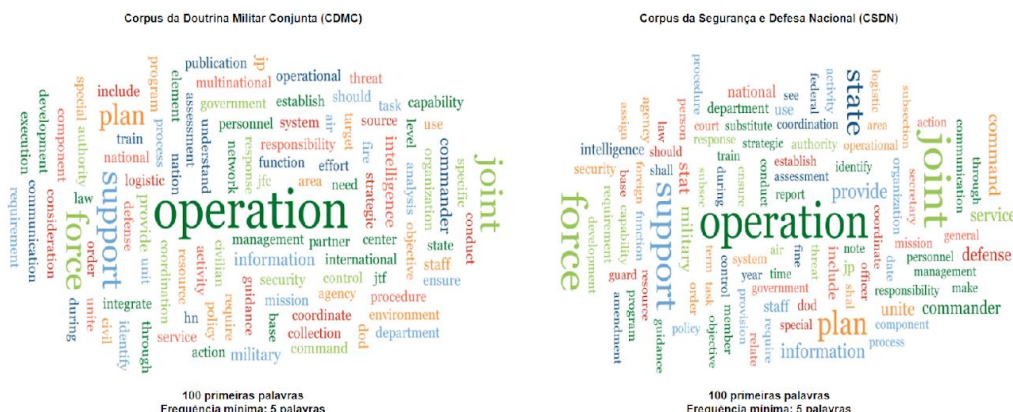


Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024)..

5.2 Análise e tratamento quantitativo dos corpus norte-americano

A seguinte abordagem será na frequência de determinados elementos da mensagem, que por meio da exploração e do método estadístico buscaremos obter dados descritivos. Para Bardin (2016, p.145) “esta análise é mais objetiva, mais fiel e mais exata, visto que a observação é mais bem controlada”. Devemos ter em consideração que esta análise será útil para a verificação de nossos pressupostos. Existe uma ampla utilização das técnicas de tipo temático e frequência, sendo sempre útil numa primeira fase de abordagem dos materiais. “No entanto outros indicadores, mais formais ou estruturais, aparecem aqui e ali, deixando assim entrever desde a primeira abordagem a possibilidade de outros índices” (Bardin, 2016, p.55). Por esse motivo, o pesquisador se sentiu motivado a analisar a frequência das palavras contidas nos corpus e, ao compará-las entre si, observou-se que ambos os corpus têm características similares. Do ranking das 25 palavras com maior frequência, 19 delas estão presentes em ambos corpus: *operation, force, support, plan, commander, information, intelligence, military, provide, JP, staff, command, include, service, security, use, DoD e state*.

Figura 18 - Nuvem de palavras: frequências de palavras



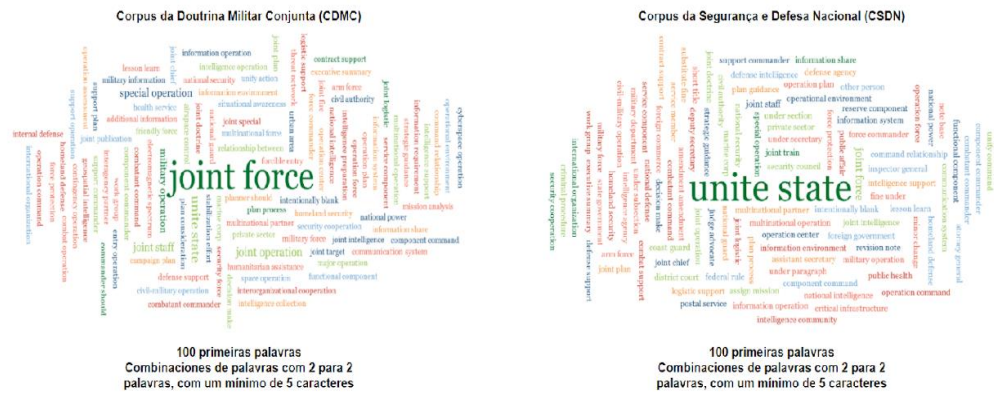
Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

Nota: Foi utilizada a função de Lematização (*Lemmatization*) de palavras.

Seguinte, realizamos a análise das combinações de palavras, sendo procurado combinações de palavras “com 2 para 2 palavras”, lematizando¹⁴³ as palavras ao idioma inglês, com um mínimo de 5 caracteres por cada um dos corpus, permitindo-nos identificar palavras que poderiam constituir indícios e de ajuda, no processo de codificação. Por exemplo: *national security*, *homeland security*, *communication system*, *national intelligence*, *support commander*, *civil authority*, *private sector*, *international organization*, *multinational operation*, *intelligence community*, *critical infrastructure*, *information share*, *defense support*, *information system*, *information operation*, *national power*, *information environment*, *threat network*, *cyberspace operation*, *interagency coordination*, *weapon system*, *legal support*, entre outros (Figura N°19). Esse análise foi repetida múltiplas vezes com diversas combinações de palavras. Apesar da simplicidade e rapidez da análise, ela nos ajuda a ter uma visualização das palavras que poderiam constituir-se nas palavras chaves ou palavras-temas. Segundo Bardin (2016, p.133), “tratar o material é codificá-lo”, seguindo regras precisas dos dados brutos até atingir uma representação do conteúdo que facilita ao analista esclarecer certas características do texto.

¹⁴³ O MAXDictio permite a lematização de palavras em vários idiomas para funções de frequência e combinação de palavras. Quando esta opção é ativada, as palavras são retornadas às suas respectivas formas básicas, de modo que as palavras com o mesmo significado sejam combinadas independentemente da declinação ou maiúsculas e minúsculas. Por exemplo, apenas a palavra "dar" será contada para as várias formas "dar", "deu" e "dado". Disponível em < <https://www.maxqda.com/help-mx24/maxdictio/lemmatization> >. Acesso em 19 de agosto de 2024.

Figura 19 - Nuvem de palavras: combinações de palavras



Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

A soma total dos segmentos codificados, no Corpus da Doutrina Militar Conjunta (CDMC) e no Corpus da Segurança e Defesa Nacional (CSDN), é de 5785 segmentos. Ao analisar a frequência dos códigos nos documentos do CDMC, o código “*Threat to national security*” apresentou a maior frequência, sendo encontrado em 278 segmentos desse corpus. Da mesma forma, aconteceu no CSDN encontrado em 340 segmentos. No entanto, a análise se torna interessante quando a mesma análise é feita conjuntamente em ambos corpus. Observa-se a Figura N°36, os cinco primeiros códigos com maior frequência, nos segmentos com códigos, são: “*Threat to national security*”, “*National protection*”, “*Cyber defense*”, “*Intelligence community*”, “*Mission capability*” e “*Instruments of national power*”.

Figura 20 - Frequência de códigos (unidade: segmentos com códigos)

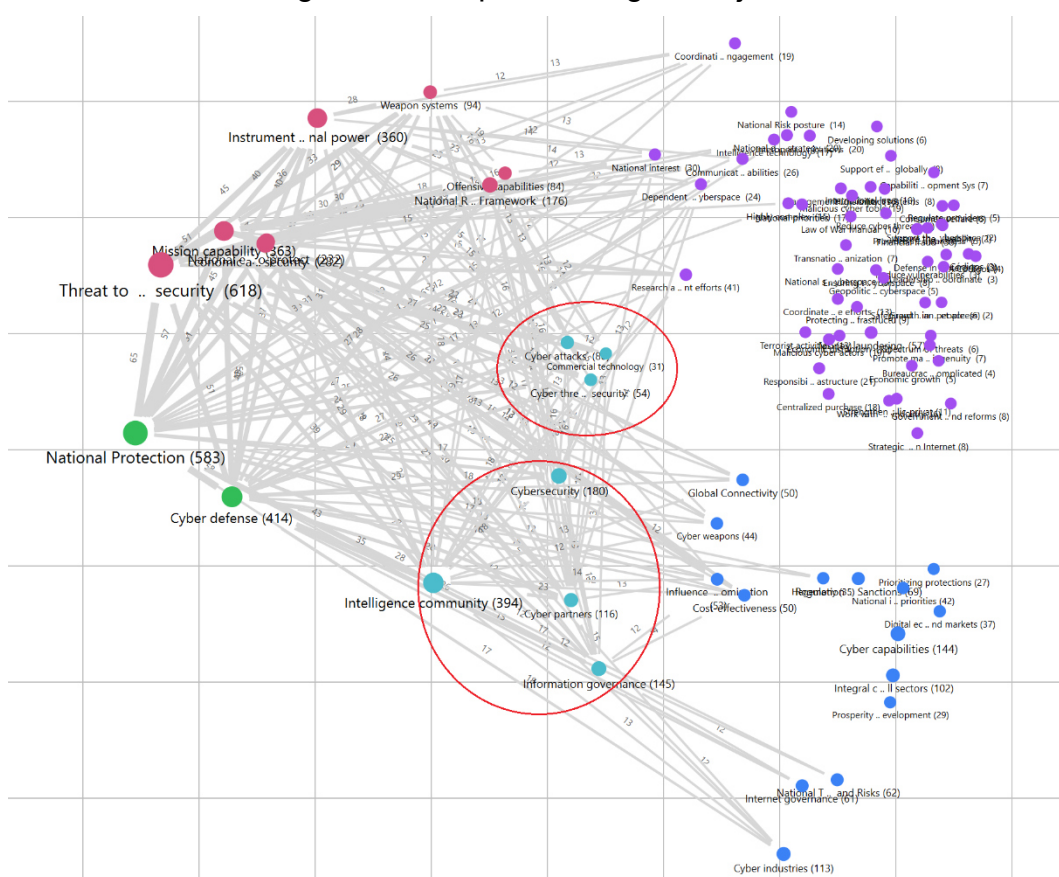
123 Frequência de códigos		
	Unidade: Segmentos com código	
	Frequência	Porcentagem
Threat to national security	618	10.7
National Protection	583	10.1
Cyber defense	414	7.2
Intelligence community	394	6.8
Mission capability	363	6.3
Instruments of national power	360	6.2
Economic and national security	282	4.9
National effort to protect	232	4.0
Cybersecurity	180	3.1
National Response Framework	176	3.0
Information governance	145	2.5
Cyber capabilities	144	2.5
Cyber partners	116	2.0
Cyber industries	113	2.0
Integral component of all sectors	102	1.8
Weapon systems	94	1.6
Offensive capabilities	84	1.5
Cyber attacks	80	1.4
Regulations and Sanctions	69	1.2
National Threats and Risks	62	1.1
Internet governance	61	1.1
Money laundering	57	1.0
Cyber threats to national security	54	0.9
Influence of expansion and ...	53	0.9
Global Connectivity	50	0.9
Cost-effectiveness	50	0.9
Cyber weapons	44	0.8
National interests and priorities	42	0.7
Research and development efforts	41	0.7
Financial fraud	38	0.7

Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

Ao realizar a análise do mapa de código das ocorrências de códigos em um mesmo documento, podemos observar que as relações entre os códigos são sinalizadas com uma linha de cor cinza. Quanto maior é a frequência com a qual dois códigos foram atribuídos juntos, mais próximo eles irão aparecer no mapa. É neste tipo de análise que foram identificadas as relações diretas e indiretas entre os códigos (ou elementos) existentes em nossos corpus. Observa-se que os nós de cor azul têm o maior número de conexões diretas, mas não necessariamente são códigos que têm a maior frequência nos documentos. Na Figura N°21, o código “*offensive capabilities*” tem uma frequência de 40 sendo de menor valor, em relação aos códigos do cluster que pertence (Cluster de cor rosa). Essa análise pode nos proporcionar uma compreensão mais profunda das relações existentes entre os elementos em sua definição. Outro ponto a considerar na construção da compreensão da análise são as relações dos elementos satélites, que orbitam com uma determinada intensidade em relação ao nó (ou código) que desejamos compreender. Por exemplo, na compreensão do nodo “*instrument of national power*”, os elementos satélites de maior intensidade são: “*National protection*”, “*threat to national security*”, “*national effort to protect*”, “*mission capability*”, “*cyberdefense*”, etc., porém, existem relações de menos intensidade com outros nós: “*cyber weapons*”, “*offensive capabilities*”, como relações indiretas com códigos de outros cluster (Cluster cor azul): “*intelligence community*”, “*national response framework*” entre outros, ampliando desse jeito nossa compreensão do nodo “*instrument of national power*”, respeito aos outros códigos que não estejam citados em um único documento. Ainda assim, esses elementos estão presentes nos demais documentos do corpus, ampliando a compreensão envolvida em sua concepção e podendo reforçar uma re-teorização da nossa pesquisa.

(frequência) dentro do grupo céu azul, seguido pelos códigos: “cybersecurity”, “Information governance” e “Cyber partners”, respectivamente. Não obstante, os códigos “Cyber attacks”, “Commercial technology” e “Cyber threat to national security” integram o mesmo grupo com uma menor frequência, porém, possuem a maior proximidade. Este tipo de visualizações amplia nossa compreensão das relações existentes entre os códigos. Consequentemente, o conjunto dos grupos de códigos nos mostra em sua constituição os elementos e os agentes (intermediários) que estariam envolvidos na concepção desses documentos.

Figura 23 - Mapa de códigos conjunto



Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

A seguinte análise apresenta a distribuição de frequências dos códigos através dos corpus, sendo os nós representados como quadrados. Percebeu-se que em ambos os corpus há uma maior relevância nas categorias de poder e dominação (“*Aspect of power and domination*”) e de capacidades e respostas (“*Aspect of capabilities and response*”). Porém, no CSDN as outras categorias possuem uma equilibrada relevância. Observa-se a Figura N° 40, desde a perspectiva da co-ocorrência de dois códigos em um segmento, se evidencia que dentro a categoria de capacidades e respostas, os códigos “*Mission capability*” e “*Cyber defense*” possuem

uma maior relação. Ademais, as categorias de aspecto socioeconômico e mercado (“*Socioeconomic aspect and trade*”) e a de poder e dominação (“*Aspect of power and domination*”) possuem uma maior relação por intermédio dos códigos “*Economic and national security*” e “*Threat to national security*” respectivamente.

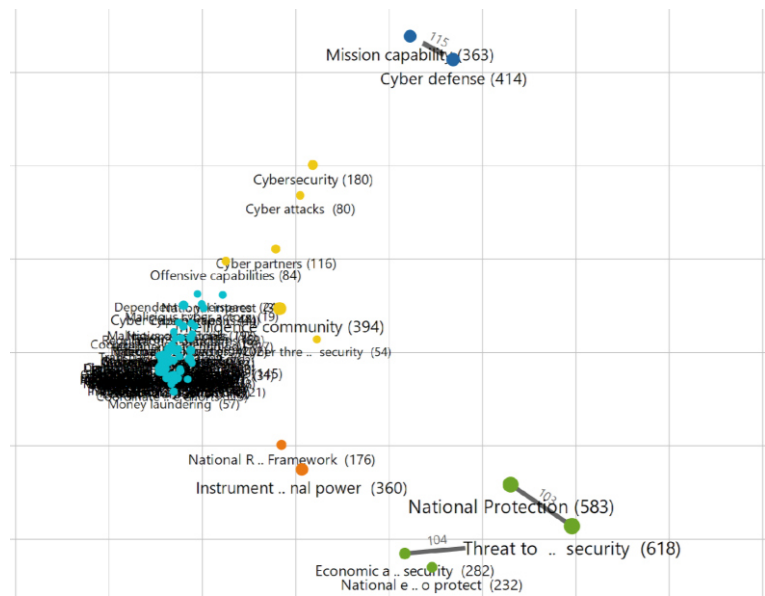
Figura 24 - Visualizador das conexões entre códigos

Lista de Códigos	Corpus_Doutrina_Militar_Conjunta_Norte-americana	Corpus_Segurança_e_Defesa_Nacional_Norte-americana	SOMA
> Technological and industrial aspect			230
> Socioeconomic aspect and trade			543
> Sociocultural and organizational aspect			431
> Geopolitical and diplomatic aspects			177
> Aspect of power and domination			2227
> Aspect of capabilities and response			1450
> Aspects of threats and risks			727
Σ SOMA	2070	3715	5785

Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

Continuando com o análise, na Figura N°25 foi representada uma visualização geral, dos cinquenta (50) códigos que tem a maior frequência nos documentos analisados, estando representado com o maior tamanho, os códigos que possuem a maior frequência. Por exemplo: “*Threat to national security*”, “*National Protection*” e “*Cyber defense*” aparecem em 618, 583 e 414 segmentos codificados respectivamente, em todo o conjunto dos documentos que conformam o caso protótipo norte-americano.

Figura 25 - Visualizador das conexões entre os códigos



Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

Desta forma, temos analisado e observado uma abordagem quantitativa com base na frequência dos elementos da mensagem e as relações entre eles e seus agentes, que foram emergindo na exploração documental, sendo amplamente

facilitada pela capacidade computacional. Desde a perspectiva quantitativa, as diversas análises que podem ser realizadas aos documentos deixam em evidência as concepções e valores de referência em relação aos elementos e agentes presentes nesses documentos. São encontrados dados descritivos através do método estatístico. No entanto, é importante entender que esses são nossos primeiros *insights* para o fortalecimento na definição das categorias e a verificação das explicações provisórias, que serão apresentadas nos próximos parágrafos.

Figura 26 - Nuvem de códigos conjuntos



Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

5.3 Análise qualitativa dos corpus: protótipo norte-americano

O análise qualitativo trata-se de um procedimento mais intuitivo, segundo Bardin (2016, p.145) é “também mais maleável e mais adaptável a índices não previstos, ou à evolução das hipóteses”. Nesta fase, serão definidas as categorias que irão agrupar aos códigos e subcódigos, para serem estudados na análise quantitativa. Com a análise qualitativa buscamos fundamentar o lançamento de nossos pressupostos, onde serão sugeridas as relações entre um índice da mensagem e uma ou diversas variáveis do locutor (ou da situação de comunicação)” (BARDIN, 2016, p.145).

Um princípio que guia o esforço indutivo da codificação é buscar evitar que conceitos teóricos existentes possam se sobrepor à nossa análise. Buscamos a possibilidade de identificar e desenvolver novos conceitos e teorias. “Este análise permite a elaboração de deduções específicas sobre um acontecimento ou uma variável de inferência precisa e não em inferências gerais” (Bardin, 2016, p.145). Para esta análise, temos seguido a categorização indutiva, o que significa, que o sistema

de categorias não foi fornecido. Nesta passagem dos dados brutos para dados estruturados ou organizados, buscamos conhecer índices invisíveis ao nível dos dados brutos. O agrupamento de nossos códigos vai caracterizar a criação e nomeação das categorias, as quais vão abarcar um número variável de temas. Através de sua análise, são apresentados significados e elaborações relevantes que fornecem nossos objetivos de estudo e novos conhecimentos, fornecendo uma visão sobre os temas propostos. No processo da construção das categorias, o pesquisador precisa ser sutil e mergulhar engenhosamente desde a própria seleção dos documentos que constituem os corpus, percorrendo pela exploração feita através da codificação e ao ser triangulada com os resultados observados conformaram nossas unidades de registros, assim ser realizada nossa categorização. As categorias descritas na Tabela N°28, dizem respeito à temática que a presente tese se propôs, não buscando ser um modelo para outras pesquisas, tendo em vista as peculiaridades inerentes e o contexto de cada tópico. Porém, nos traz luzes do “Estado da Arte” no que tange à política e estratégias da segurança e defesa cibernética norte-americana, sendo identificado, sistematizado e analisado os elementos e os agentes envolvidos na sua construção, por meio de um esquema geral, facilitar os tópicos mais importantes para nossos próximos análises dedicados aos estudos de caso dos países sul-americanos selecionados na tese.

Quadro 20 - Categorias e explicações provisórias do Estado da Arte

Categorias	Explicações provisórias	Tipos de categorias	Código	Notas Analíticas preliminares
Aspecto das ameaças e riscos	A estratégia cibernética exige uma coordenação e integração com o sistema de inteligência e deverá dispor de suporte legislativo e judicial.	Categorias temáticas	<i>Intelligence community</i>	Nas situações de crise cibernética o sistema de inteligência coordena, monitora e comunica o cenário situacional cibernético nacional.
	As estratégias no âmbito nacional cibernético, buscam proteger das ameaças e da espionagem global em todos seus níveis de atuação.	Categorias temáticas	<i>National Threats and Risks</i>	Proteger das ameaças e da espionagem global (inteligência de ameaças).
	A estratégia cibernética tem prioritariamente na sua proteção às infraestruturas críticas nacionais, desde o âmbito interno e externo.	Categorias temáticas	<i>Prioritizing protections</i>	Priorizar a proteção nos sistemas dos setores mais críticos da nação.
Aspecto das capacidades e resposta	A estratégia cibernética orienta na criação das capacidades cibernéticas nos diversos sectores do sistema nacional.	Categorias temáticas	<i>Cyber capabilities</i>	Criação de ciber capacidades no sistema nacional.
	A Internet como o ciberespaço, são do controle e interesse do mecanismo da defesa e da segurança nacional.	Categorias temáticas	<i>Cyber defense</i>	Exercer controle no ciberespaço pelo mecanismo da defesa e segurança nacional.
	As estratégias nacional cibernética justificam a carreira da Ciber-militarização e das Ciber-armas para a defesa do ciberespaço e da Internet.	Categorias temáticas	<i>Cyber weapons</i>	Carreira de militarização e armas no ciberespaço.
	A proteção do espaço cibernético incrementa a segurança, reduz as ameaças e os riscos na	Categorias temáticas	<i>Cybersecurity</i>	Proteção do espaço cibernético.

	sociedade informacional.			
	As estratégias militares no ciberespaço, dispõe nas forças armadas sua maior capacidade, atuando na ofensiva orientada nos interesses e objetivos estratégicos nacionais, como uma entidade segregada, independente e com autonomia.	Categorias temáticas	<i>Offensive capabilities</i>	As operações na ofensiva cibernética, dispõe nas forças armadas sua maior capacidade e independência nos demais setores, que também, estejam atuando na segurança e defesa cibernética.
Aspecto do poder de dominação	O ciberespaço como a Internet, são instrumentos de interconexão mundial e globalizador.	Categorias temáticas	<i>Global Connectivity</i>	Instrumentos de interconexão e globalização.
	A estratégia de segurança cibernética irá apoiar na influência da expansão e dominação nacional.	Categorias temáticas	<i>Influence of expansion and domination</i>	Influência de expansão e dominação.
	A política da segurança cibernética e suas estratégias têm como prioridade a segurança nacional. Elas devem estar alinhadas e subordinadas ao sistema da defesa e segurança nacional.	Categorias temáticas	<i>National Protection</i>	Proteção da Segurança Nacional.
	A estratégia nacional cibernética busca regular ou punir as ações cibernéticas que possam atentar aos interesses nacionais.	Categorias temáticas	<i>Regulations and sanctions</i>	Punir as ações cibernéticas que põem em perigo os interesses nacionais.
Aspecto geopolítico e diplomático	Para o fortalecimento da estratégia nacional cibernética se precisa dos outros sistemas nacionais, de seus aliados e sócios estratégicos.	Categorias temáticas	<i>Cyber partners</i>	Integração em outros sistemas nacionais, aliados e sócios estratégicos.
	O poder cibernético nacional estrutura-se em base ao incremento e gestão centralizada do ciberespaço e dos princípios da governança na Internet.	Categorias temáticas	<i>Internet governance</i>	Governança centralizada do ciberespaço através dos princípios da Internet: livre acesso, interoperabilidade, confiável e segura.
Aspecto sociocultural e organizacional	A estrutura da burocracia nos setores é elevada e complexa, a política e programas em segurança cibernética, deverão ser definidos adequadamente para cada um dos setores e suas necessidades. O nível de maturidade do controle interno se torna em um facilitador para que a política seja implementada.	Categorias temáticas	<i>Bureaucracy is vast and complicated</i>	A política e os programas de segurança cibernética devem dispor de mecanismos de controle interno e de facilitadores para sua adequada implementação, devendo ser superada a burocracia e o acionar tecnicista das agências e setores.
	A política de segurança cibernética complementa-se à Lei da transparência e da reforma do sistema nacional de TIC. Pode-se dizer que ela possui características que fazem dela ser um indexador governamental e facilitador de mudanças setoriais.	Categorias temáticas	<i>Government transparency and reforms</i>	A política em segurança cibernética promove e incentiva outras Leis como a criação de reformas nos outros setores do sistema nacional.
	A estratégia em defesa e segurança cibernética orienta dispor nos componentes nacionais uma estrutura de governança da informação e de processos de comando e controle.	Categorias temáticas	<i>Information governance</i>	Governança das informações para a tomada de decisão.
	A política nacional cibernética é um instrumento que promove a integração dos demais componentes do sistema nacional, coordenando e priorizando responsabilidades entre o mecanismo do governo e do setor privado. Sendo o setor da segurança interna os encarregados primários dessas integrações, embora o setor defesa seja quem irá exercer a liderança e condução com os demais componentes em situações de crise nacional de emergências.	Categorias temáticas	<i>Integral component of all sectors</i>	Exercer controle no ciberespaço pelo mecanismo da defesa e segurança nacional.
	O ciberespaço como a Internet, são do interesse geopolítico e da segurança internacional, configurando-se novas relações de poder e de priorização econômica nos atores.	Categorias temáticas	<i>National interest and priorities</i>	Valor geopolítico e econômico.
	As estratégias nacionais no ecossistema cibernético promovem a criação de um entorno de prosperidade e desenvolvimento na sociedade e sujeitos informacionais.	Categorias temáticas	<i>Prosperity and development</i>	Prosperidade e Desenvolvimento na Sociedade.
Aspecto socioeconômico	A política em segurança cibernética encoraja o consumo das tecnologias de informação e da	Categorias temáticas	<i>Centralized purchase</i>	Consumo de tecnologia nacional e consciência da

e comércio	comunicação nacionais buscando consciência de sua dependência tecnológica.			dependência tecnológica.
	O ciberespaço é altamente complexo com grandes investimentos em segurança, desde a perspectiva de custo e efetividade, os programas em segurança e defesa cibernética orientam de forma centralizada a efetivação dos esforços conjuntos em busca de uma otimização de custos e benefícios.	Categorias temáticas	<i>Cost-effectiveness</i>	Elevados investimentos e muito complexo para poder ser securitizado.
	A política de segurança cibernética promove a economia e o mercado digital, tornando -se um pilar do ecossistema digital nacional.	Categorias temáticas	<i>Digital economy and markets</i>	Ecossistema digital, mercado e economia digital.
Aspecto tecnológico e industrial	O impulso das ciber-indústrias em conjunto com a investigação, desenvolvimento e inovação, são um fator prioritário nas estratégias nacionais da segurança e defesa cibernética.	Categorias temáticas	<i>Cyber industries</i>	Promover e impulsionar a inovação, padrões e indústrias em TIC.
	A estratégia de segurança cibernética faz das empresas nacionais, sejam públicas ou privadas, um instrumento de poder cibernético com a finalidade de possuir uma hegemonia política-tecnológica.	Categorias temáticas	<i>Hegemony</i>	Serve como instrumento de poder e de hegemonia política-tecnológica.
	A política e estratégias em segurança cibernética, vão promover a inovação tecnológica com foco estratégico no aumento no acesso à Internet e banda larga nacional.	Categorias temáticas	<i>Strategic focus on Internet</i>	Nações industrializadas modernas promovem o acesso e conectividade à Internet.

Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

Em complemento à definição das categorias, são confirmadas as seguintes características do total de documentos analisados¹⁴⁴:

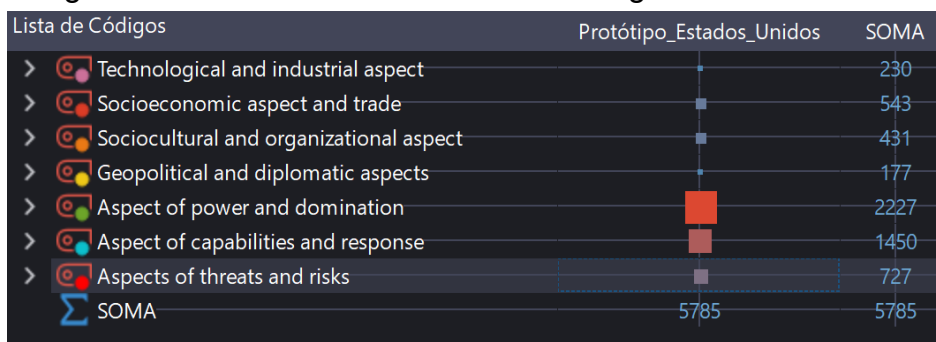
- São 46 os documentos que contém os códigos que representam a categoria temática definida: Aspecto das ameaças e riscos. O código mais influente é “*Intelligence community*” se encontrando em 394 segmentos codificados, representando um 54.2% dos códigos que formam a citada categoria.
- São 86 os documentos que contém os códigos que representam à categoria temática definida: Aspecto das capacidades e resposta, o código mais influente é “*Cyber capabilities*” se encontrando em 541 segmentos codificados, representando um 37.3% dos códigos que formam a citada categoria.
- São 98 os documentos que contém os códigos que representam a categoria temática definida: Aspecto do poder e dominação, o código mais influente é “*National Protection*” se encontrando em 1,998 segmentos codificados, representando um 89.7% dos códigos que formam a citada categoria.
- São 33 os documentos que contém os códigos que representam à categoria temática definida: Aspecto geopolítico e diplomático, o código mais influente é “*Cyber partners*” se encontrando em 116 segmentos codificados, representando um 65.5% dos códigos que formam a citada categoria.

¹⁴⁴ São 106 os documentos analisados no caso do protótipo norte-americano.

- São 58 os documentos que contém os códigos que representam a categoria temática definida: Aspecto sociocultural e organizacional, o código mais influente é “*Information governance*” se encontrando em 161 segmentos codificados, representando um 37.4% dos códigos que formam a citada categoria.
- São 75 os documentos que contém os códigos que representam à categoria temática definida: Aspecto socioeconômico e comércio, o código mais influente é “*Digital economy and markets*” se encontrando em 457 segmentos codificados, representando um 84.2% dos códigos que formam a citada categoria.
- São 46 os documentos que contém os códigos que representam a categoria temática definida: Aspecto tecnológico e industrial, o código mais influente é “*Cyber industries*” se encontrando em 180 segmentos codificados, representando um 78,3% dos códigos que formam a citada categoria.

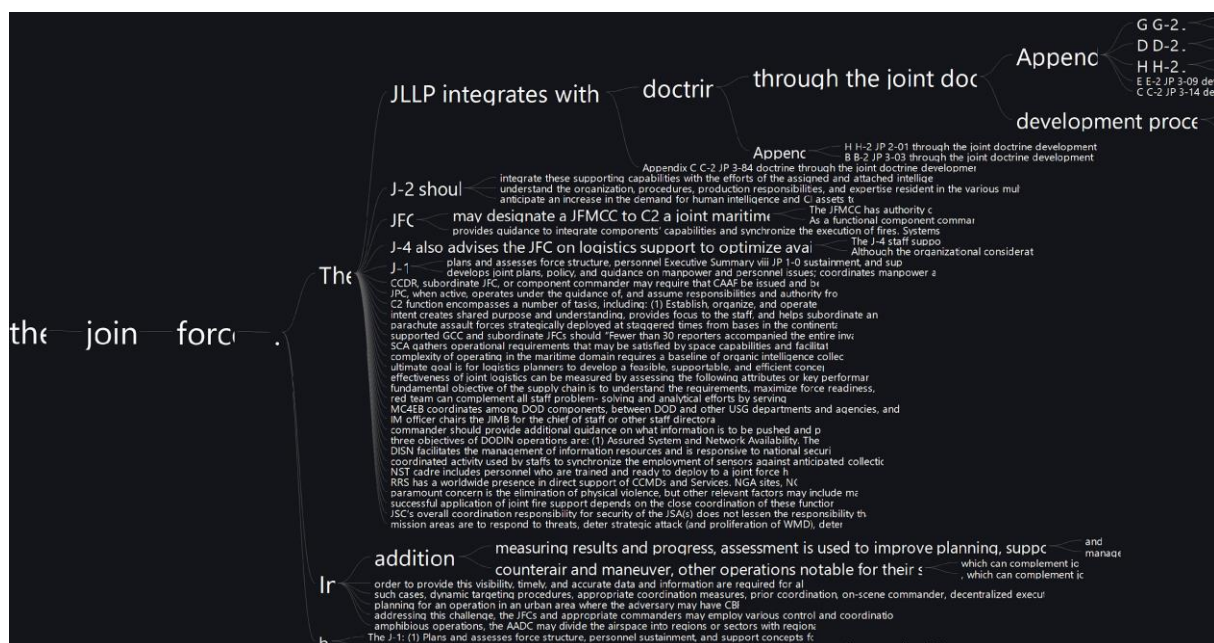
Desta forma, podemos dizer que a categoria: **Aspecto de poder e dominação** (2,227), é a temática de maior relevância para os fins das políticas e estratégicas norte-americanas, no âmbito da segurança e defesa cibernética, seguida da categoria: Aspecto das capacidades e respostas (1450) e do Aspecto das ameaças e riscos (727).

Figura 27 - Visualizador da matriz de códigos norte-americano



Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

Figura 28 - Estrutura de palavras interativas do CDMC



Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

5.4 Conclusões do protótipo norte-americano

Ao finalizar o presente capítulo, do caso protótipo norte-americano, foram testados os diversos tipos de análises que serão aplicados nos estudos de caso de Argentina, Brasil e Peru. Este caso protótipo serviu de auxílio e melhoria de nossos planos de coleta dos dados, desde o próprio conteúdo dos dados até nos procedimentos executados, portanto foi formativo e de treinamento, sendo de ajuda para o pesquisador. Assim, os resultados deste capítulo têm proporcionado *insights* no desenvolvimento das questões relevantes, além de terem esclarecido os conceitos que serão tratados nos próximos capítulos.

Podemos inferir que o panorama da configuração das políticas e estratégias do caso protótipo norte-americano trata-se de sete aspectos: das ameaças e riscos, das capacidades e respostas, do poder e dominação, geopolítico e diplomático, sociocultural e organizacional, socioeconômico e comércio, e tecnológico e industrial.

Ficou demonstrado que o uso dos recursos computacionais na análise de conteúdo tem sido favorável na organização, simplicidade e rapidez, especialmente no que diz respeito ao tratamento quantitativo. Assim, o MAXQDA tem facilitado ao pesquisador na análise das características próprias do documento, como a frequência em que aparecem as palavras e como elas estão sendo combinadas, trazendo os indícios dos subcódigos e códigos tentativos para nossa codificação. Outro aspecto importante a ser citado são as relações descobertas entre os códigos e se aquela

relação é repetitiva nos demais documentos que constituem os corpus estudados. Certamente, muitas dessas simulações foram realizadas fortalecendo a compreensão dos fenômenos, que em princípio não eram do conhecimento e experiência do pesquisador, sendo apresentadas algumas delas na tese. Neste ponto, observa-se a existência de relações indiretas, denominadas pelo pesquisador, de elementos satélites que estariam influenciando na composição de um código, ampliando desta forma as concepções envolvidas desse código em reforço de uma re-teorização na pesquisa.

Com base no exposto, realizamos a análise qualitativa na qual a intuição e o esforço indutivo da codificação desempenham um papel fundamental. A categorização indutiva e os aportes da análise quantitativa ajudaram a desenvolver nossas explicações provisórias, as quais acolhem aos códigos. Finalmente, a integração das explicações são transformadas nas categorias. Dessa forma, obtivemos um ranking das categorias, com a categoria: *“Aspect of power and domination”* ocupando a primeira posição. Isso demonstra a relevância que essa temática possui nos corpus estudados que fizeram parte do protótipo, o caso norte-americano.

Com esse Trabajo, buscamos demonstrar e fornecer orientações para a identificação, análise e sistematização dos elementos e sujeitos envolvidos nas discussões, preocupações e concepções da política, estratégias e doutrinas em segurança e defesa cibernética. Além disso, por meio da identificação das explicações provisórias e categorias, conseguimos ter uma visão inicial dos detalhes e indícios não óbvios presentes nos documentos pesquisados, permitindo-nos estruturar nosso “Estado do Arte” que irá orientar as próximas análises e estudos de casos. Sem dúvida, os Estados Unidos é uma potência mundial que possui influência significativa na arena global da segurança cibernética, como hegemonia política-tecnológica no âmbito cibernético que é reconhecida não apenas por estudos acadêmicos e geopolíticos, mas também por outros países desenvolvidos. No contexto dos países da América do Sul, é razoável afirmar que estão sujeitos à influência dos Estados Unidos no desenvolvimento de políticas e estratégias de segurança cibernética, assim como na organização e estruturação necessárias para esse fim. Para este capítulo em particular, a compreensão e o domínio dos conceitos básicos das teorias que fundamentam nossa coleta de dados foram essenciais para orientar nossa análise, e

esperamos que esses fundamentos sejam igualmente úteis para o desenvolvimento dos próximos capítulos.

“Un día nos daremos cuenta de que en realidad somos el único país de la tierra que trata de entrar em el siglo XXI con la ideología obsoleta del siglo XIX”
Boris Yeltsin, Memórias, 1990, pág. 245

6 APRESENTAÇÃO DOS DADOS DA PESQUISA QUANTITATIVA

O presente capítulo refere-se aos resultados quantitativos obtidos nos estudos de caso argentino, peruano e brasileiro, por meio do software MAXQDA. De forma semelhante ao caso protótipo norte-americano temos realizado o processamento, tratamento e análise dos corpus listados nos apêndices II, III e IV. Desde a perspectiva quantitativa e utilizando a técnica da análise de conteúdo. O processo de exploração e o método estatístico realizados nos corpus dos países pesquisados, buscam obter dados descritivos com o intuito de reforçar, nossa análise qualitativa.

Evidencia-se que a análise e tratamento quantitativo dos estudos de caso pesquisados, têm se beneficiado dos recursos computacionais, servindo de apoio na análise de conteúdo e das características próprias dos documentos estudados, facilitando a codificação. Uma característica importante são as relações diretas e indiretas, avistadas entre os códigos nos corpus estudados.

6.1 Organização e características dos corpus dos países estudados

Para o processo de organização dos documentos, foram constituídos três grupos temáticos com base na hierarquia dos documentos nos países estudados.

Tabela 5 - Organização e características dos corpus estudados

Estudo de Caso	Documentos analisados	Temáticas que constituem um grupo			Características do Corpus
		Leis e regulações nacionais (LRN)	Política e linhas de ação estratégica (PLA)	Publicações do Departamento da Defesa (PDD)	
Argentina	39	5	27	7	Em sua maioria, eles estão no formato website (html) os quais foram exportados e transformados ao “.txt”
Peru	36	13	18	5	Em sua maioria, eles estão em formato PDF (Portable Document Format)
Brasil	33	6	23	4	Em sua maioria, eles estão no formato Portable Document Format (PDF) e “.txt”

Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).
Nota: Recomendamos ler o artigo da investigação (Huamani Cuba, Moura, 2024b, p. 120-125).

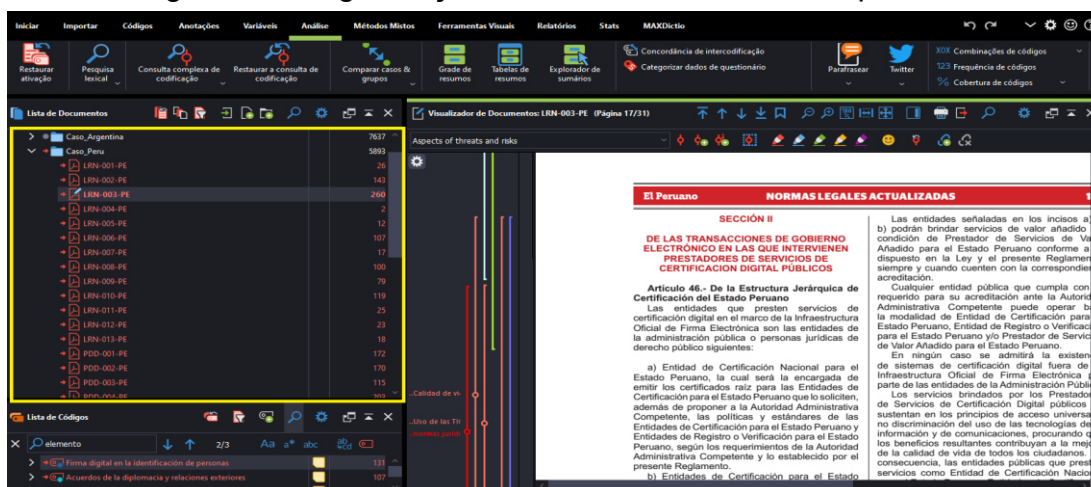
Em seguida, os corpus dos países em estudo foram organizados e etiquetados para, posteriormente, serem submetidos ao *software* MAXQDA para processamento e análise.

Figura 29 - Organização dos documentos do caso argentino



Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

Figura 30 - Organização dos documentos do caso peruano



Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

6.2 Análise e tratamento quantitativo: estudo de caso argentino

A seguir, será apresentado o processo de exploração e o método estatístico realizado no corpus argentino na busca da obtenção dos dados descritivos. Um exemplo, foi a análise do ranking das 20 palavras com maior frequência, resultando as seguintes palavras: nacional, informação, segurança, público, sistema, organismo, defesa, político, ministério, dado, digital, controle, lei, desenvolver, poder, serviço, pessoal, procedimento, modernização e militar. Dessa forma, sucederam outras análises similares, fazendo variações na frequência das palavras. Na Figura 31,

Na seguinte análise das interseções dos códigos, com a opção de exibição binarizada, temos evidenciado que a categoria “*Aspecto sociocultural y organizacional*”, por meio dos códigos: “*Internet y banda ancha*”, “*Personas y organizaciones*”, “*Sociedade*” e “*Tecnologías de la información y las comunicaciones*” possuem o maior número das interseções respeito as outras categorias. Em forma semelhante, foi com a categoria “*Aspecto tecnológico e industrial*”, por meio do único código: “*Redes, sistemas de información y telecomunicaciones*”. Desse jeito foram observadas, a relevância dos subcódigos e códigos nas categorias, bem como a interceptação deles nas outras categorias.

Figura 35 - Visualizador das conexões entre códigos

Lista de Códigos	Recibir el futuro próspero de las tecnologías	Cooperación internacional	Escenario internacional	Mecanismos internacionales de cooperación	Realidad y cambio tecnológico	Visión integradora y desarrollo	SOMA
> [C] Aspecto de las amenazas y riesgos							6230
> [C] Aspecto de las capacidades y respuesta							19334
> [C] Aspecto de poder y dominación							7421
> [C] Aspecto geopolítico y diplomático							1593
> [C] Aspecto sociocultural y organizacional							17872
> [C] Aspecto socioeconómico y comercio							855
> [C] Aspecto tecnológico e industrial							5289
Σ SOMA	19	203	148	47	79	65	50554

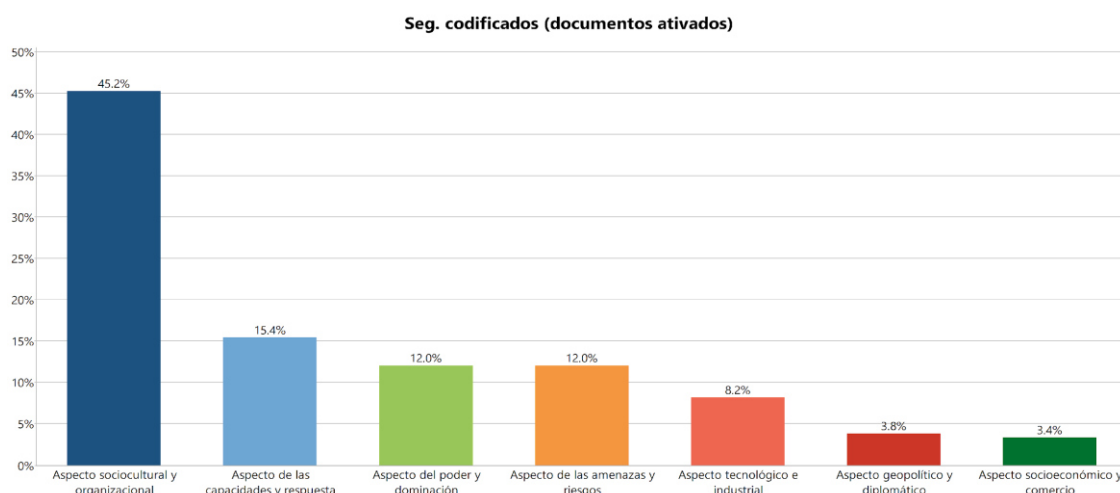
Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

Portanto, evidencia-se que os códigos “*Personas y organizaciones*” e “*Seguridad de la información*” possuem as maiores frequências, com 224 e 185 segmentos codificados respectivamente. Assim inferimos que o corpus do caso argentino busca atender critérios ou necessidades relacionadas às pessoas e organizações, para os fins da política da segurança da informação. Para o Estado argentino seriam de maior relevância em suas pretensões, as ações voltadas para as capacidades e respostas nacionais em segurança cibernética.

capacidades e resposta (15,4%). Ao comparar esses resultados com a análise documental é o inverso, porém com um menor valor diferencial entre elas.

Finalmente, tanto na análise do corpus como nos questionários, tem resultados semelhantes, onde as preocupações relacionadas com o aspecto socioeconômico e comercio se encontram na última posição do ranking das categorias.

Figura 38 - Visão geral dos códigos no primer nível dos questionários analisados do caso argentino (categorias)



Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

6.3 Análise e tratamento quantitativo: estudo de caso peruano

Em seguida, apresentamos a exploração e o método estatístico realizado no corpus peruano, para obtenção de dados descritivos. Ao analisar a frequência das palavras contidas no corpus, observamos uma sutil semelhança com o caso argentino. No ranking das 20 palavras com maior frequência, aparecem as palavras: informação, nacional, público, lei, sistema, segurança, dado, serviço, entidade, processar, digital, software, pessoal, desenvolvimento, gestão, governar, acesso, político, norma, eletrônico. Dessa forma sucederam outras análises similares, sendo testadas múltiplas variações na frequência das palavras. Na Figura 39, observa-se as 100 primeiras palavras, com uma frequência mínima de 5, lematizando as palavras no idioma espanhol.

Figura 40 - Combinações de palavras caso peruano



Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

No caso peruano se teve como resultado um total de 5,898 segmentos codificados. Ao analisar a frequência dos códigos, o código de maior frequência foi “*Personas y organizaciones*”, com 485 segmentos com código, um pouco mais que o dobro do caso argentino. Porém, os próximos códigos de maior frequência são: “*Capacidades*”, “*Normas jurídicas, marcos regulatorios, estándares y protocolos*”, “*Atribuir responsabilidad*”, “*Gobierno digital e electrónico*” e “*Redes, sistemas de información y telecomunicaciones*”, estando em evidência as diferenças entre o conteúdo do corpus peruano, em relação ao argentino. Nesta análise é evidente que o caso peruano, trouxe uma maior preocupação na adoção das capacidades e estratégias na governança digital e jurídica pelas entidades públicas. Não obstante, no caso argentino, está mais relacionado com a segurança da informação e do emprego dos instrumentos militares na proteção, atribuição de responsabilidades e jurídicas.

Figura 41 - Frequência de códigos caso peruano (unidade: segmentos com códigos)

	n	Frequência	Porcentagem
Personas y organizaciones		485	8.2
Capacidades		217	3.7
normas jurídicas, marcos regulatorios, estándares y protocolos		216	3.7
Atribuir responsabilidad		202	3.5
Gobierno digital e electrónico		186	3.2
redes, sistemas de información y telecomunicaciones		174	3.0
Componentes		132	2.2
Prevención, detección, respuesta y recuperación		131	2.2
Gestión pública o del gobierno		130	2.2
Internet y banda ancha		115	2.0
Seguridad de la información		92	1.6
Presupuesto para necesidades		84	1.4
Tecnologías de la Información y las comunicaciones		83	1.4
Gestión de riesgos		83	1.4
Amenazas		82	1.4
Defensa nacional		76	1.3
Entidades de la administración pública		74	1.3
Seguridad nacional		71	1.2
Poder Ejecutivo		67	1.1
Sector público		62	1.1
Sistemas de Información		61	1.0
economía		60	1.0
Inteligencia		52	0.9
Constitución política-nacional		51	0.9
Formación de profesionales, técnicos e investigadores		50	0.8

Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

Para as duas seguintes análises só tomamos em consideração os subcódigos que dispõem de 5 a mais segmentos codificados. Observando-se no mapa de códigos que as relações entre os códigos “*Capacidades*” e “*Atribuir responsabilidad*” constituem o mesmo grupo (cor amarelo). Em comparação com o caso argentino, o código “*Capacidades*” tinha uma relação mais próxima, com o acionar das forças armadas e defesa nacional. No caso peruano, acontece em menor intensidade, adotando a maior frequência no código “*Personas y organizaciones*”. Este entendimento nos permite inferir que as capacidades desejadas no contexto peruano estão sendo focalizado no âmbito das pessoas e entidades públicas.

Figura 42 - Mapa de códigos corpus caso peruano



Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

Na Figura N° 42 se visualizam as conexões entre códigos, por meio das interseções dos códigos em um segmento e em base à soma total das interseções. Com a análise realizada as categorias tiveram as seguintes resultados: “*Aspecto sociocultural y organizacional*” (16,985), “*Aspecto de las capacidades y respuesta*” (8,671), “*Aspecto de poder y dominación*” (4,027), “*Aspecto tecnológico e industrial*” (3,083), “*Aspecto de las amenazas y riesgos*” (2,640), “*Aspecto socioeconómico y comercio*” (1,338) e “*Aspecto geopolítico y diplomático*” (306). Ao aprofundar a análise das interseções dos códigos, se evidencia que 36 dos códigos da categoria “*Aspecto sociocultural y organizacional*” possuem o maior número das interseções em relação a todas as categorias, porém, existem códigos das outras categorias que possuem mais de duas interseções, como no caso da categoria “*Aspecto geopolítico y diplomático*”, por meio dos códigos “*Fenómenos*” e “*Control de recursos naturales y estratégicos*”.

nas respostas dos especialistas. Os três códigos com maior relevância dentro dessa categoria são as seguintes:

- a. Governo e gestão da informação governamental (31 segmentos codificados).
- b. Impulsar o governo eletrônico na gestão pública (22 segmentos codificados).
- c. Instrumentar as políticas públicas para sua articulação estatal (18 segmentos codificados).

Figura 45 - Comparar frequências de categorias com tabela cruzada do caso peruano

Tabela de referência cruzada

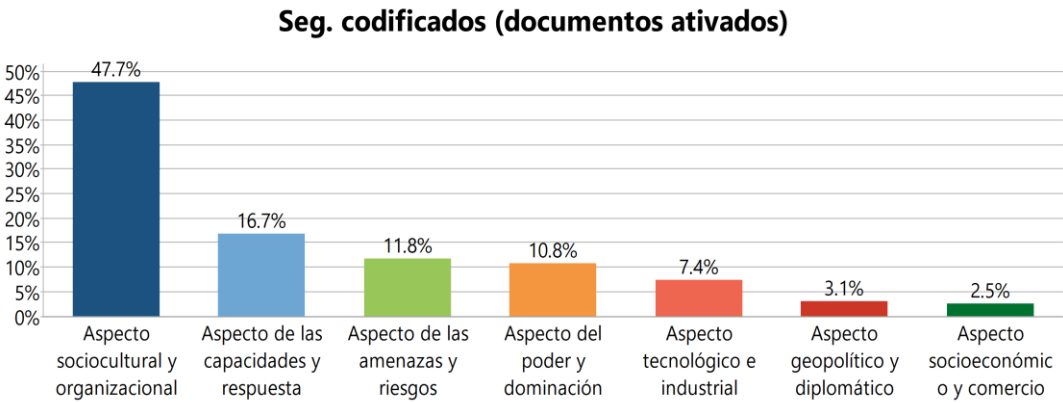
	Questionario_Peru_1	Questionario_Peru_2	Questionario_Peru_3	Questionario_Peru_4	Questionario_Peru_5	Questionario_Peru_6	Questionario_Peru_7	Questionario_Peru_8	Total
> Aspecto tecnológico e industrial	2.6%	17.6%			13.6%	5.9%	7.5%	9.1%	7.4%
> Aspecto socioeconómico y comercio	7.9%				3.4%	2.0%	3.0%		2.5%
> Aspecto sociocultural y organizacional	34.2%	29.4%	63.4%	72.7%	45.8%	39.2%	52.2%	63.6%	47.7%
> Aspecto geopolítico y diplomático	7.9%	2.9%			1.7%	5.9%	3.0%		3.1%
> Aspecto del poder y dominación	13.2%	5.9%	19.5%		11.9%	11.8%	9.0%	9.1%	10.8%
> Aspecto de las capacidades y respuesta	23.7%	29.4%	12.2%	22.7%	13.6%	13.7%	11.9%	18.2%	16.7%
> Aspecto de las amenazas y riesgos	10.5%	14.7%	4.9%	4.5%	10.2%	21.6%	13.4%		11.8%
Σ SOMA	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
# N = Documentos	1 (12.5%)	1 (12.5%)	1 (12.5%)	1 (12.5%)	1 (12.5%)	1 (12.5%)	1 (12.5%)	1 (12.5%)	1 (100.0%)

Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

Dessa análise, segundo as respostas dos especialistas podemos deduzir que a categoria do aspecto sociocultural e organizacional tem a maior relevância (47,7%), após do aspecto das capacidades e resposta (16,7%). Esse resultado ao compará-lo aos resultados da análise documental, se obteve resultados semelhantes e próximos em proporção.

Finalmente, se observa que as preocupações relacionadas com o aspecto socioeconômico e comércio possui só um 2,5% do ranking das categorias, resultado semelhante ao caso argentino.

Figura 46 - Visão geral dos códigos no primer nível dos questionários analisados do caso peruano (categorias)

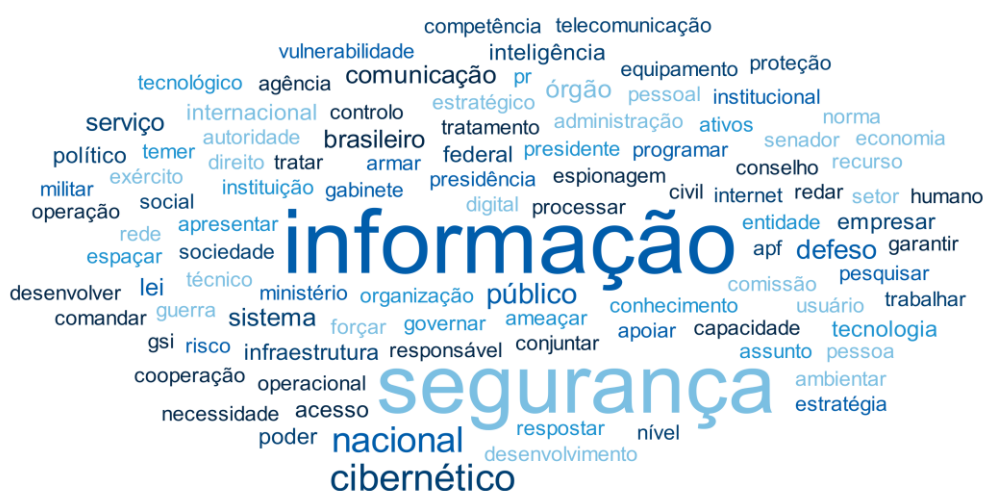


Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

6.4 Análise e tratamento quantitativo: estudo de caso brasileiro

Ao igual que nos dois casos anteriores, apresentamos a exploração e o método estatístico realizado no corpus brasileiro, buscando obter dados descritivos. Ao analisar o ranking das 20 palavras com maior frequência, nossos resultados foram as seguintes palavras: informação, segurança, cibernético, nacional, pessoa (brasileiro), público, defesa, comunicação, serviço, órgão, sistema, lei, acesso, processar (tratar), inteligência, federal, empresa, poder, político, tecnologia. Na Figura N°64, observa-se as 100 primeiras palavras, com uma frequência mínima de 5, palavras lematizadas em idioma português.

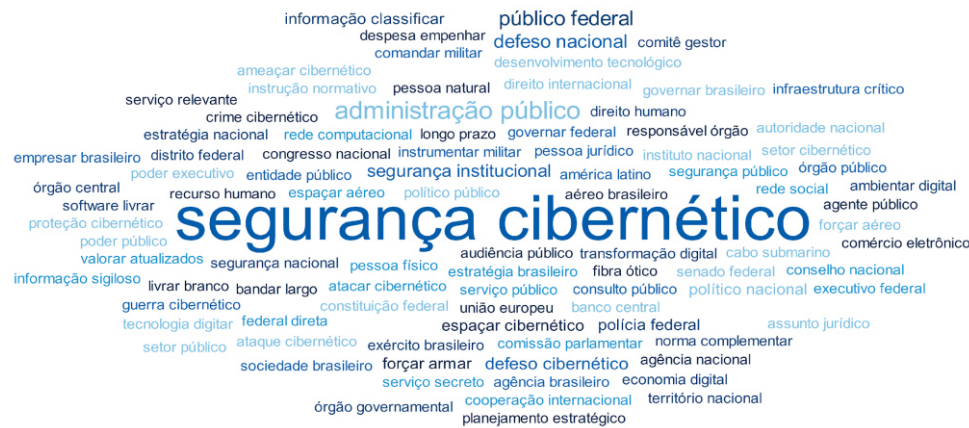
Figura 47 - Nuvem de palavras do caso brasileiro



Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

Em seguida, realizamos a análise das combinações de palavras, procurando combinações de palavras “com 2 para 2 palavras”, com um mínimo de 5 caracteres. Se observa que as duas primeiras palavras do ranking são: Segurança cibernética e Administração pública, sobressaindo em um 54.55% e 78.79% respectivamente. Após, as palavras: Público federal, Defesa nacional e Segurança institucional, percebeu-se em um 78.79%, 51.52% e 66.67% respectivamente.

Figura 48 - Combinações de palavras caso brasileiro



Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

Evidencia-se também que a soma dos segmentos codificados, no corpus estudado é de 13,783. Na análise da frequência de códigos, a Segurança cibernética, tem a maior frequência com 372 segmentos. Porém, os próximos códigos de maior frequência são: Internet, Segurança da informação e comunicações, Inteligência, Economia e financeiro e Riscos.

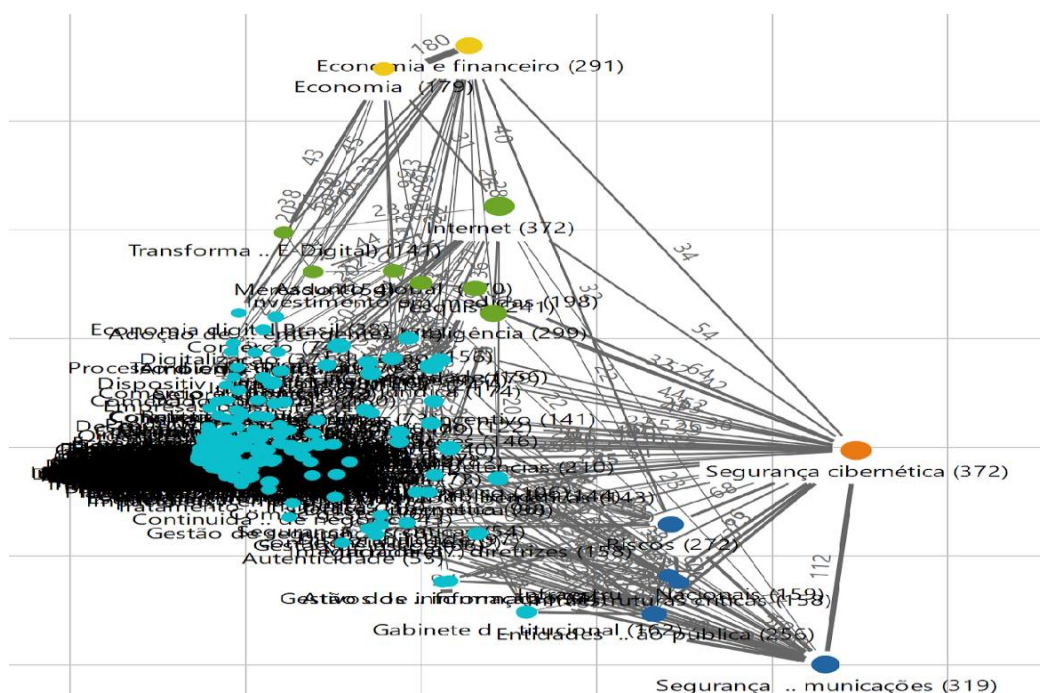
Figura 49 - Frequência de códigos caso brasileiro

Unidade: Segamentos com código		
	Frequência	Porcentagem
Segurança cibernética	372	2,7
Internet	372	2,7
segurança da informação e comunicações	319	2,3
Inteligência	299	2,2
Economia e financeiro	291	2,1
Riscos	272	2,0
Entidades da administração pública	256	1,8
Militar	241	1,7
Pesquisa	241	1,7
Espionagem	222	1,6
Atribuições e competências	210	1,5
Investimento em medidas	198	1,4
Cooperação	169	1,2
Economia	179	1,3
Legislação e assitência jurídica	174	1,3
Assunto global	170	1,2
Gabinete de segurança institucional	162	1,2
Infraestruturas Críticas Nacionais	159	1,1
Infraestruturas críticas	158	1,1
Marrodiretores ou diretores	159	1,1
Cultura cibernética e de sociedade	156	1,1
Educação	156	1,1
Mercado	154	1,1
Dados pessoais	150	1,1
Organizações	148	1,1

Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

Desde a análise do mapa de código, observamos que as relações entre o código Segurança cibernética, com o grupo de códigos de cor azul envolvem preocupações dos riscos, da segurança das informações e das comunicações e das infraestruturas críticas nacionais. Porém, é mais distante a relação com o grupo amarelo que concentra os tópicos econômicos e financeiros. Desse mesmo modo, os códigos que integram o grupo de códigos de cor verde tratam tópicos como estratégia digital, Internet, investimentos, pesquisa, assuntos globais e de mercado.

Figura 50 - Mapa de códigos corpus caso brasileiro



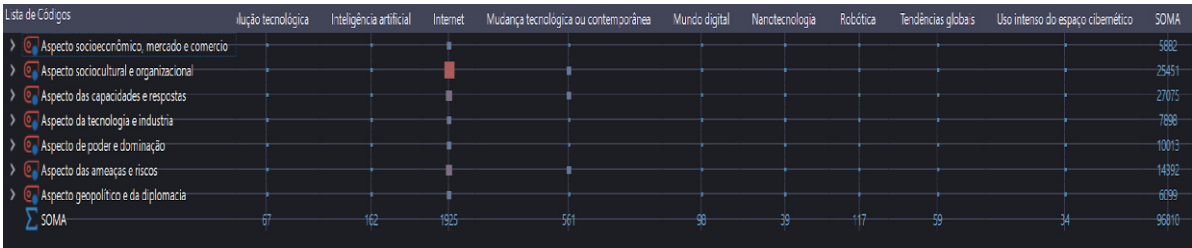
Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

Na Figura N° 68, observamos as conexões das interseções dos códigos em um segmento. Se evidenciando as categorias por sua relevância, sendo as seguintes: Aspecto das capacidades e resposta (27,075), Aspecto sociocultural e organizacional (25,451), Aspecto das ameaças e riscos (14,392), Aspecto de poder e dominação (10,013), Aspecto da tecnologia e industrial (7,898), Aspecto geopolítico e diplomático (6,099) e Aspecto socioeconômico, mercado e comércio (5,882). Com a análise mais aprofundada das interseções dos códigos, se evidencia que a categoria “Aspecto das capacidades e respostas” por intermeio do código atividades sobrepostas de SIC (segurança da informação e da comunicação) e SegCiber (segurança cibernética) possuem o maior número das interseções (exibição binarizada: 402), em relação às

outras categorias. Porém, existem códigos das outras categorias que possuem interseções com os outros códigos das demais categorias, como por exemplo:

- Participação dos atores públicos, privados e sociedade (exibição binarizada: 370),
- Ameaças, riscos e problema de interesse nacional (exibição binarizada: 359),
- Governo e gestão da informação governamental (exibição binarizada: 352),
- Fatores de preocupação e impacto geopolítico e geoeconômico (exibição binarizada: 349),
- Instrumentalizar as políticas públicas na articulação nacional (exibição binarizada: 344).

Figura 51 - Visualizador das conexões entre códigos caso brasileiro



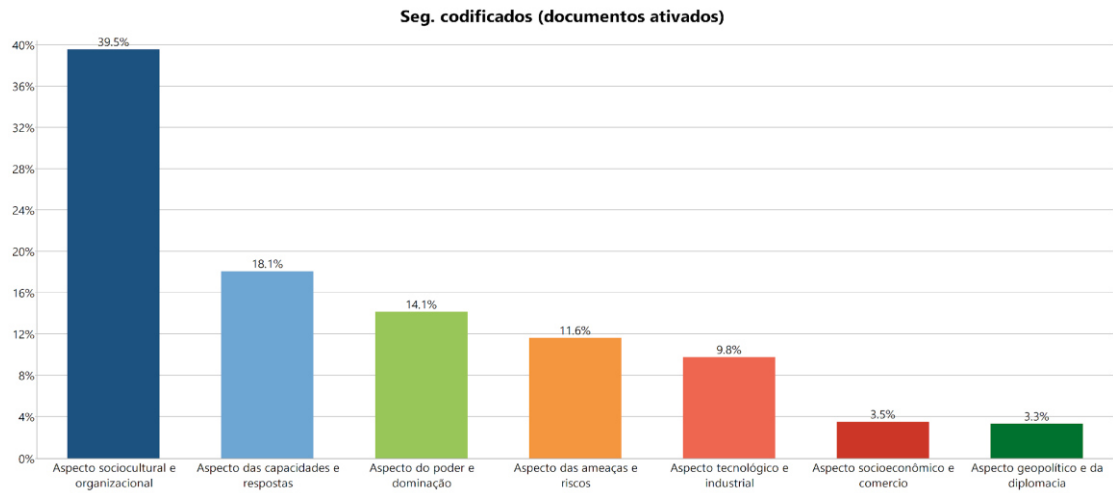
Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

A seguir na Figura N°69 são apresentados os códigos que possuem uma maior frequência nos documentos analisados. Por exemplo: Segurança cibernética e Internet, ambos aparecem em 372 segmentos codificados, bem como, Segurança da informação e comunicações, Inteligência e Economia e financeiro com 319, 299 e 291 segmentos codificados respectivamente.

Podemos inferir, no caso brasileiro, que o aspecto das capacidades e resposta estão motivadas, principalmente, pelas atividades sobrepostas entre a SIC e a SegCiber, tendo ao GSI (Gabinete de Segurança Institucional da Presidência da República) como seu principal ator. Outro sim, é que no aspecto sociocultural e organizacional, os maiores esforços estariam desde a busca de uma participação dos atores públicos, privados e sociedade, não obstante, o instrumentalizar as políticas públicas na articulação nacional e as preocupações do governo e gestão da informação governamental, seriam parte desses esforços.

relacionadas ao aspecto geopolítico e da diplomacia possui somente um 3,3% do ranking das categorias, esses resultados são próximos ao estudo de caso argentino.

Figura 54 - Visão geral dos códigos no primer nível dos questionários analisados do caso brasileiro (categorias)



Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

6.5 Síntese quantitativa dos reflexos observados na Argentina, Peru e Brasil

Uma vez concluídas as análises quantitativas dos estudos de casos da Argentina, Peru e Brasil, buscaram-se apresentar uma síntese dos reflexos observados. Com o intuito de providenciar a propagação dos dados quantitativos, facilitando uma compreensão comparativa dos casos estudados.

Quadro 21 - Síntese quantitativa dos reflexos observados na Argentina, Peru e Brasil

Assuntos	Corpus documental argentino	Corpus documental peruano	Corpus documental brasileiro
Frequência dos códigos	São trazidas em maior frequência as seguintes códigos: • <i>Personas y organizaciones.</i> • <i>Seguridad de la información.</i> • <i>Sector público.</i> • <i>Prevención, detección, respuesta y recuperación.</i> • <i>Atribuir responsabilidad.</i> • <i>Ministerio de modernización.</i>	São trazidas em maior frequência as seguintes códigos: • <i>Personas y organizaciones.</i> • <i>Capacidades.</i> • <i>Normas jurídicas, marcos regulatorios, estándares y protocolos.</i> • <i>Atribuir responsabilidad.</i> • <i>Gobierno digital e electrónico.</i> • <i>Redes, sistemas de información y telecomunicaciones.</i>	São trazidas em maior frequência as seguintes códigos: • Segurança cibernética. • Internet. • Segurança da informação e comunicações. • Inteligência. • Economia e financeiro. • Riscos.
Relações e conexões dos códigos	O código “ <i>personas y organizaciones</i> ” ocupam uma posição central e de conexão com os outros grupos de códigos. Porém, ele tem maior proximidade com as temáticas trazidas da segurança da informação, cibersegurança, ameaças, incidentes, regulações e os riscos. Outro aspectos foi que as “ <i>capacidades</i> ” estão relacionadas em maior	As relações entre os códigos “ <i>Capacidades</i> ” e “ <i>Atribuir responsabilidad</i> ” constituem um grupo, possuindo menor ponderação no âmbito da defesa e das forças armadas peruanas. Porém, essas capacidades estão sendo focalizadas no âmbito das pessoas e das outras entidades públicas.	As relações e conexões do código de segurança cibernética e o grupo azul (envolvem preocupações dos riscos, da segurança das informações e das comunicações e das infraestruturas críticas nacionais) são as mais próximas e intensas. Porém, a segurança cibernética tem relações e conexões menos

	ponderação no âmbito da defesa e das forças armadas argentinas.		intensas com o grupo em amarelo (concentra os tópicos econômicos e financeiros).
Análise das interseções dos códigos	É evidenciado que a categoria “ <i>Aspecto sociocultural y organizacional</i> ” por meio dos códigos: <i>Internet y banda ancha</i> , <i>Personas y organizaciones</i> , <i>Sociedade</i> e <i>Tecnologías de la información y las comunicaciones</i> ; possui o maior número de interseções com as outras categorias. De forma similar, foi encontrado com a categoria “ <i>Aspecto tecnológico e industrial</i> ” por meio do único código: <i>Redes, sistemas de información y telecomunicaciones</i> .	36 dos códigos da categoria “ <i>Aspecto sociocultural y organizacional</i> ” possuem o maior número das interseções em relação a todas as categorias. Existem códigos das outras categorias que possuem mais de duas interseções, como no caso da categoria: “ <i>Aspecto geopolítico y diplomático</i> ”, por meio de seus códigos “ <i>Fenómenos</i> ” e “ <i>Control de recursos naturales y estratégicos</i> ”.	Se evidencia que a categoria “ <i>Aspecto</i> das capacidades e respostas” por intermédio do código atividades sobrepostas de SIC (segurança da informação e da comunicação) e SegCiber (segurança cibernética), possuem o maior número das interseções (exibição binarizada: 402) em relação às outras categorias. Existem códigos das outras categorias que possuem interseções significativas, entre eles as seguintes: • Participação dos atores públicos, privados e sociedade (exibição binarizada: 370), • Ameaças, riscos e problema de interesse nacional (exibição binarizada: 359), • Governo e gestão da informação governamental (exibição binarizada: 352), • Fatores de preocupação e impacto geopolítico e geoeconômico (exibição binarizada: 349), • Instrumentalizar as políticas públicas na articulação nacional (exibição binarizada: 344).
Inferências do análise de frequências	Se evidencia, que os códigos “ <i>Personas y organizaciones</i> ” e “ <i>Seguridad de la información</i> ” tem as maiores frequências, com 224 e 185 segmentos codificados respectivamente. Podemos inferir que o corpus do caso argentino busca atender critérios ou necessidades relacionadas às pessoas e organizações para os fins da política da segurança da informação. Para o Estado argentino seriam de maior relevância em suas pretensões, as ações voltadas para as capacidades y respostas nacionais em segurança cibernética.	Se observa que os códigos “ <i>Personas y organizaciones</i> ” e “ <i>Capacidades</i> ” possuem a maior frequência nos segmentos codificados. Os tópicos como: governo digital e eletrônico, normas jurídicas, marcos regulatórios, padrões e protocolos, também, tem uma maior frequência no corpus analisado. Podemos inferir, no caso peruano, que a busca das capacidades é em atenção aos critérios e necessidades relacionadas às pessoas e organizações, desde os objetivos das políticas e estratégias do governo digital e eletrônico, tendo como seu principal ator à SegDi (Secretaría de Gobierno e Transformación Digital da Presidência do Conselho de Ministros).	Entre os códigos que possuem uma maior frequência no corpus analisado estão a segurança cibernética e a Internet, ambos possuem 372 segmentos codificados. Porém, códigos como a segurança da informação e comunicações, inteligência, economia e financeiro seguem a listagem. Podemos inferir, no caso brasileiro, que o aspecto das capacidades e resposta vem sendo motivadas principalmente pelas atividades sobrepostas entre a SIC e a SegCiber, tendo o GSI (Gabinete de Segurança Institucional da Presidência da República) como seu principal ator. Outro sim, é que no aspecto sociocultural e organizacional, os maiores esforços estariam desde a busca de uma participação dos atores públicos, privados e sociedade, não obstante, o instrumentalizar as políticas públicas na articulação nacional e as preocupações do governo e gestão da informação governamental, seriam também, parte desses esforços.
Análises aos questionários realizados aos especialistas	A categoria “ <i>Aspecto sociocultural y organizacional</i> ” está em maior porcentagem nas respostas dos especialistas. Os códigos mais discutidos pelos especialistas são as seguintes: Governo e gestão da informação governamental, Instrumentar as políticas públicas para sua articulação estatal,	A categoria “ <i>Aspecto sociocultural y organizacional</i> ” está em maior porcentagem nas respostas dos especialistas. Os códigos mais discutidos pelos especialistas são as seguintes: Governo e gestão da informação governamental. Impulsar o governo eletrônico na	A categoria do “ <i>Aspecto sociocultural e organizacional</i> ” está em maior porcentagem nas respostas dos especialistas. Os códigos mais discutidos pelos especialistas são as seguintes: Instrumentalizar as políticas públicas na articulação nacional. Participação dos atores públicos,

	Formação e tecnificação do recurso humano da rede pública.	gestão pública. Instrumentar as políticas públicas para sua articulação estatal.	privados e sociedade. Governo e gestão da informação governamental.
Ranking das categorias, segundo os questionários realizados aos especialistas.	• Aspecto sociocultural e organizacional (45,2%), • Aspecto das capacidades e resposta (15,4%), • Aspecto do poder e dominação (12%), • Aspecto das ameaças e riscos (12%), • Aspecto tecnológico e industrial (8,2%), • Aspecto geopolítico e diplomático (3,8%), • Aspecto socioeconômico e comércio (3,4%).	• Aspecto sociocultural e organizacional (47,7%), • Aspecto das capacidades e resposta (16,7%), • Aspecto das ameaças e riscos (11,8%), • Aspecto do poder e dominação (10,8%), • Aspecto tecnológico e industrial (7,4%), • Aspecto geopolítico e diplomático (3,1%), • Aspecto socioeconômico e comércio (2,5%).	• Aspecto sociocultural e organizacional (39,5%), • Aspecto das capacidades e resposta (18,1%), • Aspecto do poder e dominação (14,1%), • Aspecto das ameaças e riscos (11,6%), • Aspecto tecnológico e industrial (9,8%), • Aspecto socioeconômico e comércio (3,5%), • Aspecto geopolítico e diplomático (3,3%).

Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

No presente capítulo, foram aproveitadas as diversas análises, ferramentas visuais e métodos estatísticos do software MAXQDA, sendo observado e analisado uma abordagem analítica-quantitativa, combinadas desde três componentes: dados, evidências e ideias.

Os “dados transformados em evidências” sustentam a afirmação sobre um exemplo particular de alguma ideia geral em que queremos que outras pessoas (colegas de nossa tribo científica, de outros campos, políticos, o público em geral) acreditem ou pelo menos aceitem por enquanto. Para os cientistas, a ideia na maior parte das vezes pertence a um sistema mais geral de ideias ou conceitos que chamamos de “teoria”. O apoio que os dados dão a uma ideia transforma-a em evidência. Dados, evidências e ideias formam um círculo de interdependências (Howard, p.20, 2022).

Como parte de nossos resultados preliminares, foram apresentadas as diferenças entre os estudos de casos argentino, peruano e brasileiro desde diversas perspectivas, alcançando assim um de nossos objetivos, de buscar ampliar nossa compreensão dos aspectos, categorias e códigos relacionados com a segurança cibernética dos três países estudados. Entre as perspectivas analisadas temos: o conteúdo, o contexto dos temas, as relações produzidas dos códigos e/ou das categorias, como também, dos elementos e agentes que se organizam nos três estudos de casos citados. Portanto, este capítulo serve de antessala aos próximos capítulos onde desenvolveremos em profundidade nossa análise qualitativa.

“Não esmaga as vontades, mas enfraquece-as, domina-se e as dirige; raramente força alguém a agir, mas constantemente opõe resistência à ação; não destrói, mas impede nascimento; não tiraniza, mas torna-se obstáculo”

Alexis de Tocqueville

7 ANÁLISE QUALITATIVA DOS ESTUDOS DE CASOS PESQUISADOS

O propósito deste capítulo é descrever de forma sistemática a aplicação da análise de conteúdo no âmbito da segurança e defesa nacional cibernética dos três países pesquisados. Lembrando, no caso protótipo norte-americano foram analisados um total de 106 documentos oficiais com o apoio computacional, sendo testadas diversas técnicas de análise tanto na perspectiva quantitativa e qualitativa. Ademais, nos permitiu identificar, sistematizar e analisar os elementos e agentes, conformando nosso Estado da Arte que vai direcionar, principalmente, a uma análise qualitativa mais ampla para os estudos de caso pesquisados.

Logo, por cada estudo de caso foi organizado um único corpus por cada país. Assim, analisamos um total de 108 documentos oficiais, devido às limitadas publicações oficiais no âmbito da segurança cibernética, no Internet. Esta limitação é mais expressiva, em relação às publicações da doutrina militar conjunta para a defesa cibernética dos três países estudados.

Portanto, apoiados no preliminar análise quantitativa, foram definidas as categorias que agrupam os códigos e subcódigos identificados na análise indutiva dos corpus. Infere-se que a exploração precoce realizada no caso protótipo norte-americano, proporcionou *insight* nos tópicos e teorias envolvidas no estudo. Dessa forma, servem de complemento aos reflexos observados no referencial teórico, servindo de apoio ao refinamento da nossa coleta de dados em relação ao conteúdo dos dados e aos procedimentos realizados. As longas e indispensáveis leituras em conceitos abrangendo a defesa e segurança cibernética, compreendendo a fundo a historicidade e as perspectivas teóricas das diversas áreas de conhecimento, facilitou nossa observação e condução da análise para a identificação dos subcódigos e códigos, dos quais foram agrupados em sete aspectos que constituem nossas categorias.

No processo de construção das categorias, o pesquisador percorreu pela exploração através da codificação para ser triangulada com os resultados observados, onde foram concebidas nossas unidades de registros, dessa forma a realizar a categorização. Ressalta-se que os subcódigos e códigos, em relação ao estudo de caso argentino e peruano, por estar no idioma espanhol, há a probabilidade de se repetir para ambos os estudos, porém, o *software* MAXQDA, permite ativar e desativar de modo seletivo os documentos e as codificações realizadas nos diversos corpus, segregando dessa forma os resultados de ambos os estudos.

Além disso, serão apresentados a técnica de **entrevistas semiestruturadas** que foram conduzidas a partir de um roteiro de perguntas abertas e que guardam relação com as nossas categorias, pressupostos e temas envolvidos em nosso problema de pesquisa, com o intuito de vasculhar nas experiências dos especialistas governamentais para extrair as informações valiosas que não estariam detalhadas nos corpus estudados. Os **questionários semiestruturados** foram realizados via formulários online, com a promessa de confidencialidade e anonimato, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. Os instrumentos de pesquisa utilizados foram enviados desde a conta de e-mail da UFMG, com a finalidade de formalizar, estimular e gerar confiança nos participantes para que possam responder livremente em relação aos tópicos questionados ou consultados nas entrevistas e questionários. Todas as entrevistas foram gravadas com a permissão dos entrevistados, sempre com a promessa de proteger seus dados pessoais, segundo a Lei 13,709 LGPD¹⁴⁹.

O objetivo do pesquisador, foi explorar ao máximo as percepções dos entrevistados frente aos fenômenos próprios dos contextos e das particularidades problemáticas de suas localidades pesquisadas, ou seja, as entrevistas confirmaram a importância de cada uma delas para o objetivo da pesquisa. A estratégia adotada foi muito importante, ao ponto de ter levado aos entrevistados a manifestarem segundo sua consciência descritiva e prática, aspectos particulares de seu contexto, meio social e opinião crítica do exercício de suas funções, relacionamentos e atividades, que se envolvem, nas políticas públicas governamentais do âmbito da pesquisa, relatando eventos marcantes que fortaleceram as questões de interesse de

¹⁴⁹ Lei Geral de Proteção de Dados Pessoais. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm>. Acesso em 20 de setembro de 2021.

nosso estudo. Redigido, ao final, nos relatórios dos estudos de caso dos três países pesquisados na tese.

A partir de então, nas próximas seções apresentaremos os temas que norteiam o estudo de caso argentino, peruano e brasileiro. Nesta vez, vamos nos focalizar no estudo das categorias e aspectos, através da análise qualitativa. A fim de poder abordá-los de forma crítica e produtiva, no desejo de fortalecer as análises preliminares, como também, elucidar os achados quantitativos descritos nos capítulos anteriores. Além disso, as questões analisadas nas entrevistas e dos questionários envolvem particularidades estruturais, aspirando ampliar nossa compreensão dos fenômenos presentes nos casos citados. Portanto, identificar práticas que poderiam definir o panorama das configurações políticas e estratégicas no âmbito da segurança cibernética dos três países pesquisados.

7.1 Análise qualitativa do estudo de caso argentino

Segundo a Tabela N°31 podemos observar as categorias definidas para o corpus do estudo de caso argentino, considerando as peculiaridades inerentes e o contexto que as envolvem. Porém, no estudo de caso argentino, se vislumbram os elementos e seus agentes, que possam estar envolvidos nas estratégias, como também, dos elementos que constituem a política em segurança cibernética.

Quadro 22 - Categorias do caso argentino

Categorias	Tipos de categorias	Código	Notas Analíticas preliminares
Aspecto das ameaças e riscos	Categorias temáticas	<i>"Vigilancia y control de los individuos"</i>	Preocupação do Estado em dispor das ferramentas e instrumentos de vigilância digital e de controle informacional para prevenção criminal, por meio do monitoramento e observação dos indivíduos nas redes informáticas e da comunicação.
	Categorias temáticas	<i>"Factores de preocupación nacional y de impacto en la sociedad"</i>	Devido ao multiculturalismo, as discussões e preocupações da sociedade estão centradas nas relações de trabalho, direitos humanos e na sustentabilidade econômica, além de serem inclusivas. Busca a segurança estratégica na proteção dos direitos essenciais do cidadão e a troca de ideias e o diálogo democrático.
	Categorias temáticas	<i>"Amenazas, riesgos y problemas del interés nacional"</i>	As maiores ameaças e riscos estão relacionados à criminalidade organizada no ambiente interno de sua ciber sociedade, porém, existem preocupações relacionadas à complexidade, interdependência econômica e financeira, compreensão mínima de suas vulnerabilidades e dependência nas tecnologias cibernéticas.
	Categorias temáticas	<i>"Actividades de inteligencia como instrumento de control"</i>	Em situações de crises cibernéticas o sistema de inteligência coordena, monitora e comunica o cenário situacional nacional no âmbito cibernético, com maior atuação na inteligência criminal. Em outras situações, na proteção e classificação do segredo militar e no acesso das pessoas autorizadas.
Aspecto das capacidades e resposta	Categorias temáticas	<i>"Actividades sobrepuestas de la seguridad de la información y la"</i>	As funções de segurança da informação e cibersegurança, são apresentadas como ações complementares, sobrepostas nas ações e responsabilidades por parte dos atores governamentais.

		<i>ciberseguridad"</i>	
	Categorias temáticas	<i>"Ejercer el rol de la defensa nacional"</i>	O exercício da defesa nacional no uso da força e do poder militar conjunta, possui limitações doutrinárias, orçamentárias, de recursos e de reestruturação na sua organização.
	Categorias temáticas	<i>"Desarrollar capacidades competencias institucionales"</i>	A preocupação do Estado não somente é possuir capacidades cibernéticas, mas também, no desenvolvimento de capacidades humanas, logísticas e operacionais que lhe permitam articular competências e recursos institucionais.
Aspecto do poder e dominação	Categorias temáticas	<i>"Naturaleza y atributo del poder estatal"</i>	Poder e comportamento do Estado: atributo do poder, natureza do poder, atribuição de responsabilidade, paradigma.
	Categorias temáticas	<i>"Actores de la seguridad interna nacional"</i>	Forças policiais e agências de segurança nacional, no âmbito da segurança interior.
	Categorias temáticas	<i>"Organizaciones y asuntos internacionales de influencia"</i>	A influência e dinâmica das organizações internacionais, dos acordos de governança global e a integração dos organismos multilaterais, nos assuntos nacionais e interesses governamentais.
	Categorias temáticas	<i>"Actuación en el ámbito regulador, judicial y de sanción"</i>	Existem mecanismos que buscam regular, processar e punir ações e responsabilidades nas novas formas de crimes no uso das fontes digitais abertas e campo tecnológico.
Aspecto geopolítico e diplomático	Categorias temáticas	<i>"Acuerdos de diplomacia y relaciones exteriores"</i>	Os fenômenos que envolvem a tecnologia exigem nos países, negociações por meio de acordos de cooperação e ações de resolução de conflitos.
	Categorias temáticas	<i>"Factores de preocupación e impacto geopolítico y geoeconómico"</i>	As preocupações trazidas a debate por organismos internacionais ou pelas principais potências mundiais têm como características de estudo o aspecto geopolítico e geoeconômico.
Aspecto sociocultural e organizacional	Categorias temáticas	<i>"Firma digital en la identificación de personas"</i>	Uso da assinatura digital em cidadãos para identificação de pessoas no âmbito digital
	Categorias temáticas	<i>"Modelo de gestión y supervisión de la red pública"</i>	A fiscalização dos serviços da rede pública, a celebração de contratos e a sua integração requerem de planejamento e acordos que integram uma estratégia e um modelo de gestão em rede.
	Categorias temáticas	<i>"Protección de la privacidad y libre expresión"</i>	A preocupação do Estado de regular e salvaguardar a proteção da privacidade dos dados pessoais, como também, a liberdade de expressão de seus cidadãos.
	Categorias temáticas	<i>"Formación y tecnificación del recurso humano de la red pública"</i>	Uma das grandes preocupações do setor público, no âmbito das tecnologias de informação e da comunicação, é instruir, capacitar e tecnificar a seus recursos humanos em todos os níveis de governo. Deixando em evidência que o foco principal da instrução e treinamento corresponde à usabilidade e consumo das tecnologias de informação e da comunicação.
	Categorias temáticas	<i>"Gobierno y gestión de la información gubernamental"</i>	A necessidade das entidades públicas busca estabelecer níveis de maturidade na governança e gestão de suas informações.
	Categorias temáticas	<i>"Participación de los actores públicos, privados y sociedad"</i>	A busca de unificar os esforços na segurança e defesa nacional incentivando a integração, participação e consenso dos atores públicos, privados e sociedade.
	Categorias temáticas	<i>"Impulsar el motor de desarrollo, progreso y bienestar nacional"</i>	Promover o desenvolvimento, o progresso e o bem-estar que gerem impacto socioeconômico, cultural e tecnológico sobre os indivíduos e organizações nacionais.
	Categorias temáticas	<i>"Transformación y reforma de la estructura pública"</i>	Esforços para a reforma e modernização na governança e da gestão pública por meio da utilização das tecnologias de informação e da comunicação.
	Categorias temáticas	<i>"Impulsar el gobierno electrónico en la gestión pública"</i>	Execução das estratégias e planos em todos os níveis de governo, para a adoção do governo eletrônico ou digital na prestação de serviços públicos digitais em favor da sociedade.
	Categorias temáticas	<i>"Factores y elementos envueltos en la globalización"</i>	Vários elementos estão envolvidos no fenômeno da globalização: empresas multinacionais, ciberespaço, países em desenvolvimento, países desenvolvidos. Porém, existem fatores comuns como a economia digital, o uso infinito de dados, pacificação e coordenação pelo ciberespaço, entre outros.
	Categorias temáticas	<i>"Instrumentar las"</i>	Políticas e estratégias, nos níveis de governo, permitem a

		<i>políticas públicas para su articulación estatal</i>	articulação do aparato estatal na coordenação dos esforços para o acatamento dos objetivos nacionais.
Aspecto socioeconômico e comércio	Categorias temáticas	<i>"Integración del aparato económico, financiero y productivo"</i>	A preocupação do Estado em atender às necessidades essenciais, subsídios e controle, implica basicamente na integração do sistema econômico e social ao do setor produtivo e financeiro.
Aspecto tecnológico e industrial	Categorias temáticas	<i>"La concepción de la tecnología en el contexto internacional"</i>	As necessidades de mudança tecnológica no País trazem expectativas de um futuro próspero, inclusivo e de desenvolvimento sobre a provocação de dispor de mecanismos de cooperação internacional.
	Categorias temáticas	<i>"Elementos estructurales en la creación del ciberespacio"</i>	A materialização do ciberespaço é baseada na construção de elementos como: infraestrutura, dados, informação, conhecimento, automação, inteligência, conectividade global e controle.

Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

Com o intuito de explorar e analisar os códigos e categorias de forma visual em seus respectivos contextos, foi aplicado o uso das árvores de palavras interativas. Este tipo de análise ofereceu interatividade bidirecional: A primeira, trata-se em que a palavra ou combinações delas podem ser navegadas por meio de seus "ramos" individuais para visualizá-las em seus contextos. Em segundo lugar, as palavras são vinculadas aos parágrafos originais, deste jeito, para visualizar as palavras e frases no navegador de documentos do *software* MAXQDA. Esta análise permitiu ao pesquisador, dispor de um suporte visual das palavras-chave no contexto (*keyword-in-context* – KWIC). Segundo o observado na análise KWIC, podem ser elaboradas as ideias chaves dos códigos que possuem a maior relevância em nosso corpus. Por exemplo, podemos inferir o seguinte:

1. *"Personas y Organizaciones"*. Conforme aconteça a massividade do uso do ciberespaço, serão maiores os riscos e vulnerabilidades, ficando em evidência da necessidade de dispor de um contexto seguro em vantagem das pessoas e organizações públicas e privadas, onde sejam adoptadas medidas de proteção aos dados pessoais.
2. *"Seguridad de la información"*. A política de segurança da informação tem como objetivo o articular seu desenvolvimento com as outras políticas públicas necessárias, que incluem mecanismos de controle e ao responsável na sua aplicação.
3. *"Prevención, detección, respuesta y recuperación"*. O comitê de cibersegurança é o encarregado do desenvolvimento da estratégia nacional em cibersegurança com o objetivo de garantir a integração da segurança e o progresso nacional.
4. *"Capacidades"*. Dispor de capacidades que permitam enfrentar todo tipo de desafios, na busca do fortalecimento e desenvolvimento das capacidades: de prevenção, detecção, vigilância, controle, militares, de ciberdefesa, institucionais e humanas.

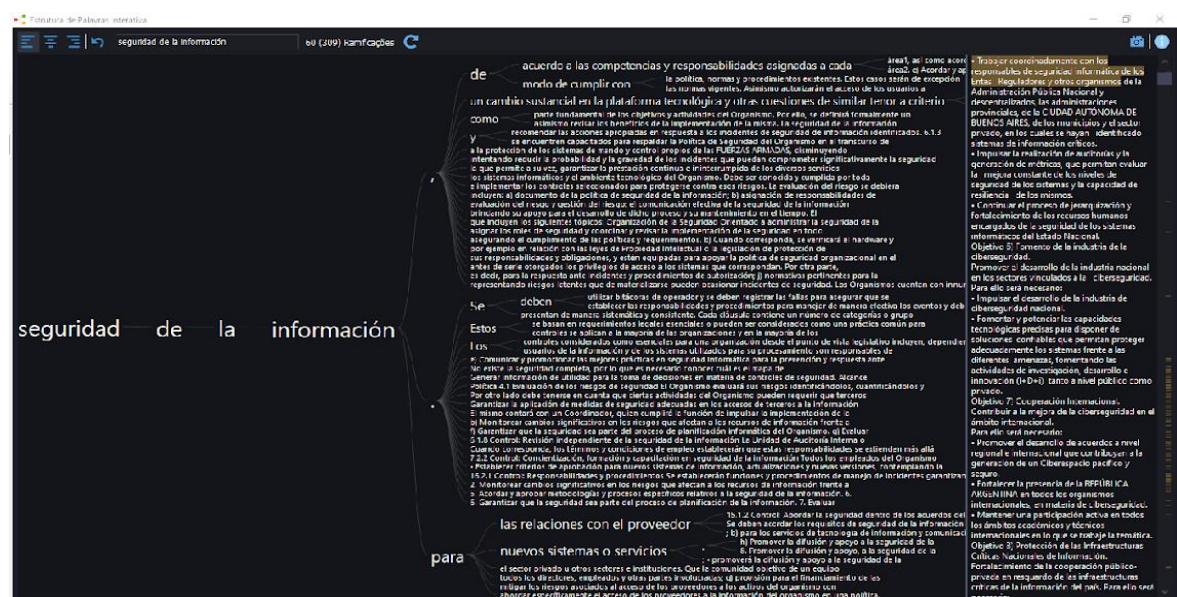
5. “Fuerzas armadas”. Como instrumento militar da defesa militar, deverá adequar sua estrutura em base às demandas de reestruturação e atenção ao âmbito cibernético, toda operação militar é conduzida pelo Estado Maior Conjunto, órgão que propiciará os planos de apoio (PA) e os gastos no marco do planejamento de curto prazo à secretaria de ciência, tecnologia e produção para a defesa.

Figura 55 - Árvore de palavras interativas do estudo de caso argentino (KWIC: “personas y organizaciones”)



Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

Figura 56 - Árvore de palavras interativas do estudo de caso argentino (KWIC: “seguridad de la información”)



Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

Além disso, as categorias concebidas, junto a uma análise qualitativa mais detalhada são complementadas com as seguintes características evidenciadas nos documentos estudados:

- São 35 os documentos que contém os códigos que representam a categoria temática definida como: Aspecto das ameaças e riscos. O código mais influente é *“Amenazas, riesgos y problemas del interés nacional”* se encontrando em 378 segmentos codificados, representando um 47.1% dos códigos que formam a citada categoria. Sutilmente podemos dizer que o código menos influente neste caso foi *“Vigilancia y control de los individuos”* com 104 segmentos codificados, representando um 13% de sua categoria.
- São 38 os documentos que contém os códigos que representam à categoria temática definida como: Aspecto das capacidades e resposta. O código mais influente é *“Actividades sobrepuestas de la SI y la Ciberseguridad”* se encontrando em 883 segmentos codificados, representando um 44.1% dos códigos que formam a citada categoria. Sutilmente podemos dizer que o menos influente neste caso seria *“Desarrollar capacidades y competencias institucionales”* sendo reportado com 264 segmentos codificados, representando um 13.2% de sua categoria.
- São 37 os documentos que contém os códigos que representam à categoria temática definida como: Aspecto do poder e dominação. O código mais influente é *“Actuación en el ámbito regulador, judicial y de sanción”* se encontrando em 528 segmentos codificados, representando um 55.2% dos códigos que formam a citada categoria. Sutilmente podemos dizer que o menos influente neste caso seria *“Actores de la seguridad interna nacional”* tendo sido reportado com 122 segmentos codificados, representando um 12.7% de sua categoria.
- São 24 os documentos que contém os códigos que representam à categoria temática definida como: Aspecto geopolítico e diplomático. O código mais influente é *“Factores de preocupación e impacto geopolítico y geoeconómico”* se encontrando em 114 segmentos codificados, representando um 55.3% dos códigos que conformam a citada categoria. Neste caso o código *“Acuerdos de la diplomacia y relaciones exteriores”* se posiciona próximo com 92 segmentos codificados, sendo o 44.7% de sua categoria.
- São 39 os documentos que contém os códigos que representam à categoria temática definida como: Aspecto sociocultural e organizacional. O código mais influente é *“Participación de los actores públicos, privados y sociedad”* se encontrando

em 561 segmentos codificados, representando um 19.7% dos códigos que formam a citada categoria. Podemos observar que o código menos influente é “*Modelo de gestión y supervisión de la red pública*” tendo sido reportado com 17 segmentos codificados, representando um 0.6% de sua categoria.

- São 28 os documentos que contém os códigos que representam à categoria temática definida como: Aspecto socioeconômico e comércio. O código mais influente é “*Integración del aparato económico, financiero y productivo*” se encontrando em 116 segmentos codificados, representando um 92.8% dos códigos que formam a citada categoria. Podemos observar que o código menos influente é “*Economía digital Argentina*” tendo sido reportado com 4 segmentos codificados, representando um 3.2% de sua categoria.

- São 36 os documentos que contém os códigos que representam à categoria temática definida como: Aspecto tecnológico e industrial. O código mais influente é “*Elementos estructurales en la creación del ciberespacio*” se encontrando em 649 segmentos codificados, representando um 91,8% dos códigos que formam a citada categoria. Podemos observar que o código menos influente seria “*La concepción de la tecnología en el contexto internacional*” tendo sido reportado com 58 segmentos codificados, representando um 8.2% de sua categoria.

Dessa forma, inferimos que a categoria: “**Aspecto sociocultural y organizacional**”, com 2,841 segmentos codificados, é a temática de maior relevância para os fins das políticas e estratégias no âmbito da segurança cibernética na Argentina, seguida da categoria: “*Aspecto de las capacidades y respuestas*” com 2,004 segmentos codificados.

Figura 57 - Visualizador da matriz de códigos caso argentino



Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

A mesma análise realizada nos questionários, de forma geral, não se difere nos resultados. Porém, observou-se que a metade dos especialistas que participaram nos questionários, as categorias: “*Aspecto socioeconómico y comercio*”, “*Aspecto*

geopolítico y diplomático” e *“Aspecto de poder e dominação”* não são parte das respostas e preocupações.

Figura 58 - Visualizador da matriz de códigos nos questionários do caso argentino

Lista de Códigos	Respondente_Argentina_1	Respondente_Argentina_2	Respondente_Argentina_3	Respondente_Argentina_4
Aspecto socioeconómico y comercio				
Integración del aparato económico, financiero y productivo				
Aspecto geopolítico y diplomático				
Acuerdos de diplomacia y relaciones exteriores				
Factores de preocupación e impacto geopolítico y geoeconómico				
Aspecto del poder y dominación				
Actores de la seguridad interna nacional				
Actuación en el ámbito regulador, judicial y de sanción				
Naturaleza y atributo del poder estatal				
Organizaciones y asuntos internacionales de influencia				

Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

7.1.1 Aspecto das ameaças e riscos, segundo os especialistas argentinos

Neste aspecto busca-se identificar as prioridades, partes interessadas e elementos que constituem as estratégias de segurança e defesa cibernética argentina, na perspectiva das ameaças e riscos cibernéticos. Nesse sentido foram desenvolvidas 3 perguntas abertas, deixando as seguintes evidências:

a. Entre as prioridades da segurança e defesa cibernética nacional argentina, foi comentado pelos especialistas diversos temas de preocupação. Entre elas foram os tópicos das infraestruturas críticas e da disponibilidade da informação, para a tomada de decisão.

Na minha opinião, as prioridades da segurança e defesa cibernética devem ser a infraestrutura crítica onde repousa o funcionamento integral do Estado Nacional (defesa, segurança, saúde, economia, educação, transporte etc.) e os sistemas de informação públicos e privados que garantem o 24/7 da disponibilidade das informações, para os níveis de tomada de decisão estratégica e operacional (Respondente_Argentina_1).

Outra prioridade em comum para os 3 respondentes, é a necessidade de um acultramento digital, devendo ser elaborados programas e planos de formação, treinamento e capacitação em cibersegurança.

Educação ou “Culturização Digital” da sociedade em todos os seus estratos, pois quando as pessoas alcançam cargos hierárquicos ou de responsabilidade, não incorporamos hábitos digitais saudáveis, o que coloca em grande risco as organizações e a sociedade (Respondente_Argentina_2).

Para o Respondente_Argentina_4, uma das prioridades deve ser o desenvolvimento integral das estratégias entre os ministérios, permitindo a avaliação e mitigação dos riscos mais críticos. Também, foi enfatizado pelo Entrevistado_Argentina_1, que a situação da pandemia como prioridade atual do Governo Federal, tem impulsado a relevância da segurança online e que estão

orientados os esforços em relação aos delitos informáticos e da ação judicial correspondente. Porém, o Entrevistado_Argentina_2 comentou que existe a boa intenção de priorizar os projetos, porém, não se dispõem dos recursos adequados para essa implementação, sendo buscada sempre uma solução imediata, sem um planejamento adequado. “Atrevo-me a dizer que a burocracia vai contra as boas intenções” e “sempre o urgente faz deixar de lado o mais importante” (Entrevistado_Argentina_2).

b. Sobre os atores envolvidos na segurança e defesa cibernética, se correspondem adequadamente na governança dos riscos cibernéticos, foi comentado por três dos respondentes, que os esforços dos atores são individualistas, com uma falta de coordenação e de visão holística.

As diferentes administrações têm feito esforços e implementado iniciativas de acordo com suas percepções particulares no risco cibernético. Acredito que falta uma visão holística da complexidade que enfrentam, bem como, um compromisso de dar continuidade e reforçar as ações desenvolvidas por cada um deles. (Respondente_Argentina_1).

Segundo o Respondente_Argentina_4, os atores envolvidos na segurança e defesa cibernética são reativos e que deveriam investir em mais recursos para ser resilientes aos riscos cibernéticos, sendo destacado que as entidades financeiras possuem um melhor desenvolvimento devido aos requisitos obrigatórios e do regulador.

Segundo o Entrevistado_Argentina_2, especificamente no seu setor, “estão treinados para pensar nos riscos como uma oportunidade de melhoria”, o que nos fez inferir, que em consequência às deficiências e necessidades dos recursos, os atores buscam sempre inovar na solução a seus problemas.

c. Sobre as principais ameaças externas e internas que podem originar uma crise nacional. Para três dos respondentes, as ameaças que possam gerar uma afetação às infraestruturas críticas nacionais, como por exemplo, as de subministro energético se seriam categorizadas como de crise nacional. Sendo relatado pelo Respondente_Argentina_4, um caso acontecido no 16 de junho de 2019, em que praticamente 3 países¹⁵⁰ foram afetados por um conjunto de interrupções do subministro de energia elétrica produto de um erro operacional da empresa Transener. Outra preocupação pelo Respondente_Argentina_4, esteve relacionado com a

¹⁵⁰ Disponível em <<https://www.ip.gov.py/ip/un-error-operativo-de-empresa-electrica-causo-apagon-en-argentina-y-uruguay/>>. Acesso em 26 de outubro de 2021.

descontinuidade dos serviços em nuvem de onde muitas empresas dependem desses serviços.

Tem-se observado nas respostas dos especialistas argentinos que as ameaças relacionadas à ciberespionagem dos Estados e à ciberguerra, são do amplo conhecimento deles, porém, esses tipos de ameaças não são uma preocupação no momento. Para eles as maiores preocupações estão relacionadas com as ações dos cibercriminosos.

Um dos comentários que chamou nossa atenção é que os ataques dirigidos concebidos por motivos políticos e ideológicos, seriam um tipo de ameaça que poderiam provocar uma crise interna, devido à vulnerabilidade sociocultural e de coordenação entre os afetados. Segundo o Respondente_Argentina_2, “a oposição do governo pode utilizar a vulnerabilidade sociocultural e a falta de coordenação para a obtenção de vantagem política”.

Outra das maiores ameaças internas é não saber como preservar o talento humano e que em princípio seria o aspecto econômico o motivo de escolher o setor privado. “A entidade pública investe muito em formar um talento, porém, esse talento se termina indo” (Entrevistado_Argentina_2).

Além disso, segundo a opinião do Entrevistado_Argentina_2, a própria denominação de declarar que tem acontecido uma ameaça cujos efeitos foram categorizados como um ataque cibernético nacional, ninguém o faria por aspectos de imagem política. Nesse sentido, ele declarou desconhecer a existência de uma autoridade capaz de responder e afirmar que é um ataque cibernético nacional, sendo o fator da atribuição uma dificuldade do problema. Assim como, da existência de um protocolo para reagir a um ataque cibernético nacional.

Nós que estamos na área cibernética podemos medir que foi um risco elevado, porque houve muita informação sensível/sigilosa afetada. Porém, para o comum da gente não entende, não está conscientizado ou talvez prefiram não se conscientizar porque ao ser consciente dos riscos te faz ser consciente das vulnerabilidades, portanto se prefere não saber. Os que estamos na comunidade, nós entendemos, que isso foi um risco muito importante e que pode trazer algumas consequências a futuro porque envolviam dados sensíveis/sigilosos, mas que alguém diga que foi um ataque cibernético nacional eu acho que ninguém o afirmaria (Entrevistado_Argentina_2).

Desde a perspectiva da identidade nacional e latino-americana, foi comentado da penetração dos diversos grupos que desejam uniformizar os entendimentos, atacando as individualidades do sujeito, onde a Internet tem um poder imenso para o

uso das “armas da desinformação e as velhas táticas ajudadas pela tecnologia podem se influenciar a uma maior quantidade de pessoas” (Entrevistado_Argentina_2).

Existem a meu entendimento um sexto domínio, do aspecto cognitivo, onde se toma a mente do cidadão como um novo campo de batalha. Para tratar de influenciar na mente dos decisórios e do cidadão em comum” (Entrevistado_Argentina_2).

7.1.2 Aspecto das capacidades e resposta, segundo os especialistas argentinos

Neste aspecto busca-se identificar as ações de proteção, partes interessadas e desafios nas estratégias de segurança e defesa cibernética, sob a perspectiva de capacidades e resposta. Nesse sentido foram desenvolvidas 3 perguntas abertas, deixando as seguintes evidências:

a. Para uma proteção adequada do espaço cibernético nacional, que estratégias e ações no nível político-estratégico estão sendo promovidas. Se evidencia nas respostas dos especialistas a necessidade de ter uma coordenação e entendimento das ameaças e dos riscos cibernéticos pelos atores (privados, públicos e sociedade). Outro aspecto diz respeito ao desenvolvimento das capacidades cibernéticas, onde devem ser elaborados programas públicos-privados e que disponibilizam aos cidadãos as ferramentas tecnológicas que incorporam a segurança da informação e cibernética.

Conscientizar aos cidadãos não só nos riscos que estão expostos, mas também dotá-los das ferramentas adequadas para incorporar as melhores práticas e conscientizá-los da possibilidade de que seu descompromisso a esse respeito, os torna cúmplices de uma atividade cibercriminal que também afeta seu ambiente pessoal e profissional (Respondente_Argentina_1).

Além disso, para o Respondente_Argentina_4, as preocupações não somente deveriam estar em aspectos de proteção, capacitação e resiliência. Em complemento, se tem que buscar melhorar o desenvolvimento industrial nacional considerando a soberania dos dados e o desenvolvimento local. Onde o marco regulador seja um catalisador na gestão dessas ações, sem perder de foco o desenvolvimento socioeconômico nacional.

Complementarmente a essas diretrizes, deve haver programas público-privados onde a sinergia alcance não apenas melhor proteção e resiliência, mas também, levando em consideração essas questões, melhorando o desenvolvimento da indústria nacional, tecnologias como IoT, 5G, blockchain etc. sempre levando em consideração a soberania dos dados e o desenvolvimento local (Respondente_Argentina_3).

b. Onde estariam os maiores desafios e capacidades cibernéticas na Argentina.

Para a maioria dos especialistas argentinos, o principal desafio estaria relacionado ao ciclo do recurso humano no âmbito da segurança e defesa cibernética. Isso envolve desde a sua formação, treinamento, especialização e retenção uma vez alcance o nível de expertise desejado desse recurso. Segundo o Respondente_Argentina_3, existem desafios no Estado argentino em “procurar, atrair e manter recursos qualificados em segurança cibernética e TI”.

O maior desafio é poder oferecer uma educação adequada no país. A formação de recursos idôneos desde suas bases, com uma inclinação expressa na cibersegurança, que terá um impacto total na defesa cibernética nacional. Falta-nos educação desde suas bases e escassez de especialização diversificada (Respondente_Argentina_2).

Porém, para o Respondente_Argentina_1, “o maior desafio é a falta de percepção do risco cibernético e do valor da informação, nos níveis privado e público” e as capacidades cibernéticas no âmbito público estaria sendo concentrada nos setores de defesa e segurança. Segundo o Respondente_Argentina_3, essas capacidades estariam nos CERTs, não obstante, existem muitas iniciativas que não estão sendo priorizadas.

Em relação às capacidades, acredito que a Argentina tem feito grandes avanços em políticas de gestão da cibersegurança, desde com os diversos CERTs no país, que ajudam à prevenção e resiliência tanto para as infraestruturas críticas. E com os dados e sistemas administrados pelos estados provinciais e nacionais, existindo um comitê especializado apenas para o desenvolvimento da estratégia nacional de cibersegurança e os vários setores responsáveis das infraestruturas críticas, realizando atividades e precauções suficientes, ao ponto, não terem tido um incidente crítico grave de cibersegurança, por mais de 4 anos. Minha maior crítica seria que muitas coisas são feitas, mas não com a velocidade e a dedicação que a segurança cibernética exige (Respondente_Argentina_3).

c. Que deve ser alcançado com tecnologias como a Internet e outras envolvidas no ciberespaço.

Em geral, o que foi exposto pelos especialistas se concentra na educação digital e na conscientização sobre o uso seguro da Internet e do ciberespaço. Em acréscimo, para o Respondente_Argentina_2, deve ser alcançada uma “educação integral digital da população, alfabetização digital e inclusão digital”. Segundo o Respondente_Argentina_1, propõe a “desconstrução da narrativa circundante e reconhecer as próprias vulnerabilidades”, devendo ser incentivada a inovação tecnológica e integração da região para reduzir a dependência tecnológica.

Além disso, o Respondente_Argentina_4, comenta a necessidade de “investir em processo de formação nos conceitos fundamentais na cibersegurança”.

Outro aspecto a ser alcançado com essas tecnologias é que “tecnologicamente ainda não se tem democratizado o conhecimento através da Internet. Existem diversas áreas ou províncias onde ainda não dispõem do serviço da Internet” (Entrevistado_Argentina_2).

7.1.3 Aspecto do poder e dominação, segundo os especialistas argentinos

Neste aspecto busca-se analisar os elementos que constituem uma política de segurança cibernética, na perspectiva do poder e da dominação. Nesse sentido, foram desenvolvidas duas perguntas abertas, deixando as seguintes evidências:

a. Em relação às estratégias nacionais no campo cibernético dos países desenvolvidos, têm-se impulsionado a expansão e a dominação por meio das tecnologias de informação e da comunicação. As respostas de dois especialistas poderiam ser consideradas neutras, no entanto, não houve negação da provável expansão e dominação por meio das TIC.

Não concordo totalmente com essa posição, os países mais desenvolvidos perceberam cedo, desde a década de 1950 no século passado, o valor do acesso à informação e desenvolveram uma infraestrutura de telecomunicações que suportasse esse objetivo. Os países em desenvolvimento limitaram-se a incorporar tecnologia da informação e comunicação sem a correspondente avaliação de riscos e oportunidades (Respondente_Argentina_1).

Segundo o Respondente_Argentina_1 tem-se transferido responsabilidades para outros, como em discursos de dominação. Segundo o especialista, os países em vias de desenvolvimento, têm subestimado sua capacidade de inteligência estratégica e de sua concepção, ao ter concentrado suas ações no âmbito militar e da segurança, trazendo resultados reativos e limitados.

Sem falar que a maioria dos países em desenvolvimento não possuem capacidade de inteligência científico-tecnológica, que lhes permita enfrentar a complexidade inesgotável do ciber ambiente. Como resultado, as estratégias dos países em desenvolvimento acabam sendo limitadas e extremamente reativas (Respondente_Argentina_1).

Foi abordado durante a entrevista, em forma de exemplo, de como nos países desenvolvidos estão sendo realizados exercícios cibernéticos em resposta aos ataques e indisponibilidade, afetando ao serviço nacional da Internet ou da própria rede do sistema nacional financeiro. Nesse sentido, foi comentado pelo Entrevistado_Argentina_2, ter desconhecimento que existam na prática, ações para o

desenvolvimento dessas capacidades ao ponto de permitir uma desconexão do serviço da Internet, para a continuidade dos serviços públicos.

Para o Respondente_Argentina_2, a expansão e dominação pelas TIC é um processo inevitável estando instaurada uma dependência nos países menos desenvolvidos, devido a produção do conhecimento que é realizado nas infraestruturas e recursos dos países desenvolvidos.

b. Se regulam e punem as ações no âmbito cibernético, que possam afetar os interesses nacionais. Se tem casos dessas punições ou sanções desde o ponto de vista da segurança e defesa nacional. Segundo os especialistas não se tem casos em que foram reportadas sanções específicas nesse tipo. O Respondente_Argentina_1 comentou: “não tenho o conhecimento de uma estrutura legal destinada a sancionar ações tecnológicas, além daquelas associadas ao crime cibernético”. Porém existem outros marcos legais e regulatórios envolvidos indiretamente no tema, como são os aspectos da proteção de dados pessoais e os delitos informáticos na Argentina. Outro ponto de vista que toma nossa atenção, foi que na Argentina não se tem um posicionamento de punição ou sanção em relação aos quesitos da segurança cibernética. Onde sobressai a peculiaridade cultural e da estrutura governamental na Argentina.

A Argentina não possui um espírito sancionador em relação ao não cumprimento de estratégias ou políticas de segurança cibernética, bem como, em várias outras áreas por ser um país federal, onde cada província tem sua própria governança, e as ideias centrais geralmente são desenvolvidas com o espírito de que o governo nacional dita as diretrizes e as províncias aderem a elas, é que os regimes sancionatórios são deixados à vontade para cada uma delas. No que diz respeito à regulamentação, nossa estratégia nacional de segurança cibernética também não declara tais questões, cabendo a cada agência e seus poderes garanti-las (Respondente_Argentina_3).

Segundo o Respondente_Argentina_4, muitas das políticas e estratégias que foram elaboradas, tem sido uma cópia integral das boas práticas, sem ter passado por um planejamento estratégico e sua avaliação dos riscos à cibersegurança nacional argentina. Para o Entrevistado_Argentina_2, não se tem regulações para a propaganda ou a desinformação. Nesse sentido, comentou que “deve haver em relação a este novo risco uma normativa relacionada de como proteger o aspecto cognitivo” (Entrevistado_Argentina_2).

7.1.4 Aspecto geopolítico e diplomático, segundo os especialistas argentinos

Neste aspecto busca-se analisar a geopolítica no campo cibernético e suas repercussões na consolidação das políticas e estratégias de segurança cibernética. Portanto, foram desenvolvidas duas perguntas abertas, deixando as seguintes evidências:

a. A Política Nacional de Segurança Cibernética (ou iniciativas semelhantes) têm atuado com ingerência na esfera diplomática nacional. Se tem casos que transcenderam a esfera diplomática. Neste ponto, quase todos os especialistas apontam que não há relatos de casos nessa magnitude, porém, enfatizam que existem acordos de cooperação internacional no intercâmbio das informações.

Não, não somos propriamente um país que tenha um registro de ciber guerra ou ciberspionagem declarada como tal, no aspecto diplomático. E até o que conheço, nunca foi necessária nos aspectos da segurança cibernética. Se tivermos vários acordos marcos a nível regional e internacional, porém, mais ao nível da cooperação ou da participação prática, do que no domínio da diplomacia (Respondente_Argentina_3).

Segundo o Respondente_Argentina_2, foi reportado um caso recente, relacionado com o vazamento de dados sigilosos na Direção de Assuntos Migratórios¹⁵¹ e da Agência Federal de Inteligência¹⁵². Porém, não poderia ser considerada como uma situação de crise nacional.

b. A Instituição responsável da geoestratégia nacional, assim como, os estudos de perspectiva geopolítica e socioeconômica no domínio ciberespacial. Segundo os especialistas, não está claro qual é a entidade responsável pela coordenação da geoestratégia nacional. Segundo o Respondente_Argentina_1, essa função estaria espalhada nos diferentes Ministérios, por meio dos comitês interministeriais, no entanto, ele propõe que sejam integrados aos organismos da inteligência nacional. Outra perspectiva foi do Respondente_Argentina_3, que comentou que a questão geopolítica deverá ser uma responsabilidade do governo que está no exercício do poder.

Para mim, qualquer questão geopolítica é uma responsabilidade do governo atual, desde a administração presidencial até os vários ministérios que são o órgão competente e operacional das questões específicas. No âmbito

¹⁵¹ Disponível em <https://www.clarin.com/tecnologia/ciberataque-migraciones-informacion-robaron-publicaron-ciberdelincuentes_0_Pfe1OVNII.html>. Acesso em 27 de setembro de 2021.

¹⁵² Disponível em <<https://elpais.com/internacional/2020-10-06/escandalo-en-argentina-por-una-gran-filtracion-de-datos-de-sus-servicios-de-espionaje.html>>. Acesso em 27 de setembro de 2021.

espacial e segurança cibernética, bem como, o desenvolvimento do ciberespaço e suas tecnologias, hoje na Argentina, dependem do Chefe de Gabinete de Ministros, que tem à Secretaria de Inovação Pública, à empresa público-privada ArSat e à Direção Nacional de Segurança Cibernética, entre outros próprios de desenvolvimentos interministeriais (Respondente_Argentina_3).

Segundo o Entrevistado_Argentina_2, em cada um dos estamentos das forças armadas se faz prospectiva tecnológica militar. “Existe um observatório nacional responsável do monitoramento do acontecer mundial: Observatório Argentino de Ciberespaço¹⁵³ (Entrevistado_Argentina_2). Porém, a busca é atender aos objetivos nacionais, uma limitante dessa atenção, são as necessidades urgentes do país. Para o Respondente_Argentina_2 e o Respondente_Argentina_3, um aspecto de melhoria está relacionado a dispor de um maior orçamento para os setores responsáveis.

7.1.5 Aspecto sociocultural e organizacional, segundo os especialistas argentinos

Neste aspecto busca-se analisar os incentivos e benefícios da Política de Segurança Cibernética, na esfera sociocultural e organizacional. Foram desenvolvidas duas perguntas abertas, deixando as seguintes evidências:

a. A Política Nacional de Segurança Cibernética tem incentivado reformas institucionais. Segundo os especialistas, eles consideram que as iniciativas relacionadas à segurança cibernética exigem reformas institucionais, para se adaptar às demandas da sociedade contemporânea. No entanto, para o Respondente_Argentina_3 é fundamental ter uma Lei em cibersegurança abrangendo o setor público quanto o privado.

É imprescindível que a Argentina tenha uma Lei de Cibersegurança, a qual, embora a política tenha maior validade do que a estratégia nacional de cibersegurança, a partir dela devem ser transmitidas as diretrizes que auxiliem essa lei para melhorar a prevenção, proteção e resiliência das infraestruturas críticas nacionais. As quais sem dúvida, requerem diversas reformas institucionais para garantir esses fatores, tanto na esfera pública como privada, e a cooperação de ambas (Respondente_Argentina_3).

Um aspecto comentado é que existem grupos de trabalho de especialistas ou comitê assessor dos diversos ministérios que não possuem uma formalidade em sua estruturação, sem recursos próprios e que respondem às suas motivações próprias.

"Eles trabalham de forma articulada em um grupo de trabalho que não está institucionalizada, mas que na prática funciona, basicamente, para ir comparando as ações conjuntas e que obviamente desde o governo estão se

¹⁵³ Disponível em <<https://www.esqcfaa.edu.ar/esp/oac-boletines.php>>. Acesso em 08 de dezembro de 2021.

trabalhando de forma compartimentada, duplicando esforços para questões que necessitam uma abordagem completo" (Entrevistado_Argentina_1).

Segundo o Entrevistado_Argentina_2, para o Estado é de alto custo sair da zona de conforto, além que o aspecto político muda muito, afetando na celeridade das reformas e das condições de melhoria. "Existindo diversos interesses pessoais na política, no discurso está a intenção, mas depois não se observa isso" (muitas vezes nem são executadas).

b. A Política Nacional de Segurança Cibernética (ou iniciativas semelhantes) têm incentivado benefícios sólidos, prosperidade e desenvolvimento da sociedade.

Todos os especialistas comentam que não podem apreciar esses benefícios, justificando que para alcançar a prosperidade e desenvolvimento na sociedade argentina é necessário abordar primeiro outros problemas sociais, como é a redução dos indicadores de pobreza na Argentina.

O objetivo seria incentivar essas melhorias e benefícios, mas para alcançar um Estado de prosperidade e desenvolvimento em nossa sociedade, devemos modificar os indicadores que colocam 50% da população abaixo da linha da pobreza. Isto significa, que nenhum programa ou projeto planejado para trazer benefícios e desenvolvimento, pode ser evidenciada na sociedade (Respondente_Argentina_2).

Outra justificativa seria que as estratégias em cibersegurança são recentes, atingindo somente aspectos conceptuais sem abordar profundamente as responsabilidades e os benefícios que têm que ser realizados.

Eu entendo que isto se deve que nossa estratégia nacional de cibersegurança é muito nova, aprovada no 2019 em forma antecipada. Devido à saída do governo oficialista de aquele então. Nesta versão se faz referência somente aos conceitos que abrangem mais à estratégia, a definição das infraestruturas críticas de informação, como aos setores e critérios para a detecção destas, junto ao glossário de termos, sem citar temas de responsabilidades ou benefícios (Respondente_Argentina_3).

Para o Entrevistado_Argentina_1, "o que funcionou muito na prática foi o CERT.ar" trazendo benefícios concretos em termos de cooperação na gestão técnico-administrativa dos incidentes da segurança cibernética no setor público nacional. Apoiando aos organismos que não possuem áreas técnicas e que não possuem especialistas em segurança, como acontecem em muitos organismos do Estado. Sendo justificado pelo experto: "por que não teria muito sentido dispor de um corpo ou uma área técnica grande em cibersegurança nesses organismos, inclusive, não é algo 100% necessário quando falamos de prioridades e se tenham que contratar profissionais ou recursos tecnológicos" (Entrevistado_Argentina_1).

Para o Entrevistado_Argentina_1, o Governo Federal tem impulsionado a elaboração e aprovação da Política Modelo de Segurança da Informação, tendo como seus principais beneficiários os organismos de menor dimensão ou do nível municipal que tem recursos e orçamentos limitados.

7.1.6 Aspecto socioeconômico e de mercado, segundo os especialistas argentinos

Neste aspecto busca-se analisar os incentivos ao consumismo e à dependência tecnológica, compreender os agentes e elementos envolvidos na política de segurança cibernética, no âmbito socioeconômico e de mercado. Assim, foram elaboradas três perguntas abertas, das quais destacam as seguintes evidências:

a. Se tem incentivado o consumo nacional das TIC. As ações ou iniciativas promovidas pelo governo em equilibrar a dependência tecnológica externa. De acordo com os especialistas existem esforços, porém são imaturos na prática. Para o Entrevistado_Argentina_1, não se tem uma vinculação direta das ações de segurança cibernética com o incentivo nacional das TIC. A estratégia que mais se tem realizado é nas redes sociais oficiais do governo, para a conscientização do uso seguro das TIC. O questionamento foi justificado pelos especialistas desde a perspectiva das propostas futuras que deveriam ser consideradas e debatidas nas iniciativas do governo.

Segundo o Respondente_Argentina_1, “se necessita mais esforço em inovação tecnológica e na proteção da propriedade intelectual, assim como, apoiar às startups nacionais”. Para o Respondente_Argentina_2 é fundamental incentivar o conhecimento técnico, a inclusão digital e reduzir a *brecha digital*. Assim como, minguar a carga tributária nos desenvolvimentos tecnológicos.

Para equilibrar a dependência tecnológica estrangeira deveria se dar relevância à robótica nacional, ao desenvolvimento de Pymes e empreendimento locais e zonais que tenham como proposta gerar e desenvolver novas tecnologias. É fundamental o incentivo minguando a carga tributária nesses desenvolvimentos (Respondente_Argentina_2).

Finalmente, uma proposta sugerida pelos especialistas é em relação às iniciativas promovidas: “variam muito em base ao governo de turno” (Respondente_Argentina_4). Existe a necessidade de unificar os esforços em uma política de Estado integral.

Acredito que a primeira ação que devemos promover é justamente criar essa política no nível nacional e que todas as províncias e organizações a cumpram de forma integral. A partir deste ponto, a construção de ações, políticas e programas que promovam a não dependência tecnológica

estrangeira de forma segura, se desenvolvem de forma muito mais fluida e organizada. A soberania tecnológica na Argentina também é uma questão muito forte, mas de novo é desenvolvido a partir de cada organização e não de forma integral (Respondente_Argentina_3).

Para o Entrevistado_Argentina_1, "desde o Estado se tem fomentado muito, que as informações públicas estejam hospedadas no datacenter do ArSat". Porém, existem limitações nos serviços de ArSat relacionados à obsolescência tecnológica o que não permite estar na mesma competitividade das empresas estrangeiras. Por esse motivo, uma das iniciativas promovidas pelo governo para equilibrar a dependência tecnológica externa, segundo o Entrevistado_Argentina_1, se tem aprovado o *Plano Conectar*¹⁵⁴, "tendo como um eixo o desenvolver investimentos para ampliar a capacidade do datacenter do ArSat".

Segundo o Entrevistado_Argentina_2, as forças armadas têm incentivado a produção e cooperação tecnológica na região, mas de certa forma bastante limitada.

Na área de cooperação tecnológica e industrial existe o Sistema de Cooperação entre as Forças Aéreas Americanas, como um sistema resiliente e de contingência, onde se incentiva o trabalho conjunto frente à situação de crise e desastres naturais. SICOFAA¹⁵⁵ treina a todos seus países membros simulando uma catástrofe para organizar os times nas ajudas humanitárias. O software que é utilizado nessa ajuda humanitária permite gerenciar as doações e os movimentos das aeronaves que vão transportar as ajudas humanitárias. (Entrevistado_Argentina_2, Pos. 57).

b. Na perspectiva do orçamento e investimento público em ciência e tecnologia, os programas em segurança e defesa cibernética visam criar esforços intersetoriais conjuntos. Somente um especialista limitou-se a dar uma resposta devido à pouca informação que dispõe para opinar. No entanto, os outros especialistas coincidem que existem limitações no orçamento e investimento público em ciência e tecnologia. Entretanto, nenhum comentou da existência de esforços intersetoriais conjuntos. Próximo disso, o Entrevistado_Argentina_1 comentou: "nesse sentido desde o próprio espaço (da ONTI) se procura não coordenar, mas sim brindar sugestões não vinculantes, para fazer uso mais eficiente da infraestrutura que está disponível".

Desde a ONTI são emitidos os pareceres sobre os projetos de tecnologia do setor público nacional, nos pareceres quando se observa que existem organismos que não possuem a tecnologia fundamental, é sugerido para que sejam contratados os serviços da ArSat (Entrevistado_Argentina_1).

¹⁵⁴ Disponível em <<https://www.arsat.com.ar/tag/plan-conectar/>>. Acesso em 10 nov 2021.

¹⁵⁵ Disponível em <<https://www.sicofaa.org/argentina>>. Acesso em 10 nov 2021.

Segundo o Respondente_Argentina_3 para o governo de turno passado, na partida do orçamento e investimento em ciência e tecnologia eram considerados gastos públicos.

Acho que essa questão requer uma análise temporal. Por um lado, a Argentina sofreu uma punição muito grave nos orçamentos e nos investimentos públicos em ciência e tecnologia, durante o período de 2016 a 2019, pois a política governamental daquele período considerava essas duas questões como um gasto público, retirando grandes rubricas orçamentárias que o constituíam impossível desenvolvê-los (Respondente_Argentina_3).

Uma preocupação expressa pelo Respondente_Argentina_1, é que estas iniciativas orçamentarias e investimentos em ciência e tecnologia, não tem um planejamento estratégico integral. Nesta linha o Respondente_Argentina_2, afirmou que essas iniciativas são não coordenadas, sem indicadores ou estratégias de otimização. Aliás, foi comentado que não se tem um seguimento dos projetos executados, “os motivos de não ter sido executado pode ser por questões de orçamento, tempo, mudança de gestão ou decisão política. A rastreabilidade chega até o que se está procurando fazer” (Entrevistado_Argentina_1).

Segundo o Respondente_Argentina_3, o contexto atual da pandemia foi uma limitante nos esforços em ciência e tecnologia, porém está sendo adotada uma estratégia de investimento, através das instituições internacionais de desenvolvimento.

O contexto da pandemia, como em todos os países, obrigou ao reforço de orçamentos a serem implementadas no setor da saúde, embora seja notório o crescimento destas em ciência e tecnologia, evidentemente não foi o suficiente, para gerar a força necessária que os dois setores exigem. Na minha opinião, os investimentos mais significativos estão sendo buscados por meio das instituições internacionais de desenvolvimento e não intersetorialmente, mas existem vários programas que buscam otimizar os gastos públicos nessa área, principalmente com o CONICET e o ArSat, entre outros (Respondente_Argentina_3).

c. As iniciativas em segurança cibernética têm dado impulso na economia e mercado digital nacional. Os especialistas coincidem que existam limitações nestas iniciativas, devendo ser mais valorizado e menos influenciado por ideologias políticas. Segundo o Entrevistado_Argentina_1, uma forma de se impulsionar o item questionado, seria a criação de polos científicos-tecnológicos oferecendo ferramentas digitais para empreendedores¹⁵⁶. Segundo o Respondente_Argentina_4, a economia

¹⁵⁶ Disponível em <<https://www.argentina.gob.ar/efatura/innovacion-publica/gobierno-abierto-y-pais-digital/paisdigital/marketing-digital-desde-casa/empreendedores>>. Acesso em 07 Set 2021.

e mercado digital é “um dos objetivos da estratégia nacional em cibersegurança”. Para o Respondente_Argentina_3, existem ainda aspectos a serem melhorados, especialmente, na busca de uma política integral que tenha de marco à economia digital e o desenvolvimento local de indústrias

A Argentina recentemente vem desenvolvendo grandes avanços no que diz respeito à economia e ao mercado digital, desde a aprovação da Lei da Economia do Conhecimento, o desenvolvimento de 5G, IoT e cidades inteligentes, ademais em programas que promovem o desenvolvimento como o "Programa Argentina" ou o expansão da Rede Federal de Fibra e em todos eles há pouco tratamento da segurança cibernética. Uma vez mais, acredito que o aspecto a ser melhorado é a política integral que consegue enquadrar e melhorar substancialmente as questões inerentes à segurança cibernética na economia digital e ao desenvolvimento das indústrias locais (Respondente_Argentina_3).

7.1.7 Aspecto tecnológico e industrial, segundo os especialistas argentinos

Neste aspecto busca-se compreender quais atores e elementos constituem uma política de segurança cibernética, no campo tecnológico e industrial. Nesse sentido, foram desenvolvidas três perguntas abertas, deixando as seguintes evidências:

a. O responsável nacional por regular e estabelecer os padrões em TIC. Com exceção do Respondente_Argentina_3, foi confirmado pelos especialistas que as estratégias nacionais em segurança cibernética deveriam considerar a capacitação da entidade pública para regular e estabelecer os padrões em TIC, como também, dos mecanismos de avaliação no seu cumprimento. Porém, o Respondente_Argentina_3 é da posição de ter uma Lei em cibersegurança que permita ordenar as questões do benefício dos cidadãos e das empresas locais. Não obstante, o Entrevistado_Argentina_1 comentou o seguinte:

"Desde a ONTI se publicam os padrões tecnológicos para a administração pública que tem modelos de *pliego* e alinhamentos sobre as opções de tecnologias específicas e especificações técnicas gerais. Elas estão coordenadas com todos os fornecedores para que sejam abertas e não direcionadas, para que desde os distintos organismos possuam uma base nas aquisições tecnológicas".

Segundo o Entrevistado_Argentina_1, "não se obriga às empresas privadas a cumprirem padrões específicos nacionais". A Política Modelo de Segurança da Informação tem como cliente final os Ministérios e os Organismos do Estado Nacional, para que sejam adotadas, porém não estariam inseridas ao setor privado. Desde a

apreciação do Entrevistado_Argentina_1, o setor privado possui um nível de maior exigência em suas políticas de segurança.

b. As empresas multinacionais estrangeiras estão incluídas na Política Nacional de Segurança Cibernética. Qual setor é responsável por essa articulação. Os especialistas têm coincidido na necessidade de integrar a estas empresas em uma política nacional em segurança cibernética, porém os esforços nesse item deveriam ser melhorados. Segundo o Respondente_Argentina_4 “ainda não se aplica em forma eficiente para articular a relação empresa e governo”. Desde a posição do Respondente_Argentina_3, ele reitera a necessidade de integrar essas iniciativas em segurança cibernética com um único organismo governamental e desde esse ator, sejam realizadas as tarefas de articulação com as empresas multinacionais.

Novamente, a inclusão de multinacionais estrangeiras não é acertada, porque não existe uma política de segurança cibernética abrangente na Argentina. Estas empresas são consideradas, reguladas e administradas por cada um dos órgãos competentes delas, bem como, a sua articulação no país, seja na prestação de um serviço público ou de colaboração com o Estado. Na minha opinião, acho que tudo é sempre mais eficiente quando se constrói a partir da integridade, e não da unicidade, sendo conveniente definir um único ator que articule com as empresas multinacionais em termos de cibersegurança, e a seguir o referido ator se articular com os diversos órgãos públicos, enquanto às necessidades que devem ser atendidas (Respondente_Argentina_3).

c. Tem-se incentivado a competição de fornecedores de acesso à Internet (ISP).

O governo tem capacidade em regular de forma eficiente e permanente aos ISP.

Se evidencia nas respostas dos especialistas que o acesso à Internet é uma preocupação que está na agenda dos governos, sendo considerado como um serviço público, porém, depende da decisão política de realizá-lo. Segundo o Respondente_Argentina_2, existem diferenças nos níveis da gestão nacional que devem ser consideradas.

Existem diferenças na gestão do Estado Nacional em relação aos Estados Provinciais. Vários deles garantem o acesso à Internet para a população (*San Luis* o incluiu em sua constituição provincial há muitos anos). O governo nacional não tem capacidade política para garantir acesso eficiente e permanente a setores da sociedade que não se encontram em situação econômica de acesso (Respondente_Argentina_2).

Outrossim, é que a Argentina possui a ArSat que é uma empresa pública no âmbito das telecomunicações e segundo o Respondente_Argentina_3, o governo tem a capacidade de efetuar uma regulação eficiente aos ISP estrangeiros incentivando a competitividade.

A Argentina tem a ArSat, uma empresa ISP pública que concorre e está no mesmo nível das grandes empresas privadas locais. Além disso, em 2020 a Internet foi apontada como serviço público, o que além de torná-la imprescindível para todo o país, regula e incentiva o desenvolvimento do acesso, é complementado com programas de desenvolvimento da Rede Federal de Fibra Óptica (REFEFO) e contribuições não reembolsáveis para o desenvolvimento de ISPs provinciais. Na minha opinião, o governo tem capacidade suficiente para regular os ISPs estrangeiros e incentiva a competitividade do ArSat e dos desenvolvimentos nomeados (Respondente_Argentina_3).

O governo tem estabelecido que o uso e acesso às redes de telecomunicações era considerado um serviço público e estratégico. Existe um fundo fiduciário do serviço universal¹⁵⁷ onde está a obrigação aos fornecedores de abrir suas redes para que exista uma maior competitividade (Entrevistado_Argentina_1).

Finalmente, outro ponto comentado é que a questão política não tem incentivado de que exista um maior acesso e competitividade. “Deve haver muitas empresas que desejem brindar seus serviços, mas podemos dizer que aqui o mercado está dividido somente para uns quantos. Não se tem um incentivo e ao ter poucos no serviço é caro e ruim” (Entrevistado_Argentina_2).

7.1.8 Relatório do estudo de caso argentino

No estudo de caso argentino foi analisado um único corpus documental, devido à limitada existência de publicações oficiais em segurança e defesa cibernética. Desde a origem da DSN até seu impacto na política nacional de segurança cibernética, tem-se evidenciado que o Presidente da Nação Argentina ocupa a Direção do Conselho da Defesa Nacional (CODENA). O planejamento e emprego da segurança e defesa cibernética está localizada aos níveis da subsecretaria, diretorias nacionais e de coordenação interministerial, sendo adotado uma estratégia de desintegrar a responsabilidade da segurança cibernética em diversas entidades civis do Estado argentino. Em resposta às memórias da ditadura militar se tem segregado os instrumentos do poder cibernético, ao declarar que no ciberespaço tem que ser um domínio pacífico, subtraindo-o dos conflitos armados.

Em seguida, foi realizado a análise qualitativa para se obter um ranking das categorias. Sendo a categoria “**Aspecto sociocultural y organizacional**” de maior relevância no corpus argentino (45,2%). Destacando-se a busca da participação e unificação dos esforços na segurança e defesa cibernética pelos atores públicos,

¹⁵⁷ Disponível em <https://www.enacom.gob.ar/servicio-universal_p2246>. Acesso em 10 Oct 2021.

privados e sociedade em geral. Além disso, as intenções focalizadas na transformação e reforma da estrutura pública mediadas pelo Ministério da Modernização, são formas de instrumentalizar as ações políticas e estratégicas nos níveis de governo. Possibilitando a articulação multissetorial do aparato estatal nos esforços para o acatamento de suas diretrizes e prioridades estratégicas, com os objetivos de alcançar um desenvolvimento, progresso e bem-estar nacional. Aponta-se também, o impulso do governo eletrônico e digital na gestão pública argentina, orientado principalmente no acesso à Internet e à banda larga. Porém, existe a necessidade da administração pública de dispor de sistemas de gestão e processamento das informações desde um modelo de medição e monitoração, que possam permitir dos mecanismos de auditoria e geração de métricas e indicadores, tal como, fomentar a formação e capacitação do recurso humano da rede pública.

Outra peculiaridade, não menos relevante, encontra-se na categoria “**Aspecto de las capacidades y respuestas**” (15,4%). Destaca-se que o modelo adotado no estudo de caso argentino envolve as atividades sobrepostas em segurança da informação e cibersegurança, com a responsabilidade da cibersegurança desintegrada entre os diversos organismos e instituições. Contudo, as capacidades desejadas são orientadas para os mecanismos de segurança cibernética e da informação, tais como prevenção, detecção, resposta e recuperação das ameaças, riscos e problemas que afetam a segurança e defesa nacional. Uma segunda perspectiva da categoria, se tem o exercício do papel da defesa nacional, que por intermédio do Ministério da Defesa foram estabelecidas as bases políticas, orgânicas e funcionais fundamentais para a reestruturação das Forças Armadas Argentinas. Outro aspecto é que as capacidades cibernéticas estão relacionadas em maior ponderação com o âmbito do setor defesa, por meio das Forças Armadas.

Segundo as diretrizes da Diretiva de Política de Defesa Nacional (DPDN) se estabelece o dever da Política de Ciberdefesa na redução gradual das vulnerabilidades que emergem da informatização dos ativos estratégicos de interesse da defesa nacional, em cooperação com outros setores responsáveis da Política Nacional em Segurança Cibernética. Deve ser considerado, que o Sistema de Defesa Nacional argentino não pode planejar nem desenvolver atividades relacionadas com questões da segurança interna.

Em resumo, para os especialistas argentinos, no aspecto das ameaças e riscos, suas preocupações estão relacionadas principalmente com as seguintes tópicos:

- A proteção das infraestruturas críticas nacionais, a disponibilidade da informação e dos serviços essenciais.
- A vulnerabilidade sociocultural e de uma coordenação nacional no âmbito da segurança cibernética, existindo a necessidade de um acultramento digital. À vista disso, os cidadãos argentinos estão expostos às operações de desinformação e influência em massas.
- As ações relacionadas aos delitos informáticos, juntamente com a ação judicial frente ao crime cibernético.
- A busca de desenvolver estratégias integrais entre os atores, na otimização dos escassos recursos, com visão holística e de coordenação no âmbito da segurança e defesa cibernética argentina.
- Inexistência de protocolos de respostas diante crises cibernéticas nacionais.
- Imaturidade na governança dos riscos e ineficácia nas estratégias para mitigar a fuga de talento humano no setor público.

No aspecto das capacidades e respostas, foram abordadas as seguintes questões:

- Dispor de capacidades na coordenação e compreensão das ameaças e os riscos cibernéticos, tal como, a percepção do valor da informação para as instituições do setor público.
- Desenvolvimento industrial nacional que tenha em consideração a soberania dos dados e o desenvolvimento local.
- Inovação tecnológica e integração da região para reduzir a dependência tecnológica e a brecha digital.
- Educação integral digital da população, alfabetização digital e inclusão digital.
- O ciclo do recurso humano no âmbito da segurança e defesa cibernética (formação, treinamento, especialização e retenção).

No aspecto do poder e dominação, os especialistas argentinos não se têm negado à provável expansão e dominação por meio das TIC. Outro aspecto ressaltado é a ausência de casos de punição ou sanções que tragam a justificativa da segurança cibernética nacional, como vêm acontecendo nos países desenvolvidos no âmbito cibernético. Eles têm-se manifestado nos seguintes tópicos:

- Consciência que a expansão e dominação das TIC é um processo inevitável, sendo instaurado uma dependência tecnológica nos países menos desenvolvidos.
- Desvalorização da capacidade de inteligência estratégica e de sua concepção, ineficácia na implementação das ações estratégicas e de responsabilidades.
- As iniciativas são na sua maioria cópia integral das boas práticas, sem ter passado por um planejamento estratégico e uma avaliação dos riscos em segurança cibernética. Na Argentina não se tem identificado exercícios de continuidade dos serviços públicos essenciais desde um âmbito nacional, similar aos realizados pela Rússia de se desligar por um período da Internet com o objetivo de validar a disponibilidade de seus serviços essenciais nacionais.
- Não se tem conhecimento de uma estrutura governamental destinada a sancionar as ações tecnológicas, além daquelas que estejam associadas ao crime cibernético. Se desconhecem as iniciativas que regulem a propaganda e a desinformação.

No aspecto do geopolítico e diplomático, os especialistas argentinos têm argumentado o seguinte:

- Não se tem reporte de casos de incidentes cibernéticos que transcenderam a esfera diplomática, porém, foi comentado o vazamento de dados sigilosos na Direção de Assuntos Migratórios e da Agência Federal de Inteligência que aparentemente foi tratado internamente pelas autoridades nacionais.
- Existem acordos de cooperação internacional no intercâmbio das informações.
- Não está claro qual é a entidade responsável da coordenação da geoestratégia nacional responsável dos estudos de prospectiva ciberespacial. Os especialistas entendem que esse papel está dissipado nos diferentes ministérios, por exemplo, através dos comitês interministeriais.
- A questão geopolítica deverá ser uma responsabilidade do governo que está no exercício do poder, porém, os incentivos de melhoria estão relacionados a dispor de um maior orçamento nos setores responsáveis.

No aspecto do sociocultural e organizacional, os especialistas argentinos têm expressado o seguinte:

- Consideram que as iniciativas em segurança cibernética têm incentivado necessárias reformas institucionais. Não obstante, eles apreciam que o Estado argentino tem um alto custo para sair da zona de conforto. Essas iniciativas são de curto prazo ou temporais devido a que o aspecto político muda muito.

- Não se pode apreciar os benefícios da segurança cibernética na sociedade argentina, são abordados primeiro outros tipos de problemas sociais. Se atingem aspectos conceptuais sem tocar de fundo as responsabilidades e os benefícios que têm que ser alcançados.
- Iniciativas que buscam beneficiar aos organismos de menor dimensão que possuem recursos limitados.
- Existem grupos de trabalhos (GTs) ou comitê assessor dos diversos ministérios que improvisam, não tem uma formalidade em sua estruturação, sem recursos próprios e que respondem às motivações próprias deles.

No aspecto do socioeconômico e de mercado, os especialistas argentinos têm expressado o seguinte:

- Existem limitações nas iniciativas no âmbito digital e cibernético, devendo ser mais valorizado e menos influenciado por ideologias políticas.
- Existem esforços de incentivar o consumo nacional das TIC, porém são imaturos na prática, existindo a necessidade de ter uma política de Estado que ajude integrar os esforços dos setores, como por exemplo, incentivar o desenvolvimento tecnológico desde o âmbito tributário, que os investimentos em ciência e tecnologia não sejam considerados gastos públicos, incentivando o conhecimento técnico em todos os níveis sociais, impulsionar a criação de polos científicos-tecnológicos e o oferecimento de ferramentas digitais para empreendedores por parte do Estado.
- Não se tem indicadores ou estratégias na otimização dos programas em segurança e defesa cibernética, não se tem um seguimento da eficácia e performance dos projetos executados.

No aspecto do tecnológico e industrial, os especialistas comentaram o seguinte:

- Se tem elaborado uma política modelo em segurança da informação, porém o setor privado está isento, porque se tem o paradigma que o setor privado tem adotado padrões em segurança mais exigentes e robustos.
- Para os especialistas argentinos é aceitável que o Estado argentino crie estratégias para regulamentar e estabelecer padrões nacionais em TIC, para serem aplicados pelas empresas multinacionais, porém se tem requerimentos em treinamento e de capacitação para os órgãos responsáveis de executar essas atividades.
- Ter uma empresa nacional em serviços de telecomunicações, tem permitido criar capacidades em regulamentar aos ISP estrangeiros, bem como ter incentivado a competição entre os outros ISP. Porém, a dependência na decisão política tem

limitado que as iniciativas de acesso à Internet nos lugares mais afastados não têm permitido minguar a brecha digital.

- Não se tem precisado qual entidade teria a responsabilidade em articular a política de segurança e defesa cibernética com as empresas multinacionais estrangeiras em TIC que operam na Argentina.

Afinal, destacam-se os reflexos qualitativos observados na identificação, análise e sistematização dos elementos e agentes envolvidos nas concepções, discussões e preocupações no que concerne às políticas e estratégias em segurança cibernética no estudo de caso argentino.

7.2. Análise qualitativa do estudo de caso peruano

A análise da codificação indutiva no corpus peruano, apresentou certas similitudes com o estudo de caso argentino, sendo um dos fatores o idioma e os tópicos trabalhados nos documentos analisados. Por essa razão, apresentam-se quase as mesmas categorias que foram identificadas no estudo argentino. Como resultado, existem certos rasgos diferenciais, como por exemplo, os códigos da categoria do **Aspecto socioeconômico e comércio**, cujo uso é menos frequente no estudo argentino. No entanto, a quantidade de segmentos codificados é maior. Essa característica nos leva a supor que essa categoria tem sido de maior relevância e importância para o caso peruano.

Figura 59 - Subcódigos e códigos não identificados: Argentina e Peru

Lista de Códigos	Caso_Argentina	Caso_Peru	SOMA
Aspecto tecnológico e industrial			0
Elementos estructurales en la creación del ciberespacio			0
Activos de información			2
Almacenar datos de personas			1
Características intrínsecas del ciberespacio			1
Ciberespacio o espacio cibernético			2
Comunicación electrónica ou digital			2
Conocimiento científico			2
Control de los registros			2
Desafíos interconectados y complementarios			2
Diseño de la arquitectura tecnológica			2
Generar información			1
Herramientas informáticas de análisis de datos			1
Herramientas transversales			1
Información y conocimiento			2
Informatización de los activos estratégicos			2
Infraestructura digital			2
Infraestructuras críticas			2
Infraestructuras de tecnología de la información			2
Intercambio de conocimientos digitales			2
Internet de las cosas			2
Inversión en telecomunicaciones			1
Masividad			1
Mecanismos de control			2
Medios informáticos compatibles e interoperables			1
Medios y plataformas de información			2
Modelos predictivos			1
Naturaleza dual			1
Principio de control			1
Procesamiento informático de sistemas			2
Red Federal de Fibra Óptica			2

Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

Nota: Exibição binarizada.

Tabela 6 - Resumo do visualizador da matriz de códigos

CATEGORIA	DESCRIÇÃO	CORPUS ARGENTINO	CORPUS PERUANO	SOMA
Aspecto das Ameaças e Riscos	Exibição binarizada (Total de códigos que aparecem na categoria)	114	56	170
	Total de segmentos codificados na categoria	802	357	1159
Aspecto das Capacidades e Resposta	Exibição binarizada (Total de códigos que aparecem na categoria)	125	74	199
	Total de segmentos codificados na categoria	2004	1186	3190
Aspecto de Poder e Dominação	Exibição binarizada (Total de códigos que aparecem na categoria)	76	44	120
	Total de segmentos codificados na categoria	957	795	1752
Aspecto Geopolítico e Diplomático	Exibição binarizada (Total de códigos que aparecem na categoria)	39	14	53
	Total de segmentos codificados na categoria	206	50	256
Aspecto Sociocultural e Organizacional	Exibição binarizada (Total de códigos que aparecem na categoria)	265	173	438
	Total de segmentos codificados na categoria	2841	2783	5624
Aspecto Socioeconômico e Comercio	Exibição binarizada (Total de códigos que aparecem na categoria)	13	10	23
	Total de segmentos codificados na categoria	125	251	376
Aspecto Tecnológico e Industrial	Exibição binarizada (Total de códigos que aparecem na categoria)	50	37	87
	Total de segmentos codificados na categoria	707	476	1183

Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

Durante a análise KWIC, se observam as ideias chaves com os códigos de maior relevância em nosso corpus. Nos permitindo inferir no seguinte:

1. “*Personas y Organizaciones*”. A estrutura básica dos padrões e especificações desde uma interoperabilidade do governo eletrônico, buscam alcançar as necessidades de conectividade no âmbito interno peruano e a relação de uma interação com a sociedade, entre pessoas e organizações.
2. “*Capacidades*”. Desde a perspectiva da inteligência, a Direção Nacional de Inteligência (DINI) identifica as capacidades nacionais e propõe ao Conselho de Segurança e Defesa Nacional (COSEDENA) sua aprovação. Busca-se proteger as capacidades nacionais de todo tipo de ameaça à segurança nacional, criando confiança no entorno digital, através da gestão dos riscos, das medidas de cibersegurança e as capacidades da ciberdefesa devendo estar alinhadas aos objetivos nacionais. Desde a perspectiva da alfabetização digital e fortalecimento das capacidades, se busca incluir nas políticas de educação a formação de capacidades necessárias para o aproveitamento da banda larga e o uso das TIC nos processos administrativos e produtivos.
3. “*Estándares*”. Impulsar o cumprimento de padrões internacionais e desde a estratégia do governo eletrônico buscar a aprovação dos padrões tecnológicos para garantir as medidas de segurança da informação nas entidades públicas.

citada categoria. Sutilmente, podemos dizer, que o menos influente neste caso seria: “*Vigilancia y control de los individuos*”, com 5 segmentos codificados, representando um 1.4%.

- São 32 os documentos que contém os códigos que representam à categoria temática: “*Aspecto de las capacidades y respuesta*”, o código mais influente é: “*Actividades sobrepuestas de la SI y la Ciberseguridad*”, se encontrando em 617 segmentos codificados, representando um 52% dos códigos dessa categoria. Sutilmente, podemos dizer, que o menos influente neste caso seria: “*Desarrollar capacidades y competencias institucionales*”, com 244 segmentos codificados, representando um 20.6%.

- São 35 os documentos que contém os códigos que representam à categoria temática: “*Aspecto de poder y dominación*”, o código mais influente é: “*Actuación en el ámbito regulador, judicial y de sanción*”, se encontrando em 524 segmentos codificados, representando um 65.9% dos códigos dessa categoria. Sutilmente, podemos dizer, que o menos influente neste caso seria: “*Actores de la seguridad interna nacional*”, com 18 segmentos codificados, representando um 2.3%.

- São 13 os documentos que contém os códigos que representam à categoria temática: “*Aspecto geopolítico y diplomático*”, o código mais influente é: “*Factores de preocupación e impacto geopolítico y geoeconómico*”, se encontrando em 35 segmentos codificados, representando um 70% dos códigos dessa categoria. Neste caso o código “*Acuerdos de la diplomacia y relaciones exteriores*”, possui 15 segmentos codificados, sendo o 30%.

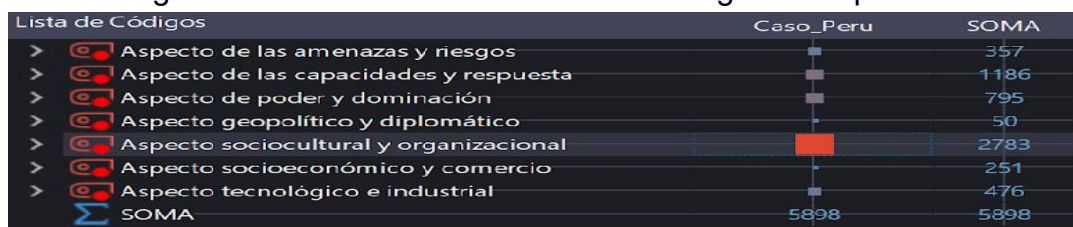
- São 36 os documentos que contém os códigos que representam à categoria temática: “*Aspecto sociocultural y organizacional*”, o código mais influente é: “*Impulsar el gobierno electrónico en la gestión pública*”, se encontrando em 726 segmentos codificados, representando um 26.1% dos códigos dessa categoria. Podemos observar que o código menos influente é: “*Modelo de gestión y supervisión de la red pública*”, com 10 segmentos codificados, representando um 0.4%.

- São 27 os documentos que contém os códigos que representam à categoria temática: “*Aspecto socioeconómico y comercio*”, o código mais influente é “*Integración del aparato económico, financiero y productivo*”, se encontrando em 243 segmentos codificados, representando um 96.8% dos códigos dessa categoria. Podemos observar que o código menos influente é: “*Economía digital Perú*”, com 3 segmentos codificados, representando um 1.2%.

- São 27 os documentos que contém os códigos que representam à categoria temática: “*Aspecto tecnológico e industrial*”, o código mais influente é: “*Elementos estructurales en la creación del ciberespacio*” se encontrando em 28 segmentos codificados, representando um 5.9% dos códigos dessa categoria. Podemos observar que o código “*La concepción de la tecnología en el contexto internacional*”, com 28 segmentos codificados, representando um 5.9%.

Dessa forma, podemos dizer que a categoria: “**Aspecto sociocultural y organizacional**”, com 2,783 segmentos codificados é a temática de maior relevância para os fins das políticas e estratégias no âmbito da segurança cibernética no Peru, seguida da categoria: “*Aspecto de las capacidades y respuestas*”, com 1,186 segmentos codificados.

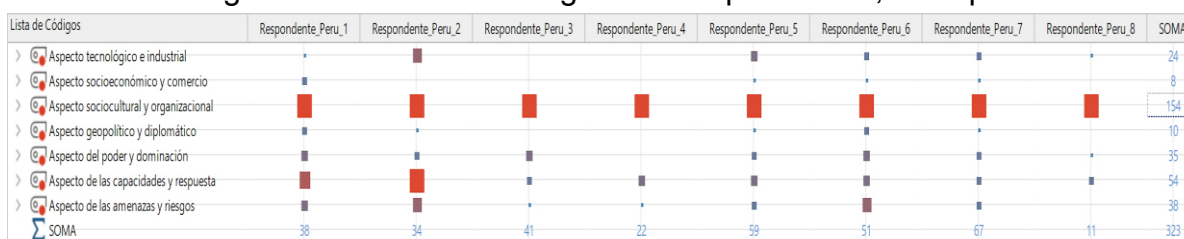
Figura 61 - Visualizador da matriz de códigos caso peruano



Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

Esse análise trazido aos questionários, em forma geral, diferem sutilmente dos resultados, sendo observado que as categorias: “*Aspecto sociocultural y organizacional*” e “*Aspecto de las capacidades y respuestas*” se mantem, porém nas outras categorias diferem em relevância.

Figura 62 - Matriz de códigos dos respondentes, caso peruano



Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

Observou-se que dos especialistas que participaram nos questionários, a categoria: “*Aspecto socioeconómico y comercio*”, não tem sido de maior relevância nas respostas e preocupações dos especialistas peruanos. Somente foram parte das justificativas os Respondentes: Respondente_Peru_1, Respondente_Peru_5, Respondente_Peru_6 e Respondente_Peru_7.

Em relação à categoria: “*Aspecto geopolítico y diplomático*”, com seu código “*Acuerdos de diplomacia y relaciones exteriores*”, foi parte das justificativas dos Respondentes: Respondente_Peru_5, Respondente_Peru_6 e Respondente_Peru_7. E para o outro código “*Factores de preocupación e impacto geopolítico y geoeconómico*”, estiveram nas justificativas dos Respondentes: Respondente_Peru_1, Respondente_Peru_2, Respondente_Peru_6 e Respondente_Peru_7.

Para a categoria: “*Aspecto tecnológico e industrial*”, com seu código “*La concepción de la tecnología en el contexto internacional*”, esteve nas justificativas dos Respondentes: Respondente_Peru_2, Respondente_Peru_5, Respondente_Peru_7 e Respondente_Peru_8.

7.2.1 Aspecto das ameaças e riscos, segundo os especialistas peruanos

Neste aspecto busca-se identificar as prioridades, partes interessadas e elementos que constituem as estratégias de segurança e defesa cibernética, sob a perspectiva das ameaças e riscos cibernéticos. Foram desenvolvidas três perguntas abertas, deixando as seguintes evidências:

a. Entre as prioridades da segurança e defesa cibernética nacional peruana, foi comentado pelos especialistas diversos temas de preocupação. Entre os comentários que coincidem, são os temas de dispor de capacidades técnicas nos diversos níveis de educação. Orientados aos cidadãos desde o ensino básico até nos profissionais de todas as áreas, assim como, do fortalecimento regulatório e legal no âmbito cibernético.

1) Atualizar os instrumentos legislativos e regulatórios, focalizando-os no mundo digital. 2) Educar e sensibilizar ao cidadão continuamente para que conheça os novos instrumentos e faça uso de seus direitos. Incluir como parte dos currículos primários e secundários o uso da tecnologia e sua segurança (Respondente_Peru_7).

Para o Respondente_Peru_3, outra das prioridades seriam o “gerar confiança digital nos cidadãos do país”. Segundo o Respondente_Peru_5, não se tem uma Política Nacional em Cibersegurança ou de segurança cibernética, sendo necessário ter uma instituição estatal na liderança dessa condução, com autonomia na implementação das estratégias em segurança cibernética. Porém, para o

Entrevistado_Peru_2, é importante ter essa política nacional com caráter multissetorial e com perspectiva através do CEPLAN¹⁵⁸.

Em princípio, estabelecer uma Política Nacional de Segurança Cibernética, um instrumento que conduz e possa integrar ao sistema nacional. Em segundo lugar, a implementação de uma Estratégia Nacional de Segurança Cibernética, tanto nas Forças Armadas quanto na sociedade civil estejam representadas. Terceiro, o fortalecimento das capacidades para a implementação da estratégia nacional. Quarto, fortalecer a instituição que regula e governa a política nacional, tendo total autonomia em sua condução e não dependendo diretamente dos governos, devendo ser uma instituição do Estado, transversal ao Executivo (Respondente_Peru_5).

Outra prioridade estaria relacionada com a proteção dos ativos críticos nacionais e a manutenção corretiva-preventiva das infraestruturas de telecomunicações nas entidades públicas. Segundo o Entrevistado_Peru_1, deve ser definida qual Entidade terá a liderança e responsabilidade na governança da segurança cibernética no Peru. Foi comentado pelo experto que “no tema da transformação digital e governo digital existem muitas leis, mas não se tem uma liderança clara” (Entrevistado_Peru_1). Citando a modo exemplo, que em matéria de governo digital seria a SEGDI e em ciberdefesa o MINDEF, porém, a nível das redes e infraestrutura em geral, não se identifica quem seria a Entidade responsável, porque diante de uma iniciativa do MTC em regular ou impulsionar um projeto nesse nível, se é observado uma duplicidade nos papéis, funções e competências com a SEGDI e o MINDEF, que finalmente, desvirtuam ou dificultam as iniciativas e projetos futuros.

b. Sobre os atores envolvidos na segurança e defesa cibernética e se correspondem adequadamente na governança dos riscos cibernéticos, foi comentado por seis dos respondentes, que os esforços na governança dos riscos cibernéticos possuem pouca maturidade. Para o Entrevistado_Peru_1, se tem que reforçar as coordenações entre as entidades públicas e privadas, na tomada de decisões, que envolvem os serviços públicos digitais. Em relação, aos outros dois especialistas, se teve uma resposta mais conceptual, que afirmativa ao item questionado.

Segundo o Respondente_Peru_3, a SEGDI tem promovido a definição das políticas, leis e regulamentos, porém, não se teve em consideração as “*brechas tecnológicas*” de outras entidades públicas, dificultando que o Peru não disponha de

¹⁵⁸ Centro Nacional de Planejamento Estratégico – CEPLAN. Disponível em <<https://www.gob.pe/ceplan>>. Acesso em 11 Nov 2021.

uma Política Nacional de Cibersegurança e se integre a todo o sistema nacional (Respondente_Peru_5).

Acredito que a Secretaria de Governo e Transformação Digital (SEGDI), fez grandes avanços na definição das políticas, leis e regulamentos que regulamentam a segurança digital como questão de interesse público no país. No entanto, considero que além da regulamentação, é importante ter em consideração a lacuna tecnológica que algumas entidades públicas apresentam na implementação. É importante que a SEGDI efetue a monitorização e disponibilização das tecnologias necessárias para salvaguardar a segurança nas organizações em soma à conscientização nacional sobre a confiança digital. Em especial, agora onde as condições de trabalho mudaram (trabalho remoto devido à pandemia), somada ao uso de transações digitais pelos cidadãos (Respondente_Peru_3).

Nessa mesma linha, segundo o Entrevistado_Peru_1, existem instituições públicas que devido a não se ter uma liderança clara e de coordenação nos assuntos da segurança cibernética, poderiam estar dificultando o acionar das outras instituições, assim como, ter lacunas funcionais que permitam às instituições fugirem de suas responsabilidades no tema.

Se teve a modificação da normativa de telecomunicações para que o MTC possa realizar o próprio concurso do espectro, algo que era feito com pro inversão. Está facultado na Lei desde o ano de 1994¹⁵⁹, porém o MTC nunca quis fazê-lo por ser um tema complexo [...]. Me dizem que ainda não se tem a decisão, em um primeiro momento, se desejava que o MTC faça o concurso de espectro de 5G, porque justo se tem um inconveniente com a SEGDI que quer participar pelo tema de segurança digital. Se tem ciberdefesa, segurança digital e a mesma infraestrutura de Telecom. Então se tem 3 entidades que não chegam a um acordo e para mim esse é o principal problema, se tem aprovado normativas, que na minha opinião, estão complicando as iniciativas (Entrevistado_Peru_1).

Poderia ser pensado que a PCM possui uma série de marcos normativos e definições que estão forçados e não são completos, em vez de gerar uma certa liderança, é gerado uma obstrução. A construção de políticas, particularmente se são planejadas desde a inovação e perspectiva de alto nível, não pode ser dado criando mais burocracia. Tem que seguir naturalmente, toda uma estrutura que já está definida no Estado, por isso, eu falava do CEPLAN (Entrevistado_Peru_2).

Em relação a esse problema, para o Entrevistado_Peru_2, não haveria um comum entendimento dos atores relacionados com a defesa e segurança cibernética.

Para mim é importante comentar como uma debilidade, é que não existe um entendimento comum sobre o que é a segurança, defesa cibernética, assim como, a segurança digital (Entrevistado_Peru_2).

¹⁵⁹ Disponível em

<[https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/36D86F8F00994A010525833100078DB5/\\$FILE/16.DS06-94-TCC-reg-General-Ley-de-Telecomunicaciones.pdf](https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/36D86F8F00994A010525833100078DB5/$FILE/16.DS06-94-TCC-reg-General-Ley-de-Telecomunicaciones.pdf)>. Acesso em 10 Nov 2021.

Segundo o Respondente_Peru_7 suas preocupações estariam relacionadas aos problemas da burocracia estatal, à falta de automação de processos e à competição do setor privado na captação dos talentos em cibersegurança.

A aceleração da transformação digital nas empresas e o ambiente globalizado tem gerado mais distanciamento nas organizações públicas, muitas das quais, senão quase todas, avançam lentamente. Os processos burocráticos e a falta de automação de seus processos não os ajudam a acompanhar o contexto da cibersegurança e mitigar os riscos atuais quando ainda tratam de necessidades básicas, como preparar seus funcionários em especialidades de cibersegurança. Por outro lado, as empresas privadas estão atualmente em busca de talentos na especialidade de segurança cibernética e isso deixa pouco espaço para que as instituições envolvidas em segurança e defesa estejam em uma posição melhor para abordar e mitigar riscos (Respondente_Peru_3).

c. Sobre as principais ameaças externas e internas que podem originar uma crise nacional. Segundo os especialistas peruanos, não se tem uma uniformidade na compreensão das ameaças que poderiam deixar exposto ao país a uma crise nacional. “A principal ameaça que pode se tornar uma crise nacional mais tarde é que não há um entendimento claro e que precisamente seja construído em base nisso” (Entrevistado_Peru_2).

Também entre as justificativas dos especialistas, está a insuficiência dos recursos e de orçamentos na capacitação e proteção contra os delitos digitais. É evidenciado a preocupação nas fraudes digitais e a indisponibilidade dos serviços digitais sociais do Estado, como na desinformação nas redes sociais. Segundo o Respondente_Peru_5 “em todos os países existem fraudes eletrônicas, roubo de identidade, falsificação de portais no caso dos bônus ou programas sociais do Estado. Internamente, redes sociais em torno das notícias falsas”.

Para três dos respondentes, as ameaças que possam gerar uma afetação significativa seriam aquelas dirigidas aos Ativos Críticos Nacionais (ACN) e vazamento das informações sensíveis e críticas das entidades públicas.

Eu penso em três supostos. O primeiro, um ataque cibernético por uma ameaça externa de uma organização criminosa ou terrorista nas redes SCADA que desabilita parcial ou totalmente os ACN, como a estação de tratamento de água “La Atarjea” ou o Aeroporto Internacional Jorge Chávez. Segundo um ataque cibernético que inclui a negação dos serviços digitais que afetam o funcionamento do sistema bancário e, por extensão, na economia nacional. Terceiro, o roubo ilegal de dados pessoais que afeta à privacidade dos cidadãos (Respondente_Peru_6).

Segundo o Entrevistado_Peru_1, uma ameaça cibernética no nível de uma crise nacional, seria o corte do cabo submarino da fibra óptica da Internet.

7.2.2 Aspecto das capacidades e resposta, segundo os especialistas peruanos

Neste aspecto busca-se identificar as ações de proteção, partes interessadas e desafios nas estratégias de segurança e defesa cibernética, sob a perspectiva de capacidades e resposta. Para isso foram desenvolvidas 3 perguntas abertas, deixando as seguintes evidências:

a. Para uma proteção adequada do espaço cibernético nacional, que estratégias e ações no nível político-estratégico estão sendo promovidas. Para os especialistas peruanos existe a necessidade de ter uma Política Nacional em Cibersegurança. Consequentemente, dispor de estratégias direcionadas desde a Presidência de Conselho de Ministros (PCM), que permitam a participação dos setores público e privado (Respondente_Peru_3) e a conscientização dos líderes políticos das instituições (Respondente_Peru_1). Porém, o Entrevistado_Peru_2 deu a saber sua preocupação com as diversas normas que finalmente não tem uma objetividade nos resultados desejados.

Desde minha perspectiva se trabalha muito em ter normas como resultados. O fato de publicar uma norma deve ser pensado como uma fase inicial de um objetivo. Se publica uma norma sobre segurança digital ou talento digital, além disso, se tem muito esforço que se tem que gerenciar (Entrevistado_Peru_2).

Além disso, para o Entrevistado_Peru_2, o tema das capacidades deve ser observado desde a perspectiva própria do Estado, onde existem falências e uma delas está relacionada em “como o Estado construí capacidades em geral e não do tema em particular”, se tem conhecimento dos esforços desde a perspectiva dos programas de capacitação, porém, não temos a convicção que seja o suficiente para dispor das capacidades cibernéticas desejadas. De onde podemos inferir que as capacidades no Peru são capacidades orientadas ao consumo das tecnologias. Segundo os especialistas, outro aspecto que deveria ser impulsionado é a criação de uma Entidade, Agência ou Organismo autônomo que possa liderar e regular no país, as iniciativas na segurança cibernética.

Principalmente para ter uma Política Nacional de Segurança Cibernética, que o governo promova um Ministério de Tecnologia ou um Centro Nacional de Segurança Digital que seja o órgão regulador em tudo que diga respeito à segurança cibernética e à ciberdefesa (Respondente_Peru_4).

É necessário um arranjo institucional. Na medida em que existem competências, entendimentos comuns, não apenas para forçar as instituições, também, às instituições precisam ser reavaliadas, repensadas, redesenhadas com base nas experiências internacionais e no modo como os outros países estão operando. Sempre foi comentado sobre um Vice

ministério, Ministério ou Agência de TIC, seria um passo interessante para que as questões de segurança digital sejam totalmente abordadas nessa futura entidade. No momento é uma definição dentro de uma norma da PCM, não acredito que existam, além desses esforços, outros tipos de entendimentos (Entrevistado_Peru_2).

b. Onde estariam os maiores desafios e capacidades cibernéticas no Peru. Para a maioria dos especialistas peruanos, o principal desafio estaria relacionado com a geração de capacidades na proteção cibernética. Segundo o Respondente_Peru_4, “os maiores desafios estariam na proteção de dados, transparência, segurança digital e proteção de cidadãos e empresas no ambiente digital”. Porém, para o Respondente_Peru_8, os maiores desafios estariam em dispor de “orçamento, pessoas qualificadas e na gestão de mudanças”.

Segundo o Respondente_Peru_5, as capacidades cibernéticas estariam principalmente nas seguintes entidades: na SEGDI, no Comando Conjunto das Forças Armadas (CCFFAA) e nas universidades.

Todas essas capacidades devem estar centralizadas na Secretaria de Governo e Transformação Digital. No Comando Conjunto das Forças Armadas, em sua função de Defesa Cibernética. Nas Universidades, em seu papel de capacitação em segurança nacional (Respondente_Peru_5).

Os dois especialistas entrevistados comentaram que um dos maiores desafios é o unificar os esforços em segurança cibernética, desde uma ampla coordenação e sem interferências nas competências dos atores envolvidos. E outro dos desafios seria em definir os padrões mínimos para a segurança em redes, através, de uma política em telecomunicações que considere as preocupações da segurança cibernética.

Em relação às capacidades humanas no âmbito cibernético a serem desenvolvidas, para o Entrevistado_Peru_1 a MINEDU não é uma entidade idônea para impulsionar esse tipo de capacidades e que deveria ser desenvolvida na entidade que terá a liderança na governança da segurança cibernética, que pode ser um novo ministério, uma agência ou uma entidade com perfil de regulador. A proposta do Entrevistado_Peru_2, é que exista um Ministério que em suas competências tenha os aspectos de desenvolvimento e economia digital, sendo tratados como temas transversais: a conectividade, a geração de talentos, o desenvolvimento produtivo digital, a segurança e defesa cibernética. Ele também comentou que “a capacidade de segurança cibernética não é algo que seja valorado ou pensado, e deve ser

direcionado com um enfoque transversal à construção das políticas” (Entrevistado_Peru_2).

c. Que deve ser alcançado com tecnologias como a Internet e outras envolvidas no ciberespaço. O exposto pelos especialistas, se centraliza em garantir o total acesso ao serviço de Internet e a conscientização no uso seguro da Internet e do ciberespaço. Segundo o Respondente_Peru_3, é importante fechar as “*brechas tecnológicas*” existentes e fortalecer a confiança digital.

Garantir que o serviço de Internet chegue a todos os seus cidadãos com custo e segurança adequados. Também que o uso do ciberespaço de forma segura deve ser uma política de Estado, desenvolvida em cada entidade (Respondente_Peru_1).

Para o Entrevistado_Peru_1, deveriam ser alcançados dois aspectos, o primeiro, em orientar que o Internet seja parte da qualidade de vida nas comunidades rurais e outro aspecto é no impacto da Internet no crescimento econômico. Além disso, ele comentou a necessidade de ter concluída a Rede Dorsal Nacional de Fibra Óptica e em complemento incentivar outros tipos de tecnologias para o subministro do serviço da Internet, especialmente nos lugares mais remotos do Peru.

Segundo o Entrevistado_Peru_2 deve se entender que no Peru está se fazendo um seguimento das TIC e não um desenvolvimento de tecnologias. Isto acontece tanto para o âmbito cibernético, como para a inteligência artificial ou outras tecnologias mais complexas. Para o experto é muito remoto pensar em competir com as grandes potenciais, porque somente temos sido observadores e desde esse sentido é que devemos definir que desejamos alcançar com a Internet e as tecnologias envolvidas no ciberespaço.

7.2.3 Aspecto do poder e dominação, segundo os especialistas peruanos

Neste aspecto busca-se analisar os elementos que constituem uma política de segurança cibernética, na perspectiva do poder e da dominação. Foram desenvolvidas duas perguntas abertas, deixando as seguintes evidências:

a. Em relação às estratégias nacionais no campo cibernético dos países desenvolvidos, se têm impulsionado a expansão e a dominação por meio das tecnologias de informação e da comunicação. Não existe uma negação dos especialistas peruanos da provável expansão e dominação dos países desenvolvidos por meio das TIC. Porém, é reconhecida a vantagem que pode se ter frente aos outros

países, ao dispor das infraestruturas de telecomunicações, pessoal capacitado e disponibilidades dos dados no controle da identidade digital.

Portanto, acredito que os países mais desenvolvidos certamente buscam obter mais vantagens neste contexto, como quase sempre tem sido nos bens e espaços comuns da Terra, por exemplo, com o processo de colonização da América Latina e da África, em séculos XVI ao XIX (Respondente_Peru_6).

Segundo o Respondente_Peru_7, se revelam dois modelos de vigilância e controle existentes. O primeiro no lado chinês, desde a perspectiva da soberania dos dados e o segundo no lado norte-americano que é exercido por meio dos instrumentos jurídicos e regulatórios nas empresas multinacionais estadunidenses. As duas formas citadas pelo respondente, apresentam o domínio dos Estados desenvolvidos em relação ao acesso à informação.

Os EUA, China, Rússia e Israel são exemplos de países que possuem uma forte estratégia de segurança cibernética. O mundo de hoje já é mais digital do que físico, os dados de hoje são o novo ouro que todas as empresas desejam ter. Portanto, a origem para começar a ter controle é conhecer a identidade digital das pessoas, pois a partir deste ponto você pode começar a definir perfis, saber do que gostam, quais preferências políticas têm, quais são os vínculos ou relações que mantêm com outras pessoas etc. A China é um exemplo de controle centralizado e monitorado, uma vez que as principais aplicações de controle de acesso ao mundo digital são governamentais. Hoje os EUA estão trabalhando em regulamentações que permitem ter certo controle sobre grandes empresas como um exemplo a Facebook. Hoje as grandes empresas têm todas as nossas informações, portanto, elas têm um certo domínio de todos os países que ainda estão em processo de transformação digital (Respondente_Peru_7).

Para o Respondente_Peru_8, apesar de ter casos de sucesso em segurança cibernética dos países desenvolvidos, é preciso criticar a real necessidade dessas estratégias onde o contexto e a cultura social sejam abordados. Segundo o Entrevistado_Peru_1, a expansão tecnológica em infraestrutura de telecomunicações é dominada pela tecnologia asiática, principalmente pelos países de China, Coreia do Sul Japão. Um dos principais motivos é o custo e a compatibilidade de seus produtos em relação com outros fabricantes, condições que diferem da tecnologia ocidental.

b. Se regulam e punem as ações no âmbito cibernético, que possam afetar os interesses nacionais. Se tem casos de punições ou sanções desde o ponto de vista da segurança e defesa nacional. Segundo o Respondente_Peru_1, si se tem um caso de espionagem e revelação de segredos nacionais no ano 2009, conhecido como o caso Ariza¹⁶⁰. Outrossim, para os especialistas não se tem outros casos em

¹⁶⁰ Disponível em <<https://encr.pw/56TeZ>>. Acesso em 10 nov 2021.

que se tinha reportado sanções específicas no âmbito cibernético, porém, apesar de ter inúmeras iniciativas legais e regulamentares no âmbito digital é evidenciado que os procedimentos punitivos e de controle têm pouca maturidade.

Não acredito porque os regulamentos no Peru são sempre muito flexíveis e o Estado nem sempre tem capacidade para fazer cumprir a lei (*Law Enforcement*), que é essencial na soberania estatal. Não tenho conhecimento sobre o tema das sanções às empresas (Respondente_Peru_6).

Segundo o Respondente_Peru_7, pode-se constatar que as políticas, leis e regulamentações existem, somente que a forma como estão sendo articuladas e aplicadas no nível gerencial é sombria e pouco compreendida, no sentido da falta de profissionais especializados jurídicos em TIC no setor público, impactando na idoneidade do controle e punição em base à Lei.

Acredito que até o momento o Peru já passou pela primeira etapa em que se elaboram ou se adotam legislações como instrumentos jurídicos em segurança ou cibersegurança. Muitas delas ainda transcritas em forma genérica, requer de especialistas para uma melhor interpretação, portanto, isso expõe a falta de especialistas jurídicos em tecnologia que utilizem essas ferramentas para obter sanções a favor ou contra das empresas e do cidadão comum (Respondente_Peru_7).

7.2.4 Aspecto geopolítico e diplomático, segundo os especialistas peruanos

Neste aspecto busca-se analisar a geopolítica no campo cibernético e suas repercussões na consolidação das políticas e estratégias de segurança cibernética. Nesse sentido foram desenvolvidas duas perguntas abertas, deixando as seguintes evidências:

a. A Política Nacional de Segurança Cibernética (ou iniciativas semelhantes) tem atuado com ingerência na esfera diplomática nacional. Se tem casos que transcenderam a esfera diplomática. Dois dos especialistas comentaram desconhecer do assunto questionado. Outros dois comentaram do caso de espionagem e revelação de segredos nacionais no ano 2009, conhecido como Ariza. Porém, existe outro grupo de especialistas que comentam que no caso peruano, as iniciativas em segurança cibernética não têm uma ingerência direta na esfera diplomática. Isto pode ser devido, que não se tem uma Política Nacional em Cibersegurança e que nas propostas de comitês multisetoriais relacionados ao âmbito cibernético ou digital, o Ministério de Relações Exteriores não esteja participando como membro do comitê.

Parece que infelizmente não é o caso do Peru, porque o Ministério das Relações Exteriores não figura no Comitê Nacional de Segurança

Cibernética, que é uma instância multissetorial de segurança digital a cargo do PCM. Se assim for, se dá o erro de considerar a cibersegurança como algo alheio aos interesses nacionais que inclui à política externa e à segurança nacional (Respondente_Peru_6).

Um aspecto a ressaltar neste ponto, foi o comentado pelo Entrevistado_Peru_1, se observando que existe um evidente intervencionismo das entidades e organizações internacionais. Quando expressava parte de suas experiências, em uma reunião na Embaixada Norte Americana, como convidado, se lhe foi informado que por iniciativa própria se tinham realizado bloqueios na rede a seu homólogo chinês. Em resposta a essa iniciativa o Entrevistado_Peru_1, comentou sua preocupação, porque “pelo marco legal em telecomunicações nós somos neutros devido ao Acordo de Livre Comercio¹⁶¹ que se tem com o próprio Estados Unidos, nós somos neutros tecnologicamente”, justificando também, que essas ações poderiam afetar os próprios serviços das empresas de Telecom e projetos de banda larga nas províncias, porque elas fazem uso da infraestrutura chinês.

b. A Instituição responsável da geoestratégia nacional, assim como, os estudos de perspectiva geopolítica e socioeconômica no domínio ciberespacial. Segundo as respostas dos especialistas não fica claro qual é a entidade responsável da coordenação da geoestratégia nacional. Alguns deles acham que é a própria PCM por intermeio da SEGDI, para outros a Direção Nacional de Inteligência (DINI), o Ministério da Defesa (MINDEF) e o CCFFAA. Em consequência, não se tem comentários em relação aos estudos de perspectivas e da sua eficiência.

O Ministério da Defesa (MINDEF) e a Presidência do Conselho de Ministros (PCM) têm papéis compartilhados para este fim. Acredito que os limites de um e de outro que devem ser melhorados ainda não estão claros (Respondente_Peru_8).

Segundo o Entrevistado_Peru_1, o MINDEF si tem demonstrado preocupação nos esforços de perspectiva no domínio ciberespacial, porém, essa atitude não é imitada pelos outros Ministérios, existindo recursos tecnológicos que muitas vezes pela falta de interesse e desconhecimento, tiveram que ser entregues ao MINDEF.

Porém, para o Entrevistado_Peru_2, não identifica que entidade do Estado estaria sendo a responsável da geoestratégia nacional, no âmbito ciberespacial, o que lhe faz pensar que não existe um enfoque geopolítico nesse âmbito. Comentando

¹⁶¹ Em espanhol: *Tratado de Livre Comercio* -TLC

também que nossa situação tecnológica é uma situação preconcebida, em atraso em relação às potências tecnológicas. Segundo ele, os usuários peruanos são alheios às preocupações geopolíticas nas tecnologias como a Internet. “Eu penso que não estamos em uma capacidade para propor uma estratégia geopolítica, que minimamente nós possamos permitir participar no debate tecnológico dos próximos anos a nível global” (Entrevistado_Peru_2).

7.2.5 Aspecto sociocultural e organizacional, segundo os especialistas peruanos

Neste aspecto busca-se analisar os incentivos e benefícios da Política de Segurança Cibernética, na esfera sociocultural e organizacional. Foram desenvolvidas duas perguntas abertas, deixando as seguintes evidências:

a. A Política Nacional de Segurança Cibernética tem incentivado reformas institucionais. Segundo as respostas dos especialistas, eles concordaram que as iniciativas em segurança digital e cibernética trouxeram reformas institucionais, assim como, mudanças culturais, organizacionais e de paradigmas. Para os especialistas, se tem avanços nas iniciativas de segurança digital, especificamente, no âmbito normativo e regulador. Porém, muitas das entidades públicas possuem tecnologia obsoleta com uma débil maturidade de seus processos, não tendo alcançado níveis de automação.

Sim, o positivo é que já houve avanços no desenvolvimento e formalização das políticas e diretrizes em segurança cibernética. No entanto, as instituições ainda estão em processo de mudança, não é segredo que as instituições públicas têm tecnologia desatualizada ou processos que ainda não são automatizados. Portanto, isso significa um impulso maior para essa transformação digital e isso requer mudanças organizacionais dentro das instituições que hoje são responsáveis pela segurança cibernética nas diferentes funções (Respondente_Peru_7).

A nível organizacional, segundo o Entrevistado_Peru_1, existem iniciativas públicas em criar decretos de urgência, porém na prática não são. Neste caso o entrevistado referência dois decretos de urgência: DU N°006-2020¹⁶² Decreto de urgência que cria o Sistema Nacional de Transformação Digital e o DU N°007-2020¹⁶³ Decreto de urgência que aprova o Marco de Confiança Digital e dispõe medidas para seu fortalecimento. Sendo evidenciando a burocracia e ineficácia nas iniciativas de interesse público, porque estando a quase “um ano e médio de ter aprovado esses

¹⁶² Disponível em <<https://acesse.dev/jPM80>>. Acesso em 10 Nov 2021.

¹⁶³ Disponível em <<https://l1nq.com/eYNoh>>. Acesso em 10 Nov 2021.

dois decreto de urgência, não há regulamentação para nenhum dos dois” (Entrevistado_Peru_1). Além, de existir também uma falta de coordenação entre as entidade públicas e distorção nos papéis e funções das entidades públicas. Também foi comentado que muitos das reformas e esforços de melhoria são inconclusos quando se dá uma mudança de gestão do Governo.

Vale ressaltar que o fato de serem problemas no âmbito cibernético, não dá uma solução automática aos problemas que existem no aparato público. “Os problemas da segurança cibernética vão estar sempre afetados pelos problemas que tem o Estado” (Entrevistado_Peru_2).

b. A Política Nacional de Segurança Cibernética (ou iniciativas semelhantes) tem incentivado benefícios sólidos, prosperidade e desenvolvimento da sociedade.

O Respondente_Peru_8 tem-se reservado em sua resposta, justificando que no Peru essas iniciativas estão sendo recém implementadas, pelo que não teria como dar uma resposta concreta para este item. Porém, a maioria dos especialistas peruanos acreditam que as iniciativas em segurança cibernética, sim traz benefícios, incentivando a prosperidade e desenvolvimento da sociedade. Para seis especialistas, o maior beneficiado seria o Estado peruano, especificamente nos serviços relacionados com o cidadão e ao setor da defesa com suas forças armadas.

Acredito que sim, estimulam benefícios sólidos para o desenvolvimento da sociedade, os primeiros setores a serem beneficiados são aqueles relacionados ao atendimento direto ao cidadão, como os ministérios da saúde, educação, justiça e outros, que possuem programas de apoio ao cidadão (Respondente_Peru_1).

Não obstante, para o Respondente_Peru_7 a confiança digital instaurada nos cidadãos geraria esses benefícios, sendo as empresas as primeiras em se beneficiar, para logo ser transmitidos, esses benefícios, aos outros setores.

Um dos pontos importantes é gerar confiança no ambiente digital. Em outras palavras, se o cidadão comum puder confiar nas interações digitais que são geradas entre empresas e indivíduos, isso trará, de qualquer forma, muitos benefícios e crescimento em todos os setores. Em primeiro lugar, vai incentivar aos cidadãos, que hoje ainda pensam e querem realizar as suas transações fisicamente, possam acessar sem receio a realizar suas operações no mundo digital. E consequentemente, gere maiores benefícios para as empresas, assim sucessivamente, beneficiando a todos os setores (Respondente_Peru_7).

Segundo o Entrevistado_Peru_1 os principais setores beneficiários da política de segurança cibernética, seriam os setores de telecomunicações, de energia e minas, assim como, o setor agrícola. Sempre e quando o objetivo principal da política

é a articulação transversal com os setores. Não obstante para o Entrevistado_Peru_2, as iniciativas como o acesso à Internet nas áreas rurais não têm sido inclusivas aos benefícios desejados, sendo uma problemática a cobertura das operadoras nesses setores. Sendo comentado também pelo experto, que o setor mais beneficiado no âmbito econômico é o bancário e privado. Porém, no âmbito social, seriam os cidadãos peruanos de ensino médio das áreas urbanas.

7.2.6 Aspecto socioeconômico e de mercado, segundo os especialistas peruanos

Neste aspecto busca-se analisar os incentivos ao consumismo e à dependência tecnológica, compreender os agentes e elementos envolvidos na política de segurança cibernética, no âmbito socioeconômico e de mercado. Nesse sentido foram desenvolvidas três perguntas abertas, deixando as seguintes evidências:

a. Se tem incentivado o consumo nacional das TIC. As ações ou iniciativas promovidas pelo governo em equilibrar a dependência tecnológica externa.

Segundo as respostas dos especialistas, eles acreditam que de ter uma Política Nacional em Cibersegurança se estaria incentivando ao consumo nacional tecnológico. Segundo as respostas, existem esforços, porém, são imaturos na prática pelo fato de não ter uma política e de se ter ações isoladas pelas instituições no tema. Este item foi justificado pelos especialistas desde a perspectiva das propostas futuras que deveriam ser consideradas ou debatidas nas iniciativas do governo, como por exemplo: fortalecer à CONCYTEC¹⁶⁴, fortalecer à academia em promoção de uma cultura da confiança digital e de intercâmbio internacional com bolsas de estudos entre universidades.

A melhor iniciativa que deveria ser promovida pelo governo nacional seria promover a formação de mais profissionais nesta área, paralelamente ao investimento público e privado em universidades e cursos de pós-graduação. Outra iniciativa é promover o intercâmbio, por meio de programa de bolsas no exterior, com universidades especializadas nessas capacidades. Os benefícios do intercâmbio seriam multiplicados de se aproveitar (Respondente_Peru_6).

Somente um experto expressou não concordar em relação ao equilíbrio da dependência tecnológica externa, justificando o seguinte:

Não concordo, porque sempre tem que ser adquirida a melhor tecnologia não importe de onde ele venha. Si o Peru é capaz de produzir ferramentas

¹⁶⁴ Conselho Nacional de Ciência, Tecnologia e inovação Tecnológica (CONCYTEC) Disponível em <<https://portal.concytec.gob.pe/index.php>>. Acesso em 30 Nov 2021.

tecnológicas de alta qualidade, como nos outros países, pode ser bem-vindo. Enquanto não existir, seria um desperdício de dinheiro, criando uma falsa sensação de segurança (Respondente_Peru_4).

Segundo o Entrevistado_Peru_1, existe uma clara dependência tecnológica estrangeira a nível de infraestrutura de telecomunicações. Além de se ter normas ou iniciativas em segurança cibernética, na prática, não têm incentivos claros na inclusão dos usuários em tecnologias de médio porte (celulares, notebook, tablets etc.), especialmente, nos lugares mais afastados. Nessa linha de pensamento, foi sugerido que a promoção de iniciativas como a isenção de impostos sobre esses tipos de dispositivos tecnológicos beneficiaria ao consumo nacional em TIC (Entrevistado_Peru_1).

b. Na perspectiva do orçamento e investimento público em ciência e tecnologia, os programas em segurança e defesa cibernética visam criar esforços intersetoriais conjuntos. em relação a este item dois especialistas comentaram não ter conhecimento sobre o gasto público e dos investimentos nesses programas. Para os outros especialistas, o orçamento destinado não é o suficiente. Esses orçamentos e investimentos são iniciativas isoladas e não estão sendo monitoradas em sua implementação e efetividade por parte das instituições.

Sei que atualmente cada instituição tem uma parte de responsabilidade, tem seus próprios orçamentos, portanto, seus próprios planos de implementação não estão centralizados nem monitorados para validar que realmente estão sendo usados em implementar a segurança cibernética. Por isso, é necessário ter ativo o comitê multissetorial de cibersegurança nacional. Meu ponto de vista é que o Ministério da Defesa e a Direção Nacional de Inteligência devem ser responsabilizados na liderança da implementação da segurança cibernética nacional (Respondente_Peru_7).

Segundo o Respondente_Peru_5, as autoridades competentes não estariam tomando seriamente os investimentos em segurança cibernética, existem ainda projetos nacionais que não tem concluídos, como por exemplo, a *Red Dorsal Nacional de Fibra Óptica*.

A Secretaria continua publicando normativos que regulam o governo Digital. Em concreto o Ministério de Economia e Finanças, e o Ministério de Transportes e Comunicações mantem como critério principal, concluir a Rede Dorsal Nacional de Fibra Óptica. Não existe investimento ao menos evidente por parte do estado em Governo digital (Respondente_Peru_5).

c. As iniciativas em segurança cibernética têm dado impulso na economia e mercado digital nacional. Os **especialistas** têm coincidido que existem limitações nestas iniciativas, sendo umas delas o não dispor de uma política e de não ter estratégias integrais. Essas iniciativas acontecem em forma lenta ou desacelerada, no ponto de se perder com o ritmo das mudanças e transformações tecnológicas. O Respondente_Peru_6, é da opinião, que as iniciativas em segurança cibernética impulsariam à economia e mercado digital, si ela estaria no marco do livre mercado, ao ponto de sugerir algumas ações que poderiam ser implementadas:

Penso que devem ser melhorados os seguintes aspectos: 1) Garantias do Estado ao investimento privado; 2) Reduzir o custo do equipamento informático; 3) Melhoria da cobertura de sinal digital a nível nacional, pelo menos em todas as cidades do Peru; 4) Sanção drástica contra crimes informáticos e hacktivismo; 5) Promoção de estudos e especializações em segurança cibernética, entre outros (Respondente_Peru_6).

7.2.7 Aspecto tecnológico e industrial, segundo os especialistas peruanos

Neste aspecto busca-se compreender quais atores e elementos constituem uma política de segurança cibernética, no campo tecnológico e industrial. Nesse sentido, foram desenvolvidas 3 perguntas abertas, deixando as seguintes evidências:

a. O responsável nacional por regular e estabelecer os padrões em TIC. Foi dito pelos especialistas, que as estratégias nacionais em segurança cibernética deveriam considerar a capacitação da entidade pública para regular e estabelecer os padrões em TIC, como também, dos mecanismos de avaliação no seu cumprimento. Porém, evidencia-se que não se tem uma clara ideia de que entidade do Estado estaria exercendo esta função, entre as entidades citadas estão: SEGDI, INDECOPI e o CONCYTEC.

Acredito que seja um trabalho conjunto com a Secretaria de Governo e Transformação Digital (SEGDI), que define as diretrizes a serem seguidas e em base a elas as entidades definem a melhor tecnologia a utilizar de acordo com o setor a que pertencem (Respondente_Peru_3).

Segundo o Respondente_Peru_6, no Peru deveria existir um oficial da continuidade do serviço digital nas entidades públicas. Pelo analisado no corpus do caso peruano e nos capítulos anteriores, existem precedentes nos quesitos da segurança da informação que as instituições do Estado peruano devem ter um Oficial de Segurança da Informação de forma obrigatória.

Concordo, mas ao mesmo tempo deve haver um funcionário responsável pela continuidade do serviço digital. Deve haver também uma entidade supervisora responsável pelas entidades públicas. Algo semelhante ao papel desempenhado pela Autoridade Nacional do Serviço Civil (SERVIR) na

contratação de pessoal nas diferentes entidades do Sector Público (Respondente_Peru_6).

Para o Respondente_Peru_2, “antes de elaborar normas e regulações é importante ter um diagnóstico apropriado na identificação das necessidades”. Segundo o Entrevistado_Peru_1, não estaria a favor de que as entidades públicas definam seus padrões em TIC, considerando que a norma de contratação pública orienta à neutralidade tecnológica, nesse sentido, declarou que deve se orientar em dispor de tecnologias com um enfoque mais aberto e modular.

De meu ponto de vista tecnológico, não concordaria que cada entidade tenha o seu requisito técnico específico, devendo ser um requisito adequado à necessidade e que o fornecedor o adapte com a tecnologia mais idônea dentro do âmbito de orçamento disponível da entidade (Entrevistado_Peru_1).

b. As empresas multinacionais estrangeiras estão incluídas na Política Nacional de Segurança Cibernética. Qual setor é responsável por essa articulação. São 5 os especialistas que têm expressado sua falta de conhecimento do tema, justificando que não se tem uma política em atenção ao ponto questionado e menos ainda de alguma norma ou iniciativa que atenda ou traga a discussão às multinacionais estrangeiras, no marco da segurança cibernética e quem seria o articulador.

Segundo o Respondente_Peru_3, as empresas multinacionais se estariam imersos nas iniciativas da segurança cibernética. Comentando o seguinte: “o setor responsável é a PCM, sou da consideração que o investimento deve ser fortalecido e em apoiar às organizações para sua implantação”. Em reforço a esse comentário, foi comentado:

É todo um processo. Existem sérias iniciativas privadas em torno à segurança digital. Promovendo serviços e oferecendo infraestrutura. As entidades estão aumentando as compras de bens e serviços em segurança digital (Respondente_Peru_5).

Outro aspecto comentado, teve relação com atender aos interesses nacionais no domínio digital:

Mas considero que os interesses nacionais do Estado peruano devem prevalecer em caso de disputa ou controvérsia com empresas multinacionais estrangeiras. A soberania nacional, também se aplica ao campo digital, com particularidades e diferenças (Respondente_Peru_6).

Segundo o Entrevistado_Peru_1, não está claro que entidade teria a responsabilidade dessa articulação, comentando que entre a SEGDI e o MINDEF existem situações adversas nesse tema.

c. Se tem incentivado a competição de fornecedores de acesso à Internet (ISP). O governo tem capacidade em regular em forma eficiente e permanente aos ISP. Evidencia-se nas respostas dos especialistas que o acesso à Internet é uma preocupação que está na política de Estado, porém, foi identificado que existem divergências de que entidade teria uma posição de regulador. Segundo o Respondente_Peru_3, se tem progressos nesse item e que está “sendo feito na coordenação direta entre a Secretaria de Governo e Transformação Digital (SEGDI) e o Ministério de Transportes e Comunicações (MTC). Porém, para o Respondente_Peru_7, a OSIPTEL é a instituição responsável de aplicar as regulações, nesse âmbito. Neste aspecto, também se tem evidenciado que o Peru não tem uma empresa pública que oferece esses serviços, em consequência, não teria as capacidades para uma regulação eficiente (Respondente_Peru_4).

Segundo o Entrevistado_Peru_1, deve ser lembrado que “praticamente em telecomunicações não se tem quase nada regulado, o único regulado é a tarifa da telefonia fixa, mas poucos a utilizam”. Desde que ENTEL-CPT¹⁶⁵ foi privatizada no governo do presidente Fujimori, existem zonas que não tem conectividade, sendo uma das causas a pouca rentabilidade para as empresas privadas. O experto comenta, que no passado se teve a iniciativa de elaborar uma lei onde o Estado peruano participaria nessa problemática, mas essa intenção gerou desconforto e várias discussões no setor privado, como competência desleal, que finalmente não chegaram a nenhum objetivo. Além disso, ele comenta que em forma similar, aconteceu com o projeto da Rede Dorsal de Fibra Óptica que tinha uma tarifa fixa, porém, os privados ao ter um margem de manobra diminuem a tarifa, de forma que não permitiu o massivo uso dessa rede.

Apesar de ter impulsado o princípio de livre competência nos ISP, o Peru tem como caso negativo, ter outorgado a concessão da Rede Dorsal Nacional de Fibra Óptica ao setor privado que até a data de hoje, não foi concluído (Respondente_Peru_8).

¹⁶⁵ “En 1994, el gobierno peruano inició la privatización de la Compañía Peruana de Teléfonos (CPT) –encargada de brindar los servicios de telefonía básica en Lima- y la Empresa Nacional de Telecomunicaciones (ENTEL) –proveedor de los servicios de larga distancia nacional e internacional y operador local para el resto del país” (RUIZ, 2002, p.50).

7.2.8 Relatório do estudo de caso peruano

No estudo de caso peruano foi analisado um único corpus documental, devido à limitada existência de publicações oficiais em segurança e defesa cibernética. O objetivo foi descrever de forma sistemática a aplicação da análise de conteúdo, com o processamento dos documentos listados no Apêndice III. No entanto, as experiências e conhecimentos adquiridos nesse âmbito pelo pesquisador durante os anos de 2013 a 2018 reforçaram nossa observação e compreensão no presente estudo de caso. Desde a historicidade de sua DSN e seu impacto na política nacional de segurança cibernética, tem-se evidenciado que a direção do Sistema de Defesa Nacional está a cargo do Presidente da República. Desde o ano 2012, foi criada a SEDENA como uma secretaria anexa à PCM com a responsabilidade de articular a Política de Segurança e Defesa Nacional, porém a partir do 2016, é absorvida pelo MINDEF.

Em seguida, ao serem observadas as relações diretas e indiretas existentes nos códigos evidencia-se que a categoria “**Aspecto sociocultural y organizacional**” possui a maior relevância no corpus peruano (47,7%), destacando-se as intenções do nível estratégico de impulsionar do governo eletrônico e digital na gestão pública, orientado principalmente desde o acesso à Internet e a banda larga, sendo essencial a participação dos atores públicos, privados e da sociedade. Além disso, a gestão pública e governamental são as preocupações mais relevantes na instrumentalização das ações políticas e estratégicas nos níveis de governo, possibilitando a articulação multissetorial do aparato estatal mediada por diversas comissões, com o objetivo de concordar em conceitos, coletar experiências e contribuições dos diferentes participantes na implementação e nos esforços para o cumprimento dos objetivos estratégicos. Observa-se que o Foro do Acordo Nacional, organizado pela Câmara de Comércio de Piura, a Confederação Nacional de Instituições Empresariais Privadas (CONFIED) e as Nações Unidas em Peru, é um espaço tripartido de diálogo e construção de consensos, constituído pelas três esferas do Governo e as principais instituições políticas e sociais do país, instaurado desde o ano 2002. Neste espaço é onde também se definem as Políticas de Estado, servindo de instrumento para propor mudanças necessárias nos aspectos sociais, políticos e econômicos, com a finalidade de alcançar o bem comum no marco do desenvolvimento sustentável e afirmar a

governabilidade democrática. Estando na quarta Política de Estado chamado “*Estado eficiente, transparente y descentralizado*”, em sua política 35, “*Política de Sociedad de la Información y Sociedad del conocimiento*”, de onde ficaram materializadas as preocupações mais relevantes que conseqüentemente inserem à segurança da informação e a segurança cibernética nas ações políticas e estratégicas.

A seguinte peculiaridade, encontra-se entre duas categorias, as quais são: “**Aspecto de las capacidades y respuestas**” (16,7%) e “**Aspecto de poder y dominación**” (10,8%), devido a que nos análises realizados elas aparecem próximas e relevantes. Destaca-se que na primeira categoria citada, o modelo adotado no estudo de caso peruano envolve às atividades sobrepostas em segurança da informação e de cibersegurança, sem uma distinção clara de seu acionamento nos nível político, estratégico, operacional e tático. Porém, as capacidades desejadas foram orientadas à gestão dos riscos e aos mecanismos da segurança da informação e cibernética como a prevenção, detecção, resposta e recuperação das ameaças, riscos e problemas que afetam à segurança e defesa nacional. Outra característica é que essas capacidades estariam sendo focalizadas no âmbito das pessoas e das entidades públicas. Desde a perspectiva do análise de frequências, podemos inferir que a busca das capacidades é em atenção às necessidades das pessoas e organizações desde os objetivos das políticas e estratégias do governo digital e eletrônico, sendo seu principal ator a SEGDI.

A atuação do Estado peruano no âmbito regulador, judicial e de punição tem uma relevância significativa em suas ações da segurança digital e cibernética. Especificamente desde as normas jurídicas, os marcos regulatórios, os padrões e protocolos de obrigatório cumprimento para a implementação dos quesitos da governança eletrônica e digital.

Em sínteses os especialistas peruanos comentaram no aspecto das ameaças e riscos, as seguintes preocupações:

- Dispor de uma Política Nacional em Segurança Cibernética, que defina a entidade responsável da sua implementação e articulação multissetorial através da CEPLAN. Esta entidade deverá ter autonomia e recursos próprios, sendo o articulador da segurança cibernética nacional, abrangendo desde uma política de Estado à segurança da informação, segurança digital e às redes e infraestruturas de Telecom como um todo.

- Proteção dos ativos críticos nacionais, desde uma base de compreensão do nível de exposição que possam causar as ameaças cibernéticas, na busca de mitigar de forma proativa e eficiente os distintos ataques cibernéticos que possam afetar esses ativos. Um exemplo, que poderia causar uma crise nacional no Peru, seria o corte dos cabos marítimos de fibra óptica.
- Os Problemas burocráticos e falta de alinhamento nos atores, existindo duplicidade de suas funções dificultando o acionar de outros atores, e no pior dos casos permitindo brechas para fugir das responsabilidades em matéria da segurança digital e cibernética. Necessidade de um governança e gestão dos riscos da informação nas instituições públicas.
- Necessidade de fortalecer a confiança digital nos cidadãos, com iniciativas no marco legal e regulamentar que considerem as brechas digitais e tecnológicas existentes nas instituições públicas.
- Priorizar as iniciativas que permitam dar uma resposta ao acionar dos cibercriminosos e às operações de desinformação na redes sociais.

Em outro aspecto nas capacidades e respostas, em forma geral foi reiterado a necessidade de ter uma Política Nacional em Segurança Cibernética e da entidade que terá essa liderança, sendo abordadas as seguintes questões:

- Necessidade de conscientizar aos líderes políticos e decisórios das instituições públicas em matéria de segurança cibernética e digital, se tem comentado que a capacidade em segurança cibernética não é valorada desde um enfoque transversal nas políticas públicas.
- Amplo panorama normativo em matéria de segurança digital, porém sem uma clara objetividade nos resultados desejados. Onde sejam garantidos o total acesso do serviço da Internet na população rural, o impacto que essas tecnologias irão se influenciar na economia digital e a qualidade da Internet como de outros serviços tecnológicos disponibilizados aos cidadãos.
- Estabelecer estratégias e ações no nível político-estratégico para a construção de capacidades no desenvolvimento nacional de tecnologias e buscar equilibrar a dependência das tecnologias.

No aspecto do poder e dominação, ao igual no caso argentino, os especialistas peruanos têm consciência da provável expansão e dominação dos países desenvolvidos por meio das TIC, estando ressaltado o seguinte:

- A expansão tecnológica em infraestrutura e redes de telecomunicações é motivada pelo custo e a compatibilidade que esses produtos possuam em relação a outros.
- São revelados dois modelos instaurados de dominação, uma da soberania dos dados e a outra no exercício dos instrumentos jurídicos e regulamentares.
- Ausência de casos em que empresas multinacionais tinham sido punidas desde o ponto de vista da segurança e defesa cibernética. Se tem uma ampla base legal e regulamentar no âmbito da segurança digital, porém o exercício dos processos de avaliação e control tem pouca maturidade frente a essas empresas.

No aspecto do geopolítico e diplomático, evidencia-se de um caso de espionagem militar por parte do país de Chile. Além disso, não se tem outro caso de conhecimento público que tinha transcendido à esfera diplomática. Porém, segundo os comentários dos especialistas peruanos a geopolítica aplicada ao domínio do ciberespaço não estariam em suas preocupações. Nesse sentido, se cita a continuação os pontos principais nas respostas dos especialistas:

- São comuns as práticas de intervencionismo e de influência das entidades e organizações internacionais no âmbito cibernético. Sendo parte desse mecanismo, os acordos de cooperação e capacitação internacional pelos países com tecnologia avançada.
- Não se tem uma compreensão em comum de qual seria a entidade responsável da coordenação de uma geoestratégia no âmbito ciberespacial no Peru.

No aspecto do sociocultural e organizacional, os especialistas peruanos têm expressado que as iniciativas em segurança digital e cibernética têm incentivado reformas institucionais. Nesse aspecto, eles têm ressaltado as seguintes preocupações:

- Os problemas da segurança cibernética sempre serão afetados pelos problemas que o Estado peruano possui. Um exemplo desses problemas, estaria relacionado a que as entidades públicas possuem tecnologia obsoleta, com uma débil maturidade de seus processos, não tendo alcançado níveis de automação.
- Burocracia e ineficácia nas iniciativas de interesse público, devido a que foram pensadas no curto prazo ou para atender a aspectos político-partidário. As reformas e esforços de melhoria são inconclusos e deixam de ser priorizados quando se dá uma mudança de gestão no governo.

- A segurança digital e cibernética tem trazido benefícios, prosperidade e desenvolvimento no setor urbano. Estando entre os mais beneficiados o setor bancário no âmbito econômico e os cidadãos com ensino médio no âmbito social.
- As iniciativas de acesso à Internet nas áreas rurais não têm sido inclusivas aos benefícios desejados. Uma problemática é o fator da cobertura das operadoras (ISP), devido a que são áreas afastadas, de difícil acesso e de baixo interesse lucrativo.

No aspecto do socioeconômico e de mercado, os especialistas peruanos tiveram respostas pouco objetivas que relacionem às iniciativas na economia e mercado digital no Peru, os pontos comentados e sugeridos são as seguintes:

- Existem esforços, porém, são imaturos na prática pelo fato de não ter uma política nacional em segurança cibernética, existindo iniciativas asiladas pelas instituições no tema. Os orçamentos e investimentos em tecnologia não são monitoradas em sua implementação e efetividade por parte das instituições. Tendo sido observado, que as autoridades competentes não tomam seriamente os investimentos em segurança cibernética, existem ainda projetos nacionais que não tem concluídos (*Red Dorsal Nacional de Fibra Óptica – RDNFO*).
- Incentivar iniciativas de isenção de impostos sobre os dispositivos tecnológicos que impulse o consumo nacional em TIC, tendo como objetivo aos usuários rurais, como seus principais beneficiários.

Finalmente, no aspecto do tecnológico e industrial, os especialistas comentaram o seguinte:

- Não se tem um comum entendimento do responsável nacional em regular e estabelecer os padrões em TIC no âmbito da segurança cibernética. Entre as entidades citadas estão: SEGDI, INDECOPI e o CONCYTEC. Nesse sentido, foi observado que as normas e regulações impulsadas desde as entidades não possuem um diagnóstico apropriado na identificação de suas reais necessidades.
- Não se tem uma política, norma ou iniciativa em atenção à discussão das multinacionais estrangeiras no marco da segurança digital e cibernética.
- Não se tem uma empresa nacional em serviços de telecomunicações que permita criar capacidades em regulamentar aos ISP estrangeiros, bem como, ter incentivado à competição entre os outros ISP. Sendo argumentado pelos especialistas que em telecomunicações não se tem quase nada regulado, o único regulado é a tarifa da telefonia fixa, mas poucos a utilizam.

Dessa forma, destacam-se os reflexos qualitativos observados na identificação, análise e sistematização dos elementos e agentes envolvidos nas concepções, discussões e preocupações relacionadas às políticas e estratégias em segurança cibernética do estudo de caso peruano.

7.3 Análise qualitativa do estudo de caso brasileiro

Analogamente aos estudos de casos anteriores, foi aplicada a codificação indutiva, abrindo a possibilidade de identificar e desenvolver novos conceitos e teorias. A Tabela 23 reproduz as categorias definidas no corpus do caso brasileiro, considerando, as peculiaridades inerentes e o contexto que os envolvem. No caso brasileiro, vislumbram-se os agentes envolvidos nas estratégias, bem como os elementos que constituem a política em segurança cibernética.

Quadro 23 - Categorias do caso brasileiro

Categorias	Tipos de categorias	Código	Notas Analíticas preliminares
Aspecto das ameaças e riscos	Categorias temáticas	Monitoramento e prevenção em segurança	Preocupação do Estado em dispor de mecanismos de detecção de ataques e rotinas de verificações de conformidade, para o monitoramento do cenário cibernético que garanta o acesso autorizado e aos requisitos de segurança. Se destaca a preocupação da segurança cibernética do Governo frente aos ataques sofisticados às cadeias de suprimentos.
	Categorias temáticas	Preocupação nacional e impacto na sociedade	Devido à falta de um alinhamento normativo, estratégico e operacional se gera retrabalho e perda de conhecimento. Destaca-se a necessidade de uma cooperação nacional e internacional, com foco no respeito dos direitos humanos e garantias fundamentais como a liberdade de expressão, proteção dos dados pessoais e da privacidade e à transparência e acesso às informações públicas. No âmbito internacional, ao respeito da democracia e direitos humanos. Ampliar o acesso à Internet e às tecnologias digitais, sendo as telecomunicações, o principal motor do desenvolvimento social e econômico no cenário global.
	Categorias temáticas	Ameaças, riscos e problema de interesse nacional	Destaca-se como função estratégica a manutenção das infraestruturas críticas para evitar ou minimizar os ataques cibernéticos às redes e sistemas de informação do governo e dos segmentos da sociedade. As maiores ameaças e riscos estão relacionados ao crime organizado, espionagem, ilícitos e fraudes cibernéticos, porém, existem preocupações relacionadas à falta de alinhamento normativo, estratégico e operacional e dependência nas tecnologias cibernéticas e externas.
	Categorias temáticas	Atividades de inteligência como instrumento de control	A forma de atuação cibernética política-estratégica tem foco na obtenção de inteligência, com um nível de envolvimento nacional, normalmente interministerial, requerendo ações diplomáticas desde o tempo de paz, fazendo parte de uma operação de informação ou de inteligência. As atividades principais estão relacionadas com a classificação e sigilo da informação e das comunicações, e à restrição do tratamento das informações sensíveis e sigilosas.
Aspecto das capacidades e respostas	Categorias temáticas	Atividades sobrepostas de Segurança da informação e comunicação e Segurança Cibernética	As funções de segurança da informação e comunicações abrangem às da segurança cibernética coordenadas pela Presidência da República (PR) e a defesa cibernética a cargo do Ministério da Defesa (MD), sendo nomeado o Exército Brasileiro (EB) responsável das coordenações de defesa e guerra cibernética.
	Categorias temáticas	Exercício de segurança e defesa nacional	A segurança e defesa nacional, se dá em 4 níveis: político, estratégico, operacional e tático. A Estratégia Nacional de Segurança da Informação tem sido construída em módulos, a fim de contemplar a segurança cibernética, a defesa cibernética, a segurança das infraestruturas críticas, a segurança da informação sigilosa e a proteção contra vazamento de

			dados. O alinhamento estratégico e normativo às ações da segurança cibernética, deve ser atribuída com especial atenção ao setor produtivo, as quais, pela natural força advinda do mercado, são mais bem-sucedidas que as dedicadas exclusivamente às ações do setor público e à fiscalização regulatória.
	Categorias temáticas	Capacidades, articulação e competências nacionais	Preocupação em estender a capacidade da defesa do País para a proteção da nação no espaço cibernético. Incrementar a capacidade dissuasória da defesa para fazer frente às ameaças cibernéticas. Preocupação do Estado em desenvolver capacidades humanas, de educação, pesquisa e de habilidades em segurança cibernética que lhe permita articular o marco legal, competências e recursos institucionais e privados em atenção às necessidades nacionais em segurança.
Aspecto do poder e dominação	Categorias temáticas	Natureza e atributo do poder estatal	Atribuições e competências em estabelecer os mecanismos de governança multiparticipativa e de projetar poder em defesa da soberania e sociedade brasileira, integrando os setores envolvidos na proteção do ciberespaço nacional.
	Categorias temáticas	Atores da segurança interna nacional	O Gabinete de segurança institucional da Presidência da República, liderando a Política Nacional de Segurança da Informação coordenando a participação das forças policiais, de justiça e segurança pública.
	Categorias temáticas	Organizações e assuntos internacionais de influência	A influência das organizações internacionais nos assuntos nacionais e exigências na construção de confiança e segurança para o desenvolvimento nacional. Adoção de uma estratégia interamericana integral na abordagem multidimensional e multidisciplinar para a criação de uma cultura de segurança cibernética.
	Categorias temáticas	Atuação no âmbito regulatório, judicial e punição	Existem mecanismos que buscam regular, processar, combater e sancionar ações delituosas no campo tecnológico. Estabelecer normas e eventuais leis que rejam o espaço cibernético.
Aspecto geopolítico e da diplomacia	Categorias temáticas	Acordos da diplomacia e relações exteriores	Os fenômenos que envolvem à tecnologia exigem nos países, negociações por meio de acordos de cooperação e ações de resolução de conflitos. O tema de segurança cibernética nos objetivos da Câmara de Relações Exteriores e Defesa Nacional (CREDEN) do Conselho de Governo acompanha as conjunturas político-estratégica relacionadas à defesa nacional, como também de fatos relevantes com potencial de risco à estabilidade institucional, para prover informações ao Presidente da República.
	Categorias temáticas	Fatores de preocupação e impacto geopolítico e geoeconômico	As preocupações trazidas a debate por organismos internacionais e pelas principais potências mundiais têm como características de estudo os cenários geopolítico e geoeconômico. A necessidade de uma mudança de paradigma na reestruturação do ecossistema digital para a adoção e desenvolvimento de tecnologias emergentes.
Aspecto sociocultural e organizacional	Categorias temáticas	Fatores e elementos envolvidos na globalização	Vários elementos estão envolvidos no fenômeno da globalização: consumidores, cidades inteligentes, ciberespaço, redes de dados etc. Porém, existem fatores comuns como a economia digital, revolução tecnológica o uso de ferramentas tecnológicas e a conectividade, entre outros.
	Categorias temáticas	Formação de profissionais e recursos	As preocupações do setor público, no âmbito da segurança cibernética, é instruir, capacitar e tecnificar a seus recursos humanos em todos os níveis do governo. Nesse contexto, as instituições públicas devem buscar a articulação e o fortalecimento na área de segurança cibernética, por meio de ações colaborativas e de parcerias com o setor privado, com a academia e com o terceiro setor, no País e no exterior, para estimular o contínuo desenvolvimento de massa crítica e de talentos.
	Categorias temáticas	Governo e gestão da informação governamental	A necessidade do setor público em buscar estabelecer um modelo centralizado de governança e gestão de suas informações. Dispor de um modelo de maturidade na produção de conhecimento e tomada de decisões com métricas e mecanismos de avaliação e revisão periódica.
	Categorias temáticas	Rede pública	A necessidade de acesso à Internet de banda larga de alta velocidade e incrementar a relação computador/aluno das escolas públicas. Porém, as interconexões de redes públicas e privadas e o compartilhamento de recursos expõem as organizações às diversas ameaças.
	Categorias temáticas	Identificação de pessoas no digital	Restrita capacidade de gestão de pessoas, particularmente no que concerne à identificação, seleção, capacitação e retenção de talentos. A confiança pelo certificado digital, é um aspecto que se aborda na proteção e segurança cibernética, para garantir de forma inequívoca a identidade eletrônica de um indivíduo ou de uma organização.
	Categorias temáticas	Impulsar o governo eletrônico na gestão pública	Execução das políticas, estratégias e planos em todos os níveis de governo, que visam criar um ambiente propício para o desenvolvimento de transformação digital da economia e do governo, com iniciativas essenciais para impulsar a digitalização.
	Categorias temáticas	Impulsar o desenvolvimento	Promover o desenvolvimento, o progresso e o bem-estar que gerem impacto socioeconômico, científico, cultural e tecnológico sobre os

		, progresso e bem-estar	indivíduos e organizações nacionais.
	Categorias temáticas	Instrumentalizar as políticas públicas na articulação nacional	Políticas e estratégias, nos níveis de governo, permitem a articulação multisetorial do aparato estatal na coordenação, no monitoramento, na avaliação e na supervisão das ações de investimentos em parcerias e no apoio às ações setoriais à sua execução dentro dos esforços para o acatamento dos objetivos estratégicos.
	Categorias temáticas	Participação dos atores públicos, privados e sociedade	A busca de unificar os esforços na segurança e defesa nacional incentivando a integração, participação e consenso dos atores públicos, privados e sociedade.
	Categorias temáticas	Proteção à privacidade e liberdade de expressão	A preocupação do Estado de regular e salvaguardar a proteção da privacidade dos dados pessoais, como também, a liberdade de expressão de seus cidadãos.
	Categorias temáticas	Transformação e a modernização da estrutura pública	Esforços para a reforma educativa e legislativa, como também, para a modernização da estrutura pública por meio da utilização das tecnologias de informação e da comunicação, segundo os eixos temáticos transformadores da estratégia nacional de segurança cibernética.
Aspecto socioeconômico e comercio	Categorias temáticas	Comércio	Promoção do comércio digital nacional e internacional, incentivando investimentos e competitividade na comercialização dos serviços e produtos do País, apoiando com ações de fiscalização e controle do comércio exterior.
	Categorias temáticas	Economia financeiro e	A economia digital, a inserção do País na indústria 4.0 e o alcance dos objetivos de desenvolvimento sustentável, exigem que tenha condições de construir a confiança e a segurança necessárias para o desenvolvimento nacional na era da informação. Erradicação da pobreza pela inclusão financeira dos mais pobres com a combinação dos terminais móveis com acesso à Internet, pagamentos móveis e novos instrumentos financeiros no ambiente digital.
	Categorias temáticas	Mercado	A indústria de defesa competitiva e consolidada gera empregos qualificados e incentiva o desenvolvimento tecnológico, com encadeamentos produtivos para outros setores da indústria. Em decorrência, esforços em segurança cibernética e da informação podem representar um salto da inserção da indústria nacional de tecnologia da informação e comunicação (TIC) nos mercados interno e global, bem como, de evolução e excelência da pesquisa, desenvolvimento e inovação dessas áreas em nível nacional e internacional.
Aspecto tecnológico e industrial	Categorias temáticas	Elementos estruturais na criação do ciberespaço	A materialização do ciberespaço é baseada na construção de elementos como: infraestrutura, dados, informação, conhecimento, automação, inteligência, conectividade global e controle.
	Categorias temáticas	Inovação tecnológica	O Governo, a indústria, a academia e a sociedade em geral devem incentivar a inovação tecnológica e a adoção de tecnologias de ponta, e manter constante atenção à segurança nacional, à economia e à livre expressão.
	Categorias temáticas	Desenvolvimento e inovação	A expansão do ambiente digital se traduz em enormes oportunidades de desenvolvimento econômico, inclusão social e inovação tecnológica. O avanço tecnológico evidenciou a relevância do incentivo à pesquisa e à inovação em prol do desenvolvimento, e demonstrou o papel essencial dessas áreas para a sociedade.
	Categorias temáticas	Propriedade intelectual	Os riscos dos ataques cibernéticos cresceram, em especial as violações de informações acessadas por fornecedores terceirizados e o furto de informações (informações pessoais identificáveis, propriedade intelectual e segredos comerciais). Preocupação do País na discussão mundial da Propriedade Intelectual no ambiente digital.
	Categorias temáticas	Industria cibernética	A Segurança cibernética orienta uma oportunidade favorável ao investimento, nas universidades, em atividades de pesquisa, desenvolvimento e inovação, bem como na criação de um complexo industrial voltado especificamente para as “tecnologias de fronteira”.
	Categorias temáticas	Cooperação internacional	Deve ser viabilizada por meio de ações que assegurem seu desenvolvimento e sua contínua implementação, contemplando o compartilhamento de informações (benchmarking, conhecimento tecnológico, doutrina, análise de ameaças, compartilhamento de inteligência cibernética, avaliação de crises cibernéticas de vulto) e a celebração de instrumentos sobre o tema.
	Categorias temáticas	Cenário internacional	O cenário internacional caracterizado por incertezas tem influência direta tanto na definição da política externa do País, quanto em sua política de segurança e defesa.
	Categorias temáticas	Universo conectado e seguro	As necessidades de mudança tecnológica no País trazem expectativas de um futuro próspero, inclusivo e de desenvolvimento sobre a provocação de dispor com mecanismos de cooperação internacional. Construir uma

			sociedade conectada tem sido um desafio para o País. Entretanto, essa realidade trouxe uma série de novas preocupações, especialmente em relação às vulnerabilidades e às ameaças cibernéticas.

Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

Em relação ao análise KWIC, são apresentadas as ideias chaves que se relacionam com os códigos de maior relevância do corpus estudado. Por exemplo, podemos inferir no seguinte:

1. Segurança cibernética. Trata-se no nível político a cargo da Presidência da República, abrangendo à Administração Pública Federal (APF), bem como as infraestruturas críticas da informação inerentes às infraestruturas críticas nacionais. Definida como a arte de assegurar a existência e a continuidade da sociedade da informação do País, garantindo e protegendo, no espaço cibernético, seus ativos de informação e suas infraestruturas críticas. No contexto da mobilização, em situações de normalidade ou crise, pode haver o recrutamento de especialistas em segurança cibernética. O relatório final da Comissão Parlamentar de Inquérito (CPI) da Espionagem, apontou fragilidade do Brasil nas telecomunicações e do sistema de inteligência e defesa, frente a espionagem eletrônica internacional.
2. Internet. Trata-se no nível político, tendo como ator ao Comitê Gestor da Internet. A doutrina de Guerra Cibernética do Exército Brasileiro (EB) busca contribuir no desenvolvimento das capacidades nesse domínio. O projeto Geoestacionário de Defesa e Comunicações (SGDC) busca prover cobertura de Internet ao 100% do território brasileiro. A disciplina do uso da Internet tem como fundamento o respeito à liberdade de expressão e seu acesso é essencial ao exercício da cidadania.
3. Segurança da Informação e comunicações (SIC). Se tem uma política nacional em Segurança da Informação e Comunicações que abrange à segurança cibernética, sendo reconhecida pelos atores do governo como relevante e de competência político estratégica. As ações da SIC objetivam viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade dos dados e informações. No Brasil, os assuntos da SIC e segurança das infraestruturas críticas estão sendo tratados no âmbito do Conselho de Defesa Nacional (CDN) e da Câmara de Relações Exteriores e Defesa Nacional (CREDEN).
4. Inteligência. A necessidade do uso da fonte cibernética, que pode ser integrada às outras fontes: humanas, imagens e sinais; para a produção do conhecimento de inteligência. Se tem ações conjuntas de Guerra Cibernética com a Inteligência, através da coleta e busca de dados de potenciais ameaças ou adversários, análise de dados

coletados das redes e ativos de informação e o compartilhamento dos dados nos diversos níveis da segurança.

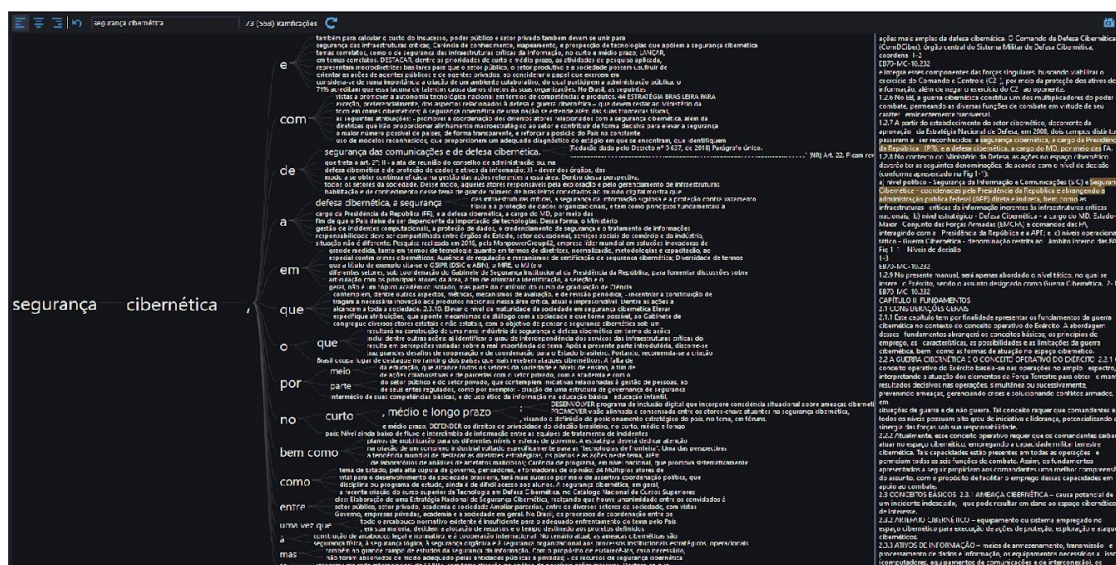
5. Economia digital. Os indicadores de desenvolvimento econômico e social no Brasil tem apresentado expectativas no sucesso da economia digital. Se busca a concertação de iniciativas governamentais ligadas à economia digital. Nesse contexto de oportunidades e desafios, se busca uma ação coordenada governamental com agentes privados para mitigar os riscos, evitando deste jeito, a geração de uma sensação de insegurança que pode retardar o ritmo e desenvolvimento da economia digital. Se tem adotado ações estratégicas que tem como objetivo a internacionalização de empresas brasileiras na economia digital, promovendo a exportação de produtos e serviços, assim como a atração de investimentos estrangeiros para setores estratégicos.

Figura 63 - Árvore de palavras interativas do caso brasileiro (KWIC: Internet)



Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

Figura 64 - Árvore de palavras interativas do caso brasileiro (KWIC: Segurança Cibernética)



Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

Em complemento à tabela das categorias concebida do análise qualitativo, foram evidenciadas as seguintes características nos documentos analisados:

- São 33 os documentos que contêm os códigos que representam à categoria temática: Aspecto das ameaças e riscos. O código mais influente nessa categoria é: Ameaças, riscos e problemas de interesse nacional, se encontrando em 1,254 segmentos codificados, representando um 55.4% dos códigos que formam a citada categoria. Sutilmente, podemos dizer, que o menos influente neste caso seria: Monitoramento e prevenção em segurança, com 58 segmentos codificados, representando um 2.6%.
- São 32 os documentos que contêm os códigos que representam à categoria temática: Aspecto das capacidades e resposta, o código mais influente é: Atividades sobrepostas de SIC e SegCiber, se encontrando em 2,142 segmentos codificados, representando um 61.5% dos códigos dessa categoria. Sutilmente, podemos dizer, que o menos influente neste caso seria: Capacidades, articulação e competências nacionais, com 646 segmentos codificados, representando um 18.5%.
- São 32 os documentos que contêm os códigos que representam à categoria temática: Aspecto de poder e dominação, o código mais influente é: Natureza e atributo do poder estatal, se encontrando em 446 segmentos codificados, representando um 28.5% dos códigos dessa categoria. Sutilmente, podemos dizer,

que o menos influente neste caso seria: Atores da segurança interna nacional, com 247 segmentos codificados, representando um 15.8%.

- São 30 os documentos que contém os códigos que representam à categoria temática: Aspecto geopolítico e da diplomacia, o código mais influente é: Fatores de preocupação e impacto geopolítico e geoeconômico, se encontrando em 778 segmentos codificados, representando um 88.8% dos códigos dessa categoria. Neste caso o código Acordos da diplomacia e relações exteriores, possui 98 segmentos codificados, sendo o 11.2%.

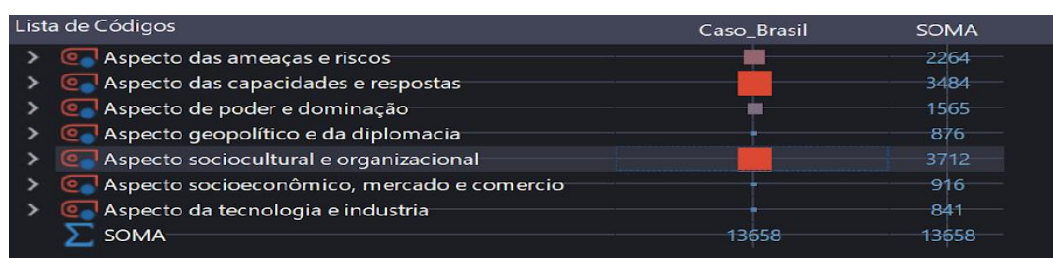
- São 33 os documentos que contém os códigos que representam à categoria temática: Aspecto sociocultural e organizacional, o código mais influente é: Participação dos atores públicos, privados e sociedade, se encontrando em 977 segmentos codificados, representando um 26.3% dos códigos dessa categoria. Podemos observar que o código menos influente é: Identificação de pessoas no digital, com 6 segmentos codificados, representando um 0.2%.

- São 22 os documentos que contém os códigos que representam à categoria temática: Aspecto socioeconômico, mercado e comercio. O código de maior influência é Economia e financeiro, se encontrando em 607 segmentos codificados, representando um 66.3% dos códigos dessa categoria. Podemos observar que o código menos influente é: Comércio, com 124 segmentos codificados, representando um 13.5%.

- São 24 os documentos que contém os códigos que representam à categoria temática: Aspecto da tecnologia e indústria, o código mais influente é: Elementos estruturais na criação do ciberespaço se encontrando em 720 segmentos codificados, representando um 85.6% dos códigos dessa categoria. Podemos observar que o código menos influente é: Universo conectado e seguro, com 5 segmentos codificados, representando um 0.6%.

Dessa forma, temos evidenciado que a categoria: **Aspecto sociocultural e organizacional**, com 3,712 segmentos codificados é a temática de maior relevância para os fins das políticas e estratégias no âmbito da segurança cibernética no Brasil, seguida da categoria Aspecto das capacidades e respostas, com 3,484 segmentos codificados.

Figura 65 - Visualizador da matriz de códigos caso brasileiro

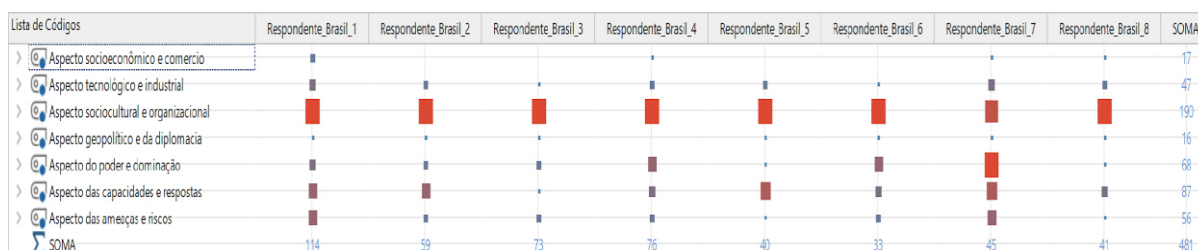


Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

Esse análise trazido aos questionários, em forma geral, diferem sutilmente dos resultados, como pode ser observado na Figura 66, as categorias: “Aspecto sociocultural e organizacional” e “Aspecto das capacidades e respostas” se mantem, porém nas outras categorias diferem em relevância.

Torna evidente que a categoria: “Aspecto geopolítico e da diplomacia” tem sido de menor relevância nas respostas e preocupações dos especialistas brasileiros, que participaram nos questionários. Além disso, o código “Acordos da diplomacia e relações exteriores” que é parte dessa categoria, somente foi do interesse nas respostas do Respondente_Brasil_1 e do Respondente_Brasil_7.

Figura 66 - Matriz de códigos dos respondentes, caso brasileiro



Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

Observou-se também, que para a metade dos especialistas, a categoria: “Aspecto socioeconômico e comercio” não foi parte das respostas e preocupações desses Respondentes. E o código “Comércio” que é parte dessa categoria, somente foi do interesse nas respostas do Respondente_Brasil_1 e do Respondente_Brasil_4.

7.3.1 Aspecto das ameaças e riscos, segundo os especialistas brasileiros

Neste aspecto busca-se identificar as prioridades, partes interessadas e elementos que constituem as estratégias de segurança e defesa cibernética, na perspectiva das ameaças e riscos cibernéticos. Nesse sentido, foram desenvolvidas três perguntas abertas, deixando as seguintes evidências:

a. Entre as prioridades da segurança e defesa cibernética nacional brasileira. Foi comentado pelos especialistas diversos temas de preocupação. Entre os tópicos que

coincidem está o dispor de capacidades técnicas, desde “a conscientização em segurança cibernética visando a proteção das infraestruturas críticas (Respondente_Brasil_7), assim como, o fortalecimento da resiliência e do marco regulatório e legal no âmbito cibernético.

Desenvolver um time multidisciplinar, com estatura de Ministério, para congregar todas as ações referentes a defesa cibernética no âmbito tanto do governo federal quanto da sociedade civil, principalmente das indústrias consideradas infraestrutura crítica do país. Além de definir padrões, regulamentações e legislação competente para o tema, deverá também implementar infraestrutura para coordenação nacional contra grandes campanhas realizadas pelos adversários do crime cibernético, principalmente compartilhando e divulgando inteligência cibernética. (Respondente_Brasil_4).

Outra prioridade estaria relacionada com o investimento em soluções integradas de segurança.

O investimento em proteção segura, especialmente a partir da atuação de equipes multidisciplinares. A meu ver, o ideal seria que as organizações investissem em soluções integradas visando permitir a visualização rápida da linha de atuação na atividade respectiva, com potencialização da capacidade de automação de procedimentos de resposta e, de preferência, com a implementação de rotinas cíclicas de revisão de métodos e processos de segurança para que se possa saber se são adequados e atuais (Respondente_Brasil_3).

Para dois dos especialistas, uma das prioridades deveria estar centrada em melhorar o nível de governança da segurança cibernética, onde seja segregado eficientemente as limitações e responsabilidades da proteção cibernética (Respondente_Brasil_5), o que estaria gerando uma duplicidade de agendas no setor público e ineficácia na comunicação e reação para o tratamentos dos incidentes cibernéticos.

No Brasil há tratamento segregado entre segurança e defesa cibernéticas. As atribuições são divididas entre as Forças Armadas (Defesa Cibernética) e a segurança cibernética (órgãos civis). Com isso são criadas iniciativas paralelas que poderiam e deveriam ser complementares. Por exemplo, a proteção de infraestruturas críticas é missão da Defesa Cibernética, mas a maioria dos operadores dos setores críticos são entidades civis (muitas delas privadas). Nesse caso, há duplicidade de agendas do setor público, o que gera ineficiência em processos de comunicação e tratamento de incidentes. Minha opinião, é de que deve haver uma definição prévia e unificada das atribuições e missões da defesa e segurança cibernéticas. Esse elemento normativo descreveria as hipóteses em que órgãos de segurança cibernética atuariam e a partir de qual momento a situação fática seria de competência da defesa cibernética. Por exemplo: um ataque de *ransomware* contra setor elétrico - a primeira resposta seria de órgãos de segurança cibernética (foi uma atividade criminosa? atores são nacionais ou estrangeiros?). Se a ação provocar a interrupção do serviço essencial seria o caso de as forças de defesa cibernética engajarem. Assumindo que essa distribuição de

competências esteja clara, os papéis de tratamento e respostas a incidentes devem ser as prioridades para as ações de segurança e defesa cibernética (Respondente_Brasil_1).

b. Sobre os atores envolvidos na segurança e defesa cibernética e se correspondem adequadamente na governança dos riscos cibernéticos. Foi comentado pelos especialistas que os esforços na governança dos riscos cibernéticos, possuem um nível aceitável de maturidade, porém, o engajamento dos atores dos outros setores, incluindo ao empresarial privado, estariam sendo uma limitante. Segundo o Respondente_Brasil_3, “com a vigência da LGPD, o tema ganhou enormes proporções, passando a demandar esse segmento profissional (segurança da informação) como nunca se viu”.

Desde a perspectiva geral dos especialistas, a nível da defesa cibernética se tem uma boa compreensão e coordenação de seus atores, em comparação com a segurança cibernética.

Há uma confusão de responsabilidades entre os atores envolvidos em segurança e defesa cibernética, pois essas esferas são coisas distintas. No Brasil vejo que há muito envolvimento militar em segurança cibernética, deveria ser menos, eles deveriam manter o foco em defesa cibernética (Respondente_Brasil_5).

Segundo o dito por três especialistas, se precisa de um fórum, um grupo de especialistas ou uma Agência nacional que permita trazer uma visão holística da governança em segurança cibernética.

Pela natureza complexa da dimensão cibernética é natural que muitos atores estejam envolvidos na defesa e segurança. Acredito que mais atores da iniciativa privada poderiam ser incluídos em rotinas de segurança e defesa cibernética. Não existe um fórum para compartilhamento de informações sobre ameaças cibernéticas organizado pelo Ctir.gov, ComDCiber ou Cert.br. Em geral, os próprios setores econômicos se articulam, mas sem a participação ativa das entidades responsáveis pela segurança e defesa cibernética (Respondente_Brasil_1).

Quanto ao GSI, percebemos que ele foi enfraquecido com o tempo, hoje ele se tornou um órgão muito mais normativo do que executivo, percebemos a necessidade da criação de uma agência Nacional de Segurança da Informação, com a função de coordenar toda a proteção cibernética do país, nos mesmos moldes que temos como a CISA nos EUA, a CNCS de Portugal, o Centro Nacional de Segurança Cibernética (NCSC) do Reino Unido entre outros. Quanto ao ComDCiber e a Defesa Cibernética as atribuições já estão bem definidas, como pode ser percebido na Portaria de criação do SMDC. Observa-se que hoje existe um hiato entre a Segurança Cibernética a cargo do GSI, a quem compete a árdua missão de coordenar a proteção cibernética das Infraestruturas críticas e a Defesa Cibernética, que hoje possui todos os seus atores bem definidos (Respondente_Brasil_7).

É necessário pensar em uma visão holística da segurança cibernética, em termos de governança. Portanto, os atores envolvidos na elaboração de políticas preventivas e de resposta e mitigação devem considerar a variedade de setores da sociedade para além das entidades da administração pública, ou seja, os agentes econômicos privados, a comunidade acadêmica, a sociedade civil e as entidades multissetoriais de interesse especial, como o Comitê Gestor da Internet (CGI.br). Esse modelo, além de prever um nível de representatividade na elaboração de políticas e ações de resposta, buscar endereçar os diversos interesses e perspectivas sociais e econômicas componentes da sociedade, como construído, originalmente, âmbito da Cúpula Mundial da Sociedade da Informação e desenvolvido em fóruns e espaços internacionais e multissetoriais de Governança da Internet (Respondente_Brasil_8).

c. Sobre as principais ameaças externas e internas que podem originar uma crise nacional. Segundo as respostas dos especialistas brasileiros, evidencia-se que possuem certa uniformidade na compreensão das ameaças que poderiam deixar exposto ao país em uma crise nacional. Foram justificadas nas respostas dos especialistas a indisponibilidade dos serviços, as ações do cibercrime organizado e os ataques que puderam afetar às infraestruturas críticas e setor financeiro.

Um ataque coordenado ao setor financeiro, apesar de mais difícil, seria uma grande ameaça. A outra seria que atores criminosos fossem bem-sucedidos em ataques às infraestruturas operativas, como usinas, plantas de energia ou antenas de telecomunicações, causando disruptiva em alguma infraestrutura crítica que fosse além da paralização de sistemas corporativos (Respondente_Brasil_4).

Hoje temos diversos fatores que podem gerar uma crise nacional, atores internos, como por exemplo, criminosos individuais ou grandes organizações criminosas, que já perceberam que o crime cibernético pode gerar muito dinheiro. Internamente, temos também alguns movimentos Hacktivistas que podem causar graves problemas cibernéticos e alguns movimentos políticos que podem utilizar as mesmas ferramentas. Em relação às ameaças externas, temos as APT¹⁶⁶ que sempre procuram buscar fragilidades a serem exploradas com diversas finalidades, algumas com intuito de obter vantagens financeiras, outras para obter superioridades em caso de um conflito, outras procurando desestabilizar ou desacreditar o País perante a opinião pública. Todos esses ataques possuem um objetivo claro e caso atinja uma infraestrutura crítica pode causar sérios danos ao país, como podemos observar no ataque a Colonial Pipeline ocorrido nos EUA (Respondente_Brasil_7).

Segundo o Respondente_Brasil_2, tem que ser uma preocupação os países da China, no tocante com a Inteligência Artificial e os Estados Unidos, pelo domínio que tem no espaço cibernético. Também foi sugerido pelo Entrevistado_Brasil_2, que “deveria ser atacada a falta de cultura popular em relação à segurança digital no Brasil”, devendo ser impulsado desde o nível primário da educação, evitando assim

¹⁶⁶ *Advanced Persistent Threat.*

vulnerabilidades que possam ser exploradas pelas ameaças. Para o Respondente_Brasil_5 e o Entrevistado_Brasil_2, as ameaças da desinformação (citado como *Fake News*) com fins políticos e ideológicos deveriam também estar dentro das preocupações que poderiam gerar uma crise nacional ou desprestígio do país na comunidade internacional.

7.3.2 Aspecto das capacidades e resposta, segundo os especialistas brasileiros

Neste aspecto busca-se identificar as ações de proteção, partes interessadas e desafios nas estratégias de segurança e defesa cibernética, sob a perspectiva de capacidades e resposta. Nesse sentido, foram desenvolvidas três perguntas abertas, deixando as seguintes evidências:

a. Para uma proteção adequada do espaço cibernético nacional, que estratégias e ações no nível político-estratégico estão sendo promovidas. Foi evidenciado que para os especialistas brasileiros existe a necessidade de ter uma estratégia para o compartilhamento de informações promovida pelo mais alto nível, estando nas propostas dos especialistas a criação um grupo de especialistas ou uma agência nacional que permita trazer uma visão holística da governança em segurança cibernética.

Acredito que a primeira ação político-estratégica seria a clara distribuição de competências entre as entidades públicas e privadas. A criação de fóruns para compartilhamento de informações e planejamento de contramedidas é outra iniciativa que poderia ser promovida a partir do mais alto nível (Respondente_Brasil_1).

Há uma série de ações. As mais estratégicas passam pela criação de um órgão que centralize o tema, com especialistas de toda a sociedade e que possa propor regulamentação e legislação sobre o assunto, além de coordenar ações de defesa, treinamento, simulações e exercícios (Respondente_Brasil_4).

Outras das ações estratégicas propostas pelos especialistas estão relacionadas ao desenvolvimento da indústria tecnológica nacional e sua priorização nos investimentos.

Acho que seremos realmente fortes na defesa e segurança cibernética nacional quando academia, indústria e defesa se unirem realmente, proporcionando desenvolvimento tecnológico nacional. Uma indústria que promova o desenvolvimento tecnológico e alavanque o setor cibernético é fundamental no fortalecimento da defesa cibernética nacional. Não há muito sentido falarmos em defesa cibernética forte quando importamos os principais ativos de rede (Respondente_Brasil_2).

Segundo o Respondente_Brasil_7 se deve dar maior “protagonismo ao GSI, ao poder judiciário e do legislativo”. Se tendo evidenciado que nos últimos anos a privacidade e proteção dos dados pessoais tem adquirido um protagonismo relevante desde a vigência da LGPD e ANPD.

Marco legal imediato sobre uso de dados pessoais no contexto do estado, da segurança pública e dos sistemas de justiça. Independência da Autoridade Nacional de Proteção de Dados. Treinamento em segurança da informação (Respondente_Brasil_6).

Segundo o Entrevistado_Brasil_1, desde sua experiência no combate ao crime cibernético, observa-se a falta de capacitação na América Latina. Porém, desde uma visão nacional tem-se percebido que a segurança cibernética ainda parte desde as forças armadas, não percebendo que seja também nas instituições públicas.

b. Onde estariam os maiores desafios e capacidades cibernéticas no Brasil.

Segundo o comentado pelos especialistas, no âmbito público seria a qualificação do recurso humano e a permanência do talento humano nas entidades públicas, devido a que existe um considerável número desses talentos que optam por iniciativas privados ou estrangeiras.

O principal desafio reside na preparação de mão-de-obra qualificada para atuar operacionalmente na defesa e segurança cibernéticas. A formação de pessoas requer tempo e investimento, algo pouco disponível atualmente. Além disso, servidores públicos civis e militares não são escolhidos - em regra - por suas aptidões técnicas para atuar na área cibernética, o que reduz o número de pessoas na administração pública aptas a atuar e receber formação técnica no tema. Por fim, a retenção de servidores qualificados é um problema adicional. Dentre as pessoas qualificadas há considerável número que deixa funções públicas para atuar na iniciativa privada nacional ou estrangeira (Respondente_Brasil_1).

Para outro grupo de especialistas, um dos maiores desafios estaria em “ter autonomia na produção de hardware e em construir uma mão de obra cada vez mais qualificada para o setor” (Respondente_Brasil_1) e a proteção das infraestruturas críticas. Porém, para o Entrevistado_Brasil_2, um desafio na legislação é em equilibrar entre o ótimo e o urgente, em especial quando se trata de regulamentar e legislar quando abraça diversos interesses desde políticos até empresariais.

Segundo o Respondente_Brasil_8, os maiores desafios estariam no aspecto socioeconômico e a brecha digital, porém se tem destaque a potencialidade do Brasil em modelos de governança plurais do tipo de CGI.br.

Um dos maiores desafios é orçamentário. Em detrimento de outras estratégias nacionais de investimento em desenvolvimento tecnológico, o país investe pouco em capacidades domésticas, principalmente em termos de defesa e segurança. Outro desafio é de caráter socioeconômico. A brecha digital no Brasil tem como consequência direta um nível de literacia além do desejado, gerando a vulnerabilidade dos usuários, algo que se torna ainda mais grave caso esses operem sistemas estratégicos/críticos à administração pública ou de entidades privadas. Por outro lado, uma potencialidade no Brasil é o pioneirismo em modelos de governança plurais - com destaque para o CGI.br - que fortalecem uma visão holística do campo tecnológico, incluído o de segurança. Os centros de resposta a incidentes de segurança no Brasil (CSIRTs) têm, por exemplo, atuando em constante diálogo, estreitando relações interinstitucionais (Respondente_Brasil_8).

Segundo o Entrevistado_Brasil_1 o maior desafio estaria relacionado com a falta de importância na segurança da informação, mas com a vigência da LGPD, se deram maiores discussões na segurança trazendo a responsabilidade das instituições pelas falhas na segurança. Outro aspecto que é percebido pelo experto, é que não existe uma comunicação ágil de uma rede de especialistas em relação aos incidentes da segurança. Como efeito, existe uma ausência na articulação e prevenção na resposta dos incidentes cibernéticos como também de uma adequada capacitação em segurança da informação, sendo os maiores desafios.

Segundo o Entrevistado_Brasil_2, um desafio é em construir uma visão de Estado-Nação, a onde se quer chegar em um meio e longo prazo, em segurança e defesa cibernética. Que seja independente da sucessão dos governos. Sendo comentado também, que ainda está se buscando em superar o estabelecimento das relações de confiança entre os atores privados e governamentais. Outro desafio comentado pelo experto é a sustentação da capacidade operacional do recurso humano, para mitigar o nível de dependência nas ferramentas tecnológicas estrangeiras que foram adquiridas para os fins da defesa cibernética.

c. Que deve ser alcançado com tecnologias como a Internet e outras envolvidas no ciberespaço. Segundo o comentado pelo especialistas, o que deveria ser alcançado é garantir o total acesso e conectividade ao serviço de Internet, com uma cultura em segurança e proteção dos dados inerentes a esses serviços.

A conectividade tem a capacidade de alavancar negócios e difundir conhecimentos em escala sem precedentes. Acredito que os países em desenvolvimento deverão promover medidas para conectar o maior número de cidadãos e disponibilizar o maior volume de serviço online possível (Respondente_Brasil_1).

Outro aspecto está relacionado com a “autossuficiência humana e tecnológica” (Respondente_Brasil_2). E outros mais otimistas comentam em alcançar uma “autonomia digital, velocidade nos processos burocráticos, maior privacidade dos dados de seus cidadãos, maior desenvolvimento tecnológico de seus meios de produção” (Respondente_Brasil_5).

Segundo o Entrevistado_Brasil_1, a criminalidade no mundo físico tem se fortalecido e migrado cada vez mais ao virtual ou cibernético. Em termos do momento brasileiro, desde a perspectiva de quem está no enfrentamento depois que o problema ocorreu, o experto comentou que:

Não é uma prioridade ainda na agenda de percepção penal ou de atenção das próprias polícias em tratar a segurança cibernética com a importância em que ela deve tomar. Eu olho dois aspectos: um aspecto que é a questão da faixa etária das pessoas que estão hoje vivenciando os problemas, como atores do sistema de justiça que muitas vezes não tem nenhuma habilidade ou facilidade para manejar temas que envolvam crimes cibernéticos, incidentes, segurança cibernética ou inteligência artificial, enfim preferem se afastar. Temos hoje uma geração jovem que está chegando no sistema de justiça e nas polícias, que já tem uma afinidade (Entrevistado_Brasil_1).

Segundo o Entrevistado_Brasil_2, os usos da Internet como as tecnologias envolvidas no desenvolvimento das sociedades estão já afirmados. Porém, o que deve ser alcançado é como manter esses usos funcionando, buscando manter o que foi conseguido, tendo um suporte de base sólida para evoluir em novos desafios. Outro aspecto a ser incentivado pelo experto, é construir uma governança maior na parte das comunicação e da informação, porque se tem décadas com a Internet e a maioria dos “servidores root” estão disseminados na América do Norte, outros na Europa e a Ásia. Na atualidade, se conhece que somente existem espelhos na América do Sul, então deve-se buscar uma soberania e uma autonomia dessas tecnologias.

7.3.3 Aspecto do poder e dominação, segundo os especialistas brasileiros

Neste aspecto busca-se analisar os elementos que constituem uma política de segurança cibernética, na perspectiva do poder e da dominação. Nesse sentido foram desenvolvidas duas perguntas abertas, deixando as seguintes evidências:

a. Em relação às estratégias nacionais no campo cibernético dos países desenvolvidos, se têm impulsionado a expansão e a dominação por meio das tecnologias de informação e da comunicação. Não existe uma negação dos especialistas brasileiros da provável expansão e dominação dos países desenvolvidos por meio das TIC. Porém é reconhecida a vantagem que pode se ter frente aos outros

países, o dispor de padrões tecnológicos, investimento em ciência e tecnologia, como também no fomento da indústria tecnológica local.

Alguns países que já eram dominantes tendem a aumentarem ainda mais seu domínio, por outro lado aqueles que ficaram à margem do processo de desenvolvimento tecnológico tendem a permanecer nessa situação. Isso é influenciado por diversos fatores a começar pelo desenvolvimento e investimento em educação passando por investimento em ciência e tecnologia até a fomentação da indústria (Respondente_Brasil_2).

Outro aspecto relacionado com o tema consultado, é que os países desenvolvidos vêm elaborando documentos estratégicos, legislações e regulações internacionais como um meio de exercício de influência e poder internacional, como por exemplo o RGPD¹⁶⁷, que claramente tem influenciado na elaboração da LGPD.

Os países ditos desenvolvidos estão começando a criar legislação e corpos técnicos federais para tratar o tema da segurança cibernética de forma coordenada. Claramente a GDPR europeia inspirou a criação da LGPD no Brasil, o que mostra que há uma influência direta também na questão da regulamentação sobre o tema aqui no Brasil (Respondente_Brasil_4).

Os países centrais em termos de poder cibernético (CHINA, EUA, ISRAEL, RUSSIA) estão através de seus documentos estratégicos nacionais nessa área criando uma arcabouço internacional que pode virá um padrão de comportamento institucional. Isso é um meio de exercício do poder (Respondente_Brasil_5).

Dois dos especialistas tem comentado que o campo cibernético não tem que ser deixado de lado, e que na competição econômica global dispor de produtos que alcançam altos níveis de padrões de segurança e confiabilidade tem uma vantagem comercial garantida.

Á priorização de estratégias internacionais no campo cibernético, incluindo os campos de segurança, impulsiona a economia doméstica de outros países. Consequentemente, os produtos para exportação ganham melhores níveis de segurança para os padrões internacionais e terminam por ser adotados por países em desenvolvimento. Isso configura uma geopolítica que pode ser considerada de "expansão e dominação" sobre países em desenvolvimento. A nível de competição econômica global, países com padrões de segurança e confiabilidade maiores têm vantagem comercial. Isso repercute sobre os níveis de segurança dos países em desenvolvimento, que se veem mais dependentes de infraestruturas de países desenvolvidos, repetindo o ciclo de "expansão e dominação" (Respondente_Brasil_8).

¹⁶⁷ Regulamento Geral sobre a Proteção de Dados. Disponível em <<https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679>>. Acesso em 10 nov. 2021.

Segundo o Entrevistado_Brasil_1, “não se teve ainda um grande avanço em termos de disseminação dessa agenda, de que é urgente nós pensarmos dos incidentes que podem inclusive inviabilizar infraestruturas críticas”. Outro aspecto em ser ressaltado pelo experto, foi o exercício do Guardião Cibernético 3.0 com o Exército Brasileiro, em que pela primeira vez foram convidados a compartilhar essa agenda, além do segredo de Estado e que está sendo positivo nas contribuições dos atores.

Eu acho, que a segurança cibernética em nosso país, si ela começar a ser realmente uma agenda que seja trazida a debate para outros setores de uma maneira mais enfática pelo GSI e não tratado como uma política de segurança nacional, no sentido de um segredo ou de algo se está fazendo com a inteligência. Nós temos que tentar de abrir, eu acho que o exército começou a fazer com esse convite que ele abriu para as instituições e nós conseguimos ampliar o nosso conhecimento. Lógico que não querendo abrir as nossas defesas, mas pelo contrário encontrando um caminho para tratar compartilhar essa agenda para atrair mais atores nesse processo (Entrevistado_Brasil_1).

b. Se regulam e punem as ações no âmbito cibernético, que possam afetar os interesses nacionais. Se tem casos dessas punições ou sanções desde o ponto de vista da segurança e defesa nacional. Para os especialistas brasileiros não se tem casos que se tinham reportado sanções específicas no âmbito cibernético ou de conseguir elencar um caso em que haja existido uma responsabilização (Entrevistado_Brasil_1), porém, apesar de ter inúmeras iniciativas legais e regulamentares no âmbito digital é evidenciado que os procedimentos punitivos e de controle têm pouca maturidade.

Acredito que exista legislação no Brasil para regular ações que afetem interesses nacionais (Marco Civil da Internet, LGPD, Lei Carolina Dieckman - Crimes cibernéticos que foi modificada recentemente). Porém, a aplicação delas depende de pessoal qualificado na atividade de investigação (polícias), persecução criminal (ministério público) e julgamento dos casos (judiciário). Infelizmente não acredito que exista número suficiente de pessoas qualificadas nesse sentido, o que torna as previsões normativas inofensivas em muitas situações (Respondente_Brasil_1).

A Lei que foi mais citada pelos especialistas está relacionada com a proteção dos dados (LGPD), que prevê mecanismo de sanções aos agentes do tratamento dos dados pessoais no Brasil.

Não. As estratégias nacionais de segurança, no campo cibernético, propriamente ditas não são acompanhadas de dispositivos que sancionem agentes econômicos quanto a incidentes de segurança. A Lei Geral de Proteção de Dados, por outro lado, prevê mecanismos de sanção a agentes de tratamento de dados pessoais que deem razão a incidentes de segurança. O histórico de sanções, no entanto, encontra-se em estágio de

amadurecimento, portanto, não seria possível dizer que há sanções suficientes (Respondente_Brasil_8).

7.3.4 Aspecto geopolítico e diplomático, segundo os especialistas brasileiros

Neste aspecto busca-se analisar a geopolítica no campo cibernético e suas repercussões na consolidação das políticas e estratégias de segurança cibernética. Nesse sentido foram desenvolvidas duas perguntas abertas, deixando as seguintes evidências:

a. A Política Nacional de Segurança Cibernética (ou iniciativas semelhantes) tem atuado com ingerência na esfera diplomática nacional. Se tem casos que transcenderam a esfera diplomática. Seis dos especialistas comentaram desconhecer ou não saber responder ao assunto questionado. Porém, para o Respondente_Brasil_1, a atuação da diplomacia com a Estratégia Nacional em Segurança Cibernética tem sido tratada em forma superficial.

Não acredito que o Brasil consiga atuar na esfera diplomática em harmonia com a Estratégia Nacional de Segurança Cibernética. Os canais de comunicação entre o Ministério de Relações Exteriores e entidades de segurança e defesa cibernética são ainda pouco utilizados e de forma muito superficial (Respondente_Brasil_1).

Segundo o Respondente_Brasil_7, si se tem atuações diversas desde a perspectiva do crime cibernético, no combate à pedofilia internacional.

Sim, o GSI possui acordo de cooperação cibernéticas com diversos países, o CIRT.gov atualmente possui diversas conexões com diversos países, observamos a atuação do MRE da mesma forma. Podemos observar isso em alguns casos de atuação da Polícia Federal no caso do combate a Pedofilia Internacional (Respondente_Brasil_7).

Segundo o Entrevistado_Brasil_1 um caso a citar seria a CPI que investigou as denúncias de espionagem pelos Estados Unidos a e-mails, telefonemas e dados digitais das autoridades políticas no Brasil. Então para o experto “a política influencia na diplomacia, porque a diplomacia é uma passo essencial para dar um parecer na adesão do Brasil nas convenções internacionais” (Entrevistado_Brasil_1).

Segundo o Entrevistado_Brasil_2, a política si tem incentivado ingerência na esfera diplomática, um exemplo disso são os exercícios realizados em conjunto com outras organizações internacionais, como é a OTAN, deixando em evidência o nível de maturidade construído no Brasil, no âmbito da defesa cibernética.

b. A Instituição responsável da geoestratégia nacional, assim como, os estudos de perspectiva geopolítica e socioeconômica no domínio ciberespacial. Segundo as respostas dos especialistas não se tem uma definição clara de qual é a Entidade responsável da coordenação da geoestratégia nacional. A maioria deles atribuem essa responsabilidade ao setor da defesa, por meio das Forças Armadas, porém, outro grupo dos especialistas consideram que deve ser tratado pelo GSI. Segundo o comentado pelo Entrevistado_Brasil_2, o GSI teria uma atuação com um perfil político e o setor da Defesa na parte estratégica. Também se tem sugestões dos especialistas, da necessidade de conformar uma entidade com um papel institucional atribuído, com recursos próprios e suficiente representatividade em todos os setores do Estado brasileiro.

Parece não haver uma definição específica, apesar de um protagonismo das forças armadas. Isso não parece adequado, pois concentra em um único ponto de vista, quando na verdade seria necessário maior acompanhamento de outros setores da sociedade, inclusive, para garantia dos direitos dos próprios cidadãos do país (Respondente_Brasil_6).

Apesar do Gabinete de Segurança Institucional, em associação com as Forças Armadas, terem desempenhado o papel principal nesse campo, um corpo multissetorial, a exemplo de um Conselho Nacional de Segurança Cibernética, composto por diferentes representações da sociedade, seria de fundamental importância para a constituição de uma entidade suficientemente representativa das necessidades práticas no campo da defesa cibernética (Respondente_Brasil_8).

Em consequência, não se tem comentários em relação aos estudos de perspectivas e da sua eficiência, porém, foi comentado que existe pouca produção da academia sobre a perspectiva geopolítica do campo cibernético no Brasil, falta de investimento no desenvolvimento tecnológico de sustentação dessa defesa.

Acredito que a academia tem produzido pouco sobre a perspectiva geopolítica do campo cibernético. Programas com foco em defesa e segurança cibernéticas são raros e não possuem foco no papel estratégico do espaço cibernético para o Brasil (Respondente_Brasil_1).

Não considero que os investimentos realizados tenham sido suficientes para a realização dos interesses nacionais. Se por um lado houve um aporte de recursos para a montagem da estrutura de segurança e defesa cibernética, por outro falta investimento no desenvolvimento tecnológico de sustentação dessa defesa (Respondente_Brasil_2).

7.3.5 Aspecto sociocultural e organizacional, segundo os especialistas brasileiros

Neste aspecto busca-se analisar os incentivos e benefícios da Política de Segurança Cibernética, na esfera sociocultural e organizacional. Foram desenvolvidas duas perguntas abertas, deixando as seguintes evidências:

a. A Política Nacional de Segurança Cibernética tem incentivado reformas institucionais. A metade dos especialistas tem concordado que as iniciativas em segurança digital e cibernética trazem reformas institucionais, por exemplo, mudança estrutural técnica e organizacional do Estado, assim como, criando espaços institucionais.

Concordo com a afirmação e acredito que uma plêiade de reformas estruturais, a se iniciar pela estrutura técnica e organizacional do Estado em todos os âmbitos, com destaque para a implementação da desejável governança (Respondente_Brasil_3).

Desde a posição dos especialistas que tem discordado, basicamente é porque desconhecem ou não encontram uma relação direta das reformas que seriam motivadas pela política. “Não há mecanismos que permitam acompanhar reformas institucionais do ponto de vista da sociedade civil ou participar delas de forma mais democrática” (Respondente_Brasil_6).

Eu entendo que não, eu acho que há uma falta de alinhamento entre o que se vem decidindo, se vem fazendo em termo de governança dessa matéria e efetivamente o que se está colocando em prática (Entrevistado_Brasil_1).

b. A Política Nacional de Segurança Cibernética (ou iniciativas semelhantes) tem incentivado benefícios sólidos, prosperidade e desenvolvimento da sociedade.

O Respondente_Brasil_5 tem-se reservado em sua resposta, justificando que não “é essa a função de uma política nacional que visa determinar um espaço específico”. Porém, para outros três especialistas, não se tem incentivado esses benefícios. Segundo o Respondente_Brasil_6, os beneficiados seriam “os setores estrangeiros de tecnologia de vigilância”. Para o Respondente_Brasil_8 a associação da estratégia militar na PNSC ou iniciativas semelhantes despoja a prosperidade e desenvolvimento social para uma perspectiva de Estado de defesa permanente.

De forma que a atuação estatal brasileira em segurança cibernética é historicamente associada a uma estratégia militar, não consideraria que preveja um estado de prosperidade e desenvolvimento social propriamente, mas um permanente estado de defesa militar, ou seja, mentalmente voltada para a "guerra" e à perspectiva de defesa/ofensiva em relação a outros Estados nacionais. Essa perspectiva seria diferente se diferentes setores civis da sociedade fizessem parte da atuação nacional (Respondente_Brasil_8).

Para o Entrevistado_Brasil_1 sim existem aspectos que tem contribuído em trazer benefícios, bem como os perigos da violação dos direitos.

7.3.6 Aspecto socioeconômico e de mercado, segundo os especialistas brasileiros

Neste aspecto busca-se analisar os incentivos ao consumismo e à dependência tecnológica, compreender os agentes e elementos envolvidos na política de segurança cibernética, no âmbito socioeconômico e de mercado. Nesse sentido foram desenvolvidas três perguntas abertas, deixando as seguintes evidências:

a. Se tem incentivado o consumo nacional das TIC. As ações ou iniciativas promovidas pelo governo em equilibrar a dependência tecnológica externa. Se observa para a maioria dos especialistas que o consumo tecnológico nacional, não tem sido incentivado nas iniciativas da segurança cibernética. Em consequência, se importa mais tecnologias da informação e da comunicação e os esforços para equilibrar a dependência tecnológica tem sido superficial.

A Política Nacional de Segurança Cibernética não tem incentivado o consumo nacional de tecnologias de informação e da comunicação. Não vejo qualquer reflexo prático neste sentido. Tampouco algo para equilibrar dependência tecnológica externa. A dependência tecnológica externa vem da falta de incentivos em empresas nacionais de tecnologia da informação. Em muitos países o governo compra de empresas locais, principalmente as pequenas empresas. Há um sistema de incentivo ao investimento em startups e outros mecanismos que fomentam o nascimento de empresas e o empreendedorismo. Este é o caminho. E dentro das tecnologias da informação, as do ramo da cibernética são as mais promissoras e onde deveria haver mais investimento, tanto privado quanto do governo, seja diretamente ou através de incentivos para que outros investidores fomentem o ramo (Respondente_Brasil_4).

Não se observa na PNSI este incentivo, pois ainda não temos uma indústria voltada para nacionalização do produtos de tecnologia da informação e comunicação. Ainda não consigo identificar iniciativas promovidas pelo Governo para equilibrar a dependência tecnológica externa (Respondente_Brasil_7).

Este item foi justificado pelos especialistas desde a perspectiva das propostas futuras que deveriam ser consideradas ou debatidas nas iniciativas do governo no âmbito da segurança cibernética, por exemplo: incentivos fiscais para as novas empresa (ou startups), transferência tecnológica nas compras públicas, programas de desenvolvimento tecnológico nacional para o setor cibernético, investimentos nos parques tecnológicos e projetos de segurança cibernética.

Seria muito importante criar incentivos (p.ex. fiscais) para que novas empresas (startups) pudessem criar produtos e serviços para o espaço

cibernético. A transferência de tecnologia em compras públicas (similar ao caça Gripen) não ocorre na segurança cibernética, mas seria uma forma de superar a atual distância entre o Brasil e os provedores de soluções (Respondente_Brasil_1).

As diferentes entidades da administração pública, sejam elas federais, estaduais ou municipais, carregam uma longa herança de licenciar sistemas operacionais proprietários internacionais. Esse elemento, por si somente, ilustra a falta de incentivo ao consumo de tecnologias nacionais. Investir em parques tecnológicos nacionais, a exemplo dos que existem em Minas Gerais e em Pernambuco, são medidas de longo prazo que devem ser incentivadas como forma de equilibrar a dependência de recursos internacionais (Respondente_Brasil_8).

Segundo os Entrevistados, estão se abrindo portas para várias startups brasileiras, gerando bons resultados na atenção da demanda da indústria brasileira, em especial do âmbito da defesa e de proteção cibernética. Porém, para o Entrevistado_Brasil_1 um aspecto de preocupação atual e pode se agravar, é a falta de mão de obra dos profissionais de TI, de segurança cibernética e da informação nas instituições públicas.

Outro aspecto a ser ressaltado, foi o comentário em relação a que as universidades costumam gerar informação e pesquisas que não são aplicáveis no mercado, com resultados endógenas, que não geram um lucro. Não existindo um direcionamento prático para que esses resultados sejam utilizados. “Ela trabalha para ela, ela mostra para seus pares e não vá para a sociedade” (Entrevistado_Brasil_2).

b. Na perspectiva do orçamento e investimento público em ciência e tecnologia, os programas em segurança e defesa cibernética visam criar esforços intersetoriais conjuntos. Dois dos especialistas comentaram não ter conhecimento sobre o gasto público e dos investimentos nesses programas de segurança cibernética. Segundo o Respondente_Brasil_4, existem esforços conjuntos no orçamento e investimento, porém não foi justificada a resposta com casos locais.

Sim, visam. E é justamente o principal efeito destes investimentos. Tanto intra quanto intersetoriais. A troca de experiências, tecnologias e, principalmente informação, é o caminho mais curto para a defesa cibernética. Os gastos públicos devem estar no caminho de incentivar o empreendedorismo neste setor, no desenvolvimento e compartilhamento de inteligência e na cooperação e atuação nos principais incidentes (Respondente_Brasil_4).

Porém, para os outros especialistas, o orçamento destinado não é o suficiente. Esses orçamentos e investimentos são iniciativas isoladas e poucas instituições têm procurado trabalhar em conjunto. Além disso, se tem relatado problemáticas envolvidas com: atividades de *lobby* nas entidades do Estado, por parte das empresas

multinacionais estrangeiras (Respondente_Brasil_6) e ações reativas após um problema ou incidentes de segurança cibernética ou da informação.

Não vejo essa sinergia, poderíamos otimizar isso fazendo uso racional dos recursos, uma vez que é tudo para um mesmo propósito, mas o que vemos na prática é cada um montando seu próprio centro de operações e resposta a incidentes, trabalhando de forma isoladas. Verdade seja dita, há algumas poucas instituições que procuram trabalhar em conjunto (Respondente_Brasil_2).

Não atualmente os gastos relativos à Segurança e a Defesa cibernética, por parte do governo são bastantes irrisórios, ainda vivemos sobre o manto da reação, ou seja, caso aconteça alguma coisa o investimento é realizado, por enquanto nada é feito (Respondente_Brasil_7).

c. As iniciativas em segurança cibernética têm dado impulso na economia e mercado digital nacional. Dois dos especialistas comentaram não ter conhecimento do tema. Porém, para outros três especialistas, as iniciativas em segurança cibernética não tem sido parte do impulso na economia e mercado digital nacional. No caso, do primeiro experto, comentou que não é o objetivo da PNSC (ou iniciativas semelhantes) e “o que deve ser feito são políticas públicas mais específicas” (Respondente_Brasil_5). No caso do segundo, “precisa haver mais subsídios para inovação tecnológica” (Respondente_Brasil_6).

Não acredito que a Política Nacional de Segurança Cibernética tenha impulsionado a economia nacional e o mercado digital. O estímulo a contratação simplificada de *startups* para desenvolver soluções pontuais necessárias para segurança cibernética seria uma medida salutar, pois sanaria uma demanda existente, além de fomentar mercado privado para isso. Outro ponto, poderia ser a incubação de projetos pelo setor público, hoje as contratações continuam ocorrendo por lógica de pregão de menor preço, o que dificulta a aquisição de soluções customizadas. Esse ajuste fino seria um nicho a ser ocupado por uma nova geração de empreendedores de TI (Respondente_Brasil_7).

Além do dito, existe um grupo de especialistas que tem comentado que essas iniciativas ainda têm pouco efeito prático. Ademais, no caso particular da LGPD, ela tem impulsado mais desde uma perspectiva de proteção das empresas de uma forma mandatária. Porém, para o Entrevistado_Brasil_2, a LGPD foi parte de uma iniciativa de muitos anos atrás, que recém teve relevância ao se tornar imprescindível para as relações comerciais e da área econômica com outros países, sendo sua aprovação impulsada com prontidão pela pressão externa econômica.

A Política Nacional de Segurança Cibernética ainda tem pouco efeito prático. Há muitos aspectos a serem melhorados. Começando por um debate mais

amplo, criação de um corpo executivo que tenha condições e independência de governo para discutir e regulamentar o tema (Respondente_Brasil_4).

Vemos que houve uma grande evolução em relação a proteção cibernética, depois da entrada em vigor da LGPD as empresas passaram a ter que adotar procedimentos de segurança cibernética, que antes eram somente recomendação, mas agora são mandatórios. Os ataques cibernéticos sofridos por diversas empresas também impulsionaram a economia e o mercado digital (Respondente_Brasil_7).

Porém, para o Entrevistado_Brasil_1, si se tem dado impulso ao mercado digital e que precisa ainda incentivar mais o fomento das pessoas desde muito cedo nas questões da tecnologia, assim como evitar a fuga dos talentos.

7.3.7 Aspecto tecnológico e industrial, segundo os especialistas brasileiros

Neste aspecto busca-se compreender quais atores e elementos constituem uma política de segurança cibernética, no campo tecnológico e industrial. Nesse sentido, foram desenvolvidas 3 perguntas abertas, deixando as seguintes evidências:

a. O responsável nacional por regular e estabelecer os padrões em TIC. Com exceção do Respondente_Brasil_5, os demais especialistas sim consideram que as estratégias nacionais em segurança cibernética deveriam capacitar à entidade pública para regular e estabelecer os padrões em TIC, como também, dos mecanismos de avaliação no seu cumprimento.

A participação do setor público na definição de setores é algo importante, pois cabe ao estado a definição de normas que possam ser juridicamente demandadas. No entanto, isso não deve ocorrer sem a participação ativa das empresas dos setores de TIC. São elas que tem a experiência prática na atuação cotidiana e podem avaliar com mais precisão o impacto de novos padrões de regulação (Respondente_Brasil_1).

Certamente, as estratégias devem partir do Estado, inclusive para estimular a iniciativa privada. No Brasil, iniciativas como o Decreto Federal n. 9.203/2017 e, mais recentemente, os Decretos n. 10.046 e 10.047, ambos de outubro de 2019, sinalizam a preocupação do governo federal com a governança de dados. No setor privado, a proliferação de iniciativas similares deve se coadunar com os parâmetros de normas como a LGPD (e seus fundamentos, conceitos, princípios e regras) (Respondente_Brasil_3).

Sim, considero que as políticas nacionais devem prever responsabilidades ao ente público para que sejam regulados e fiscalizados padrões, por exemplo, de segurança, a exemplo dos criptográficos, a exemplo do INTI através do ICP-Brasil. A atuação da Autoridade Nacional de Proteção de Dados também é fundamental à normalização e fiscalização de atividades de agentes públicos e privados, prevendo padrões de segurança e estipulando sanções administrativas quando necessário (Respondente_Brasil_8).

Além do comentado, foi sugerido pelo Respondente_Brasil_7, a necessidade de coordenar e discutir a elaboração dos padrões com o setor privado e academia, permitindo uma verdadeira adaptabilidade de todos os setores.

Segundo o Entrevistado_Brasil_2, seria temerário e pouco interessante o normatizar a parte tecnológica, contudo se pode influenciar, dar diretrizes ou parâmetros para construir cenários e atender às necessidades.

b. As empresas multinacionais estrangeiras estão incluídas na Política Nacional de Segurança Cibernética. Qual setor é responsável por essa articulação.

O Respondente_Brasil_7, comentou não saber dar resposta ao item questionado, porém, ele é da posição que “deva haver uma integração entre todos os setores, sendo o governo o principal articulador dessa integração”. Além disso, para o Respondente_Brasil_5, na PNSC não teria entre suas funções, o propor a articulação das empresas multinacionais estrangeiras. Segundo as respostas dos outros seis especialistas, pode-se inferir que não se tem um entendimento comum de quem seria o articulador dessas funções. É reconhecido por eles, que existem ações pontuais ao respeito, contudo não se tem atuado com papéis claros nas estratégias da segurança cibernética, eficiência, transparência e auditoria.

Não tenho conhecimento de que empresas multinacionais estrangeiras estejam inseridas na Política Nacional de Segurança Cibernética. Embora muitas empresas brasileiras apenas atuem como revendedores de tecnologias estrangeiras. Acredito que a relação entre o setor privado e pública ainda é cercada por muita desconfiança mútua. Para seu amadurecimento seria necessária a definição mais clara de expectativas e papéis (Respondente_Brasil_1).

As multinacionais são incluídas na medida em que são agentes prioritários nas respostas a incidentes de segurança e na medida em que são responsáveis pelo tratamento de dados de titulares de dados brasileiros. Entidades como a ANPD são diretamente responsáveis pela interlocução com multinacionais nas ações de articulação interinstitucionais que tenham por objetivo a segurança cibernética (Respondente_Brasil_8).

Para o Entrevistado_Brasil_2, não visualiza que possa existir uma exclusividade de que alguma Entidade brasileira possa centralizar essa articulação com as multinacionais.

c. Se tem incentivado a competição de fornecedores de acesso à Internet (ISP). O governo tem capacidade em regular em forma eficiente e permanente aos ISP. Nas respostas dos especialistas o acesso à Internet é uma preocupação de Estado. Evidencia-se também, que existem preocupações e desafios para serem atendidas a nível de qualidade e

preços praticados nos serviços brindados pelos ISP. Porém, foi identificado nas respostas a posição clara da entidade reguladora da ANATEL, como também, do MCTIC nos quesitos quanto aos provedores de conexão e de aplicação (ISPs).

O acesso à internet tem sido objeto de consideração, sobretudo em áreas remotas onde projetos públicos têm criado redes para conexão (Exército levando cabos de fibra por meio dos rios amazônicos). Não estou certo de que a competição entre provedores de acesso à internet esteja sendo realizada de forma ativa. Seria algo importante, pois a qualidade de serviço e preços praticados dependem desse tipo de medida. Acredito que agências reguladoras (ANATEL) tem condições de regular o mercado, mesmo de ISPs de capital estrangeiro (Respondente_Brasil_1).

No país, o tema foi abordado no art. 26 do Marco Civil da Internet, mas verdadeira mudança de paradigma surge no horizonte como uma perspectiva de médio a longo prazo. Quanto aos provedores de conexão e de aplicação (ISPs), o próprio Marco Civil da Internet tem se mostrado uma norma sólida, mesmo quanto àqueles que dependem de aportes de capital estrangeiro (Respondente_Brasil_3).

Segundo o Respondente_Brasil_8, o congresso tem uma árdua tarefa, desde a perspectiva de impulsar leis e normas que permitam impulsar maior acesso à Internet, competitividade de pequenos provedores locais e diversificação de provedores de Internet. Entretanto, o Respondente_Brasil_5 sugere que tem que se dar os cuidados necessários, para evitar uma regulação muito controlada pelo Estado.

Acredito que há muito o que se melhorar em termos de noções introdutórias em defesa cibernética nas agendas de inclusão digital e vice-versa, ou seja, as estratégias de defesa cibernética devem estreitar laços com outros atores governamentais responsáveis pela expansão da conectividade, como a ANATEL e o MCTIC (Respondente_Brasil_8).

Como política de promoção de desenvolvimento o Estado atua nessa área, mas como questão de defesa e segurança cibernética temos que ter cuidado quando o Estado tenta regular de forma muito controlada esses aspecto de acesso (Respondente_Brasil_5).

7.3.8 Relatório do estudo de caso brasileiro

No estudo de caso brasileiro, foi analisado um único corpus documental, devido à limitada existência de publicações oficiais em segurança e defesa cibernética. Desde a sua origem na DSN, tem-se evidenciado que o Conselho de Defesa Nacional (CDN) é constituído, sendo presidido pelo Presidente da República. As competências na segurança e defesa nacional no âmbito cibernético são descentralizadas e tratadas por diversos organismos públicos. Observa-se que existe uma segregação entre as ações de segurança da informação e da defesa cibernética, sendo os principais atores

o Gabinete da Segurança Institucional da Presidência da República (GSI) e o Exército Brasileiro, respectivamente. Ressalta-se que, no Exército Brasileiro, desde o ano 2009, foi oficializada pelo Ministério da Defesa a atribuição de força líder na condução do setor cibernético nacional, o que levou nos anos seguintes à criação do Centro de Defesa Cibernética (CDCiber).

No estudo de caso brasileiro, foram observadas as relações diretas e indiretas existentes entre os códigos do corpus estudado. A categoria **Aspecto sociocultural e organizacional (39,5%)** apresenta a maior relevância no corpus brasileiro, destacando-se a busca pela participação e unificação dos esforços em segurança e defesa cibernética pelos atores públicos, privados e a sociedade brasileira em geral. Além disso, o investimento em medidas ou iniciativas em prol da segurança é uma forma de instrumentalizar as ações políticas e estratégicas nos níveis de governo, possibilitando a articulação multissetorial do aparato estatal nos esforços para atingir os objetivos estratégicos. Porém, existe a necessidade da Administração Pública Federal contar com um modelo de governança e gestão da informação que permita a composição de um modelo de maturidade na produção do conhecimento e a tomada de decisões com mecanismos de avaliação e controle periódicos.

A seguinte peculiaridade, não menos relevante, está na categoria **Aspecto das capacidades e resposta (18,1%)**. Destaca-se que o modelo adotado no caso brasileiro consiste em dispor, desde o nível político, de uma segurança da informação e comunicações coordenadas a partir da Presidência da República, abrangendo a segurança cibernética. Além disso, a Política Cibernética de Defesa tem como objetivo orientar a defesa cibernética desde o nível estratégico, sendo que, no nível operacional e tático uma faculdade da guerra cibernética dentro das capacidades das Forças Armadas Brasileiras (FAB). Porém, as capacidades desejadas são direcionadas para atender às ameaças, riscos e problemas que são do interesse nacional, principalmente relacionados com a espionagem e os crimes cibernéticos.

Em sínteses, tem-se evidenciado que, no nível da defesa cibernética, existe uma boa compreensão e coordenação de seus atores, o que difere com a segurança cibernética. Outro ponto que foi evidenciado é a existência de certa uniformidade na compreensão das ameaças que poderiam expor o país a uma crise nacional. Os especialistas brasileiros comentaram sobre as seguintes preocupações no aspecto das ameaças e riscos:

- Melhorar a governança da segurança cibernética, se tem sinalizado pelos especialistas que está sendo gerado uma duplicidade nas agendas do setor público e uma ineficácia na comunicação e resposta no tratamento dos incidentes cibernéticos. Ressalta-se também que se precisa de um fórum, grupo de especialistas ou uma agência nacional que permita trazer uma visão holística da governança em segurança cibernética.
- Conscientização em segurança cibernética visando a proteção das infraestruturas críticas e sua resiliência. Com o intuito de engajar aos atores dos outros setores, incluindo ao empresarial privado que estariam sendo uma limitante nos objetivos.
- Incentivar o investimento de soluções integradas em segurança cibernética e da informação que atendam em especial às instituições e serviços públicos que constantemente estão sendo alvo dos ataques cibernéticos.
- Deve ser impulsado desde o nível primário da educação, evitando assim vulnerabilidades que possam ser exploradas pelas ameaças.
- As ameaças da desinformação com fins políticos e ideológicos deveriam estar dentro das preocupações que poderiam gerar uma crise nacional, bem como, no desprestígio do país na comunidade internacional.

No aspecto das capacidades e respostas, foram abordadas as seguintes questões:

- Ter uma estratégia para o compartilhamento de informações promovida pelo mais alto nível, que incentive a criação um grupo de especialistas ou uma agência nacional que permita trazer uma visão holística da governança em segurança cibernética.
- Construir uma visão de Estado-Nação de um meio e longo prazo em segurança e defesa cibernética independente da sucessão dos governos. Buscar a autossuficiência humana, soberania e autonomia dessas tecnológica. Com uma autonomia digital, velocidade nos processos burocráticos, maior privacidade dos dados de seus cidadãos, promover o desenvolvimento da indústria tecnológica nacional e sua priorização nos investimentos.
- Outorgar maior protagonismo ao GSI, poder judiciário e legislativo no âmbito cibernético. Equilibrar entre o ótimo e o urgente, em especial ao regulamentar e legislar quando abraça diversos interesses desde políticos até empresariais.
- Desenvolver capacidades de proteção nas infraestruturas críticas.
- Garantir o total acesso e conectividade ao serviço de Internet, com uma cultura em segurança e proteção dos dados inerentes a esses serviços.

No aspecto do poder e dominação, ao igual nos dois casos anteriores, os especialistas brasileiros têm consciência da provável expansão e dominação dos países desenvolvidos por meio das TIC. Assim como, não se tem casos em que foram reportadas sanções desde o ponto de vista da segurança e defesa nacional. Apesar de ter inúmeras iniciativas legais e regulamentares no âmbito digital é evidenciado que os procedimentos punitivos e de controle têm pouca maturidade. Também, foram relevantes os seguintes pontos:

- Vem sendo elaborado um conjunto de documentos estratégicos, legislações e regulações internacionais como um meio de exercício de influência e poder internacional. Um deles é a LGPD, em relação à proteção dos dados pessoais fortalecendo discussões do passado na segurança da informação e cibernética.
- Na competição econômica global, o produzir produtos com altos níveis de padrões de segurança e confiabilidade tem uma vantagem comercial garantida.

No aspecto do geopolítico e diplomático, se cita o caso de espionagem por parte dos Estados Unidos às autoridades políticas no Brasil. Além disso, não está claro qual é a entidade responsável da coordenação da geoestratégia nacional, no âmbito ciberespacial. Para os especialistas, o GSI teria uma atuação com um perfil político e o setor da Defesa na parte estratégica. A continuação os pontos importantes nas respostas dos especialistas:

- A atuação da diplomacia com a Estratégia Nacional em Segurança Cibernética tem sido tratada em forma superficial. Porém, desde a perspectiva do crime cibernético se tem diversas ações na cooperação internacional. No âmbito da ciberdefesa, se tem incentivado exercícios cibernéticos com organizações internacionais, por exemplo, com a OTAN.
- Existe pouca produção da academia sobre a perspectiva geopolítica do campo cibernético no Brasil, falta de investimento no desenvolvimento tecnológico de sustentação da defesa cibernética.

No aspecto do sociocultural e organizacional, os especialistas brasileiros têm expressado que as iniciativas em segurança cibernética e da informação tem incentivado reformas institucionais, nesse aspecto eles tem ressaltado as seguintes preocupações:

- Não se tem mecanismos para acompanhar as reformas institucionais e de participar nelas em forma mais democrática.

- É difícil que sejam apreciados os benefícios na sociedade, porém os que mais se tem beneficiado são os setores estrangeiros da tecnologia de vigilância. Outrossim, a associação com o setor militar despoja o incentivo social para uma perspectiva de Estado de defesa permanente.

No aspecto do socioeconômico e de mercado, os pontos comentados e sugeridos são as seguintes:

- Os esforços para equilibrar a dependência tecnológica tem sido superficial. O consumo tecnológico nacional, não tem sido incentivado nas iniciativas da segurança cibernética.
- As universidades acostumam gerar informação e pesquisas que não são aplicáveis no mercado da segurança cibernética, com resultados endógenas e que não geram um lucro. Não existindo um direcionamento prático para que esses resultados sejam utilizados. Além disso, falta de mão de obra dos profissionais de TI, de segurança cibernética e da informação nas instituições públicas.
- Não se tem conhecimento sobre o gasto público e dos investimentos nesses programas de segurança cibernética. Ademais, foi ressaltado como uma preocupação as atividades de lobby nas entidades do Estado, por parte das empresas multinacionais estrangeiras.
- As iniciativas em segurança cibernética não têm impulsionado à economia e mercado digital nacional. Porém, elas tomam relevância ao se tornar imprescindível para as relações comerciais e da área econômica com outros países.

No aspecto do tecnológico e industrial, ao igual nos casos anteriores, existe a necessidade de capacitar à entidade pública responsável de estabelecer os padrões em TIC, assim como, dos mecanismos de avaliação no seu cumprimento. A diferença com o caso peruano, foi identificado pelos especialistas brasileiros na ANATEL e no MCTIC, entidades governamentais com capacidade reguladora nos provedores de conexão e de aplicação (ISPs). Entre os outros pontos comentados estão as seguintes:

- Integração entre todos os setores, sendo o governo o principal articulador dessa integração. Portanto, existe a necessidade de coordenar e discutir a elaboração dos padrões tecnológicos com o setor privado e academia.
- Não se tem atuado com papéis claros nas estratégias da segurança cibernética, eficiência, transparência e auditoria nas empresas tecnológicas estrangeiras que operam no Brasil.

Finalmente, destacam-se os reflexos qualitativos observados na identificação, análise e sistematização dos elementos e agentes envolvidos nas concepções, discussões e preocupações relativas às políticas e estratégias em segurança cibernética do estudo de caso brasileiro.

7.4 Síntese qualitativa dos reflexos observados na Argentina, Peru e Brasil

Após a análise qualitativo dos estudos de casos da Argentina, Peru e Brasil, busca-se apresentar uma síntese dos reflexos observados, visando a organização e compreensão dos elementos, agentes e perspectivas revelados durante a análise quantitativa, bem como expor uma visualização primária das migalhas ou indícios, que inicialmente não foram óbvios nos corpus estudados. Estando evidenciadas, com a aplicação dos instrumentos da pesquisa qualitativa, como as entrevistas e questionários aos especialistas. Portanto, na seguinte Tabela é apresentado um comparativo qualitativo dos estudos de casos pesquisados:

Quadro 24 - Síntese qualitativa dos reflexos observados: Argentina, Peru e Brasil.

CATEGORIAS	QUESTÕES	ARGENTINA	PERU	BRASIL
Aspecto das ameaças e riscos	Prioridades da segurança e defesa cibernética nacional	1. As infraestruturas críticas e a disponibilidade da informação. 2. A necessidade de um aculturamento digital. 3. A busca no desenvolvimento de estratégias integrais entre os diversos atores. 4. Esforços orientados na luta do delito informático com a ação judicial frente ao crime cibernético. 5. Não se dispõem dos recursos adequados para os projetos.	1. Dispor das capacidades técnicas desde os níveis educativos básicos até a formação profissional. 2. Fortalecer o âmbito cibernético desde a perspectiva regulamentar e da legislação. 3. Programas que incentivem a confiança digital nos cidadãos. 4. Dispor de uma Política Nacional em Segurança Cibernética que defina a entidade responsável da implementação e articulação multissetorial através da CEPLAN. 5. Proteção dos ativos críticos nacionais. 6. A necessidade de ter uma liderança a nível das redes e infraestruturas de Telecom que regulem e articulem a segurança cibernética e digital nesse âmbito.	1. Conscientização em segurança cibernética visando a proteção das infraestruturas críticas e sua resiliência. 2. Incentivar o investimento de soluções integradas em segurança cibernética e da informação. 3. Melhorar a governança da segurança cibernética. Denota-se pelos especialistas, que existe uma duplicidade nas agendas do setor público e ineficácia na comunicação e resposta no tratamento dos incidentes cibernéticos.
	Atores envolvidos na segurança e defesa cibernética na governança dos riscos cibernéticos	1. Os esforços dos atores são individualistas com falta de coordenação e visão holística. 2. Os atores envolvidos na segurança são reativos. 3. Os atores do setor financeiro se destacam entre os outros, principalmente, pelos requisitos regulatórios que tem que cumprir. 4. O setor de defesa tem um pensar de riscos como oportunidade de melhoria. 5. Atores buscam inovar para a solução de seus problemas.	1. Os esforços de governança nos riscos cibernéticos possuem pouca maturidade. 2. Promoção de iniciativas legais e regulamentar, porém, não são consideradas as brechas tecnológicas existentes das instituições públicas. 3. Duplicidade de funções, sem uma clara liderança na segurança cibernética, dificultando o acionar de outras entidades ou fugindo de suas responsabilidades. 4. Problemas burocráticos e falta de alinhamento dos atores na segurança cibernética.	1. Engajamento dos atores dos outros setores, incluindo ao empresarial privado, estariam sendo uma limitante. 2. A nível da defesa cibernética se tem uma boa compreensão e coordenação de seus atores, em comparação com a segurança cibernética. 3. Se precisa de um fórum, grupo de especialistas ou uma agência nacional que permita trazer uma visão holística da governança em segurança cibernética. 4. Outorgar maior protagonismo ao GSI, ao poder judiciário e do legislativo.
	Ameaças externas e internas que podem originar uma crise nacional	1. Ameaças que geram uma afetação às infraestruturas críticas nacionais. 2. Descontinuidade dos serviços em nuvem, de onde muitas empresas dependem desses serviços. 3. As maiores preocupações estão relacionadas com as ações dos cibercriminosos. 4. A vulnerabilidade sociocultural e uma falta de coordenação entre os afetados. 5. A fuga do talento humano no setor público. 6. Inexistência de protocolos de respostas diante crises cibernéticas. 7. Operações de desinformação e influência nos grupos sociais.	1. Pouca compreensão no nível de exposição causado pelas ameaças cibernéticas. 2. Preocupações com o acionar dos cibercriminosos. 3. Operações de desinformação em redes sociais. 4. Ataques dirigidos aos ativos críticos nacionais e vazamento de informações sigilosas nas entidades públicas. 5. Sabotagem nos cabos submarinos de fibra óptica.	1. Evidencia-se que possuem certa uniformidade na compreensão das ameaças que poderiam deixar exposto ao país em uma crise nacional. 2. Impulsar a segurança cibernética desde o nível primário da educação, evitando assim vulnerabilidades que possam ser explotadas pelas ameaças. 3. As ameaças da desinformação com fins políticos e ideológicos deveriam também estar dentro das preocupações que poderiam gerar uma crise nacional, bem como no desprestígio do país na comunidade internacional.
Aspecto das capacidades e resposta	Estratégias e ações no nível político-estratégico	1. Necessidade de uma coordenação e entendimento das ameaças e os riscos cibernéticos. 2. Necessidade de programas públicos-privados a disposição dos cidadãos das ferramentas tecnológicas. 3. Melhorar o desenvolvimento industrial nacional considerando a soberania dos dados e o desenvolvimento local.	1. Necessidade de conscientizar aos líderes políticos das instituições em segurança cibernética. 2. Panorama normativo amplo, porém, sem uma clara objetividade nos resultados desejados. 3. Capacidades cibernéticas orientadas ao consumo e dependência de tecnologias. 4. Impulsar a criação de uma entidade que lidere a segurança cibernética nacional.	1. Ter uma estratégia para o compartilhamento de informações promovida pelo mais alto nível, que incentive a criação um grupo de especialistas ou uma agência nacional que permita trazer uma visão holística da governança em segurança cibernética. 2. Promover o desenvolvimento da indústria tecnológica nacional e sua priorização nos investimentos. 3. Outorgar maior protagonismo ao GSI, poder

				judiciário e legislativo no âmbito cibernético. Se tem a percepção de que a segurança cibernética ainda parte desde as forças armadas. Não se percebe que seja também nas instituições públicas.
	Desafios e capacidades cibernéticas	1. O ciclo do recurso humano no âmbito da segurança e defesa cibernética (formação, treinamento, especialização e retenção). 2. A falta de percepção do risco cibernético e do valor da informação. 3. As capacidades estariam nos CERTs, não obstante, existem muitas iniciativas que não estão sendo priorizadas.	1. Geração de capacidades na proteção cibernética. 2. Dispor de investimentos, orçamentos e pessoas qualificadas no âmbito cibernético. 3. As capacidades estariam na SEGDI e as Forças Armadas. Porém, o MINEDU não seria um ator significativo na criação das capacidades humanas cibernéticas. 4. As capacidade em segurança cibernética não é valorado desde um enfoque transversal nas políticas públicas.	1. Qualificação do recurso humano e a permanência do talento humano nas entidades públicas, devido a que existe um considerável número desses talentos que optam por iniciativas privados ou estrangeiras. Sustentação da capacidade operacional do recurso humano, de forma mitigar o nível de dependência nas ferramentas tecnológicas estrangeiras que foram adquiridas para os fins da defesa cibernética. 2. Ter autonomia na produção de hardware, bem como, em construir uma mão de obra cada vez mais qualificada para o setor. 3. Na proteção das infraestruturas críticas. 4. Na legislação, equilibrar entre o ótimo e o urgente, em especial quando se trata de regulamentar e legislar, quando abraça diversos interesses desde políticos até empresariais. 5. Construir uma visão de Estado-Nação, de onde se quer chegar em um meio e longo prazo em segurança e defesa cibernética que seja independente da sucessão dos governos.
	Tecnologias como a Internet e as envolvidas no ciberespaço	1. Educación integral digital da população, alfabetização e inclusão digital. 2. Inovação tecnológica e integração da região para reduzir a dependência tecnológica. 3. Democratizado o conhecimento através da Internet. 4. Acesso ao serviço da Internet nas províncias.	1. Garantir o total acesso ao serviço de Internet e a conscientização no uso seguro e de qualidade da Internet, bem como, em outras tecnologias do ciberespaço. 2. Garantir o impacto da Internet na economia digital. 3. Além de seu uso, não se tem dado impulso ao desenvolvimento nacional das tecnologias.	1. Garantir o total acesso e conectividade ao serviço de Internet, com uma cultura em segurança e proteção dos dados inerentes a esses serviços. 2. Buscar a autossuficiência humana, soberania e autonomia dessas tecnológica. Com autonomia digital, velocidade nos processos burocráticos, maior privacidade dos dados de seus cidadãos, maior desenvolvimento tecnológico de seus meios de produção.
Aspecto do poder e dominação	Expansão e dominação por meio das tecnologias de informação e da comunicação	1. Se tem transferido responsabilidades aos outros, como em discursos de dominação. 2. Desvalorização da capacidade de inteligência estratégica e de sua concepção. 3. Desconhecimento de exercícios de continuidade dos serviços no âmbito nacional. 4. A expansão e dominação pelas TIC é um processo inevitável se instaurando uma dependência com os países	1. Aceitação de uma expansão e dominação dos países desenvolvidos por meio das TIC. 2. São revelados dois modelos instaurados de dominação, uma da soberania dos dados e a outra no exercício dos instrumentos jurídicos e regulamentares. 3. A expansão tecnológica em infraestrutura de telecomunicações é motivada pelo custo e a compatibilidade de seus produtos.	1. Aceitação de uma expansão e dominação dos países desenvolvidos por meio das TIC. 2. Vem sendo elaborado um conjunto de documentos estratégicos, legislações e regulações internacionais como um meio de exercício de influência e poder internacional. 3. Na competição econômica global dispor de produtos que alcançam altos níveis de padrões de segurança e

		menos desenvolvidos.		confiabilidade tem uma vantagem comercial garantida.
	Punições ou sanções desde o ponto de vista da segurança e defesa nacional	1. Não se tem casos em que foram reportadas sanções específicas nesse tipo. 2. Não tem conhecimento de uma estrutura governamental destinada a sancionar ações tecnológicas, além daquelas que estejam associadas ao crime cibernético. 3. Cópia integral das boas práticas, sem ter passado por um planejamento estratégico e sua avaliação dos riscos em cibersegurança. 4. Não se tem regulações para a propaganda e a desinformação.	1. Não se tem casos em que foram reportadas sanções específicas nesse tipo. 2. Apesar de ter inúmeras iniciativas legais e regulamentares no âmbito digital é evidenciado que os procedimentos punitivos e de controle têm pouca maturidade.	1. Não se tem casos em que foram reportadas sanções específicas nesse tipo. Apesar de ter inúmeras iniciativas legais e regulamentares no âmbito digital é evidenciado que os procedimentos punitivos e de controle têm pouca maturidade. 2. Expectativa dos especialistas na LGPD. A proteção dos dados pessoais vem fortalecendo discussões do passado na segurança da informação e cibernética.
Aspecto geopolítico e diplomático	Ingerência na esfera diplomática nacional e se se tem casos que transcenderam a esfera diplomática	1. Não se tem reporte de casos nessa magnitude, porém, existem acordos de cooperação internacional no intercâmbio das informações. 2. Vazamento de dados sigilosos na Direção de Assuntos Migratórios e da Agência Federal de Inteligência.	1. Um caso comentado foi de espionagem e revelação de segredos nacionais no ano 2009, conhecido como caso Ariza. 2. As iniciativas em segurança cibernética não têm uma ingerência direta na esfera diplomática. 3. Práticas evidentes de intervencionismo das entidades e organizações internacionais no âmbito cibernético.	1. A atuação da diplomacia com a Estratégia Nacional em Segurança Cibernética tem sido tratada em forma superficial. 2. Desde a perspectiva do crime cibernético se tem diversas ações na cooperação internacional. 3. Um caso comentado foi da CPI que investigou as denúncias de espionagem por parte dos Estados Unidos às autoridades políticas do país. 4. No âmbito da ciberdefesa se tem incentivado exercícios cibernéticos com organizações internacionais, por exemplo: a OTAN.
	Instituição responsável da geoestratégia nacional	1. Não está claro qual é a entidade responsável da coordenação da geoestratégia nacional no âmbito ciberespacial. 2. Dissipado nos diferentes ministérios através dos comitês interministeriais. 3. A questão geopolítica deverá ser uma responsabilidade do governo que está no exercício do poder. 4. Porém, a busca seja atender aos objetivos nacionais uma limitante nessa atenção são as necessidades urgentes do país. 5. Um aspecto de melhoria está relacionado a dispor de um maior orçamento para os setores responsáveis.	1. Não está claro qual é a entidade responsável da coordenação da geoestratégia nacional no âmbito ciberespacial. 2. Os usuários peruanos são alheios às preocupações geopolíticas nas tecnologias como a Internet.	1. Não está claro qual é a entidade responsável da coordenação da geoestratégia nacional no âmbito ciberespacial. 2. Desde a compreensão dos especialistas, o GSI teria uma atuação com um perfil político e o setor da Defesa na parte estratégica. 3. Existe pouca produção da academia, sobre a perspectiva geopolítica do campo cibernético no Brasil. Falta de investimento no desenvolvimento tecnológico de sustentação da defesa cibernética.
Aspecto sociocultural e organizacional	A Política Nacional de Segurança Cibernética tem incentivado reformas institucionais	1. Sim consideram que as iniciativas em segurança cibernética têm trazidos necessárias reformas institucionais. 2. Existem grupos de trabalho de especialistas ou comitê assessor dos diversos ministérios que não tem uma formalidade em sua estruturação, sem recursos próprios e que respondem às motivações próprias deles. 3. Para o Estado é de alto custo	1. As iniciativas em segurança digital e cibernética trazem reformas institucionais, assim como, mudanças culturais, organizacionais e de paradigmas. 2. As entidades públicas possuem tecnologia obsoleta com uma débil maturidade de seus processos, não tendo alcançado níveis de automação. 3. Burocracia e ineficácia nas iniciativas de interesse público.	1. As iniciativas em segurança digital e cibernética trazem reformas institucionais, assim como, mudança estrutural técnica e organizacional. 2. Não se tem mecanismos para acompanhar as reformas institucionais e de participar nelas em forma mais democrática.

		sair da zona de conforto, além que o aspecto político muda muito.	As reformas e esforços de melhoria são inconclusos quando se dá uma mudança de gestão no governo. 4. Os problemas da segurança cibernética estão sempre afetados pelos problemas que tem o Estado.	
	Se tem incentivado benefícios sólidos, prosperidade e desenvolvimento da sociedade	1. Não podem apreciar esses benefícios. 2. Abordar primeiro outros problemas sociais. 3. Se atingem somente aspectos conceptuais sem tocar de fundo as responsabilidades e os benefícios que têm que ser alcançados. 4. Se tem iniciativas que buscam beneficiar aos organismos de menor dimensão que possuem recursos limitados.	1. Se acredita que as iniciativas em segurança cibernética sim trazem benefícios, incentivando a prosperidade e desenvolvimento da sociedade. 2. A confiança digital instaurada nos cidadãos geraria esses benefícios, sendo as empresas as primeiras em se beneficiar, para logo ser transmitidos, esses benefícios, aos outros setores. 3. As iniciativas de acesso à Internet nas áreas rurais não têm sido inclusivas aos benefícios desejados, sendo uma problemática a cobertura das operadoras nesses setores. 4. O setor mais beneficiado no âmbito económico é o bancário e privado. 5. No âmbito social, seriam os cidadãos peruanos de ensino médio das áreas urbanas.	1. Não se podem apreciar esses benefícios. 2. Os beneficiários seriam os setores estrangeiros de tecnologia de vigilância. 3. A associação com o setor militar despoja o incentivo social para uma perspectiva de Estado de defesa permanente.
Aspecto socioeconômico e de mercado	Consumo nacional de TIC	1. Existem esforços, porém são imaturos na prática. 2. Não se tem uma vinculação direta das ações de segurança cibernética com o incentivo nacional de TIC. 3. Mais esforço em inovação tecnológica e na proteção da propriedade intelectual. 4. Incentivar o conhecimento técnico, a inclusão digital e reduzir a brecha digital. 5. Minguar a carga tributária nos desenvolvimentos tecnológicos. 6. Necessidade de unificar os esforços em uma política de Estado integral. 7. Obsolescência tecnológica não permitindo estar na mesma competitividade das empresas estrangeiras.	1. Existem esforços, porém, são imaturos na prática pelo fato de não ter uma política e de se ter ações isoladas pelas instituições no tema. 2. Dependência tecnológica estrangeira a nível de infraestrutura e de redes de telecomunicações. 3. Não têm incentivos claros na inclusão dos usuários em tecnologias de médio porte, especialmente nos lugares mais afastados. 4. Promoção de iniciativas de isenção de impostos sobre os dispositivos tecnológicos, beneficiariam ao consumo nacional em TIC.	1. O consumo tecnológico nacional, não tem sido incentivado nas iniciativas da segurança cibernética. 2. Os esforços para equilibrar a dependência tecnológica tem sido superficial. 3. Falta de mão de obra dos profissionais de TI, de segurança cibernética e da informação nas instituições públicas. 4. As universidades costumam gerar informação e pesquisas que não são aplicáveis no mercado, com resultados endógenas e que não geram um lucro. Não existindo um direcionamento prático para que esses resultados sejam utilizados.
	Programas em segurança e defesa cibernética visam criar esforços intersetoriais	1. Existem limitações no orçamento e investimento público em ciência e tecnologia. 2. Ciência e tecnologia são consideradas gasto público. 3. Iniciativas no orçamento e investimento em ciência e tecnologia, não tem um planejamento estratégico integral. 4. Não se tem indicadores ou estratégias de otimização, não se tem um seguimento dos projetos executados. 5. Estratégia de investimento através das instituições	1. Orçamentos e investimentos são iniciativas isoladas e não estão sendo monitoradas em sua implementação e efetividade por parte das instituições. 2. As autoridades competentes não tomam seriamente os investimentos em segurança cibernética, existem ainda projetos nacionais que não tem concluídos.	1. Não se tem conhecimento sobre o gasto público e dos investimentos nesses programas de segurança cibernética. 2. Atividades de lobby nas entidades do Estado, por parte das empresas multinacionais estrangeiras.

		internacionais de desenvolvimento.		
	Impulso na economia e mercado digital nacional	1. Existem limitações nestas iniciativas, devendo ser mais valorizado e menos influenciado por ideologias políticas. 2. Criação de polos científicos-tecnológicos e o oferecimento de ferramentas digitais para empreendedores.	1. Existem limitações nestas iniciativas, sendo umas delas o não dispor de uma política e de não ter estratégias integrais. 2. As iniciativas acontecem em forma lenta ou desacelerada, no ponto de se perder com o ritmo das mudanças e transformações tecnológicas.	1. As iniciativas em segurança cibernética não tem sido parte do impulso na economia e mercado digital nacional. 2. As iniciativas em segurança cibernética tomam relevância ao se tornar imprescindível para as relações comerciais e econômica com outros países.
Aspecto tecnológico e industrial	Responsável nacional por regular e estabelecer os padrões em TIC	1. Capacitação da entidade pública para regular e estabelecer os padrões em TIC. 2. Não tem obrigação de cumprir às empresas privadas os padrões em TIC nacionais. 3. A Política Modelo de Segurança da Informação tem como cliente final aos organismos do Estado Nacional para que seja adotada. Porém, não estariam inseridas no setor privado. 4. O setor privado possui um nível de maior exigência em suas políticas de segurança.	1. Capacitação da entidade pública para regular e estabelecer os padrões em TIC. 2. Não se tem uma clara ideia de que entidade do Estado estaria exercendo esta função, entre as entidades citadas estão: SEGDI, INDECOPI e o CONCYTEC. 3. Antes de elaborar normas e regulações é importante ter um diagnóstico apropriado na identificação das necessidades. 4. Deve se orientar em dispor de tecnologias com um enfoque mais aberto e modular.	1. Capacitação da entidade pública para regular e estabelecer os padrões em TIC, assim como, dos mecanismos de avaliação no seu cumprimento. 2. Necessidade de coordenar e discutir a elaboração dos padrões tecnológicos com o setor privado e academia.
	Empresas multinacionais estrangeiras e a Política Nacional de Segurança Cibernética	1. Necessidade de integrar a estas empresas na política nacional em segurança cibernética. 2. Necessidade de integrar as iniciativas em segurança cibernética com um único organismo governamental e desde esse ator, sejam realizadas as tarefas de articulação com as empresas multinacionais.	1. Não se tem uma política, norma ou iniciativa que atenda ou traga a discussão às multinacionais estrangeiras no marco da segurança cibernética.	1. Integração entre todos os setores, sendo o governo, o principal articulador dessa integração. 2. Não se tem atuado com papeis claros nas estratégias da segurança cibernética, eficiência, transparência e auditoria.
	Se tem incentivado a competição de fornecedores de acesso à Internet (ISP)	1. O acesso à Internet é uma preocupação que está na agenda dos governos. 2. Dependência da decisão política. 3. Se tem a capacidade de efetuar uma regulação eficiente aos ISP estrangeiros incentivando a competitividade. 4. O mercado está dividido somente por umas quantas empresas grandes.	1. O acesso à Internet é uma preocupação que está na política de Estado, porém, foi identificado que existem divergências de que entidade teria uma posição de regulador. 2. Não se tem uma empresa pública que oferece esses serviços. 3. Em telecomunicações não se tem quase nada regulado, o único regulado é a tarifa da telefonia fixa, mas poucos a utilizam.	1. O acesso à Internet é uma preocupação de Estado. 2. Foi identificado pelos especialistas na entidade reguladora da ANATEL, como também, do MCTIC os quesitos quanto aos provedores de conexão e de aplicação (ISPs).

Fonte: Elaborado pelo autor a partir dos dados da pesquisa (2024).

“Mas as políticas que hoje são observadas em todos os lugares, oferecendo o privilégio da segurança (econômica), ora para um grupo, ora para outro, estão rapidamente criando condições nas quais a luta por segurança tende a tornar-se mais forte do que o amor pela liberdade. A razão para isso é que, sempre que se concede segurança plena a um grupo, a insegurança do restante, necessariamente aumenta”

Friedrich Hayek, 1944

8 ANÁLISES E CONCLUSÕES FINAIS ENTRE OS ESTUDOS DE CASOS PESQUISADOS

Após ter concluído nossas análises e alcançado, praticamente, os resultados que retratam o panorama das configurações das políticas e estratégias dos países da Argentina, Brasil e Peru. No presente capítulo, como cientistas sociais, temos a imensa responsabilidade de evidenciar nossa busca por verdades concretas, devido que estamos imersos em um era da pós-verdade, que se caracteriza pelo negacionismo, o menosprezo dos valores sociais e da ciência. Portanto, sendo examinados e combinados os dados e as evidências (primeiro e segundo componente, respetivamente), durante o desenvolvimento dos capítulos anteriores. É neste capítulo que teremos a difícil tarefa de incorporar um terceiro componente, que são as ideias, sendo chamado de conceitos ou teorias pelos cientistas sociais.

Os dados, nos interessam porque nos ajudam a construir um argumento sobre algo no mundo para o qual eles seriam relevantes. Esperamos que os outros possam não aceitar nosso argumento, coletamos informação que, esperamos, vá convencê-los de que ninguém poderia ter registrado a realidade dessa forma se nosso argumento não fosse correto. E a ideia de que queremos propor nos leva a buscar tipos de dados, coisas que podemos observar e registrar, que farão esse trabalho de convencer os outros. Ninguém aceitará nossa ideia se os dados que oferecemos como evidências não forem convincentes, se nosso argumento sobre o que os dados mostram, aquilo de que eles são evidências, não convencer as pessoas de que eles sustentam nossa ideia tal como dizemos que o fazem (Howard, 2022, p.20)

Por último, serão apresentados os resultados da pesquisa, realizando uma comparação entre os relatórios dos estudos de caso dos países pesquisados. Em sequência, para o desenvolvimento das implicações teóricas e do relatório de casos cruzados, de modo, possa nos permitir desenvolver as conclusões finais e proposta de trabalhos futuros de investigação.

8.1 Conclusões do relatório de casos cruzados

Após a análise teórico e da historicidade da segurança e defesa nacional dos três países estudados, foi possível perceber algumas diferenças estruturais como resultado do processo de descolonização. Enquanto o Peru foi do grupo dos países que buscavam incentivar a unificação das ex-colônias espanholas para a proteção das ameaças externas que possam afetar a soberania e independência na região. A Argentina buscava uma estratégia diferente ao estar em favor da ação colonizadora europeia, justificando de ter sido o processo colonizador como protetor e civilizador. Porém, desde a posição da política externa, a participação do Brasil foi despreendida nos assuntos da segurança na região.

Depois de muitas tentativas de unificação fracassadas, com a mediação dos Estados Unidos se observa que os três países estudados assinaram diversos tratados e acordos internacionais relacionados à segurança, em oposição à influência soviética que foi ganhando espaço na região durante o período da Guerra Fria. Neste sentido, com a criação da Organização dos Estados Americanos (OEA) é sedimentada a influência dos Estados Unidos na América Latina. Aliás, na atualidade, a América do Sul é uma das regiões que não registra incidências de conflitos internacionais. No entanto, os países que a integram são afetados pela instabilidade política, crime organizado e conflitos sociais internos, além de violência. Há uma dificuldade em consolidar os sistemas democráticos. Tanto em Argentina, Peru e Brasil, suas sociedades e economias estão sujeitas ao assédio e à influência do crime global, que exercem uma conexão significativa nestes países, resultando na redução substancial dos direitos, valores e liberdades democráticas. Isso evidencia as capacidades do crime global e dos grupos de poder empresarial transnacional, que estão até mesmo inseridos no nível político democrático por meio da corrupção.

Nesse sentido, desde o 2008, com a mudança da estratégia brasileira de inserção regional e com a ampla aceitação dos países sul-americanos, se constitui o Conselho de Defesa Sul-americano (CDS), desde onde se buscam administrar as crises regionais no plano da defesa, constituir as bases de cooperação e integração regional. E favorecer o desenvolvimento regional da indústria tecnológica de defesa. Dessa maneira, se evidencia a **necessidade para o desenvolvimento de capacidades tecnológicas nos países da América do Sul, desde uma perspectiva conjunta**. Este desenvolvimento deve ter como base na compreensão das estratégias

de defesa que estariam condicionadas às estratégias de desenvolvimento dos países integrantes. Dessa forma, é necessário desenvolver estratégias sul-americanas que possam mitigar nossa “revolução inconclusa” e a dependência das intervenções dos agentes hegemônicos político-tecnológicos (Bruziguessi, 2014, p.48).

Esta postura geopolítica contemporânea relacionada aos três (03) países pesquisados evidencia outra necessidade, que consiste no fortalecimento da confiança regional. Isso envolve o incentivo às identidades culturais para fortalecer suas soberanias estatais e legitimar seus Estados, os quais têm sido enfraquecidos pelo processo da globalização e pela dependência político-tecnologia das hegemonias ocidentais e asiáticas, que exercem influência e poder na América do Sul. Portanto, infere-se que o **Brasil é um dos países na região que teria a função de ser o Hub Sul-americano**, para estabelecer conexões na difusão de estratégias e soluções inovadoras, em atenção aos problemas e ameaças regionais, como o crime organizado, a crise alimentaria, a crise energética, a crise financeira, os ciberataques às IC, entre outros. Não obstante, para que essa função seja efetiva, é necessário entender que o **Peru e a Argentina são pilares necessários e de imensa importância na integração com os outros países do bloco, principalmente, pelos aspectos multiétnicos e de história em comum**. Posteriormente, ao atingir o amadurecimento dessa integração, eles podem constituir um **Estado-Núcleo do bloco Sul-americano**. Como resultado, exerceriam sua esfera de influência e seu papel de liderança regional, através do **Conselho Sul-americano de Defesa (CSD)**, com ênfase no desenvolvimento, produção e inovação tecnológico-militar. Além disso, este **Estado-Núcleo Sul-americano**, por meio do **BRICS**, pode se beneficiar no contexto do comércio e das finanças transfronteiriças, através de novos modelos de serviços financeiros e de negócios inteligentes. Em contingência às futuras hostilidades, restrições, sanções e coerções dos países hegemônicos, como de organizações internacionais, sendo ações constituídas como parte das guerras híbridas contemporâneas.

Dispondo do diagnóstico teórico e da historicidade, por outro lado, as evidências coletadas nas múltiplas análises realizadas nos corpus documentais dos estudos de casos da Argentina, Peru e Brasil, têm nos ajudado a inferir que os modelos e ferramentas que estão sendo utilizados na avaliação das capacidades cibernéticas relacionadas com a segurança e defesa nacional têm incentivado

medidas e ações estratégicas que não são transversais e multisetoriais às problemáticas e ameaças vigentes desses países. São ações desprovidas da abordagem social e qualitativa, na perspectiva socioeconômica, geopolítica e cultural.

Desde a análise quantitativa, se tem evidenciado, no caso peruano e argentino, os interesses da segurança cibernética estão orientados basicamente em atender às pessoas e organizações estatais, impulsionado desde as iniciativas do governo eletrônico e digital, estando em destaque o **Aspecto Sociocultural e Organizacional**. Não obstante, no caso argentino as capacidades cibernéticas estão ponderadas no âmbito da defesa e suas forças armadas. No caso peruano, essa ponderação não estaria no setor defesa, porém, intensificadas nos indivíduos públicos. O caso brasileiro, difere dos outros dois casos, por ter sido orientado em atender às entidades da administração pública federal, desde as iniciativas da segurança da informação e das comunicações, estando em destaque o **Aspecto das Capacidades e Respostas**. Estas deduções comparadas com os análises realizados aos questionários e entrevistas dos especialistas locais, difere em pouco dos resultados alcançados, estando demonstrado que para os três estudos de caso o **Aspecto Sociocultural e Organizacional** possui o maior destaque nas respostas dos especialistas, estando nas discussões dos especialistas tópicos de governo e gestão da informação governamental, bem como, preocupações relativas a instrumentar as políticas públicas para uma articulação estatal. Além disso, o **Aspecto das Capacidades e Resposta** é o segundo aspecto de relevância para os três estudos de casos pesquisados.

Esses reflexos observados, com a análise qualitativo tem revelado o panorama, de como as políticas e estratégias no âmbito da segurança cibernética estão configuradas nos países pesquisados. Nesse sentido, a metodologia da pesquisa nós permitiu em forma inovadora, identificar sete (07) aspectos que vão configurar o desenvolvimento de nossas implicações teóricas, os quais são as seguintes:

- **Aspecto das ameaças e riscos.** Entre as prioridades em comum dos três países pesquisados estão a proteção das infraestruturas e ativos críticos nacionais, mas também, melhorar a governança da segurança cibernética para desenvolver estratégias integrais e de articulação multissetorial, a fim de vetar a duplicidade de agenda e a ineficácia entre os atores do setor público. É ressaltado nos três países, que seus atores possuem uma baixa maturidade na governança de seus riscos

cibernéticos e da informação. As ameaças do crime e delito cibernético é uma preocupação em comum, bem como, as operações de desinformação e influência com viés políticos e ideológicos. Existe nos especialistas, um nível mínimo de compreensão das ameaças cibernéticas que poderiam causar uma crise nacional. Nos casos argentino e peruano, se evidenciam a ausência de uma liderança nacional no âmbito cibernético, existindo esforços com interesses individuais de seus atores estatais, uma coordenação pouco efetiva e uma visão holística infrutífera no planejamento de médio e longo prazo, tendo gerado outros riscos em consequência dos vícios ou defeitos de suas iniciativas. Por exemplo, iniciativas legislativas e de regulação sem considerar os problemas burocráticos, as brechas e obsolescência tecnológica nas instituições públicas. No caso brasileiro, sua maturidade é maior em relação aos outros dois casos, principalmente, desde o âmbito da defesa cibernética. Existindo a necessidade de ter uma visão holística, além dos interesses da defesa cibernética, em que possam ser articulados o setor empresarial e industrial privado.

● **Aspecto das capacidades e resposta.** Nos três casos é reconhecido pelos especialistas, que as capacidades cibernéticas desejadas deveriam ter como diretrizes a autossuficiência, soberania e autonomia em relação às tecnologias da informação e da comunicação estrangeira. Porém, as capacidades humanas, bem como, a sustentação da capacidade operacional desse recurso nas entidades públicas não segue um planejamento estratégico institucional. Existem diversas iniciativas de investimentos para a criação do conhecimento nesse recurso, mas não existem mecanismos que permitam motivar e atrair o talento humano, existindo uma migração considerável desse talento para o setor privado e estrangeiro, onde encontram maiores incentivos e oportunidades de desenvolvimento. É evidenciado nos três casos, que existe a conscientização desde o alto nível do governo em dispor de capacidades de conectividade e acesso ao serviço da Internet. Porém, o desenvolvimento no âmbito rural ainda tem suas limitações. No caso argentino e brasileiro, existem empresas estatais em telecomunicações que tem permitido a competitividade nos serviços e autonomia reguladora, condição não identificada no caso peruano, devido à dependência nas empresas privadas, em que muitas das motivações reguladoras uma vez elevadas ao âmbito político-econômico, são muitas vezes questionadas e desaprovadas. Nos casos argentino e brasileiro, se busca melhorar o desenvolvimento da indústria tecnológica nacional, no caso peruano nem

seu é das preocupações na construção de suas capacidades cibernéticas, estando orientado a construir capacidades na usabilidade e consumo das tecnologias de informação e da comunicação.

- **Aspecto do poder e dominação.** Nos três casos é reconhecido pelos especialistas que a expansão e dominação dos países desenvolvidos nas TIC é um processo inevitável e de dependência em direção aos menos desenvolvidos, existindo mínimos controles e padrões tecnológicos relacionados com a segurança cibernética. Nesse caso, não se tem identificado uma estrutura estatal que tenha em suas competências o monitorar e sancionar as ações tecnológicas que não cumpram com os requisitos da segurança e defesa cibernética. Somente se tem identificado punições associadas ao crime cibernético e o tratamento dos dados pessoais. Apesar, das inúmeras iniciativas legais e regulamentares no âmbito da segurança digital é evidenciado que nos três países seus processos punitivos e de controle possuem baixa maturidade. São mínimas as estratégias que permitam dispor de produtos com altos padrões tecnológicos em segurança, incentivar as patentes no âmbito cibernético, dispor de uma legislação e regulação como meios de influência e de poder internacional.

- **Aspecto geopolítico e diplomático.** Nos três casos estudados, foram identificados casos de ameaças que tem afetado à segurança cibernética e da informação de seus países, como são vazamentos de dados sigilosos até espionagem de países. Porém, a atuação da diplomacia com a estratégia nacional da segurança cibernética tem sido tratada em forma superficial, sendo evidenciado que as iniciativas em segurança cibernética e da informação destes países não teriam ingerência direta na esfera diplomática internacional. Especificamente, no caso peruano, são confirmadas práticas intervencionistas das entidades e organizações internacionais no âmbito cibernético. Nos três países tem-se evidenciado que existem instrumentos diplomáticos de cooperação no tratamento do crime cibernético internacional. Desde a questão de dispor de uma entidade responsável da geoestratégia nacional no âmbito ciberespacial, não é confirmado qual instituição estatal teria em suas funções essas atividades, sendo o reflexo dessa debilidade a mínima produção científico-acadêmica em geopolítica e geoeconomia no âmbito cibernético, o limitado orçamento para os setores responsáveis, a despreocupação dos decisórios políticos, a priorização das necessidades urgentes e de curto prazo sobre os objetivos nacionais, que em consequência limitam aos da segurança nacional cibernética.

● **Aspecto sociocultural e organizacional.** Para os três casos estudados, evidencia-se na respostas dos especialistas, que as iniciativas da segurança cibernética têm incentivado necessárias reformas nas instituições públicas. Porém, os problemas da segurança cibernética e da informação nestes países são consequência dos problemas não resolvidos que tem o Estado, por exemplo, os projetos são deixados de lado por motivos partidários ou por mudanças de gestão no governo, burocracia e processos imaturos, tecnologia obsoleta nas instituições, inexistência de mecanismos e de indicadores que acompanhem essas mudanças institucionais em forma transparente e confiável. Para os casos argentino e brasileiro, segundo os especialistas, não podem ser apreciados em forma direta os benefícios da segurança cibernética na sociedade, porque são atendidos somente aspectos conceituais e de tecnicismos, sem tocar de fundo as responsabilidades e os benefícios que deverão ser alcançados. No caso peruano, evidencia-se que os benefícios estariam orientados ao âmbito bancário e empresarial privado, bem como, à população de ensino médio das áreas urbanas.

● **Aspecto socioeconômico e de mercado.** Segundo o evidenciado nos três casos estudados podemos inferir que o incentivo ao consumo tecnológico nacional é ainda imaturo nas estratégias da segurança e defesa cibernética. Nos casos peruano e brasileiro, tem-se evidenciado no setor estatal uma maior dependência tecnológica estrangeira, com esforços superficiais que busquem equilibrar essa dependência tecnológica. Já no caso argentino, identificou-se estratégias de estender o uso do software livre na administração pública, espalhando-se nas grandes empresas nacionais, no comércio e em empreendimentos de negócios menores. Segundo os especialistas, não se tem uma vinculação direta das ações da segurança cibernética e digital em incentivar o consumo nacional das tecnologias da informação e da comunicação. O que traz à luz, a necessidade destes países em unificar seus esforços nas políticas e programas de Estado. Entre as problemáticas relevantes, estão as limitações do investimento público no âmbito da ciência e da tecnologia. Principalmente, nos casos argentino e brasileiro, nos últimos anos foram adotadas decisões políticas que tem desfavorecido esses âmbitos. Outra problemática, seria a ausência de iniciativas de inclusão dos usuários do setor pobre e das áreas não urbanas, especialmente, no consumo das tecnologias de médio porte.

Não se tem evidenciado, em como as estratégias da segurança cibernética vão se integrar ao impulso da economia e do mercado digital. No caso peruano e brasileiro, foi comentado que estas estratégias tomam relevância devido à pressão midiática ao tornar-se imprescindíveis para as relações comerciais e econômicas com outros países ou organismos internacionais. Um exemplo é a aprovação da Lei de Proteção de Dados Pessoais, estando em evidência as atividades de *lobby* nas instituições públicas por parte das empresas multinacionais, confederações nacionais e partidárias. No caso peruano, se tem evidência que muitos dos projetos que buscam impulsionar à economia digital nacional, acontecem em forma lenta, ao ponto de se perder com o ritmo das mudanças e transformações tecnológicas, por exemplo, o projeto nacional de banda larga.

● **Aspecto tecnológico e industrial.** Segundo os especialistas nos três casos estudados, o acesso e a conectividade à Internet é uma preocupação que está na agenda dos governos. Porém, o exercício da regulação dos serviços na Internet, bem como, dos mecanismos de avaliação e de transparência cumprem mínimas exigências e padrões técnicos. Por exemplo, no caso peruano, foi comentado que no setor das telecomunicações, onde as empresas são de capital privado e estrangeiro, se tem quase nada regulado, sendo unicamente regulado a tarifa da telefonia fixa, que é um serviço que poucos peruanos fazem uso. Outro aspecto a ressaltar é a necessidade de integrar às empresas multinacionais estrangeiras de produtos e serviços em tecnologias de informação e da comunicação ao marco nacional da segurança cibernética. Contudo, os especialistas comentaram que não sabiam qual entidade pública seria a responsável dessa articulação no país. Nos estudos de caso argentino e brasileiro, evidenciam possuir capacidades na regulação dos ISP estrangeiros, sem prejudicar a inversão estrangeira e a livre concorrência de mercado, devido à experiência adquirida de suas empresas estatais como ArSat e Anatel, respectivamente.

Em conclusão, após as análises desenvolvidas e considerando os benefícios quantitativos e qualitativos apresentados pelos especialistas locais, observa-se que a elaboração dos análises cruzados dos estudos de casos válida a possibilidade de identificar e compreender, a partir de uma perspectiva comparada, as peculiaridades nas relações e mecanismos expressados nas estratégias adotadas pelos países da Argentina, Peru e Brasil no âmbito da segurança cibernética.

8.2 Modificando a teoria e desenvolvendo as implicações teóricas

Portanto, a partir dos resultados observados do panorama atual das configurações políticas e estratégicas, no âmbito da segurança cibernética. Em seguida, se busca oferecer as implicações derivadas das perspectivas teóricas que tem conduzido a presente tese, com a finalidade de sugerir melhorias e modificações teóricas nas políticas e estratégias da segurança cibernética nos países da Argentina, Brasil e Peru. Uma vez, que existe pouca teoria e estudos na América do Sul, a pesquisa busca contribuir para a consulta dos outros países da região, no que concerne à segurança cibernética. Na perspectiva do autor, a tese também permitiu relacionar alguns atributos contextuais e das ideias, dando origem nas seguintes contribuições teóricas e práticas:

a. O nexos da informação e a cibernética através da esfera política seria estabelecida por sua inclusão na intervenção do Estado, como parte de suas capacidades em segurança cibernética e da informação. Estando além da dimensão administrativa, deverá ser considerado como um fator estratégico de desenvolvimento científico-tecnológico. O expressado constitui um novo modelo de soberania onde o Estado age como um agente no ciclo de vida das informações gerando-se uma representação dupla de sua intervenção nos domínios territorial, social e simbólico. De onde podemos afirmar que o metacapital de um Estado moderno está composto pelo capital da força física, o capital econômico e o capital informacional e do conhecimento. De esta forma um Estado poderá assegurar sua influência e poder sobre os outros campos de atividade e das formações de capital social, manufaturado, financeiro, entre outros.

b. A política nacional da segurança cibernética tem que ser elaborada e dirigida desde uma visão holística e multissetorial, através do sistema nacional de planejamento estratégico. Esta entidade deverá ser o responsável da coordenação entre os ministérios e os níveis da governança no país (regiões, províncias e municípios). Portanto, as estratégias no âmbito da segurança e defesa cibernética, deverão estar alinhadas aos interesses nacionais, a fim de garantir o progresso sustentável e a conquista do bem-estar nacional. Em síntese, a segurança cibernética não deve ser submetida ao princípio da representação da sociedade, tem que ser exercida desde a perspectiva do projeto social respeitando os parâmetros do ordem social, mas

aspirando às transformações fundamentais do ordem econômico, dispensando os interesses e desejos da sociedade civil.

c. Tomar consciência da evolução histórica, causalidade social e estrutural subjacente da complexa inter-relação existentes na: economia, tecnologia, sociedade e política. Em outras palavras, os processos de desenvolvimento econômico e de transformação estrutural devem ser inseridos nas instituições, orientados culturalmente e no consenso social. Por intermédio das políticas e estratégias tocante no comercial, tecnológico e de incentivo na exportação nacional.

d. Devido à pluralidade de saberes especializados e hierarquizados no âmbito da segurança cibernética e da informação, insere ao conhecimento e à ciência como princípio de credenciamento e habilitação, em relação aos novos médios civilizatórios e de produção. No caso, dos países estudados, nunca alcançariam uma plena realização se continuassem sujeitos a uma modernização subalterna e conservadora. Então surgem diversos cenários como os patrimonialistas e clientelistas de privatização do público, a convergência tecnológica e econômica, a ausência do comum e da própria vontade, a ausência de regras e padrões sociais reconhecidos e aceitos pelos sujeitos no processo de comunicação em rede, entre outros. Constituindo uma omissão ou desintegração de normas sociais e de segregação socioeconômica, sendo ao mesmo tempo um sintoma do régimen informacional presente no Estado e na sociedade, assim como das condições políticas da governança da informação.

e. Para dispor das capacidades cibernéticas que possam garantir o equilíbrio da dependência tecnológica, tem de ser fortalecida a articulação de três (03) ministérios chaves: O setor da economia e finanças, para o incentivo dos investimentos e créditos na exportação e importação, apoiando assim ao desenvolvimento científico e tecnológico das empresas nacionais. No caso do setor de infraestrutura e das telecomunicações, para outorgar as condições materiais de produção e organização seletiva para a disseminação das tecnologias da informação no setor público e industrial local. No setor da educação, para preservar a identidade cultural e organizacional do sistema de estratificação e mobilidade social. No exercício do controle estrito da meritocracia no recrutamento dos altos cargos das instituições do Estado, bem como, na sustentação da capacidade operacional do talento humano e sua distribuição idônea nos setores de suas competências profissionais.

f. Reconstruir as relações do Estado, sociedade e economia. Buscando as condições de adaptabilidade e flexibilidade nas políticas e nas empresas, em relação à demanda do mercado internacional. Entenda-se que nessas relações o Estado é o centro da experiência da economia digital, proporcionando incentivos necessários para atrair capital estrangeiro, criando infraestrutura industrial e de comunicações, que apoiem às exportações da indústria tecnológica, favorecendo principalmente à ciência e tecnologia, para a melhoria e inovação dos produtos e serviços do Estado, consequentemente da indústria nacional. Com um Ministério da Educação empoderado e articulador, para que as informações e pesquisas das universidades e institutos técnicos dialoguem e sejam aplicáveis às demandas do mercado.

g. Impulsar a combinação flexível de redes centralizadas das pequenas e médias empresas (*Pymes*), que atuam como subcontratados nas empresas fabricantes de tecnologias da informação e da comunicação. Para esse fim, o Estado deverá desenvolver uma estrutura industrial que permita a interconexão das *Pymes* com as empresas especializadas em canalizar a exportação e a importação de produtos e serviços. Como resultado, deve ser disponibilizado um sistema de bibliotecas digitais e de informação, onde sejam fornecidos programas de capacitação, serviços de consultoria e de tecnologia, colaboração e produção técnico-científica, bem como, uma rede de segurança para reduzir o risco empresarial.

h. Incentivar estratégias de segurança e defesa cibernética em contraste à dependência das multinacionais estrangeiras que operam no âmbito das tecnologias de informação e da comunicação. Consequentemente, sem desalentar os processos da globalização e estando expectantes aos fenômenos trazidos pelas assimetrias da informação existente entre os objetivos da segurança cibernética e da tecnologia da informação que tem entrelaçado por completo à pesquisa, desenvolvimento e inovação. A relevância dos centros de pesquisa, as empresas e os mercados prometem a integração de um país nas redes tecnológicas dominantes, bem como, dispor de uma melhor avaliação das necessidades estratégicas e de conhecimento da informação.

i. A Política Nacional de Segurança Cibernética não deve ser impassível às iniciativas multilaterais das relações exteriores e da diplomacia. Para esse fim, a instituição qualificada e responsável deverá constituir os grupos de especialistas militares, civis

e da comunidade científica-acadêmica especializada, para a elaboração dos estudos de perspectiva geopolítica e geoeconômica no âmbito do ciberespaço.

j. Uma forma de neutralizar os efeitos e mitigar as intervenções dos países hegemônicos que tenham como objetivos o desestabilizar o bloco Sul-americano, tanto no âmbito sociopolítico e geoeconômico. Os três países estudados devem se constituir em um Estado-Núcleo e através dos mecanismos do Conselho de Defesa Sul-Americano (CDS) sejam concertadas as políticas e estratégias em segurança e defesa, sendo priorizadas as seguintes questões:

1. A Hegemonia político-tecnológica Ocidental e Asiática de influência no bloco Sul-americano.
2. A industrialização e produção de tecnologias emergentes na região.
3. A Ciber diplomacia e ciber coerção nos interesses nacionais e tecnológicos dos países Sul-americanos.

k. Para uma efetiva governança da segurança cibernética, deve ser apontada o organismo ou a instituição responsável da articulação nacional. O articulador da segurança cibernética deverá ter autonomia, recursos e uma função reguladora nos quesitos do espaço cibernético do país, articulando estreitamente com o sistema de inteligência nacional. É de considerar que as operações de empresas em um mercado autorregulado, sem diretrizes claras e sem um controle podem ser destrutivas. Em princípio, quando as empresas têm a permissão de operar livres de leis e de regulações, sem capacidades de equilibrar as assimetrias existentes, pode gerar vícios e problemáticas no social, econômico e político.

l. A capacidade de adaptação dos países desenvolvidos ao paradigma informacional e das mudanças da economia global, através da modernização tecnológica, da expansão dos mercados e da diversificação econômica. Foi incentivada, em princípio nos decisórios dos diversos níveis de governo de um Estado. Se deve criar consciência da existência de vícios e dos problemas de um Estado que estariam afetando o alcance dos interesses e objetivos da segurança cibernética. A busca da desburocratização na gestão econômica, através de estímulos de produtividade e resultados pelas instituições de planejamento estratégico, com a inserção de controles que possam permitir o monitoramento e rendição de contas dos resultados nas

instituições através da tecnologia de informação e a automação, onde sejam atendidos princípios de transparência, eficácia e efetividade.

9 CONCLUSÕES FINAIS E PROPOSTAS PARA TRABALHOS FUTUROS

Dada a ampla diversidade e proximidade dos conceitos que foram tratados na presente tese, buscou-se durante o desenvolvimento da pesquisa se manter fiel à questão central de investigação, aos seus objetivos e à metodologia adotada fazendo uso de diversos instrumentos, métodos de pesquisa e de indispensáveis leituras relacionados com a defesa e segurança cibernética da Argentina, Peru e Brasil. Ter mergulhado na historicidade e nas perspectivas teóricas das diversas áreas de conhecimento, tem facilitado a observação e condução de nossas análises na investigação.

A escolha do estudo de casos múltiplos permitiu conhecer o contexto da segurança cibernética da Argentina, Peru e Brasil. Em seguida, desde uma perspectiva comparada poder identificar e analisar os elementos que se influenciam na consolidação das políticas e estratégias em segurança cibernética dos países estudados. Permitindo-nos obter conclusões a partir dos reflexos observados enriquecendo a qualidade da pesquisa, em relação de ter realizado um único estudo de caso. Outro aspecto relevante para a pesquisa foi o uso do software MAXQDA para o processo sistematizado no tratamento qualitativo e quantitativo dos dados coletados do corpus bibliográfico, as entrevistas gravadas semiestruturadas (vídeos) e questionários semiestruturados (formulário online), os dados pessoais foram anonimizados desta maneira os entrevistados e respondentes se manifestaram com liberdade e independência, com a garantia que suas respostas não poderiam ser avaliadas em um contexto externo aos propósitos desta pesquisa.

Devido à complexidade e escassez de pesquisas relacionados com o tema de estudo, se teve como uma estratégia metodológica articular um “Estado da Arte” tomando como referência o corpus bibliográfico dos Estados Unidos. Certamente, nossa escolha responde às particularidades da segurança cibernética desse país, em ser uma potência mundial com hegemonia política-tecnológica no âmbito cibernético. Assim, afirmamos que o protótipo norte-americano ou estudo de caso-piloto (Bardin, 2015, p.100-103) ajudou a refinar nosso planejamento na coleta dos dados, no conteúdo, como nos procedimentos realizados na pesquisa. Portanto, nesta fase de expor as conclusões finais da pesquisa, ressaltamos que o caso-piloto apoiou o desenvolvimento de linhas relevantes de questões, contribuindo com conceitos que

temos chamado de “Estado da Arte”. Assim, o “Estado da Arte” reúne as principais conclusões da defesa e segurança cibernética norte-americana, sendo objetivados os elementos e agentes contemporâneos, como das relações, divergências e lacunas dos conceitos perante a temática mapeada.

É evidente que a proximidade geográfica, o grau de influência político-tecnológica e interesses geoeconômicos dos Estados Unidos, em relação aos três estudos de caso abordados na pesquisa, foram alguns dos critérios para a seleção do caso-piloto norte-americano. Contudo, podemos afirmar que o caso-piloto serviu de laboratório, onde experimentalmente foram observados os fenômenos desde diversos ângulos. Como resultado, foi possível melhorar a conceituação das diferentes categorias temáticas e as relações organizacionais que foram visualizadas através do software MAXQDA. Porém, não se entende que a segurança cibernética norte-americana seja o melhor caminho para o contexto sul-americano. Em outras palavras, o desenvolver uma compreensão da segurança cibernética norte-americana, incentivou o estudo da mecânica por trás das políticas e estratégias, nos permitindo identificar vários casos interligados no mesmo tempo, como dos padrões e relações de causa/efeito que as governam.

Assim, como resultado da sistematização e das técnicas de análise do caso-piloto, observamos que nas configurações do panorama contemporâneo das políticas e estratégias da segurança e defesa cibernética norte-americana foram identificados sete aspectos em que o aspecto de poder e dominação é o mais relevante. Portanto, este resultado, no que se refere ao contexto atual em que a tese está sendo defendida, não está distante dos eventos importantes que estão acontecendo nos Estados Unidos. Consequentemente, existe uma enorme confluência desses eventos, como dívidas gigantescas, conflitos políticos e sociais internos, disparidade de riqueza e o surgimento de uma nova potência mundial (China) que desafia a hegemonia norte-americana (o império) e a ordem mundial existente (Dalio, 2022, p.11).

Também ressaltamos que a tese foi desenvolvida durante a pandemia do Covid-19, evento que marcou profundamente o contexto de desenvolvimento da pesquisa, principalmente, de novas experiências e desafios, sendo consciente que os fenômenos naturais inesperados têm acontecido em outras épocas de nossa história mundial.

Havendo testemunhando, como o domínio ciberespacial tem abraçado várias dimensões da vida humana, incluindo as artes e a cultura, os costumes e crenças

sociais, os mecanismos de produção etc. Domínio onde as guerras híbridas contemporâneas tomam maior relevância, através das cinco principais tipos de guerras: comerciais/econômicas, tecnológicas, de capital, geopolíticas e militares. Segundo Dalio (2022, p.41) “hoje há uma nova mudança e o maior valor está em ativos digitais sem existência física aparente (processamento de dados e de informação). Isso tem gerado um conflito quanto à obtenção de dados e seu uso para ganhar riqueza e poder”. Portanto, diante esta nova realidade, inferimos que foram afetados os interesses nacionais dos países seja em forma direta ou indireta, então sob qualquer ângulo que seja analisada, é impactada a segurança e defesa nacional.

Também, deve ser entendido que cada aspecto ou poderes tratados na tese, são desenvolvidos em cadeia, estando inter-relacionados. Nos estudos de Dalio (2022), de forma similar os aspectos descobertos são correlacionados e analisados, sendo identificados padrões e relações de causa/efeito:

Os três ciclos mais importantes [...]: o ciclo de endividamento de longo prazo e de mercado de capitais, o ciclo de ordem e desordem interno e o ciclo de ordem e desordem externo. [...] Esses ciclos fazem o pêndulo oscilar entre opostos- a paz e a guerra, o boom econômico e a recessão, a direita e a esquerda no poder, a consolidação e a desintegração dos impérios etc. (Dalio, 2022, p.36).

Assim, as análises do caso-piloto norte-americano, ao ser contrastada com a análise computacional apresentado em agosto de 2021, por Dalio (2022, p.524-527), os Estados Unidos são posicionados como uma potência vigorosa, mas em queda gradual, diretamente afetada no grau de poder e dominação que ostenta.

Os principais pontos fortes que alçam o país a posição são os mercados de capital e centros financeiros robustos, a inovação e tecnologia, o nível sólido de educação, o forte poderio militar, o status de moeda de reserva e a alta produção econômica. Os pontos fracos são a situação econômica/financeira desfavorável e os grandes conflitos internos (Dalio, 2022, p.524-525).

Então, o caso-piloto norte-americano, permitiu sintetizar uma questão complexa e multifacetada, em um procedimento inovador e esclarecedor, de fácil aplicação para os subsequentes estudos de casos da Argentina, Brasil e Peru. Não obstante, o aprendizado no desenvolvimento desta tese está longe de ser exato, ao explicar a configuração da política e estratégias da segurança cibernética. Porém, é essencial, para pôr em perspectiva os aspectos de maior influência e relevância que são aderidos nas políticas e estratégias dos países sul-americanos, podendo ser observadas repetidas vezes no decorrer do tempo.

No caso dos três países pesquisados, pelo exposto nos primeiros capítulos da presente tese, estes países são influenciados pelos Estados Unidos, no desenvolvimento de suas políticas e estratégias em segurança cibernética, como na

organização e estrutura destes países tem adotado para tal objetivo. Infere-se que a historicidade e exploração precoce realizada proporcionou insight nos assuntos estudados, servindo de complemento aos reflexos observados no referencial teórico e de ajuda no aprimoramento de nossa coleta de dados em relação ao conteúdo dos dados e aos procedimentos realizados para os três estudos de casos estudados.

Então aplicando o método de análise do conteúdo foram identificadas as explicações provisórias e categorias, para assim ter uma visualização primária, dos indícios, que em momento não eram óbvias nos documentos pesquisados. Para, posteriormente analisar os documentos e direcionar as seguintes análises em cada um dos estudos de casos tratados nesta tese. Entenda-se que a exploração e domínio dos conceitos básicos das perspectivas teóricas foi primordial para a análise crítica, sendo de potencial ajuda no desenvolvimento da investigação.

A escolha do método quantitativo neste tipo de investigação, que às vezes limita, não foi neste caso, porque a análise computacional nós permitimos realizar múltiplas análises e identificar as características e relações existentes entre os códigos que compõem os sete (07) aspectos abordados: **ameaças e riscos, capacidades e resposta, poder e dominação, geopolítico e diplomático, sociocultural e organizacional, socioeconômico e de mercado , e o tecnológico e industrial**. Neste contexto, pode ser afirmado que a análise quantitativa contribuiu para a segurança das nossas conclusões enriquecendo e inovando nosso estudo como um todo.

Como em qualquer outra tese de doutorado, busca-se apresentar à comunidade científica e acadêmica um aspecto inédito no campo investigado. Considerando-se isto como o mais relevante, a principal contribuição desta tese veio dos elementos que influenciam na elaboração das políticas e estratégias na segurança cibernética, em que foram consideradas as especificidades geopolíticas dos três países estudados: Argentina, Peru e Brasil. Foi tomado como características o diagnóstico teórico e a historicidade, as evidências coletadas nos corpus documental e nos relatórios individuais por estudo de caso investigado. Como conclusão, a pesquisa apontou que os modelos e ferramentas que estão sendo utilizadas na avaliação das capacidades cibernéticas, tem incentivados nos três (03) países estudados, medidas e ações estratégicas que não são transversais e multisetoriais às problemáticas e ameaças vigentes destes países, sendo ações despossuídas de uma tratativa social e qualitativa em sua perspectiva socioeconômica, geopolítica e cultural.

Em outras palavras, se evidencia a necessidade do desenvolvimento de capacidades tecnológicas desde uma perspectiva conjunta para o fortalecimento de suas soberanias estatais e legitimação de seus Estados, que estão debilitados pelo processo globalizador e de dependência político-tecnológica dos países hegemônicos que exercem sua influência e poder na América do Sul. Foi demonstrado que para os três (03) estudos de caso, o aspecto sociocultural e organizacional tem o maior destaque nas configurações de suas políticas e estratégias em segurança cibernética. O relevante destes achados é que ele não foi encontrado em nenhuma literatura pesquisada.

Uma limitação desta tese apresentada, sob a forma de sugestão em investigações complementares, é analisar aplicando a mesma metodologia nos outros países que integram a América do Sul, como analisar desde a perspectiva do “Estado da Arte” chinês. Isto não foi feito devido à indisponibilidade de tempo, recursos e domínio do idioma mandarim e que praticamente constituiria a elaboração de outra tese de doutorado.

Finalmente, diante do apresentado, podemos dizer que foi alcançado nosso objetivo principal de pesquisa em dispor de um panorama das configurações políticas e estratégicas no âmbito da segurança cibernética dos países de Argentina, Peru e Brasil. Todos os objetivos específicos propostos originalmente foram atingidos. Neste sentido, a presente tese serve de contribuição ao conhecimento com revelações inéditas desde a perspectivas das ciências sociais, bem como forneceu informações para as lideranças que têm responsabilidades na elaboração das políticas em segurança e defesa cibernética, principalmente da América do Sul, incentivando a análise crítica, sob o ponto de vista da evolução do sistema, com o intuito de fortalecê-lo e nos tornar sociedades mais articuladas no nível da segurança cibernética, em que sejam alcançados os adequados níveis de desenvolvimento, progresso e bem-estar nacional.

Como ainda é um tema pouco aprofundado nos países, em vias de desenvolvimento, e para dar uma continuidade de próximas pesquisas, sugere-se como opção para novos estudos:

a. Estender o estudo aplicando a mesma metodologia a todos os países integrantes da América do Sul. Desta forma seria possível ampliar a base de dados e ter um

relatório cruzado desses países, desde a perspectiva do “Estado da Arte” com influência Ocidental.

b. Realizar um estudo semelhante contemplando os países próximos à cultura asiática analisando a perspectiva do “Estado da Arte” chinês.

c. Realizar um estudo semelhante contemplando três (03) países em vias de desenvolvimento por continente e analisando desde a perspectiva do “Estado da Arte” dos países que integram o G7.

d. Aplicar outros métodos de pesquisa quantitativos e qualitativos para dar continuidade ao estudo do tema desde outra perspectiva.

REFERÊNCIAS

ALBERTS, David S.; PAPP, Daniel S. **The Information Age: An Anthology on Its Impact and Consequences**. Washington DC: Office of the Assistant Secretary of Defense Washington DC Command and Control Research Program, 1997. Disponível em < http://www.dodccrp.org/files/Alberts_Anthology_I.pdf>. Acesso em 16 de maio de 2020.

ALUÍSIO, Sandra M.; BARCELLOS, Gladis M. **O que é e como se constrói um corpus? Lições aprendidas na compilação de vários corpora para pesquisa linguística. Calidoscópio**. Vol.4,n.3, p.156-178, 2006. Disponível em < <http://revistas.unisinos.br/index.php/calidoscopio/article/view/6002>>. Acesso em 16 de maio de 2020.

ALVES, Maria Helena Moreira. Estado e oposição no Brasil (1964-1984). **5ªed. Petrópolis: Vozes**, 1989 apud BRUZIGUESSI, B. Os fundamentos da Doutrina de Segurança Nacional e seu legado na constituição do Estado brasileiro contemporâneo. **Revista Sul-Americana de Ciência Política**, v. 2, n. 1, p. 47-64, 7 out. 2014.

ARAÚJO, Carlos Alberto A. **O sujeito informacional no cruzamento da ciência da informação com as ciências humanas e sociais**. XIV Encontro Nacional de Pesquisa em Ciência da Informação (ENANCIB 2013) GT 3: Mediação, Circulação e Apropriação da Informação. Comunicação Oral. 2013. Disponível em < <https://www.brapci.inf.br/index.php/article/download/40403> >. Acesso em 16 de maio de 2020.

ARAÚJO, Wagner Junqueira de. **A SEGURANÇA DO CONHECIMENTO NAS PRÁTICAS DA GESTÃO DA SEGURANÇA DA INFORMAÇÃO E DA GESTÃO DO CONHECIMENTO**. Brasil, 2009. Disponível em < <https://encr.pw/WG5Rt>>. Acesso em 12 de maio de 2020.

ARAÚJO, Wagner Junqueira de; MELO, Renato Vieira. **Assinatura de documentos eletrônicos utilizando certificados digitais**. EDIÇÃO ESPECIAL. Biblionline, João Pessoa, v. 8, n. Esp., p. 290-302, 2012. Disponível em < <https://periodicos.ufpb.br/ojs2/index.php/biblio/article/view/14204> >. Acesso em 12 de maio de 2020.

ARNAUDO, Daniel. **O Brasil e o Marco Civil da Internet** - O Estado da Governança Digital. Igarapé Institute A think and do tank."s.d". Disponível em < <https://igarape.org.br/marcocivil/pt/> >. Acesso em 12 de agosto de 2024.

ARRUDA, Antônio de. **A Segurança Nacional e a Legislação Brasileira**. Revista do Serviço Público, [S. l.], v. 107, n. 1, p. 65-80, 2017. DOI: 10.21874/rsp.v0i1.2457. Disponível em <<https://revista.enap.gov.br/index.php/RSP/article/view/2457>> . Acesso em 28 de abril de 2024.

BARABÁSI, Albert-László; BONABEAU, Eric. Scale-Free Networks. Scientific American. May 2003. Disponível em < <https://barabasi.com/f/124.pdf> >. Acesso em 04 de novembro de 2020.

BARDIN, Laurence. **Análise de Conteúdo**. Tradução Luís Antero Reto, Augusto Pinheiro. São Paulo: Edições 70, 2016.

BARLOW, John. **A declaration of the independence of cyberspace**. Davos, Switzerland. 2016. Disponível em < <https://www.eff.org/cyberspace-independence> >. Acesso em 06 de novembro de 2020.

BEJARANO, María. **Alcance e âmbito de la seguridad nacional em el ciberespacio**. 2011, de Instituto Español de Estudios Estratégicos (IEEE). Espanha. Disponível em < <https://l1nq.com/iHx80>>. Acesso em 06 de novembro de 2020.

BEZERRA, E. P.; SILVA, Z. C. G. da; GUIMARÃES, Ítalo J. B.; SOUZA, E. D. de. **Regime de informação**: abordagens conceituais e aplicações práticas. Em *Questão*, Porto Alegre, v. 22, n. 2, p. 60–86, 2016. DOI: 10.19132/1808-5245222.60-86. Disponível em < <https://seer.ufrgs.br/index.php/EmQuestao/article/view/57935> >. Acesso em 25 de fevereiro de 2021.

BIBER, Douglas. **Representativeness in Corpus Design**. *Lit Linguist Computing*, 8:243-257, 1993. Disponível em < <http://otipl.philol.msu.ru/media/biber930.pdf> >. Acesso em 16 de maio de 2020.

BID; OEA. Ciberseguridad: **¿Estamos preparados en América Latina y el Caribe?** 2016. Disponível em < <https://acesse.dev/i56UL> >. Acesso em 30 de maio de 2022.

BID; OEA. Ciberseguridad: Riesgos, avances y el camino a seguir en América Latina y el Caribe. 2020. Disponível em < https://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=AVI-095/20>. Acesso em 30 de maio de 2022.

BICKMAN, Leonard. **The functions of program theory**. In L. Bickman (Ed.), *Using Program Theory in Evaluation, New Directions for Program Evaluation* (pp. 5-18). San Francisco, CA.: Jossey-Bass Publishers. 1987. Disponível em < <https://eric.ed.gov/?id=EJ355031>>. Acesso em 16 de maio de 2020.

BILLER, Jeffrey T.; SCHMITT, Michael N. **Classification of Cyber Capabilities and Operations as Weapons, Means, or Methods of Warfare**. *International Law Studies*. Vol.95. p.178-225. 2019. Disponível em < <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2462&context=ils> >. Acesso em 16 de maio de 2020.

BLESA, Ana López. *España y sus estrategias de seguridad (2000-2017): un análisis comparativo*. Instituto Español de Estudios Estratégicos. 2018. Disponible em < <https://acesse.dev/d6fWs> >. Acesso em 16 de maio de 2020.

BOURDIEU, Pierre. **Le sens pratique**. Paris: Les Editions de Minuit, 1980.

BOUDREAUX, Donald J. **Menos Estado e mais liberdade**. O essencial pensamento de F.A. Hayek. Tradução Leonardo Castilhone. 1ed. Barueri: Faro Editorial, 2018.

BRAMAN, Sandra. **Change of state**: information, policy, and power. Cambridge, Mass.: MIT Press, 2009. Disponível em < <https://encr.pw/GDK0d> >. Acesso em 20 de agosto de 2024.

BRITO, Vladimir de Paula; KERR P., Marta M. **Poder informacional e desinformação**. *Tendências da Pesquisa Brasileira em Ciência da Informação*, v.8, n.2, jul./dez. 2015. Disponível em < <https://revistas.ancib.org/index.php/tpbci/article/view/355>>. Acesso em 16 de setembro de 2024.

BRITO, Vladimir de Paula. **O papel informacional dos serviços secretos**. 2011. Dissertação de Mestrado (Mestrado em Ciência da Informação) –Escola de Ciência da Informação, Universidade Federal de Minas Gerais, 2011.

BRUZIGUESSI, B. **Os fundamentos da Doutrina de Segurança Nacional e seu legado na constituição do Estado brasileiro contemporâneo**. Revista Sul-Americana de Ciência Política, v. 2, n. 1, p. 47-64, 7 out. 2014.

BUSH, Vannevar. **As we may think**. *Atlantic Monthly*, v. 176, n. 1, p. 101-108, julho de 1945. Disponível em: < <https://encr.pw/FCRPr> >. Acesso em 15 de julho de 2024.

CAMATI, Odair. Uma análise da razão de Estado em Michael Foucault a partir do curso segurança, território e população. ISSN 1983-4012. **Intuitio**. Porto Alegre. Vol.8-N.1. p.171-184, 2015. Disponível em <<http://dx.doi.org/10.15448/1983-4012.2015.1.18492>>. Acesso em 26 de junho de 2020.

CAPURRO, R. Epistemologia e Ciência da Informação. In: CONGRESSO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO (**ENANCIB**), 5., 2003. Anais... Belo Horizonte, 2003.

CASAR, José. **El Ciberespacio. Nuevo escenario de confrontación**. Centro Superior de Estudios de la Defensa Nacional (CESEDEN). Febrero 2012, España. NIPOR:083-12-023-1. Disponível em < <https://encr.pw/fIUyK> >. Acesso em 26 de outubro de 2020.

CASTELLS, Manuel. **A sociedade em rede**. 10. ed. São Paulo: Paz e Terra, v.1, 1999. Disponível em < <http://dx.doi.org/10.15448/1983-4012.2015.1.18492> >. Acesso em 26 de junho de 2020.

CASTELLS, Manuel. **La era de la información, fin de milenio**. Alianza editorial, S.A. Madrid, v.3, 2018.

CEPAL. **Estudio económico de América Latina y el Caribe**. Principales condicionantes de las políticas fiscal y monetaria en la era pospandemia de COVID-19. Santiago, 2020. Disponível em < <https://encr.pw/f1beG> >. Acesso em 26 de outubro de 2020.

CIA. **Senior Research Staff on International Communism**. Soviet. Communism in the Sixties: Some Notes on Its New Dimensions. 01 Agosto de 1961, p. 8. Disponível em: < http://www.foia.cia.gov/sites/default/files/document_conversions/89801/DOC_0000247350.pdf >. Acesso em: 15 de julho de 2022.

COMISIÓN EUROPEA. **Comunicado de prensa**. Un mercado único digital para Europa: la Comisión establece 16 iniciativas para conseguirlo. Bruselas, 6 mayo de 2015. Disponível em https://ec.europa.eu/commission/presscorner/api/files/document/print/es/ip_15_4919/IP_15_4919_ES.pdf>. Acesso em 05 de fevereiro de 2024.

CPI ESPIONAGEM. **Relatório Final**. 2013. Disponível em < <https://www12.senado.leg.br/noticias/arquivos/2014/04/04/integra-do-relatorio-de-ferraco>>. Acesso em 26 de outubro de 2020.

CRAIG, Anthony. **Understanding the proliferation of Cyber Capabilities**. Council on Foreign Relations. 2018. Disponível em < <https://l1nq.com/xLi4g> >. Acesso em 26 de outubro de 2020.

CUNHA, Gustavo. **A tokenização do dinheiro**: como blockchain, stablecoins, CBDB e o DREX mudaram o futuro. São Paulo: Actual: 2024.

CUNHA, Izabella Bauer de Assis; PEREIRA, Frederico Cesar Mafra; NEVES, Jorge Tadeu de R. Análise do fluxo informacional presente em uma empresa do segmento de serviços de valor agregado (SVA). **Perspectivas em Ciência da Informação**, [S.l.], v. 20, n. 4, p. 107-128, dez. 2015. ISSN 19815344. Disponível em: < <http://portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/2474/1681> >. Acesso em 10 de julho de 2022.

DA CRUZ, Samuel C. **A segurança e defesa cibernética no Brasil e uma revisão das estratégias dos Estados Unidos, Rússia e Índia para o espaço virtual**. Instituto de Pesquisa Econômica Aplicada. Rio de Janeiro. 2013. Disponível em < https://www.ipea.gov.br/portal/images/stories/PDFs/TDs/td_1850.pdf >. Acesso em 26 de outubro de 2020.

DALIO, Ray. **Princípios para a ordem mundial em transformação**: porque as nações prosperam e fracassam. Tradução Alexandre Raposo, Claudia Mello Belhassof, Jaime Biaggio. - 1ed.- Rio de Janeiro: Intrínseca, 2022.

DERTOUZOS, Michel. **O que será: como o novo mundo da informação transformará nossas vidas**. São Paulo: Companhia das Letras, 1997.

DESIDERÁ, Walter A. **Diagnóstico da Segurança Regional Sul-americana: Classificações teóricas preliminares**. Instituto de Pesquisa Econômica Aplicada. 2013. Disponível em < <https://l1nk.dev/2SdBz> >. Acesso em 22 de Junho de 2020.

DIZARD, Wilson P. **The coming information age**. New York: Longman, 1982.

DOD. **Organization and Management of the Department of Defense**. March 2019. Disponível em < <https://fas.org/irp/agency/dod/org-man.pdf> >. Acesso em 22 de Junho de 2020.

DUHIGG, Charles. **O poder do Hábito**. Porque fazemos o que fazemos na vida e nos negócios. Tradução Rafael Mantovani. 1ed. Rio de Janeiro: Objetiva. 2012.

DUNN, Myriam; EGLOFF, Florian. The Politics of Cybersecurity: Balancing Different Roles of the State. **St Antony's International Review** 15 no.1.p.37-57, 2019. Disponível em < <https://encr.pw/e2ut5> >. Acesso em 26 de junho de 2020.

EUROPEAN PARLIAMENT. **Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States**. Policy Department for Citizens' Rights and Constitutional Affairs. Directorate General for Internal Policies of the Union. PE 608.864 - February 2019. Disponível em < [http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU\(2019\)608864_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf) >. Acesso em 06 de novembro de 2020.

FALOUTSOS, Michalis; FALOUTSOS, Petros; FALOUTSOS, Christos. **On Power-Law Relationships of the Internet Topology**. 1999. Disponível em < <http://snap.stanford.edu/class/cs224w-readings/faloutsos99powerlaw.pdf> >. Acesso em 04 de novembro de 2020.

FEM. Forum Econômico Mundial. **The Global Risks Report 2018**. 13th Edition. ISBN 978-1-944835-15-6, 2018. Disponível em < http://www3.weforum.org/docs/WEF_GRR18_Report.pdf >. Acesso em 12 de Maio de 2020.

FOUCAULT, Michel. **Em defesa da sociedade: curso no College de France (1975-1976)**; tradução: Maria Ermantina de Almeida- 4ª Triagem. São Paulo: Editora WMF Martins Fontes, 2019.

FOUCAULT, Michel. **Nascimento da Biopolítica**. Com introdução de Bruno Mações. Edições 70, Fevereiro de 2020.

FOUCAULT, Michel. **Segurança, território e população**. Editora Martins Fontes, 2009.

FOSKETT, D. J. **Psicologia do usuário**. In: FOSKETT, D. J.; et al. A contribuição da psicologia para o estudo dos usuários da informação técnico-científica. Rio de Janeiro: Calunga, 1980. p.11-30.

FUKUYAMA, Francis. **The End of History?** In: The National Interest. Outubro de 1989, n.16, reproduzido in Tuathail, G. Dalby. S. E Routledge, P. The geopolitics reader. Op. Cit., p. 114-24.

GALISSON, R. & COSTE, D. **Dicionário de didáctica das línguas**. Coimbra: Livraria Almedina, 1983.

GARCÍA-MARCO, F. J. La pirámide de la información revisitada: enriqueciendo el modelo desde la ciencia cognitiva. **El profesional de la información**, v. 20, n. 1, 2011.

GCSCC. Global Cyber Security Capacity Centre. **Cybersecurity Capacity Maturity Model for Nations (CMM)**. Revised Edition. 2016. Oxford Martin School, University of Oxford, UK. Disponível em <https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20revised%20edition_09022017_1.pdf>. Acesso em 12 de Maio de 2020.

GEERTZ, Clifford. **A interpretação das culturas**. Rio de Janeiro: Zahar, 1978. 323p.

GEERTZ, Clifford. **Estar lá, escrever aqui**. *Diálogo*, p. 59-63, 1989.

GONZÁLEZ DE GÓMEZ, Maria Nélida. Novos cenários políticos para a informação. **Ci. Inf.**, Brasília, v. 31, n. 1, p. 27-40, jan./abr. 2002. Disponível em <<http://revista.ibict.br/ciinf/article/view/975/1013>>. Acesso em 22 de agosto de 2021.

GONZÁLEZ DE GÓMEZ, Maria Nélida. Regime de Informação: Construção de um Conceito. **Inf. & Soc.:Est.**, João Pessoa, v.22, n.3, p. 43-60, set./dez. 2012. Disponível em <https://www.brapci.inf.br/repositorio/2015/12/pdf_3c42553162_0000011948.pdf>. Acesso em 22 de agosto de 2021.

HARDIN, Garret. 'The Tragedy of the Commons'. 162 **Science**. 1968. Disponível em <<https://science.sciencemag.org/content/sci/162/3859/1243.full.pdf>>. Acesso em 12 de Maio de 2020.

HATHAWAY, Melissa. **Gestão do Risco Cibernético Nacional**. Organização de Estados Americanos (OEA). Washington, EEUU, 2018. Disponível em <<https://potomacinstitute.org/images/CRI/PORT-Digital-White-paper-Edicin-2.pdf>>. Acesso em 12 de Maio de 2020.

HAYEK, Friedrich. A. VON. O Uso do Conhecimento na Sociedade. **MISES: Interdisciplinary Journal of Philosophy, Law and Economics**, v. 1, n. 1, p. 153-162, 21 Feb. 2018. Disponível

em < <https://misesjournal.org.br/misesjournal/article/view/205>>. Acesso em 12 de Maio de 2020.

HILL, Richard. **A review of Robert W. McChesney, Digital Disconnect**: How Capitalism is turning the Internet against Democracy. The New Press, 2014. Disponível em <<http://www.boundary2.org/2015/04/the-internet-vs-democracy/#authorbio>>. Acesso em 12 de Maio de 2020.

HOWARD, Becker S. **Evidências**: Sobre o bom uso de dados em ciências sociais. Tradução Maria Luíza X. de A. Borges. 1ed. Rio de Janeiro: Zahar. 2022.

HUAMANI CUBA, A. C. H.; MOURA, M. A. Ecología Social de las Redes Sociales Digitales: caso Pishtacos de Huaycán, Lima. **Brazilian Journal of Information Science**: research trends, Marília, SP, v. 18, p. e024002, 2024. DOI: 10.36311/1981-1640.2024.v18.e024002. Disponível em < <https://revistas.marilia.unesp.br/index.php/bjis/article/view/15386> >. Acesso em: 7 fev. 2024.

HUAMANI CUBA, Arthur Christian; MOURA, Maria Aparecida. Política e Estratégias da Segurança Cibernética: Argentina, Peru e Brasil. **Revista Ibero-Americana de Ciência da Informação**, [S.l.], v. 17, n. 1, p. 115–141, 2024. DOI: 10.26512/rici.v17.n1.2024.51481. Disponível em: < <https://periodicos.unb.br/index.php/RICI/article/view/51481> >. Acesso em: 14 abr. 2024.

HUNTINGTON, Samuel P. **O choque de civilizações e a recomposição da ordem mundial**. Tradução de M. H. C. Côrtes. Rio de Janeiro: Objetiva, 2010.

INNERARITY, Daniel. ¿Quién manda aquí?, **diario El Correo**, p.20, 17 de agosto de 2011. Disponível em <<https://www.danielinnerarity.es/opinion-preblog-2017/qui%C3%A9n-manda-aqu%C3%AD/>>. Acesso em 12 de Maio de 2020.

JARDIM, José; SILVA, Sérgio; NHARRELUGA, Rafael. Análise de políticas públicas: uma abordagem em direção às políticas públicas de informação. **Perspectivas em Ciência da Informação**, v.14,n.1,p.2-22,jan./abr. 2009. Disponível em < <https://www.scielo.br/pdf/pci/v14n1/v14n1a02.pdf>>. Acesso em 12 de Maio de 2020.

JP1. **Doctrine for the Armed Forces of the United States**. United States. 2017. Disponível em < <https://fas.org/irp/doddir/dod/jp1.pdf> >. Acesso em 12 de Maio de 2020.

KOLTAY, Tibor. **The media and the literacies**: media literacy, information literacy, digital literacy. *Média, Culture & Society*, v. 33, n. 2, p. 211-221, 2011.

KRAMER, Franklin D.; STARR, Stuart H.; WENTZ, Larry K (Org). **Cyberpower and National Security**. 1st ed. Center Technology and National security Policy. Washington, EEUU, April 2009.

KUEHL, Daniel T. **From cyberspace to cyberpower**: defining the problem. In KRAMER, Franklin D.; STARR, Stuart H.; WENTZ, Larry K (Org). *Cyberpower and National Security*. 1st ed. Center Technology and National security Policy. Washington, EEUU, April, 2009.

KUTT, A. N. (2015). **La importancia de dominar los global commons en el siglo XXI**. Instituto Español de Estudios Estratégicos (IEEE), España. Disponível em < http://www.ieee.es/Galerias/fichero/docs_marco/2015/DIEEEM29-2015_Global_Commons_XXI_Alexander_Kutt.pdf >. Acesso em 06 de novembro de 2020.

LAVILLE, Christian; DIONNE, Jean. **A construção do saber. Manual de Metodologia da Pesquisa em Ciências Humanas**. Porto Alegre: Artes Médicas/Belo Horizonte: Editora UFMG, 1999.

LLORENS, Maria P. Os desafios do uso da força no ciberespaço. **Anuário de Direito Internacional**, vol XVII, 2017, pp. 785-816. D.F., México. Disponível em <<http://dx.doi.org/10.22201/ij.24487872e.2017.17.11052>>. Acesso em 06 de novembro de 2020.

LOJKINE, Jean. **A Revolução Informacional**. São Paulo: Cortez Editora, 1999.

LÓPEZ YEPES, José. (1995). **La documentación como disciplina: teoría e historia**. 2. ed. Pamplona: Ediciones Universidad de Navarra (EUNSA), 1995. Publicada originalmente em 1978 sob o título: Teoría de la documentación.

LUTTWAK, Edward N. **From Geopolitics to Geo-Economics**: Logic of conflict, grammar of commerce. The National Interest. n.20. Julho 1990. Disponível em <<https://www.jstor.org/stable/42894676?seq=1>>. Acesso em 06 de novembro de 2020.

LYNN, III, William F. **Defending a New Domain: The Pentagon's Cyberstrategy**. Foreign affairs (Council on Foreign Relations). 2010. Disponível em <<https://www.law.upenn.edu/live/files/6465-12-lynn-defending-a-new->>. Acesso em 22 de Junho de 2020.

MARTELETO, Regina Maria. **Cultura informacional**: construindo o objeto informação pelo emprego dos conceitos de imaginário, instituição e campo social. Departamento de Ensino e Pesquisa (DEP-RJ) **IBICT. Brasil**, 1995 Disponível em <<http://revista.ibict.br/ciinf/article/viewFile/613/615>>. Acesso em 06 de novembro de 2020.

MASUDA, Yonegi. **A sociedade da informação como sociedade pós-industrial**. Rio de Janeiro: Editora Rio, 1982.

MAZZUCATO, Mariana. **O Estado empreendedor**: desmascarando o mito do setor público vs. Setor privado. Tradução: Elvira Separicos. 1. Ed. São Paulo: Porfolio- Penguin. Editora Schwarcz S.A. 2021.

MCCHESENEY, Robert W. **Digital Disconnect**: How Capitalism Is Turning the Internet Against Democracy. New Press, 2014.

MÍGUEZ, María C. ¿Anticomunistas, antiestatistas, antiperonistas? La “nacionalización” de la doctrina de seguridad nacional em la Argentina y la legitimación del golpe de Estado de 1966. **Revista SAAP**. Vol. 7, Nº 1. p.65-95. 2013. Disponível em <<https://i1nq.com/W7bvt>>. Acesso em 06 de novembro de 2020.

MINDEF. **La política de seguridad y defensa nacional**. Viciministerio de políticas para a defensa. 2018. Disponível em <http://www.congreso.gob.pe/Docs/DGP/CCEP/files/agenda2017-2018/files/midef-la_pol%C3%ADtica_de_seguridad_y_def.nac_jorge_l._mendoza-conf._2_de_jul..pdf>. Acesso em 06 de novembro de 2020.

MOLINA, José. **Globalización, ciberespacio y estrategia especial consideración a la estrategia de la información**. 2014. Instituto Español de Estudios Estratégicos (IEEE), España. Disponible em <

https://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEE0100-2014_Globalizacion-Ciberseguridad-Estrategia_JMMolinaMateos.pdf>. Acesso em 06 de novembro de 2020.

MOTTA, Fernando. **Organização e poder: Empresa, estado e escola**. São Paulo: Editora Atlas S.A, 1986.

MULLER, Lilly Pijnenburg. **Cyber Security Capacity Building in Developing Countries: Challenge and Opportunities**. Norwegian Institute of International Affairs. NUPI Report no. 3, 2015. Disponível em < <https://cybilportal.org/wp-content/uploads/2020/06/NUPIReport03-15-Muller.pdf>>. Acesso em 21 de fevereiro de 2021.

MULLER, Pierre; SUREL, Yves. **A análise das políticas públicas**. Pelotas: Educat, 2004.

NASCIMENTO, L. C. N. et al. Theoretical saturation in qualitative research: an experience report in interview with schoolchildren. **Rev Bras Enferm [Internet]**. 2018;71(1):228-33. Disponível em <<http://dx.doi.org/10.1590/0034-7167-2016-0616>>. Acesso em 21 de fevereiro de 2021.

NASSER, Salem. **Relatório da CIA: a nova era**. Traduzido pelo Claudio Blanc. São Paulo: Geração Editorial, 2019.

NRC - NATIONAL RESEARCH COUNCIL. **Realizing the Information Future: The Internet and Beyond**. Washington, D.C.: National Academy Press, 1994. Disponível em < <http://www.nap.edu/catalog/4755/realizing-the-information-future-the-internet-and-beyond>>. Acesso em 15 de agosto de 2024.

OSJI. **Princípios globais sobre segurança nacional e o direito à informação**: os princípios de TSHWANE. África do Sul emitidos a 12 de Junho de 2013. Disponível em < <https://www.justiceinitiative.org/uploads/f9b3f146-c00d-4657-b412-140f2eb5a694/tshwane-portuguese-20150209.pdf>>. Acesso em 01 de abril de 2024.

ONGEI. **Gobierno Electrónico**: avances e desafios. 2015. Disponível em <https://sgp.pcm.gob.pe/wp-content/uploads/2015/10/CESAR_VILCHEZ_ONGEI.pdf>. Acesso em 06 de novembro de 2020.

OEA . **Estrategia Interamericana Integral para Combatir las Amenazas a la seguridad cibernética**, 2004. Disponível em < <https://www.sites.oas.org/cyber/Es/Paginas/default.aspx> >. Acesso em 16 de maio de 2020.

ONGEI. **Gobierno Electrónico**: avances e desafios. 2015. Disponível em < https://sgp.pcm.gob.pe/wp-content/uploads/2015/10/CESAR_VILCHEZ_ONGEI.pdf>. Acesso em 06 de novembro de 2020.

OPP. **Catálogo de Documentos 2005**. El Cuerpo de Administradores Gubernamentales, la perspectiva académica. Disponível em < https://www.argentina.gob.ar/sites/default/files/catalogo_2005_0.pdf>. Acesso em 06 de novembro de 2020.

OTTER, Thomas. CORTEZ, Mónica. **Economía de la Información, Sociedad de la Información, Información Periodística**: Elementos compartidos hacia una información pluralista y equitativa. Programa Medios de Comunicación y Democracia em América Latina. 2003. Disponível em < <https://l1nq.com/xFqBk> >. Acesso em 22 de junho de 2020.

PARDO, Arvid. 'Who Will Control the Seabed?', 47 *Foreign Affairs* (1968–1969) 123; 'Address to the American Society of International Law', 62 *ASIL Proceedings* (1968) 216; 'Sovereignty under the Sea', 58 *Commonwealth Journal of International Affairs* (1968) 341. Disponível em <https://www.jstor.org/stable/20039359?read-now=1&seq=1#page_scan_tab_contents>. Acesso em 22 de junho de 2020.

PERDIGÃO, Juliana A.; NASCIMENTO, Fabrício J. Informação simbólica, representações sociais e identidade: aproximações conceituais. **Em Questão**, vol. 25, núm. 1, 2019. Disponível em <<https://www.redalyc.org/jatsRepo/4656/465657930009/html/index.html>>. Acesso em 22 de setembro de 2020.

PEREIRA, L. D. A.; FALEIROS JÚNIOR, J. L. de M. Regulação das plataformas digitais no Brasil e a defesa da soberania nacional. **Revista de Ciências do Estado**, Belo Horizonte, v. 9, n. 1, p. 1–22, 2024. DOI: 10.35699/2525-8036.2024.52248. Disponível em <<https://periodicos.ufmg.br/index.php/revise/article/view/e52248>>. Acesso em 30 de setembro de 2024.

PILON, André Francisco. A visão profética da ecologia social. **Jornal da USP**. São Paulo, 12 a 18 de março de 2007. Disponível em: <<https://www.usp.br/jorusp/arquivo/2007/jusp793/pag02.htm>>. Acesso em 20 de junho de 2021.

Pohle, J., & Thiel, T. (2022). Soberanía digital. **Revista Latinoamericana de Economía Y Sociedad Digital**. Disponível em <<https://doi.org/10.53857/olmh2516>>. Acesso em: 20 de agosto de 2024.

POPA, Iulian F. **Cyber Geopolitics and sovereignty. An introductory overview**. The 5th International Scientific Conference National and International Security 2014. 2nd – 3rd October. © Akadémia ozbrojených síl generála Milana Rastislava Štefánika, 2014 pp.413-417. Disponível em <https://www.researchgate.net/publication/280095109_CYBER_GEOPOLITICS_AND_SOVEREIGNTY_AN_INTRODUCTORY_OVERVIEW>. Acesso em 22 de setembro de 2020.

POPPER, Karl. **A sociedade aberta e seus inimigos. Primeiro Volume**: O sortilegio de Platão. Prefácio de João Carlos Espada. Vol 1. Edições 70. Outubro de 2018.

RÄDIKER, Stefan; KUCKARTZ, Udo. **Análisis de datos cualitativos com MAXQDA**: Texto, Audio, Video. Translation from the German language edition: Interviews analysieren mit MAXQDA by Stefan Rädiker/Udo Kuckartz Copyright © Springer Fachmedien Wiesbaden 2019. All Rights Reserved. Disponível em <<https://doi.org/10.36192/978-3-948768003>>. Acesso em 27 de Fevereiro de 2021.

RANGANATHAN, Surabhi. **Global Commons**. The European Journal of International Law Vol. 27 no. 3 EJIL (2016), Vol. 27 No. 3, 693–717 doi:10.1093/ejil/chw037. 2016. Disponível em <https://www.researchgate.net/publication/303388443_Global_Commons>. Acesso em 12 de Maio de 2020.

RATTRAY, Gregory J. **An environmental approach to understanding cyberpower**. In KRAMER, Franklin D.; STARR, Stuart H.; WENTZ, Larry K (Org). *Cyberpower and National Security*. 1st ed. Center Technology and National security Policy. Washington, EEUU, April, 2009.

RODRIGUES DA SILVEIRA, Henrique F. **Um estudo do poder na sociedade da informação**. Ci. Inf., Brasília, v. 29, n. 3, p. 79-90, set./dez. 2000. Disponível em < <https://revista.ibict.br/ciinf/article/view/875/909>>. Acesso em 12 de maio de 2020.

RUIZ, Ariela. El proceso de privatizaciones en el Perú durante el período 1991-2002. Instituto Latinoamericano y del Caribe de Planificación Económica y Social – **ILPES. Santiago de Chile**, julio de 2002. Disponível em < <https://11nq.com/r2bWv>>. Acesso em 11 Nov 2021.

SANTAELLA, Lucia. **A ecologia pluralista da comunicação**: conectividade, mobilidade, ubiquidade / Lucia Santaella. – São Paulo: Paulus, 2010. - (Coleção Comunicação).

SANTOS JÚNIOR, Roberto Lopes. Análise sobre o desenvolvimento do campo de estudo em informação científica e técnica nos Estados Unidos e na antiga União Soviética durante a guerra fria (1945-1991). Revista Brasileira de Biblioteconomia e Documentação, São Paulo, v. 8, n. 2, p.130-157, jul. 2012. Disponível em < <https://rbbd.febab.org.br/rbbd/article/download/217/233>>. Acesso em 05 de julho de 2019.

SEDENA. **Proceso de formulación de la política de seguridad y defensa nacional**. 2015. Disponível em < https://www.minem.gob.pe/minem/archivos/file/institucional/defensa/Sedena_Politica_Seguridad_Defensa.pdf>. Acesso em 12 de maio de 2020.

SERAFIM, Lucas A.; FREIRE, Gustavo H. **Competências em informação na contemporaneidade**. RACIn, João Pessoa, v. 1, n. 1, p. 67-87 Jan.-Jun. 2013. Disponível em < <https://brapci.inf.br/index.php/res/download/98888>>. Acesso em 12 de maio de 2020.

SOARES, Lucas. Geopolítica do espaço cibernético e o poder: o exercício da soberania por meio do controle. **Rev. Bras. Est. Def.** v. 5, nº 1, jan./jun. 2018, p. 141-165. Disponível em < <https://rbed.abedef.org/rbed/article/view/75081>>. Acesso em 06 de Novembro de 2020.

STOECKER, R. Evaluating and rethinking the case study. **The sociological Review**, 39, 88-112, 1991.

TAKAHASHI, Tadao (Org.). **Sociedade da informação no Brasil**: Livro Verde. Brasília: Ministério da Ciência e Tecnologia, 2000.

TELEGEOGRAPHY. **Submarine Cable Frequently Asked Questions**. Submarine Cable 101 | The Map. Disponível em < <https://encl.pw/EXxtO>>. Acesso em 06 de abril de 2019.

THUROW, Lester C. **Cabeça a Cabeça**. A batalha econômica entre Japão, Europa e Estados Unidos. Rio de Janeiro: Rocco, 1993. p13 – 26.

UGARTE, José M. **La política de Defensa Argentina**. Estudios en Seguridad y Defensa, 13(26), 59 – 83. 2018. Disponível em <https://www.researchgate.net/publication/330486529_La_Politica_de_Defensa_Argentina>. Acesso em 06 de Novembro de 2020.

UNIDIR. **Cyber Policy Portal**. september 2020. Disponível em <<https://unidir.org/cpp/en/states/peru>>. Acesso em 06 de novembro de 2020.

VALERIANO-FERRER, Fernando. **Apuntes sobre Defensa Nacional**. Escuela Superior de Guerra Naval. Ed. 1ra. 2013. Disponível em <<https://hdl.handle.net/20.500.12927/28>>. Acesso em 06 de novembro de 2020.

VESENTINI, José William. **Novas Geopolíticas**. As representações do século XXI. 5 ed. 4ª reimpressão. São Paulo: contexto, 2016.

WARDLE, Claire; DERA KHSHAN Hossein. **Information disorder**: Toward an interdisciplinary framework for research and policy making. Council of Europe report DGI (2017)09. Disponível em <<https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-research/168076277c>>. Acesso em 04 de setembro de 2020.

WIENER, Norbert. **Cybernetics or control and communication in the animal and the machine**. 2.ed. Cambridge: MIT Press, 1965.

WOLFGANG, Kleinwächter. **Towards a holistic approach for internet related public policy making**. January, 2018. Disponível em <https://cyberstability.org/wp-content/uploads/2018/02/GCSC_Kleinwachter-Thought-Piece-2018-1.pdf>. Acesso em 12 de maio de 2020.

WOLTON, Dominique. **La otra mundialización**. Editorial Gedisa, S.A. Primera edición, febrero, Barcelona, España, 2004. Disponível em <[209807151-Wolton-Dominique-La-Otra-Mundializacion.pdf](https://www.archive.org/details/209807151-Wolton-Dominique-La-Otra-Mundializacion.pdf) (archive.org)>. Acesso em 04 de setembro de 2020.

YIN, Robert K. **Estudo de caso: planejamento e métodos** / Robert K. Yin; trad. Daniel Grassi ' 2. ed. - Porto Alegre: Bookman, 2001.

YIN, Robert K. **Estudo de caso: planejamento e métodos** / Robert K. Yin; trad. Cristhian Matheus Herrera '5. ed. - Porto Alegre: Bookman, 2015.

ZIMET, Elibu. SKOUDIS, Edward. **A graphical introduction to the structural elements of cyberspace**. In KRAMER, Franklin D.; STARR, Stuart H.; WENTZ, Larry K (Org). *Cyberpower and National Security*. 1st ed. Center Technology and National security Policy. Washington, EEUU, April, 2009.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. Tradução George Schlesinger. 1. ed. Rio de Janeiro: Intrínseca, 2020.

APÊNDICES

APÊNDICE I – Listagem bibliográfica dos documentos digitais utilizados na pesquisa, no âmbito da segurança e defesa nacional norte-americana:

âmbito	ID	NOME	ANO	Quantidade de vezes que citam as palavras: Internet	Quantidade de vezes que citam as palavras: Cyber	Quantidade de vezes que citam as palavras: Cyberspace	Quantidade de vezes que citam as palavras: Cybersecurity
1. Leis e Regulações Nacionais nos Estados Unidos no âmbito da Segurança e Defesa Nacional	LRN-001-EU	The National Security Act of 1947, as amended	1947	0	0	0	0
	LRN-002-EU	Titles 10 and 32, USC, as amended.	1956	0	0	0	0
	LRN-003-EU	Title 14, Coast Guard	2015	0	0	0	0
	LRN-004-EU	The Goldwater-Nichols Department of Defense Reorganization Act of 1986.	1986	0	0	0	0
	LRN-005-EU	Posse Comitatus Act (Title 18, USC, Section 1385).	2018	0	28	0	0
2. Política e Linhas de Ação Estratégica dos Estados Unidos no âmbito da Segurança e Defesa Nacional	PLA-001-EU	Organization and Management of the Department of Defense	2019	5	25	13	1
	PLA-002-EU	Joint Strategic Capabilities Plan FY 2018-2022	2018	2	3	5	4
	PLA-003-EU	The National Security Strategy of the United States.	2017	9	24	11	0
	PLA-004-EU	The National Defense Strategy of the United States.	2018	0	5	2	0
	PLA-005-EU	The National Military Strategy of the United States.	2018	0	0	1	0
	PLA-006-EU	National Strategy for Homeland Security.	2007	9	15	1	0
	PLA-007-EU	National Strategy for Combating Terrorism.	2020	6	6	0	1
	PLA-008-EU	National Strategy to Combat Weapons of Mass Destruction.	2002	0	0	0	0
	PLA-009-EU	Unified Command Plan.	2013	1	21	5	2
	PLA-010-EU	National Response Framework.	2019	1	14	0	7
	PLA-011-EU	DOD Strategy for Homeland Defense and Civil Support.	2005	0	1	6	0
	PLA-012-EU	National Cyber Strategy of the United States of América	2018	44	94	38	72
	PLA-013-EU	NATO National Cyber Security Organization: United States	2016	27	300	88	114
	PLA-014-EU	U.S. DEPARTMENT OF HOMELAND SECURITY CYBERSECURITY STRATEGY	2018	19	171	34	224
	PLA-015-EU	JP 1 - Doctrine for the Armed Forces of the United States	2017				
3. Publicações do Departamento da Defesa nos Estados Unidos	PDD-001-EU	DODD 1200.17, Managing the Reserve Components as an Operational Force.	2008	1	0	0	0
	PDD-002-EU	DODD 2000.12, DOD Antiterrorism (AT) Program.	2012	1	0	0	1
	PDD-003-EU	DODD 3000.06, Combat Support Agencies.	2016	0	0	0	0
	PDD-004-EU	DODD 3000.07, Irregular Warfare.	2008	1	0	0	0
	PDD-005-EU	DODD 3020.26, Department of Defense Continuity Programs.	2009	1	0	0	0
	PDD-006-EU	DODD 3020.40, DOD Policy and Responsibilities for Critical Infrastructure.	2012	1	5	0	1
	PDD-007-EU	DODD 3025.12, Military Assistance for Civil Disturbances.	1994	0	0	0	0
	PDD-008-EU	DODD 3025.18, Defense Support of Civil Authorities (DSCA).	2010	1	0	0	0
	PDD-009-EU	DODD 5100.01, Functions of the Department of Defense and its Major Components.	2010	1	1	11	0
	PDD-010-EU	DODD 5100.03, Support of the Headquarters of Combatant and Subordinate Unified Commands	2017	0	1	0	0
	PDD-011-EU	DODD 5100.20, National Security Agency/Central Security Service (NSA/CSS).	2010	1	2	0	1
	PDD-012-EU	DODD 5101.1, DOD Executive Agent.	2003	0	0	0	0
	PDD-013-EU	DODD 5105.19, Defense Information Systems Agency (DISA).	2006	3	0	0	0
	PDD-014-EU	DODD 5105.21, Defense Intelligence Agency (DIA).	2008	1	0	0	0
	PDD-015-EU	DODD 5105.22, Defense Logistics Agency (DLA).	2017	0	0	0	0
	PDD-016-EU	DODD 5105.77, National Guard Bureau (NGB).	2015	1	0	0	0
	PDD-017-EU	DODD 5106.4, Combatant Command Inspectors General.	2006	0	0	0	0
	PDD-018-EU	DODI 1215.06, Uniform Reserve, Training, and Retirement Categories.	2015	0	0	0	0
	PDD-019-EU	DODI 3000.05, Stability Operations.	2017	0	0	0	0
	PDD-020-EU	DODI 4000.19, Interservice and Intragovernmental Support.	2018	0	0	0	0

PDD-021-EU	CJCSI 1800.01F, Officer Professional Military Education Policy (OPMEP).	2020	1	0	14	0
PDD-022-EU	CJCSI 1805.01B, Enlisted Professional Military Education Policy.	2015	1	2	0	0
PDD-023-EU	CJCSI 3100.01D, Joint Strategic Planning System.	2018	1	4	1	0
PDD-024-EU	CJCSI 3405.01, Chairman's Total Force Fitness Framework.	2013	1	0	0	0
PDD-025-EU	CJCSI 5120.02D, Joint Doctrine Development System.	2015	1	0	0	0
PDD-026-EU	CJCSI 5715.01C, Joint Staff Participation in Interagency Affairs.	2014	1	1	1	0
PDD-027-EU	CJCSM 3122.01A, Joint Operation Planning and Execution System (JOPEs), Volume I (Planning Policies and Procedures).	2001	3	0	0	0
PDD-028-EU	CJCSM 3500.03C, Joint Training Manual for the Armed Forces of the United States.	2011	11	3	0	0
PDD-029-EU	JP 1-0, Joint Personnel Support.	2016	9	0	0	0
PDD-030-EU	JP 1-02, Department of Defense Dictionary of Military and Associated Terms.	2020	9	13	50	3
PDD-031-EU	JP 1-04, Legal Support to Military Operations.	2016	2	1	11	0
PDD-032-EU	JP 1-05, Religious Affairs in Joint Operations.	2018	1	0	0	0
PDD-033-EU	JP 2-0, Joint Intelligence.	2013	5	0	1	0
PDD-034-EU	JP 3-0, Joint Operations.	2018	2	5	89	11
PDD-035-EU	JP 3-05, Special Operations.	2014	2	1	28	5
PDD-036-EU	JP 3-07.2, Antiterrorism.	2010	13	0	3	0
PDD-037-EU	JP 3-08 Interorganizational Cooperation	2017	6	0	26	5
PDD-038-EU	JP 3-13, Information Operations.	2014	3	1	15	0
PDD-039-EU	JP 3-13.2, Military Information Support Operations.	2011	3	0	1	0
PDD-040-EU	JP 3-16, Multinational Operations.	2019	10	0	37	1
PDD-041-EU	JP 3-27, Homeland Defense.	2018	1	22	63	10
PDD-042-EU	JP 3-28, Defense Support of Civil Authorities.	2018	0	14	33	3
PDD-043-EU	JP 3-30 Joint Air Operations	2019	0	5	26	2
PDD-044-EU	JP 3-31 Joint Land Operations	2019	0	3	53	2
PDD-045-EU	JP 3-32 Joint Maritime Operations	2018	0	2	22	0
PDD-046-EU	JP 3-33, Joint Task Force Headquarters.	2018	10	5	53	18
PDD-047-EU	JP 3-57, Civil-Military Operations.	2018	1	1	3	0
PDD-048-EU	JP 3-61, Public Affairs.	2016	36	0	0	1
PDD-049-EU	JP 4-0, Joint Logistics.	2019	1	1	5	0
PDD-050-EU	JP 5-0, Joint Operation Planning.	2017	1	1	23	1
PDD-051-EU	JP 6-0, Joint Communications System.	2019	16	12	122	16

Listagem bibliográfica dos documentos digitais utilizados na pesquisa, no âmbito da doutrina militar conjunta, relacionada com a **segurança e defesa cibernética norte-americana**:

DSN	SERIES	ID	Doutrina que é da SERIE	ANO	Quantidade de vezes que citam as palavras: Internet	Quantidade de vezes que citam as palavras: Cyber	Quantidade de vezes que citam as palavras: Cyberspace	Quantidade de vezes que citam as palavras: Cybersecurity
Doutrinas com palavras chaves: Internet - Cyber - Cyberspace - Cybersecurity	JP 1-0 Joint Personnel Support (PESSOAL)	JP1-045	SERIE	2016	9	0	0	0
		JP1-049	SERIE	2013	5	0	1	0
	JP 2-0 Joint Intelligence (inteligência)	JP1-068	JP 2-01 Joint and National Intelligence Support to Military Operations	2017	9	7	39	2
		JP1-069	JP 2-03 Geospatial Intelligence in Joint Operations	2017	5	0	5	2
	JP 3-0 Joint Operations (OPERAÇÕES)	JP1-050	SERIE	2018	2	16	89	11
		JP1-070	JP 3-03 Joint Interdiction	2016	0	0	13	1
		JP1-051	JP 3-05 Special Operations	2014	2	1	29	5
		JP1-071	JP 3-06 Joint Urban Operations	2013	6	0	5	0
		JP1-072	JP 3-07 Stability	2016	4	0	2	0
		JP1-053	JP 3-08 Interorganizational Cooperation	2017	6	0	26	5
		JP1-073	JP 3-09 Joint Fire Support	2019	0	2	49	0
		JP1-074	JP 3-10 Joint Security Operations in Theater	2019	0	0	13	2
		JP1-075	JP 3-12 Cyberspace Operations	2018	24	181	905	34
		JP1-054	JP 3-13 Information Operations	2014	3	1	16	0
		JP1-076	JP 3-14 Space Operations	2018	0	8	30	6
		JP1-056	JP 3-16 Multinational Operations	2019	10	0	37	1
		JP1-077	JP 3-18 Joint Forcible Entry Operations	2018	1	1	17	0
		JP1-078	JP 3-22 Foreign Internal Defense	2018	0	0	1	2
		JP1-079	JP 3-25 Countering Threat Networks	2016	7	0	11	1
		JP1-080	JP 3-26 Counterterrorism	2014	3	0	13	0
		JP1-057	JP 3-27 Homeland Defense	2018	1	41	64	11
		JP1-058	JP 3-28 Defense Support of Civil Authorities	2018	0	14	33	3
		JP1-059	JP 3-30 Joint Air Operations	2019	0	12	27	2

		JP1-060 JP 3-31 Joint Land Operations	2019	0	7	53	2
		JP1-061 JP 3-32 Joint Maritime Operations	2018	0	7	22	0
		JP1-062 JP 3-33 Joint Task Force Headquarters	2018	10	21	53	10
		JP1-081 JP 3-40 Joint Countering Weapons of Mass Destruction	2019	2	6	9	0
		JP1-082 JP 3-52 Joint Airspace Control	2014	1	0	4	3
		JP1-063 JP 3-57 Civil-Military Operations	2018	1	1	3	0
		JP1-083 JP 3-84 Legal Support	2016	2	1	11	0
	JP 4-0 Joint Logistics (LOGISTICA)	JP1-065 SERIE	2019	1	1	5	0
		JP1-084 JP 4-05 Joint Mobilization Planning	2018	1	0	0	0
	JP 5-0 Joint Planning (PLANOS)	JP1-066 SERIE	2017	1	1	25	1
	JP 6-0 Joint Communications System (SISTEMAS DE COMUNICAÇÕES)	JP1-067 SERIE	2019	16	43	125	16
		JP1-085 JP 6-01 Joint Electromagnetic Spectrum Management Operations	2012	0	8	7	0

APÉNDICE II – Listagem bibliográfica dos documentos digitais utilizados na pesquisa, no âmbito da segurança e defesa cibernética da Argentina.

ÂMBITO	ID	NOME	ANO
1. Leis e Regulações Nacionais em ARGENTINA	LRN-001-AR	Ley 26.388 de Delito informático	2008
	LRN-002-AR	Ley 25.326 de Protección de Datos Personales	2020
	LRN-003-AR	Ley 25.506 de Firma Digital	2001
	LRN-004-AR	Ley 26.904 de Grooming	2013
	LRN-005-AR	Ley 27.126 de inteligencia Nacional	2015
2. Política e Linhas de Ação Estratégica em ARGENTINA	PLA-001-AR	Resolución 144 / 2020, MINISTERIO DE SEGURIDAD, PROTOCOLO GENERAL PARA LA PREVENCION POLICIAL DEL DELITO CON USO DE FUENTES DIGITALES ABIERTAS	2020
	PLA-002-AR	Resolución 977 / 2019 MINISTERIO DE SEGURIDAD, PLAN FEDERAL DE PREVENCION DE DELITOS TECNOLOGICOS Y CIBERDELITOS	2019
	PLA-003-AR	Decreto 684 / 2019 PODER EJECUTIVO NACIONAL (P.E.N.), ADMINISTRACION NACIONAL ESTRUCTURA - MODIFICACION	2019
	PLA-004-AR	Resolución 1523 / 2019 SECRETARIA DE GOBIERNO DE MODERNIZACION, DEFINICION DE INFRAESTRUCTURAS CRITICAS	2019
	PLA-005-AR	Resolución 829 / 2019 SECRETARIA DE GOBIERNO DE MODERNIZACION ESTRATEGIA NACIONAL DE CIBERSEGURIDAD - APROBACION	2019
	PLA-006-AR	Decreto 996 / 2018 PODER EJECUTIVO NACIONAL (P.E.N), AGENDA DIGITAL ARGENTINA BASES - APRUEBANSE	2018
	PLA-007-AR	Disposición E 1 / 2018 OFICINA NACIONAL DE TECNOLOGIAS DE INFORMACION, ESTANDARES TECNOLOGICOS PARA LA ADMINISTRACION PUBLICA NACIONAL - APROBACION	2018
	PLA-008-AR	Resolución E 1107 / 2017 MINISTERIO DE SEGURIDAD, COMITE DE RESPUESTA DE INCIDENTES DE SEGURIDAD INFORMATICA - CONFORMESE	2017
	PLA-009-AR	Decreto 577 / 2017 PODER EJECUTIVO NACIONAL (P.E.N.), COMITE DE CIBERSEGURIDAD.	2017
	PLA-010-AR	Decreto 170 / 2017 PODER EJECUTIVO NACIONAL (P.E.N.), ADMINISTRACION PUBLICA NACIONAL CONFORMACION ORGANIZATIVA DEL MINISTERIO DE MODERNIZACION	2017
	PLA-011-AR	Resolución E 399 / 2016 MINISTERIO DE MODERNIZACION, Firma Digital	2016
	PLA-012-AR	Decisión Administrativa 232 / 2016 JEFATURA DE GABINETE DE MINISTROS, MINISTERIO DE MODERNIZACION ESTRUCTURA ORGANIZATIVA - APROBACION	2016
	PLA-013-AR	Disposición 1 / 2015 OFICINA NACIONAL DE TECNOLOGIAS DE INFORMACION, POLITICA DE SEGURIDAD DE LA INFORMACION MODELO - APROBACION	2015
	PLA-014-AR	Decisión Administrativa 927 / 2014 JEFATURA DE GABINETE DE MINISTROS, FIRMA DIGITAL CERTIFICACIONES DIGITALES	2014
	PLA-015-AR	Disposición 2 / 2013 OFICINA NACIONAL DE TECNOLOGIAS DE INFORMACION, GRUPO DE TRABAJO ICIC - CERT - CREACION	2013
	PLA-016-AR	Resolución 580 / 2011 JEFATURA DE GABINETE DE MINISTROS, PROGRAMA NACIONAL DE INFRAESTRUCTURAS CRITICAS DE INFORMACION Y CIBERSEGURIDAD - CREACION	2011
	PLA-017-AR	Decreto Reglamentario N° 1558/2001. Apruébase la reglamentación de la Ley N° 25.326. Principios generales relativos a la protección de datos. Derechos de los titulares de los datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones.	2001
	PLA-018-AR	Decreto Reglamentario N° 2628/2002. Reglamentación de la Ley N° 25.506. Consideraciones Generales. Autoridad de Aplicación. Comisión Asesora para la Infraestructura de Firma Digital. Ente Administrador de Firma Digital. Sistema de Auditoría. Estándares Tecnológicos. Revocación de Certificados Digitales. Certificadores Licenciados. Autoridades de Registro. Disposiciones para la Administración Pública Nacional.	2002
	PLA-019-AR	Decreto 898/2016 – Misiones y funciones de la Subsecretaría de Tecnología y Ciberseguridad (actualiza decreto anterior)	2016
	PLA-020-AR	Resolución N° 490 E/2016 – Aprueba Aperturas Inferiores de la Subsecretaría de Tecnología y Ciberseguridad	2016
	PLA-021-AR	Decisión Administrativa N° 669/2004 – Establece la obligatoriedad para los organismos públicos nacionales de contar con una Política de Seguridad de la Información, de asignar responsabilidades en Seguridad y de tener un Comité de Seguridad	2004
	PLA-022-AR	Resolución N° 69/2016 – Creación del Programa Nacional sobre Criminalidad Informática en el ámbito del Ministerio de Justicia	2016
	PLA-023-AR	Decreto N° 480/2019 – Amplia el Comité de Ciberseguridad para integrar a los ministerios de Relaciones Exteriores y Culto y de Justicia y Derechos Humanos y a la Secretaría de Asuntos Estratégicos de la Jefatura de Gabinete de Ministros	2019
	PLA-024-AR	Resolución SGM N° 829/2019 de la Secretaría de Gobierno de Modernización – Aprueba la Estrategia Nacional de Ciberseguridad y crea la Unidad Ejecutiva del Comité de Ciberseguridad en la órbita de la Secretaría de Gobierno de Modernización	2019
	PLA-025-AR	Decreto 378/2005. PLAN NACIONAL DE GOBIERNO ELECTRONICO Y PLANES SECTORIALES DE GOBIERNO ELECTRONICO	2005
	PLA-026-AR	Decreto 87/2017. Plataforma digital del sector público nacional.	2017
	PLA-027-AR	Decreto 1028/2003. Disuélvase el Ente Administrador de Firma Digital, creado por el artículo 11 del Decreto N° 2628/ 2002, cuyo accionar será llevado a cabo por la Oficina Nacional de Tecnologías de Información de la Subsecretaría de la Gestión Pública.	2003
3. Publicações do Departamento da Defesa em ARGENTINA	PDD-001-AR	Resolución 1380/2019 RESOL-2019-1380-APN-MD, CENTRO NACIONAL DE CIBERDEFENSA - CREASE	2019
	PDD-002-AR	Decreto 703 / 2018 PODER EJECUTIVO NACIONAL (P.E.N.), DIRECTIVA DE POLÍTICA DE DEFENSA NACIONAL - APRUEBASE	2018
	PDD-003-AR	Decreto 2645 / 2014 PODER EJECUTIVO NACIONAL (P.E.N.), DIRECTIVA DE POLÍTICA DE DEFENSA NACIONAL - ACTUALIZACION	2014
	PDD-004-AR	Decreto 13/2016 – Estructura del Ministerio de Modernización y del Ministerio de Defensa	2016
	PDD-005-AR	Resolución JGM N° 580/2011 – Crea el Programa Nacional de Protección de Infraestructuras Críticas de Información y Ciberseguridad	2011
	PDD-006-AR	Decreto N° 42/2016 – Crea la Subsecretaría de Ciberdefensa en el ámbito del Ministerio de Defensa	2016
	PDD-007-AR	Decreto 1311/2015. Apruébase la Nueva Doctrina de inteligencia Nacional.	2015

APÊNDICE III – Listagem bibliográfica dos documentos digitais utilizados na pesquisa, no âmbito da segurança e defesa cibernética do Peru.

ÂMBITO	ID	NOME	ANO
1. Leis e Regulações Nacionais em PERU	LRN-001-PE	Ley N° 27658: Ley Marco de Modernización de la Gestión del Estado.	2002
	LRN-002-PE	Ley N° 27806: Ley Transparencia y Acceso a la Información Pública.	2002
	LRN-003-PE	Ley N° 27269: Ley de Firmas y Certificados Digitales.	2008
	LRN-004-PE	Ley N° 27291: Ley que modifica el código civil permitiendo la utilización de los medios electrónicos para la comunicación de la manifestación de voluntad y la utilización de la firma electrónica.	2000
	LRN-005-PE	Ley N° 28493: Ley que regula el uso del Correo Electrónico comercial no solicitado (SPAM).	2005
	LRN-006-PE	Ley N° 29733: Ley de Protección de Datos Personales.	2011
	LRN-007-PE	Ley N° 28530: Ley de Promoción de Acceso a Internet para personas con discapacidad y adecuación del espacio físico en cabinas públicas de internet.	2012
	LRN-008-PE	Ley N° 30096 y su modificatoria Ley 30171: Ley de Delitos Informáticos.	2013
	LRN-009-PE	Ley N° 30618, Ley que modifica el Decreto Legislativo 1141, decreto legislativo de fortalecimiento y modernización del sistema de inteligencia nacional - sina y de la dirección nacional de inteligencia - DINI, a fin de regular la seguridad digital.	2017
	LRN-010-PE	Ley 29904: LEY DE PROMOCIÓN DE LA BANDA ANCHA Y CONSTRUCCIÓN DE LA RED DORSAL NACIONAL DE FIBRA ÓPTICA.	2012
2. Política e Linhas de Ação Estratégica em PERU	LRN-011-PE	Ley 29985. Ley que regula el uso del Dinero Electrónico como Instrumento de inclusión financiera.	2013
	LRN-012-PE	Ley 30035. Ley que regula el Repositorio Nacional Digital de Ciencia, Tecnología e Innovación de Acceso Abierto.	2013
	LRN-013-PE	Ley N° 30036. LEY QUE REGULA EL TELETRABAJO.	2013
	PLA-001-PE	Resolución Ministerial N° 166-2017-PCM, que modifica el artículo 5 de la R.M. N° 004- 2016-PCM referente al Comité de Gestión de Seguridad de la Información.	2017
	PLA-002-PE	Decreto Legislativo n° 1412, Ley de gobierno digital.	2018
	PLA-003-PE	Política Nacional de Ciberseguridad.	2017
	PLA-004-PE	Lineamientos para la formulación del Plan de Gobierno Digital.	2018
	PLA-005-PE	Resolución Ministerial N° 119-2018-PCM, Resolución de creación del Comité de Gobierno Digital.	2018
	PLA-006-PE	Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "ISO NTP/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.	2016
	PLA-007-PE	Resolución Ministerial N° 197-2011-PCM, que establece fecha límite para que diversas entidades de la Administración Pública implementen el plan de seguridad de la información dispuesto en la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de Buenas Prácticas para la Gestión de la Seguridad de la Información".	2011
	PLA-008-PE	Resolución Ministerial N° 246-2007-PCM, que aprueba la Norma Técnica Peruana "NTPISO/ IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2a. Edición" en todas las entidades integrantes del Sistema Nacional de Informática.	2007
	PLA-009-PE	Decreto Legislativo N° 1353, que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el régimen de protección de datos personales y la regulación de la gestión de intereses.	2017
	PLA-010-PE	Decreto Supremo N° 066-2011-PCM: Aprueba el "Plan de Desarrollo de la Sociedad de la Información en el Perú – La Agenda Digital Peruana 2.0"	2011
	PLA-011-PE	Decreto Supremo N° 004-2013-PCM: Aprueba la Política Nacional de Modernización de la Gestión Pública.	2013
	PLA-012-PE	Decreto Supremo N° 081-2013-PCM: Aprueba la Política Nacional de Gobierno Electrónico 2013-2017.	2013
	PLA-013-PE	Resolución Ministerial N° 179-2004-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 12207:2004 Tecnología de la Información. "Procesos del Ciclo de Vida del Software, 1ª Edición" en entidades del Sistema Nacional de Informática.	2004
	PLA-014-PE	Decreto Supremo N° 072-2003-PCM. Aprueban el Reglamento de la Ley de Transparencia y Acceso a la Información Pública.	2003
	PLA-015-PE	Decreto Supremo N° 050-2018-PCM. Aprueban la definición de Seguridad Digital en el Ámbito Nacional.	2018
3. Publicações do Departamento de Defesa em PERU	PLA-016-PE	Decreto Supremo N° 014-2013-MTC. Reglamento de la Ley N° 29904, Ley de Promoción de la Banda Ancha y Construcción de la Red Dorsal Nacional de Fibra Óptica.	2013
	PLA-017-PE	Resolución Ministerial N° 179-2004-PCM. Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información.	2012
	PLA-018-PE	Resolución Ministerial N° 179-2004-PCM. Aprueban lineamientos y mecanismos para implementar la interconexión de equipos de procesamiento electrónico de información entre las entidades del Estado.	2008
	PDD-001-PE	Proyecto de Ley 4228 de ciberdefensa.	2018
	PDD-002-PE	Decreto Legislativo N° 1141, Fortalecimiento y Modernización del Sistema de inteligencia Nacional - SINA y de la Dirección Nacional de inteligencia - DINI.	2012
	PDD-003-PE	Resolución DIN N° 033-DINI-2020-01, Norma técnica para protección de activos nacionales.	2020
	PDD-004-PE	Decreto Supremo N° 106-2017-PCM, Reglamento para la Identificación, Evaluación y Gestión de Riesgos de los Activos Críticos Nacionales (ACN).	2017
	PDD-005-PE	Decreto Supremo N° 012-2017-DE. Decreto Supremo que aprueba la Política de Seguridad y Defensa Nacional.	2017

APÊNDICE IV – Listagem bibliográfica dos documentos digitais utilizados na pesquisa, no âmbito da segurança e defesa cibernética o Brasil.

âmbito	ID	NOME	ANO
1. Leis e Regulações Nacionais em BRASIL	LRN-001-BR	Lei nº 12.965, Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.	2014
	LRN-002-BR	Lei nº 13.709, Lei Geral de Proteção de Dados Pessoais (LGPD).	2018
	LRN-003-BR	Lei nº 12.737, dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.	2012
	LRN-004-BR	Lei nº 12.735, altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências.	2012
	LRN-005-BR	Lei 12.527, Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências.	2011
	LRN-006-BR	Lei Nº 13.844, estabelece a organização básica dos órgãos da Presidência da República e dos Ministérios;	2019
2. Política e Linhas de Ação Estratégica em BRASIL	PLA-001-BR	Estratégia de Segurança da Informação e Comunicações e de Segurança cibernética da Administração Pública Federal, 2015-2018. Versão 1.0.	2015
	PLA-002-BR	DECRETO Nº 9.637, Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional.	2018
	PLA-003-BR	DECRETO Nº 10.222, Aprova a Estratégia Nacional de Segurança Cibernética.	2020
	PLA-004-BR	Gabinete de Segurança Institucional da Presidência da República. Portaria nº 93, de 26 de setembro de 2019. Aprova o Glossário de Segurança da Informação.	2019
	PLA-005-BR	Estratégia Brasileira para a Transformação Digital (E-Digital). Ministério da Ciência, Tecnologia, Inovações e Comunicações. MCTIC.	2018
	PLA-006-BR	DECRETO Nº 9.203, Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional.	2017
	PLA-007-BR	CONGRESSO NACIONAL. Senado Federal. Comissão Parlamentar de Inquérito. CPI da Espionagem.	2013
	PLA-008-BR	DECRETO Nº 9.573, Aprova a Política Nacional de Segurança de Infraestruturas Críticas.	2018
	PLA-009-BR	Banco Central do Brasil. Resolução nº 4.658, dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.	2018
	PLA-010-BR	Banco Central do Brasil. Circular nº 3.909, dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições de pagamento autorizadas a funcionar pelo Banco Central do Brasil.	2018
	PLA-011-BR	Instrução Normativa GSI/PR nº 1, de 13 de junho de 200	2008
	PLA-012-BR	DECRETO Nº 9.832, Altera o Decreto nº 9.637, de 26 de dezembro de 2018, e o Decreto nº 7.845, de 14 de novembro de 2012, para dispor sobre o Comitê Gestor da Segurança da Informação.	2019
	PLA-013-BR	DECRETO Nº 7.845, Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.	2012
	PLA-014-BR	Instrução Normativa nº 1 DSIC/GSIPR/2008 - Disciplina a Gestão de Segurança da Informação e Comunicações na APF.	2008
	PLA-015-BR	Instrução Normativa GSI Nº 1, de 27/05/2020. Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.	2020
	PLA-016-BR	NC Nº 04/IN01/DSIC/GSIPR - Gestão de Riscos de Segurança da Informação e Comunicações na APF	2013
	PLA-017-BR	NC Nº 05/IN01/DSIC/GSIPR - Criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais na APF	2009
	PLA-018-BR	Livro Verde Segurança Cibernética no Brasil (organizado e lançado pelo GSI/PR) - visa expressar potenciais diretrizes estratégicas para o estabelecimento da Política Nacional de Segurança Cibernética;	2010
	PLA-019-BR	NC Nº 06/IN01/DSIC/GSIPR – Gestão de Continuidade de Negócios na APF	2009
	PLA-020-BR	GUIA DE REFERÊNCIA PARA A SEGURANÇA DAS INFRAESTRUTURAS CRÍTICAS DA INFORMAÇÃO Versão 01 – nov./2010	2010
	PLA-021-BR	Acórdão Nº 3051 TCU-Plenário – aponta a ausência de um planejamento estratégico do Estado brasileiro que reúna e coordene ações dos diversos atores responsáveis por assuntos ligados à Segurança da Informação	2014
	PLA-022-BR	CPI DA ESPIONAGEM RELATÓRIO FINAL	2013
	PLA-023-BR	CPI de Crimes Cibernéticos (Câmara dos Deputados) – Indicação Parlamentar Nº 2238 propõe ao GSI/PR que elabore proposta de Política Nacional de Segurança da Informação	2016
3. Publicações do Departamento da Defesa em BRASIL	PDD-001-BR	DECRETO Nº 2.295, Regulamenta o disposto no art. 24, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional.	1997
	PDD-002-BR	Manual de Campanha Guerra Cibernética	2017
	PDD-003-BR	Livro Branco de Defesa Nacional, Brasil 2020	2020
	PDD-004-BR	Doutrina Militar de Defesa Cibernética MD31-M07	2014

APÊNDICE V – Listagem de Códigos e Subcódigos do caso Protótipo norte-americano.

CÓDIGOS	SUBCÓDIGOS
Bureaucracy is vast and complicated	Enrolment to the programme has been slow
Centralized purchase	Focusing government purchasing
Centralized purchase	Government play rol in accelerating the process of ITC
Centralized purchase	Plan for consolidating data centres
Centralized purchase	Reimbursable
Centralized purchase	Understand the interdependencies
Cost-effectiveness	Cyber security is a complicated task
Cost-effectiveness	Engagement efforts
Cost-effectiveness	Ensure force rebalancing
Cost-effectiveness	Funding for cyberspace operations increased
Cost-effectiveness	Global engagement
Cost-effectiveness	High-level requirements
Cost-effectiveness	Highly complex
Cost-effectiveness	Increase investment in cyber capabilities
Cost-effectiveness	Increase survivability and maintain uninterrupted capability
Cost-effectiveness	Invest in technical resources
Cost-effectiveness	Key initiatives for broadband providers
Cost-effectiveness	Maximize the use of technological solutions to provide information
Cost-effectiveness	Observed a lack of clarity on responsibility
Cost-effectiveness	Prioritised investments that support national interest
Cost-effectiveness	Properly allocate resources and prioritize efforts
Cost-effectiveness	Regularly adjusts program and policy efforts
Cost-effectiveness	Resources are optimized to meet priorities
Cost-effectiveness	Review and evaluate the effectiveness
Cost-effectiveness	Supporting ongoing investments in the defense
Cost-effectiveness	Uses existing systems, infrastructure, and services
Cyber capabilities	Achieved full operational capability
Cyber capabilities	Align Component programs
Cyber capabilities	Build and maintain ready forces
Cyber capabilities	Capabilities and strategic
Cyber capabilities	Capabilities Integration and Development System
Cyber capabilities	Capabilities to conduct cyberspace operations
Cyber capabilities	Capability to fight through a degraded environment
Cyber capabilities	Collaboration capacities
Cyber capabilities	Communications capabilities
Cyber capabilities	Competitiveness
Cyber capabilities	Created to enhance the resiliency of Defence
Cyber capabilities	Cyber warfare programme
Cyber capabilities	Deploy centralized capabilities
Cyber capabilities	Developing a response system
Cyber capabilities	Developing deterrence strategies
Cyber capabilities	Empower stakeholders
Cyber capabilities	Enhancing the ability to respond quickly
Cyber capabilities	Exercise cyber incident response plans
Cyber capabilities	Expanded full-spectrum cyberspace capabilities
Cyber capabilities	Exploitation of vulnerabilities
Cyber capabilities	Forensic capabilities, research and development efforts
Cyber capabilities	Highly skilled cybersecurity
Cyber capabilities	Identify and responses

Cyber capabilities	Identify gaps
Cyber capabilities	Improve cybersecurity
Cyber capabilities	Improving ability to attribute and defeat attacks or supporting
Cyber capabilities	Interdisciplinary activities in to cyber domain
Cyber capabilities	Mature cybersecurity
Cyber capabilities	Misconfigurations in software or hardware
Cyber capabilities	Mission capability
Cyber capabilities	National Initiative for Cybersecurity Education
Cyber capabilities	Operational capability building for the protection
Cyber capabilities	Re-skilling people and workforce
Cyber capabilities	Strengthen cybersecurity
Cyber capabilities	Talent pool and cyber education
Cyber capabilities	Technical capability to ^{CF} _{SEP} assist
Cyber capabilities	Test and exercise continuity plans
Cyber capabilities	Training programme for cyber security and emerging techonologies
Cyber capabilities	Vulnerability reduction
Cyber defense	Conduct effective operations in cyberspace
Cyber defense	Conduct international policy planning
Cyber defense	Continuity information system
Cyber defense	Control conflict escalation and conflict environment
Cyber defense	Control response and system coordination
Cyber defense	Cyber aspects of crisis, defence of homeland
Cyber defense	Cyber intelligence and Share threat information
Cyber defense	Defence against cyber attacks
Cyber defense	Defence and counter-intelligence
Cyber defense	Defence and intelligence systems
Cyber defense	Defend defense information network
Cyber defense	Defend the Nation from cyberattack on vital interests
Cyber defense	Disinformation and propaganda
Cyber defense	Evaluate and provide defence support to civil agencies
Cyber defense	Focuses primarily on abstract goals for the military such as defending networks and enhancing resiliency
Cyber defense	Gathering foreign cyber threat information
Cyber defense	Incursions into government networks
Cyber defense	Information exchange and reduce barriers to coordination
Cyber defense	Information systems of DoD and IC
Cyber defense	Investigating cybercrimes under military jurisdiction
Cyber defense	Monitoring and Information operations
Cyber defense	National defense strategy
Cyber defense	National Military Strategy for Cyberspace Operations
Cyber defense	Safeguarding the global information infrastructure
Cyber defense	Securing national security and military systems
Cyber defense	Threat reduction from cyber criminals
Cyber defense	US military's approach to cyberspace operations
Cyber industries	Adoption cybersecurity best practices and standards
Cyber industries	Companies to take steps to enhance cyber security
Cyber industries	Cybersecurity innovation worldwide
Cyber industries	Deepen technical collaboration
Cyber industries	Defence Industrial Base
Cyber industries	Defense intelligence enterprise
Cyber industries	Developing security standards
Cyber industries	Developing solutions
Cyber industries	Develops and improve platforms and mechanisms for the Defense
Cyber industries	Emerging technologies and next-generation ITC
Cyber industries	Foster a global intellectual property rights system

Cyber industries	Fostering strong domestic innovation
Cyber industries	Improving research coordination
Cyber industries	In-house development or provide of tools, infrastructures and services
Cyber industries	Ingenuity of the people and innovations
Cyber industries	Innovation and investment
Cyber industries	Innovative assessments that improve resiliency
Cyber industries	Installed a high-speed fibre-optic network
Cyber industries	Invest and benchmarking for critical infrastructure
Cyber industries	Investigating malicious cyber activities
Cyber industries	Prioritisation of Research and Development for cyberspace operations
Cyber industries	Promote standards and best practices
Cyber industries	Promote technology marketplace
Cyber industries	Promoting programs that ¹⁷ ₂₀₂₂ drive competitiveness
Cyber industries	Public private system
Cyber industries	Research and development efforts
Cyber industries	Spurring innovation in the private
Cyber industries	Strengthening security through public-private partnerships
Cyber industries	Support to develop voluntary standards
Cyber industries	Supporting cyberspace research and technology projects
Cyber industries	Work with private industry
Cyber partners	Cooperation with other nationally critical systems
Cyber partners	Cooperative responses and like-minded partners
Cyber partners	Developing a system of international cooperation
Cyber partners	Different agencies coordination
Cyber partners	Increase cyber diplomacy
Cyber partners	International Cyber Deterrence Initiative
Cyber partners	International partners to promote industry and Internet
Cyber partners	Promote and encourage cooperation
Cyber partners	Robust international alliances and partnerships
Cyber partners	Strengthen partner nations' law
Cyber partners	Throughout cooperation, shared information and intelligence
Cyber weapons	Cyberspace has emerged as a war-fighting domain in its own right
Cyber weapons	Defense 'relies on cyberspace to achieve national military objectives
Cyber weapons	Intelligence technology
Cyber weapons	Malicious cyber tools
Cyber weapons	Provides an automated process (Einstein 3)
Cyber weapons	Provides doctrinal guidance and direction for conducting cyber electromagnetic activities
Cyber weapons	Working relationships with weapon systems
Cybersecurity	Contingency plans
Cybersecurity	Coordinates national response efforts
Cybersecurity	cybersecurity objectives
Cybersecurity	Cybersecurity task and responsibilities
Cybersecurity	Develop continuity plans
Cybersecurity	Ensuring the security of cyberspace
Cybersecurity	Increasing the security
Cybersecurity	Limit the impact of cyber incidents
Cybersecurity	Manage cybersecurity risk
Cybersecurity	National cybersecurity management structure
Cybersecurity	Operational cybersecurity management
Cybersecurity	Preventing and responding to cyber security incidents
Cybersecurity	Preventing malicious traffic
Cybersecurity	Protection of their own ICT systems
Cybersecurity	Provides situational awareness
Cybersecurity	Reduce cyber threats

Cybersecurity	Reduce vulnerabilities
Cybersecurity	Reduces risk to critical infrastructure
Cybersecurity	Securing federal computer systems and networks
Digital economy and markets	Commercial service providers
Digital economy and markets	Commercial technology
Digital economy and markets	Cryptocurrencies
Digital economy and markets	Economic ^(P) _{SEP} disruption or espionage
Digital economy and markets	Economic and national ^(P) _{SEP} security
Digital economy and markets	Encourages investment and opens ^(P) _{SEP} new economic markets
Digital economy and markets	Ensure economic security for American workers and companies
Digital economy and markets	Financial fraud
Digital economy and markets	Free flow of data and digital ^(P) _{SEP} trade
Digital economy and markets	International commerce and trade
Digital economy and markets	Lead and rise of e-commerce
Digital economy and markets	Manage supply chain
Digital economy and markets	Money laundering
Digital economy and markets	Policies to ensure robust competition
Digital economy and markets	Sensitive financial ^(P) _{SEP} systems
Digital economy and markets	Thriving digital economy
Digital economy and markets	Trade-related engagement
Global Connectivity	Borderless nature
Global Connectivity	Digitized world
Global Connectivity	Global approach
Global Connectivity	Global supply chains
Global Connectivity	Growth in Internet access
Global Connectivity	Internet connected devices
Global Connectivity	Interoperable and reliable communications
Global Connectivity	Shared with the world
Global Connectivity	Support efforts globally
Global Connectivity	Universal service mechanisms
Government transparency and reforms	Pointing out policy priorities for others áreas
Government transparency and reforms	Proposal sought reforms
Government transparency and reforms	Reform services of ITC
Hegemony	Across the ^(P) _{SEP} federal government
Hegemony	Been in the vanguard of research and development
Hegemony	Cyberspace also is sustaining Global Leadership
Hegemony	Enable superiority in command and control
Hegemony	Future technological innovation
Hegemony	Intervention in economic enterprises
Hegemony	Leadership in emerging technologies
Hegemony	Mechanism to review foreign investment and operation in US
Hegemony	Promote markets for American ingenuity ^(P) _{SEP} overseas
Hegemony	Strengthening the future cyber security environment
Influence expansion and domination	Contributing to the development of cooperation
Influence expansion and domination	Cyber security policy internationally
Influence expansion and domination	Develops and maintains relationships with international partners
Influence expansion and domination	Encouraging the spread of best practices
Influence expansion and domination	Exerts influence over cyber ecosystem
Influence expansion and domination	Expand outreach to other entities
Influence expansion and domination	Freedom online Coalition
Influence expansion and domination	Induce private sector compliance
Influence expansion and domination	Influence the adoption of international conventions
Influence expansion and domination	Key Organizations
Influence expansion and domination	Leader in integrating and create state-centric frameworks

Influence expansion and domination	Leader in integrating traditional law enforcement methods
Influence expansion and domination	Leadership in building partner
Influence expansion and domination	Legally obliged to report major cyber security
Influence expansion and domination	Norms of responsible behaviour guide states
Influence expansion and domination	Push or aid other nations
Influence expansion and domination	Support of military missions worldwide
Influence expansion and domination	Supporting other nations
Information governance	Acknowledges and communicate
Information governance	Authority to secure critical infrastructure
Information governance	Awareness of the cybersecurity risk posture
Information governance	Clarifying the federal role
Information governance	Command and control
Information governance	Continuity of operations information technology
Information governance	Crisis response coordination is centralised
Information governance	Cyber security guidance and responsibility
Information governance	Designates the roles and delegates tasks
Information governance	Disseminate information
Information governance	Documents assign high-level roles
Information governance	Documents that regulate
Information governance	Efficient information exchange
Information governance	Ensure leaders have the most accurate information
Information governance	Implement a governance model
Information governance	Information sharing efforts
Information governance	Information sharing partners
Information governance	Information society
Information governance	Initiating an awareness
Information governance	Integrate information with other sectors
Information governance	Integrated and operationally relevant information
Information governance	Leader in collaborating
Information governance	Leverage information shared
Information governance	Make information and services available online
Information governance	Management responsibility
Information governance	Multi-stakeholder governance structure
Information governance	Performance metrics
Information governance	Political and strategic management and coordination
Information governance	Preserve information as records
Information governance	Primary policy coordinating role
Information governance	Prioritising information sharing
Information governance	Responsibilities for CIOs
Information governance	Responsibilities for leading cyber policy
Information governance	Stronger leadership role
Information governance	Unified approach to securing
Information governance	Uniqueness of military operations in cyberspace
Information governance	Value of information sharing programs
Information governance	Whole-of-government approach
Integral component of all sectors	Appropriately integrated, resourced, and coordinated
Integral component of all sectors	Assistance to other
Integral component of all sectors	Collaborative manner across components
Integral component of all sectors	Coordinating and prioritising national responsibilities
Integral component of all sectors	Coordination and engagement
Integral component of all sectors	Cyberspace is an integral component of all facets of the society life
Integral component of all sectors	Encourage reporting of cyber incidents
Integral component of all sectors	Information sharing partnership
Integral component of all sectors	Integrated as a total force

Integral component of all sectors	Interconnectedness of the gamut of cyber-related
Integral component of all sectors	Key roles are played
Integral component of all sectors	Leadership to coordinate
Integral component of all sectors	Mechanism that coordinates
Integral component of all sectors	Outlines partnership criteria
Integral component of all sectors	Partnership role
Integral component of all sectors	Partnerships in the government and with private sector
Integral component of all sectors	Public-private partnership initiatives
Integral component of all sectors	Reviewing incentives packages
Integral component of all sectors	Roles and responsibilities of various agencies
Integral component of all sectors	Strengthening cyber security partnerships
Intelligence community	Component intelligence
Intelligence community	Counter-intelligence
Intelligence community	Cyber intelligence
Intelligence community	Defense for Intelligence
Intelligence community	Defense Intelligence
Intelligence community	Disseminate intelligence
Intelligence community	Effectiveness of public-private information sharing
Intelligence community	Facilitating information sharing
Intelligence community	Gathering intelligence
Intelligence community	Geospatial intelligence
Intelligence community	Global intelligence assets
Intelligence community	Including disrupting foreign intelligence
Intelligence community	Increase information sharing
Intelligence community	Increased cyber threat information sharing
Intelligence community	Information sharing about vulnerability and risk assessments
Intelligence community	Information sharing centers
Intelligence community	Intelligence and analysis
Intelligence community	Intelligence communications architecture
Intelligence community	Intelligence communications planning
Intelligence community	Intelligence network
Intelligence community	Intelligence systems
Intelligence community	Intelligence-related information
Intelligence community	Provides an automated process for cyberintelligence
Intelligence community	Provides signals intelligence
Intelligence community	Sensitive information
Intelligence community	Support to intelligence
Intelligence community	use of all-source cyber intelligence
Intelligence community	Voluntary information sharing initiative
Internet governance	Access to the Internet
Internet governance	Awareness and transparency of cybersecurity practices
Internet governance	Believe that cyberspace can be secure and resilient
Internet governance	Civil rights and liberties
Internet governance	Collaborate with private sector and civil society
Internet governance	Free expression and individual liberty
Internet governance	Free flow of data across borders
Internet governance	Internet freedom
Internet governance	Net neutrality
Internet governance	Open, interoperable, reliable, and secure Internet
Internet governance	Stakeholders groups
Internet governance	Values ¹³ of freedom, security and prosperity
National interest and priorities	Achieve national security objectives
National interest and priorities	As a substitute for physical economic activity
National interest and priorities	Building cybercrime-fighting capacity

National interest and priorities	Communicating national priorities
National interest and priorities	Cyberspace is an inseparable component of ⁽¹⁾ ₃₈₇ national interests
National interest and priorities	Defend the homeland and vital interests
National interest and priorities	Deterrence strategy
National interest and priorities	Economic growth
National interest and priorities	Efforts to protect infrastructure and communications
National interest and priorities	Foreign nations
National interest and priorities	Foreign policy priorities
National interest and priorities	Geopolitic and cyberspace
National interest and priorities	Global Internet
National interest and priorities	Increasingly dependent on vendors
National interest and priorities	Integrate the employment of cyber ⁽¹⁾ ₃₈₇ options across every element of national power
National interest and priorities	Mandates of political and strategic management
National interest and priorities	National priorities from narrower cyber security areas
National interest and priorities	National security and prosperity people
National interest and priorities	Predominantly political to an economic concern
National interest and priorities	Prioritize international engagements
National interest and priorities	Research priorities to ensure reliable communications Infrastructure
National interest and priorities	RoI of the armed forces as to secure interests
National interest and priorities	Strategic advantage in cyberspace
National Protection	Adoption of voluntary norms of responsible state
National Protection	Domestic crisis management
National Protection	Establish mechanism
National Protection	Instruments of national power
National Protection	National effort to protect
National Protection	National mission teams
National Protection	National Response Framework
National Protection	National Risk posture
National Protection	National security and defence strategies outline cyber security
National Protection	National Security Strategy
National Protection	National Strategy for the Physical Protection of Critical Infrastructures
National Protection	National strategy to Secure Cyberspace
National Protection	Priority homeland security missions
National Protection	Safeguard American people
National Protection	Strengthens international security
National Protection	Threat to national security
National Protection	Unified national reponse to disasters and emergencies
National Protection	Use of total force capabilities
National Threats and Risks	Adversaries have increased the frequency and sophistication
National Threats and Risks	Cyber attacks
National Threats and Risks	Cyber threats to national security
National Threats and Risks	Cybercrimes
National Threats and Risks	Dependent ⁽¹⁾ ₃₈₇ on cyberspace
National Threats and Risks	Economic espionage and malicious ⁽¹⁾ ₃₈₇ Cyber activities
National Threats and Risks	Greatest vulnerabilities
National Threats and Risks	Indicators of malicious cyber activity with critical infrastructure
National Threats and Risks	Malicious cyber actors
National Threats and Risks	New threats
National Threats and Risks	Repressive regimes use and censorship
National Threats and Risks	Risk-management assessments
National Threats and Risks	Spectrum of threats
National Threats and Risks	State-sponsored or authoritarian states
National Threats and Risks	Steal intellectual property
National Threats and Risks	Terrorist activities

National Threats and Risks	Transnational criminal organization
Offensive capabilities	Disruptive or destructive cyberattacks
Offensive capabilities	Offensive cyberspace operations
Prioritizing protections	Assure the survivability, reliability, and availability
Prioritizing protections	Critical infrastructure sectors and ^{SEP} other systems that impact national security, public health and safety, and economic security
Prioritizing protections	Cybersecurity risk posture across critical infrastructure
Prioritizing protections	Defending against the most immediate and prioritising critical infrastructure
Prioritizing protections	Entities at greatest risk
Prioritizing protections	Establishing a threat and vulnerability reduction programme
Prioritizing protections	Focus on the high impact systems
Prioritizing protections	Information systems at greatest risk
Prioritizing protections	Priorities in the cybersecurity mission space
Prioritizing protections	Prioritize gaps in current national cybersecurity
Prioritizing protections	Priority areas for safeguarding and securing cyberspace
Prioritizing protections	Protecting critical information infrastructure
Prioritizing protections	Responsibilities for critical infrastructure
Prosperity and development	Collaboration to develop and circulate social programs
Prosperity and development	Consumer welfare
Prosperity and development	Cyber ecosystem includes people, environment and conditions
Prosperity and development	Cyberspace empowers people and enables prosperity worldwide
Prosperity and development	Cyberspace for future generations
Prosperity and development	Cyberspace has become fundamental to American wealth creation and innovation
Prosperity and development	E-government initiatives
Prosperity and development	E-government services and processes
Prosperity and development	Efforts to expand the array of government services offered electronically
Prosperity and development	Fostering strong ^{FPI} _{SEP} domestic innovation
Prosperity and development	Global competitiveness and a better way of life
Prosperity and development	Internet has generated benefit domestically
Prosperity and development	Job creation
Prosperity and development	National information society
Prosperity and development	Nurturing a secure, ^{FPI} _{SEP} thriving digital economy
Prosperity and development	Securing democratic processes
Regulations and Sanctions	Cyber regulations
Regulations and Sanctions	Cyber regulations for the industries
Regulations and Sanctions	Disrupt the ability to use marketplaces and tools
Regulations and Sanctions	Foreign policy issues
Regulations and Sanctions	Impose costs for unacceptable behavior and cyber actors
Regulations and Sanctions	Impose sanctions and consequences
Regulations and Sanctions	International laws
Regulations and Sanctions	Investigate and assistance on cyber crime
Regulations and Sanctions	Investigating and prosecuting intrusion cases
Regulations and Sanctions	Law of War Manual
Regulations and Sanctions	Legislation is less comprehensive
Regulations and Sanctions	Primary legislative vehicle to guide federal IT management
Regulations and Sanctions	Punish who use cyber tools
Regulations and Sanctions	Reforming and enforcing Federal law
Regulations and Sanctions	Regulate providers
Regulations and Sanctions	Required by law or regulation is extremely varied
Regulations and Sanctions	Responsibility to regulate in their constituency
Regulations and Sanctions	Support the rule of law in cyberspace
Strategic focus on Internet	Digital Government Strategy
Strategic focus on Internet	Infrastructure availability
Strategic focus on Internet	Leverage technology toward developing their own capabilities,

APÊNDICE VI – Roteiro de entrevista semiestruturada, idioma português.



Universidade Federal de Minas Gerais (UFMG, Brasil)
Programa de Pós-graduação em Ciência da Informação (PPGCI)
Pesquisa de Doutorado



Roteiro de entrevista a especialistas governamentais

O presente guia de entrevista foi preparado por Arthur Christian Huamaní Cuba, doutorando em Ciência da Informação na Universidade Federal de Minas Gerais (UFMG, Brasil), bolsista do programa da Organização dos Estados Americanos (OEA) e Grupo Coimbra de Universidades Brasileiras (GCUB), trabalhando sob a supervisão da professora Maria Aparecida Moura (UFMG). O objetivo da pesquisa é identificar, sistematizar e analisar em uma perspectiva comparada as políticas e estratégias de segurança cibernética implementadas na América do Sul, notadamente na Argentina, Brasil e Peru; com vista em dispor do panorama das configurações políticas e estratégicas no âmbito da segurança cibernética, definidas nos países pesquisados.

Muito obrigado pela sua participação.

Observação: As entrevistas serão conduzidas via online e gravadas, com a promessa de confidencialidade e anonimato. Por esse sentido, todo dado pessoal que relacione ao entrevistado ou das pessoas que foram relatadas serão anonimizadas. Segundo a Lei 13.709/2018 LGPD: “A anonimização de dados trata-se da utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, *por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo*”

Nome completo:
Data:
Órgão Governamental:
Cargo:
Assinatura (Firma Digital):

No aspecto das ameaças e riscos:

1.1. Quais são as prioridades que buscam alcançar as estratégias na segurança e defesa cibernética, no hipotético caso de se ativar uma situação de crise cibernética nacional?

1.2. Que agentes são os envolvidos, quais são as prioridades?

1.3. Finalmente, em sua experiência e das funções que vem exercendo atualmente, qual é a principal ameaça (externa ou interna) que pode dar origem a uma crise cibernética nacional.

Propósito da questão: *Identificar os agentes envolvidos nas estratégias em segurança e defesa cibernética.*

No aspecto das capacidades e resposta:

2.1. Para a proteção do espaço cibernético nacional, quais estratégias foram orientadas desde o nível político-estratégico?

2.2. Desde sua experiência e das funções que vem exercendo atualmente, onde se encontram as maiores capacidades cibernéticas?

2.3. Desde a perspectiva da segurança e defesa nacional, que se busca alcançar com a Internet e/ou Ciberespaço?

Propósito da questão: *Identificar os agentes envolvidos nas estratégias em segurança e defesa cibernética.*

No aspecto do poder e dominação:

3.1. Você considera que as estratégias nacionais no âmbito cibernético, impulsionam a expansão e dominação em defesa dos interesses e objetivos nacionais de seu país?

3.2. Você considera que as estratégias nacionais no âmbito cibernético, regula e sanciona toda ação tecnológica que possa atentar aos interesses nacionais? Se tem algum caso de sanções efetuadas a empresas desde a perspectiva da segurança e defesa nacional?

Propósito da questão: *Analisar os elementos que constituem uma política de segurança cibernética.*

No aspecto do geopolítico e diplomático:

4.1. A Política Nacional de Segurança Cibernética traz iniciativas no âmbito diplomático. Pode mencionar algumas dessas iniciativas?

4.1. Que órgão é responsável pela geoestratégia nacional no âmbito espacial e cibernético? Como servidor público decisor, conhece a quais interesses e objetivos nacionais a Política Nacional de Segurança Cibernética busca atender?

Propósito da questão: *Analisar a geopolítica no âmbito cibernético e suas repercussões na consolidação das políticas e estratégias em segurança cibernética.*

No aspecto do sociocultural e organizacional:

5.1. A Política Nacional de Segurança Cibernética tem conduzido ou incentivado a mudanças institucionais? Considera que a Política Nacional de Segurança Cibernética se complementa às outras políticas ou leis nacionais? Quais especificamente?

5.2. Em que forma a Política Nacional de Segurança Cibernética tem promovido benefícios, prosperidade e desenvolvimento no âmbito sociocultural?

Propósito da questão: *Compreender que agentes e elementos se constituem na política de segurança cibernética, no âmbito sociocultural e institucional.*

No aspecto do socioeconômico e comércio:

6.1. A Política Nacional de Segurança Cibernética encoraja o consumo das tecnologias de informação e da comunicação nacionais? Se tem iniciativas que sopesem a dependência tecnológica estrangeira?

6.2. Os programas em segurança e defesa cibernética orientam de forma centralizada a efetivação dos esforços conjuntos intersetoriais, em busca de uma otimização de custos e benefícios?

6.3. Em que forma a Política Nacional de Segurança Cibernética tem promovido a economia e mercado digital nacional?

Propósito da questão: *Compreender que agentes e elementos se constituem na política de segurança cibernética, no âmbito socioeconômico e do mercado.*

No aspecto do tecnológico e industrial:

7.1. Se tem nas estratégias nacionais uma entidade pública responsável por regular e estabelecer os padrões em Tecnologias da Informação e da Comunicação na indústria nacional ou privada?

7.2. Na Política Nacional de Segurança Cibernética, também são incluídas as empresas multinacionais estrangeiras? Que setor é o responsável dessa articulação e com que finalidade?

7.3. O acesso e conectividade à Internet é promovida nas estratégias de segurança e defesa cibernética? O Fornecedor de Acesso à Internet ou Provedor de Serviço Internet (em inglês Internet Service Provider, ISP) é uma empresa estatal? Que órgão regula os ISPs?

Propósito da questão: *Compreender que agentes e elementos se constituem na política de segurança cibernética, no âmbito tecnológico e industrial.*

APÊNDICE VII – Guión de entrevista semiestructurada, idioma español



Universidade Federal de Minas Gerais (UFMG, Brasil)
Programa de Pós Graduação em Ciência de la Informação
(PPGCI)
Investigación de Doctorado



Guión de entrevista a especialistas gubernamentales

La presente guía de entrevista fue elaborada por Arthur Christian Huamaní Cuba, alumno de doctorado en Ciencia de la Información en la Universidad Federal de Minas Gerais (UFMG, Brasil), becario del programa de la Organización de Estados Americanos (OEA) y el Grupo Coímbra de Universidades Brasileiras (GCUB), trabajando bajo la supervisión de la profesora María Aparecida Moura (UFMG). El objetivo de la investigación es identificar, sistematizar y analizar en una perspectiva comparada las políticas y estrategias de seguridad cibernética implementadas en América del Sur, notablemente en Argentina, Brasil y Perú; con el objeto de disponer de un panorama de las configuraciones políticas y estratégicas en el ámbito de la seguridad cibernética que fueron definidas en los tres países estudiados.

Gracias por su participación.

Observación: Las entrevistas serán conducidas vía online y grabadas, con la promesa de confidencialidad y anonimato. Por ese sentido, todo dato personal que relacione al entrevistado o a las personas que fueran descritas serán anonimizadas. De acuerdo con la Ley 13.709/2018 LGPD: “La anonimización de datos se trata de la utilización de medios técnicos razonables y disponibles en el momento del tratamiento, *por medio de los cuales un dato pierde la posibilidad de asociación, directa o indirecta, a un individuo*”

Nombres y apellidos:
Fecha:
Institución:
Cargo:
Correo:

En el aspecto de las amenazas y riesgos:

1.1. ¿Cuáles son las prioridades que buscan alcanzar las estrategias en la seguridad y defensa cibernética, en el hipotético caso de ser activada una situación de crisis cibernética nacional?

1.2. ¿Qué actores son los involucrados, cuáles son las prioridades?

1.3. Finalmente, en su experiencia y de las funciones que viene ejerciendo actualmente, ¿Cuál es la principal amenaza (externa o interna) que puede dar origen a una crisis cibernética nacional?

Finalidad de la pregunta: *Identificar los actores involucrados en las estrategias en seguridad y defensa cibernética.*

En el aspecto de las capacidades y respuestas:

2.1. Para la protección del espacio cibernético nacional, ¿Cuáles estrategias fueron direccionadas desde el nivel político-estratégico?

2.2. Desde su experiencia y de las funciones que viene ejerciendo actualmente, ¿Dónde se encuentran las mayores capacidades cibernéticas?

2.3. Desde la perspectiva de la seguridad y defensa nacional, ¿Que se busca alcanzar con el Internet y/o Ciberespacio?

Finalidad de la pregunta: *Identificar los actores involucrados en las estrategias en seguridad y defensa cibernética.*

En el aspecto del poder y dominación:

3.1. ¿Usted considera que las estrategias nacionales en el ámbito cibernético impulsan la expansión y dominación en defensa de los intereses y objetivos nacionales de su país?

3.2. ¿Usted considera que las estrategias nacionales en el ámbito cibernético regulan y sancionan toda acción tecnológica que pueda afectar a los intereses nacionales? ¿Se tiene algún caso de sanciones realizadas a las empresas desde la perspectiva de la seguridad y defensa nacional?

Finalidad de la pregunta: *Analizar los elementos que constituyen una política de seguridad cibernética.*

En el aspecto geopolítico y diplomático:

4.1. La Política Nacional de Seguridad Cibernética trae iniciativas en el ámbito diplomático. ¿Puede usted mencionar algunas de esas iniciativas?

4.1. ¿Qué institución es responsable por la geoestrategia nacional en el ámbito espacial y cibernético? ¿Como funcionario público decisorio, conoce a cuáles intereses y objetivos nacionales se busca atender con la Política Nacional de Seguridad Cibernética?

Finalidad de la pregunta: *Analizar la geopolítica en el ámbito cibernético y sus repercusiones en la consolidación de las políticas y estrategias en seguridad cibernética.*

En el aspecto sociocultural y organizacional:

5.1. ¿La Política Nacional de Seguridad Cibernética ha conducido o incentivado las reformas institucionales? ¿Considera que la Política Nacional de Seguridad Cibernética se complementa a otras políticas o leyes nacionales? ¿Cuáles específicamente?

5.2. ¿En qué forma la Política Nacional de Seguridad Cibernética ha incentivado beneficios, prosperidad y desarrollo en el ámbito sociocultural?

Finalidad de la pregunta: *Comprender que actores y elementos constituyen una política de seguridad cibernética, en el ámbito sociocultural e institucional.*

En el aspecto socioeconómico y de mercado:

6.1. ¿La Política Nacional de Seguridad Cibernética incentiva el consumo de las tecnologías de información y de la comunicación nacionales? ¿Se tienen iniciativas que equilibren la dependencia tecnológica extranjera?

6.2. ¿Los programas en seguridad y defensa cibernética orientan de forma centralizada la activación de esfuerzos conjuntos intersectoriales, en busca de una optimización de costos y beneficios?

6.3. ¿En qué forma la Política Nacional de Seguridad Cibernética ha impulsado la economía y mercado digital nacional?

Finalidad de la pregunta: *Comprender que agentes y elementos constituyen una política de seguridad cibernética, en el ámbito socioeconómico y de mercado.*

En el aspecto tecnológico e industrial:

7.1. ¿Se tienen en las estrategias nacionales una entidad pública responsable por normar y establecer los estándares en Tecnologías de la Información y de la Comunicación en la industria nacional o privada?

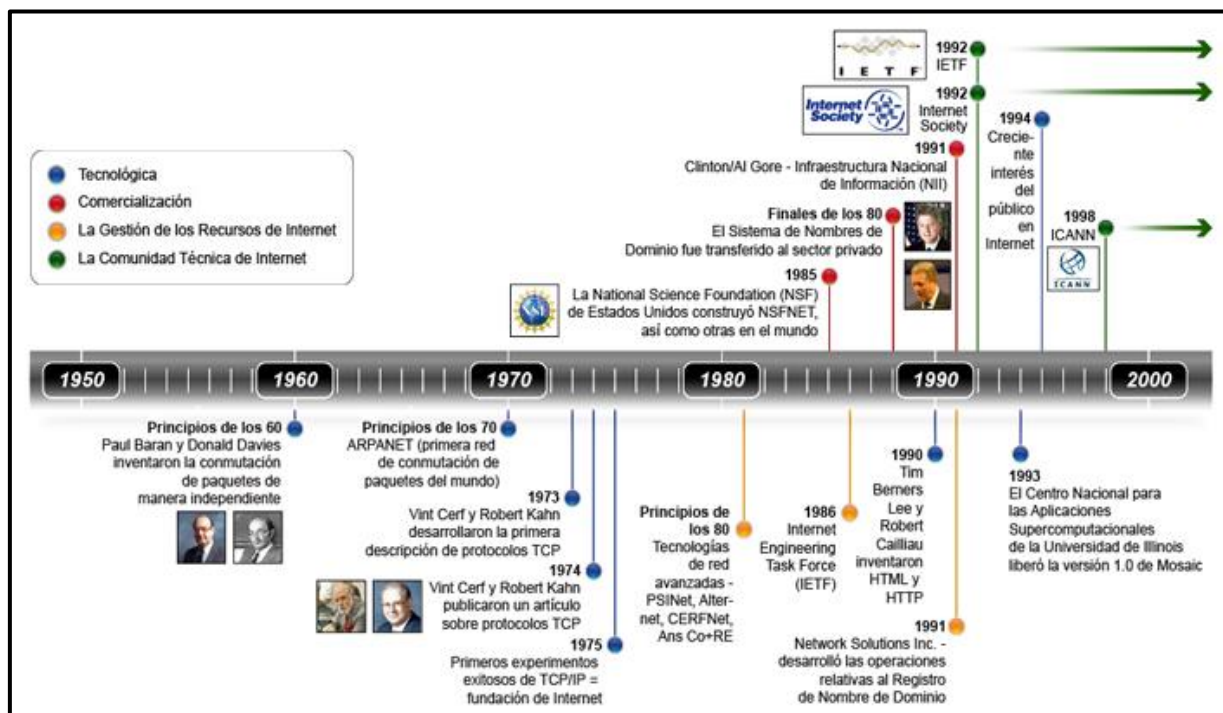
7.2. ¿En la Política Nacional de Seguridad Cibernética, también están incluidas las empresas multinacionales extranjeras? ¿Qué sector es el responsable de esa articulación y con qué finalidad?

7.3. ¿El acceso y conectividad al Internet es impulsada en las estrategias de seguridad y defensa cibernética? ¿El proveedor de Acceso a la Internet o Proveedor de Servicio de Internet (en inglés Internet Service Provider, ISP) es una empresa estatal? ¿Qué órgano regula los ISPs?

Finalidad de la pregunta: *Comprender que actores y elementos constituyen una política de seguridad cibernética, en el ámbito tecnológico e industrial.*

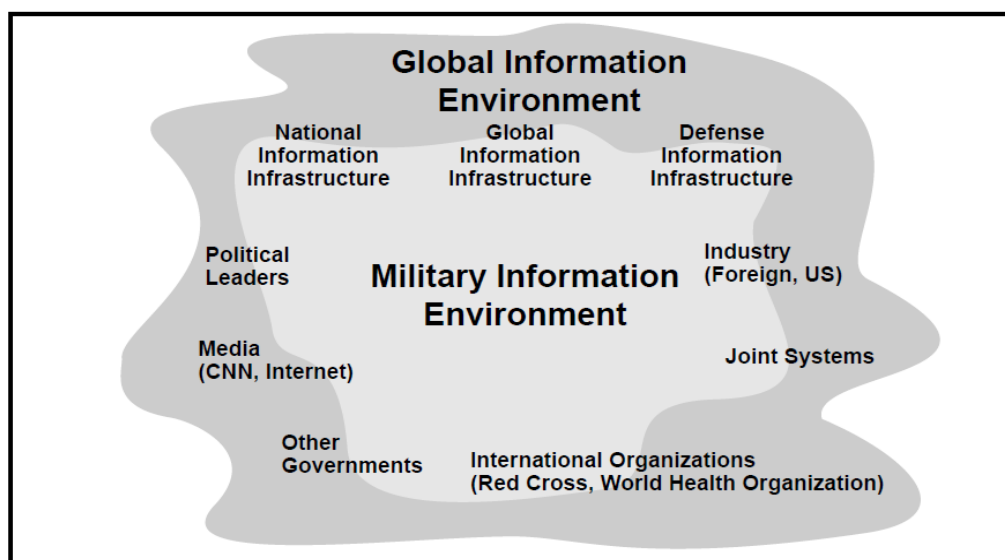
APÊNDICE VIII – Ilustrações complementarias: Figuras e Quadros

Figura 67 - Cronologia dos eventos mais importantes da história da Internet, desde as 4 dimensões chaves



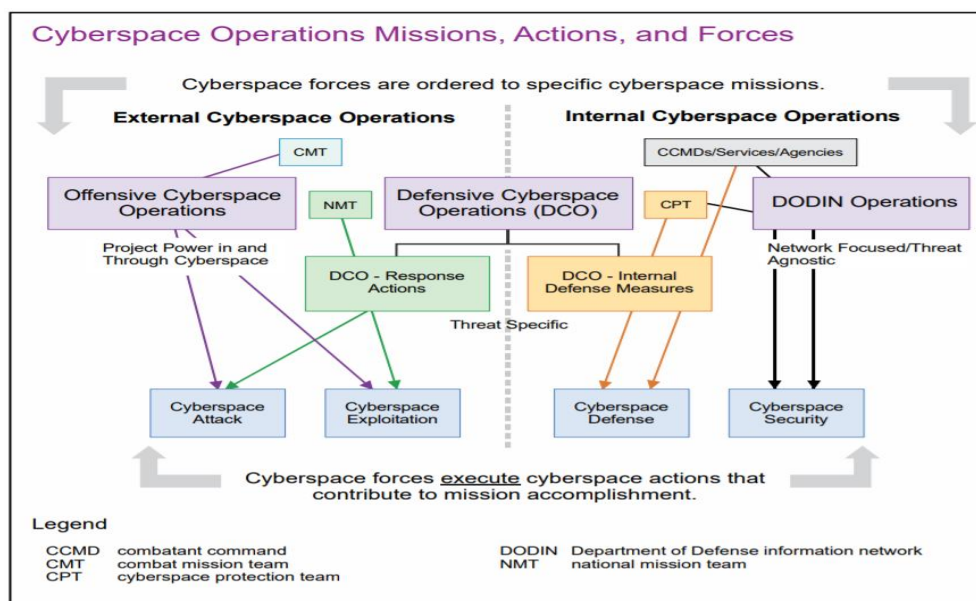
Fonte: Internet Society (ISOC).

Figura 68 - Os ambientes da informação: Global e Militar



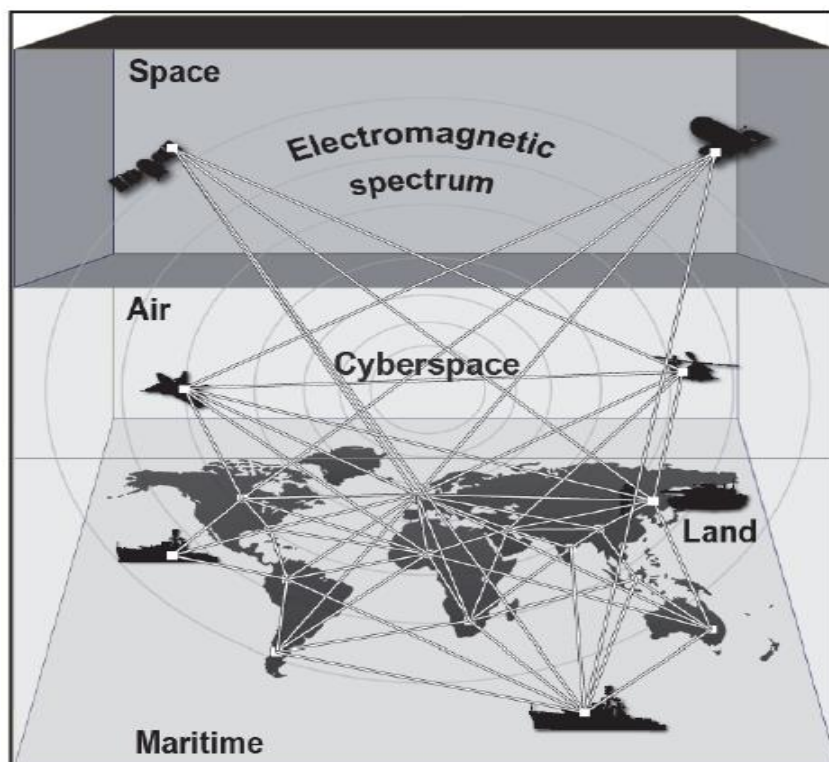
Fonte: (FM 100-6, 1996, p. 1-2).

Figura 69 - Missões, ações e forças nas operações do ciberespaço.



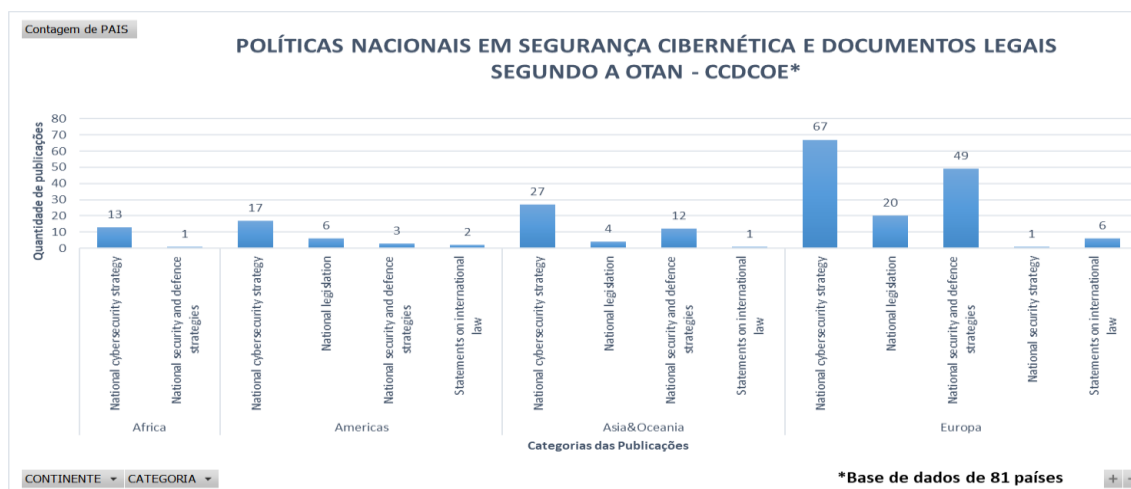
Fonte: (JP 3-12, 2018, p.II-3)

Figura 70 - A influência do espectro ciber-eletromagnético nos outros 4 domínios da batalha.



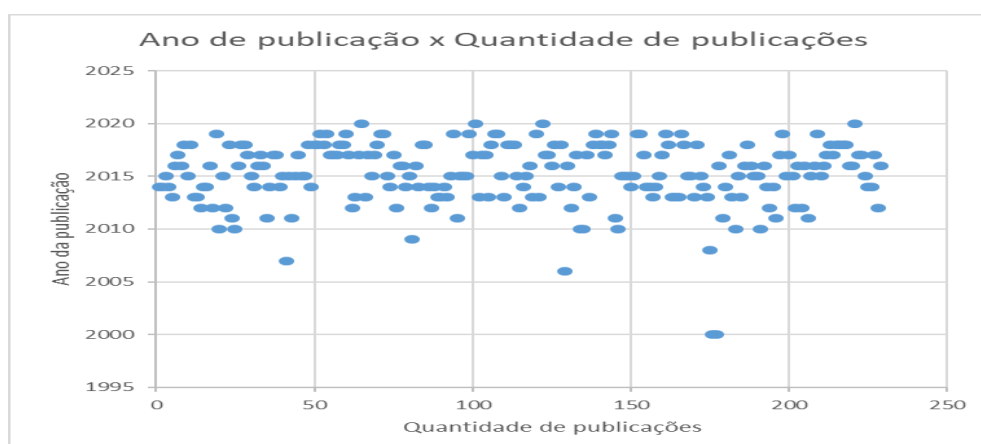
Fonte: (FM 3-38, 2014, p. 1-4).

Figura 71 - Políticas nacionais e documentos legais em segurança cibernética (OTAN-CCDCOE)



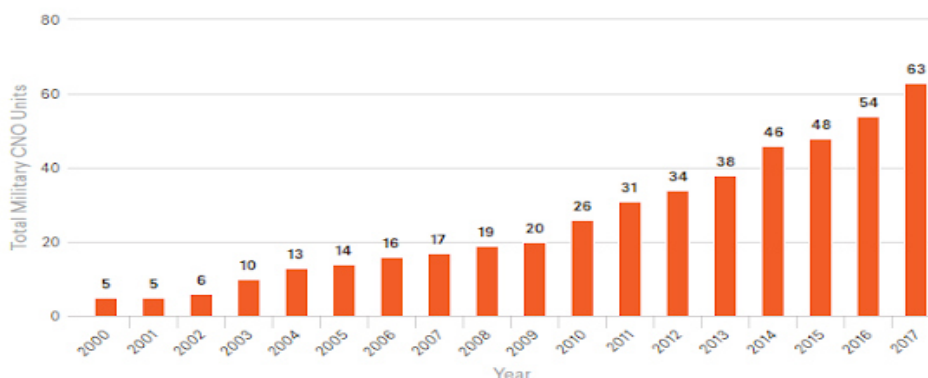
Fonte: (<https://ccdcoc.org/library/strategy-and-governance>, elaboração própria).

Figura 72 - Ano de publicação Vs quantidade de publicações (OTAN-CCDCOE).



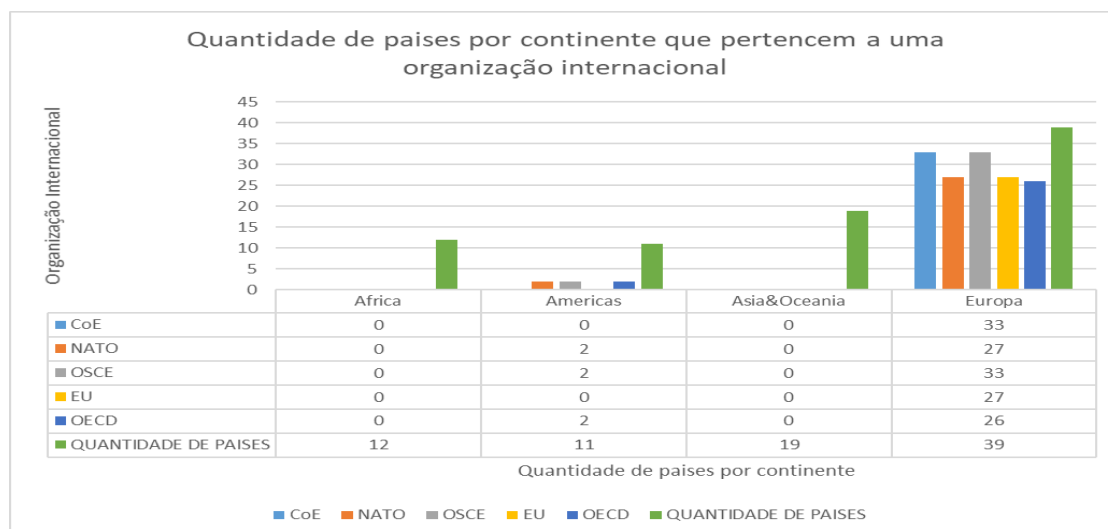
Fonte: (<https://ccdcoc.org/library/strategy-and-governance>, elaboração própria).

Figura 73 - Proliferação das unidades militares de CNO



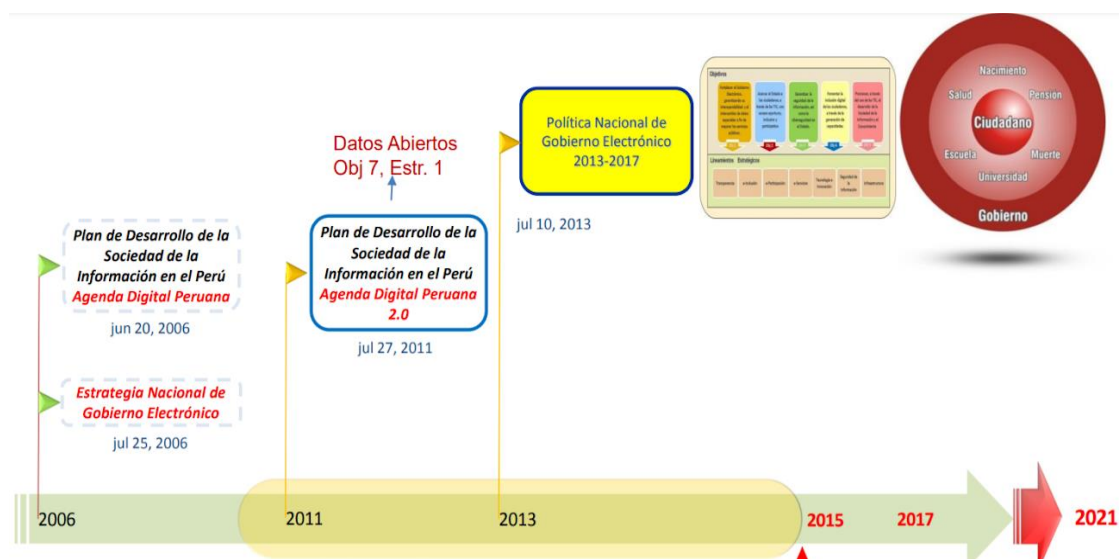
Fonte: (<https://www.cfr.org/blog/understanding-proliferation-cyber-capabilities>).

Figura 74 - Países por continente que pertencem a um organismo internacional



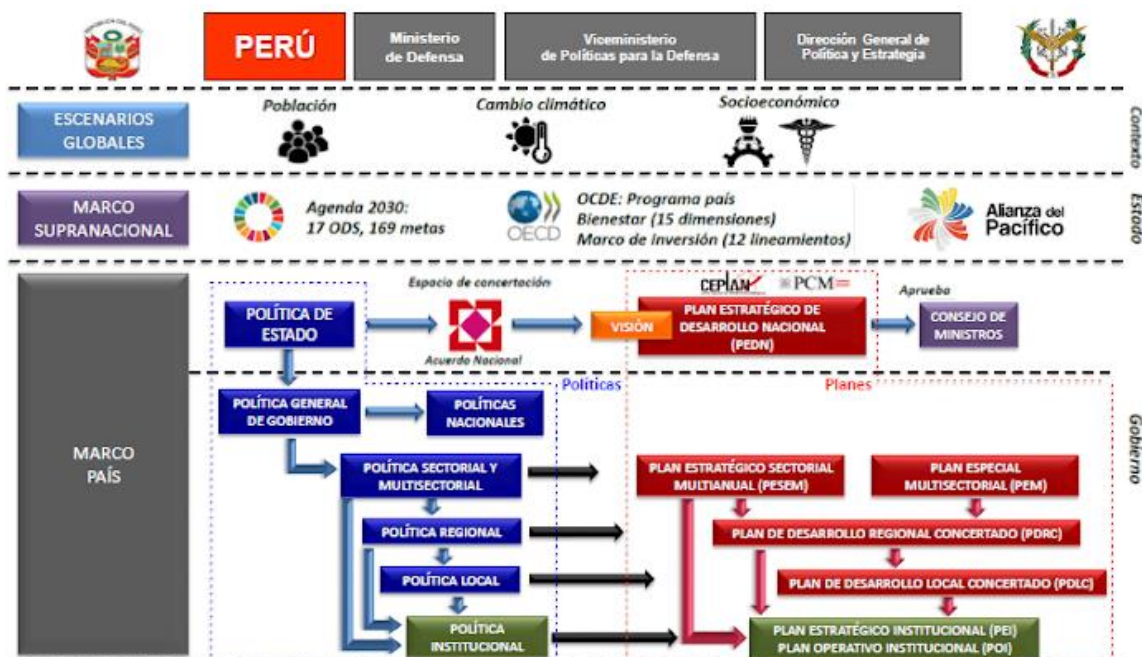
Fonte: (<https://ccdcoe.org/library/strategy-and-governance>, elaboração própria).

Figura 75 - Linha de tempo, das ações realizadas pela ONGEI



Fonte: ONGEI, 2015.

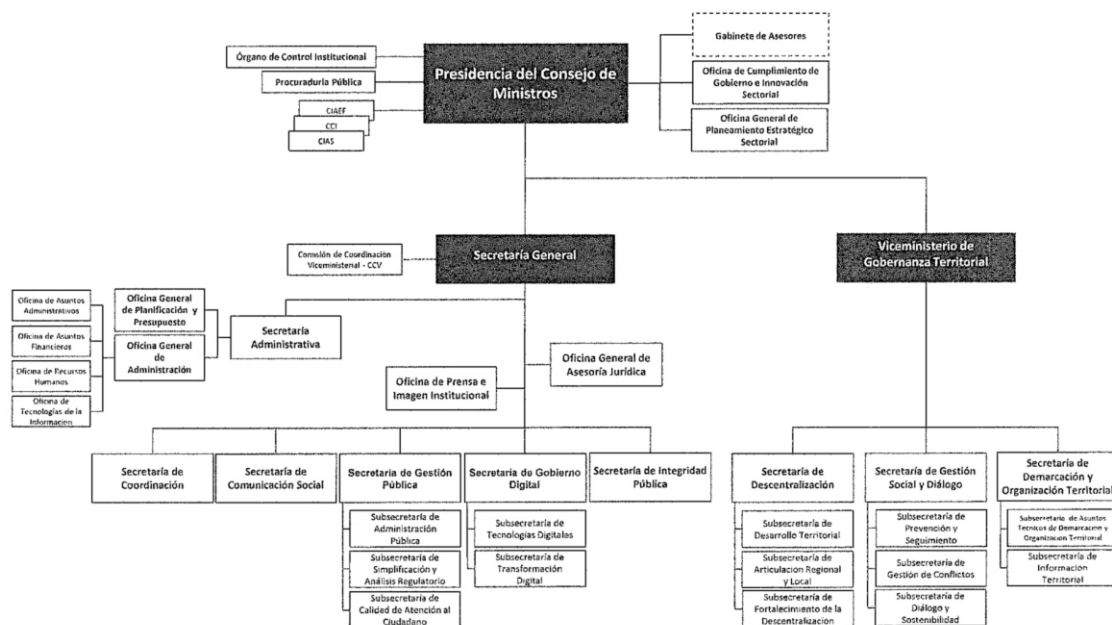
Figura 76 - Formulação das políticas no Peru



Fonte: MINDEF, 2018.

Figura 77 - Mudanças estruturais na PCM

ORGANIGRAMA DE LA PRESIDENCIA DEL CONSEJO DE MINISTROS - PCM



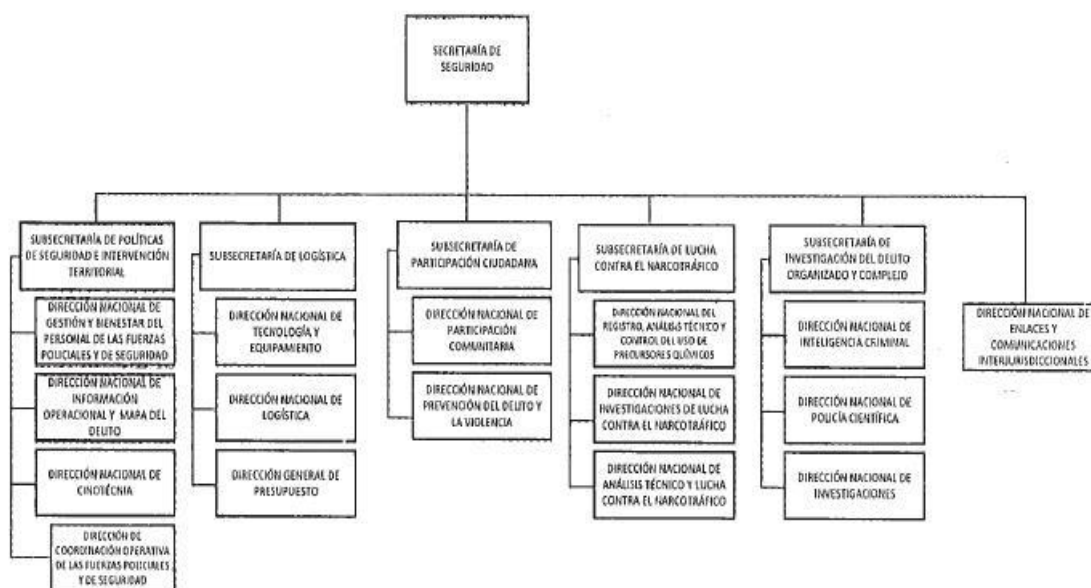
Fonte: PCM, Disponível em <<http://www.pcm.gob.pe/organigrama-sectorial/>>. Acesso em 06 de novembro de 2020.

Figura 78 - Hierarquia de documentos da segurança e defesa nacional



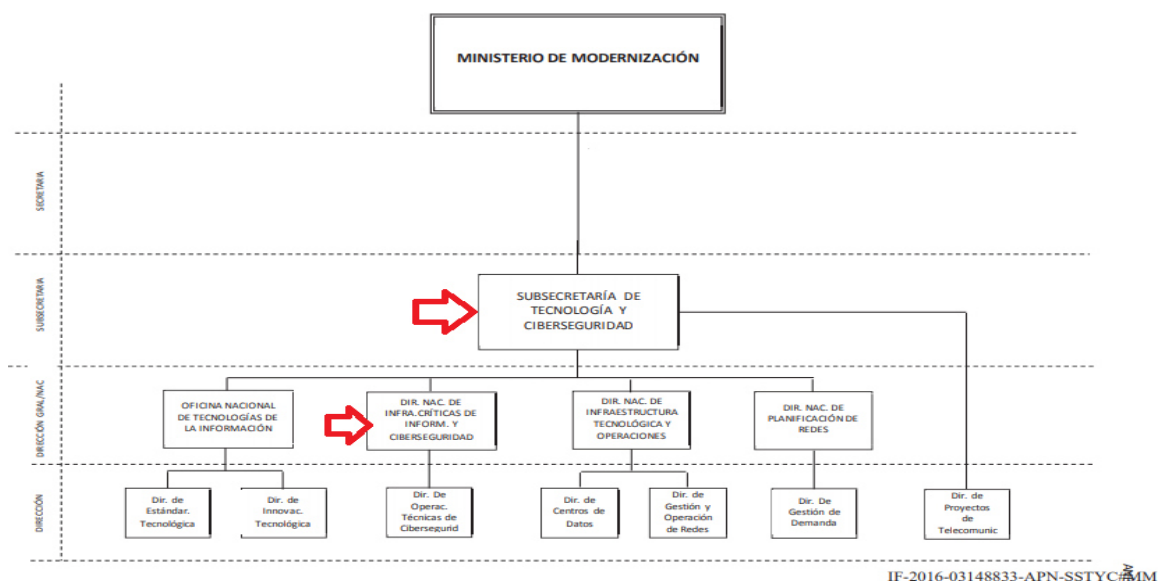
Fonte: MINDEF, 2018.

Figura 79 - Secretaria de segurança - Argentina



Fonte: Disponível em <http://servicios.infoleg.gob.ar/infolegInternet/anexos/260000-264999/261121/texact.htm>. Acesso em 10 de novembro de 2020.

Figura 80 - Subsecretaria de tecnología e cibersegurança – Argentina



Fonte: Disponível em <http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/267908/res490-1.pdf>. Acesso em 10 de novembro de 2020.

Figura 81 - Subsecretaria de tecnología e cibersegurança – Brasil



Fonte: Disponível em <https://www.youtube.com/watch?v=cWOWICGONPM>. Acesso em 10 de novembro de 2020.

Nota: A 48ª reunião do GTER e a 34ª do GTS foram realizadas nos dias 12 e 13 de dezembro de 2019, em São Paulo, e integraram a programação da 9ª Semana de Infraestrutura da Internet no Brasil - evento realizado pelo CGI.br e NIC.br com recursos do registro de domínios .br, que contou também com patrocínio do Seaborn Networks e Abranet, entre outros.

Quadro 25 - Autoridades com responsabilidade no ciberespaço, segundo o código dos Estados Unidos

CÓDIGO (USC)	TÍTULOS	FOCO-CHAVE	ORGANIZAÇÃO PRINCIPAL	PAPEL NO CIBERESPAÇO
Título 6	Segurança Interna – <i>Domestic Security</i>	Homeland Security	Departamento de Homeland	Segurança do ciberespaço EU
Título 10	Forças Armadas – <i>Armed Forces</i>	Defesa Nacional	Departamento de Segurança da Defesa	Homem, treinar e equipar as forças do EU para as operações militares no ciberespaço.
Título 18	Crimes e processo penal	Aplicação da Lei – <i>Law enforcement</i>	Departamento da Justiça	Prevenção do crime, apreensão e acusação de criminosos que operam no ciberespaço
Título 32	Guardia Nacional – <i>National Guard</i>	Defesa Nacional e treinamento e operações de apoio civil, nos EU	Guarda Nacional do Exército Estadual, Guarda Nacional Aérea do Estado	Gestão de consequências domésticas (se ativada para o serviço federal, a Guarda Nacional está integrada ao Título 10, USC, Forças Armadas.
Título 40	Edifícios públicos, propriedades e obras	Cargos e responsabilidades do Diretor de Informação	Todas as agências e departamentos federais.	Estabelecer e aplicar padrões de aquisição e segurança das tecnologias da informação
Título 50	Guerra e defesa nacional	Um amplo espectro de atividades militares, de inteligência estrangeira e de contrainteligência	Comandos, Serviços e agências do Departamento de Defesa e agências comunitárias de inteligência alinhados o Escritório do Diretor de Inteligência Nacional	Garantir os interesses dos EU na realização de operações de inteligência militar e estrangeira no ciberespaço

Fonte: JP3-12, Operações do Ciberespaço, tradução nossa.

APÊNDICE IX – Tabelas complementarias

Tabela 7 - Comparativo numérico de data centers certificados por TIER II, III e IV por continentes

CONTINENTE	TIER IV	TIER III	TIER II	QUANTIDADE DE DATACENTER CERTIFICADOS COM TIER	PORCENTAGEM MUNDIAL
AMERICA	26	226	14	266	35.80 %
AFRICA	9	25	2	36	4.85 %
EUROPA	33	75	3	111	14.94 %
ASIA	40	245	19	304	40.92 %
OCEANIA	4	22	0	26	3.50 %
TOTAL	112	593	38	743	100.00 %

Fonte: (Uptime Institute Tier Certification Map, 2019, elaboração própria).

Tabela 8 - Países com maior PIB (Produto Interno Bruto, 2019) por continentes

PAISES COM MAIOR PBI POR CONTINENTE							
CONTINENTE	PAIS	TOTAL	TIER IV	TIER III	TIER II	PORCENTAGEM MUNDIAL	PORCENTAGEM SEGUNDO SEU CONTINENTE
AMERICA	EEUU	93	8	79	6	12.52 %	34.96 %
AMERICA	CANADA	33	2	30	1	4.44 %	12.41 %
AFRICA	SUDAFRICA	11	4	7	0	1.48 %	30.56 %
AFRICA	EGYPT	2	0	2	0	0.27 %	5.56 %
EUROPA	LUXEMBOURG	11	7	2	2	1.48 %	9.91 %
EUROPA	SWITZERLAND	3	2	1	0	0.40 %	2.70 %
ASIA	QATAR	11	1	9	1	1.48 %	3.62 %
ASIA	SINGAPORE	9	1	8	0	1.21 %	2.96 %
OCEANIA	AUSTRALIA	26	4	22	0	3.50 %	100.00 %
TOTAL		199	29	160	10	26.78 %	
PORCENTAGEM MUNDIAL		26.78 %	3.90 %	21.53 %	1.35 %		
SEGUNDO SUA CATEGORIA TIER NO MUNDO			25.89 %	26.98 %	26.32 %		

Fonte: (Uptime Institute TIER Certification Map, 2019, elaboração própria).

Tabela 9 - Data centers certificados por TIER, nos países do G-8

G-8	QUANTIDADE DE DATACENTER CERTIFICADOS COM TIER	PORCENTAGEM MUNDIAL
EEUU	93	12.52 %
United Kingdom	16	2.15 %
Italy	16	2.15 %
Japan	1	0.13 %
France	4	0.54 %
Canada	33	4.44 %
Russia	32	4.31 %
Germany	1	0.13 %
TOTAL	196	26.38 %

Fonte: (Uptime Institute Tier Certification Map, 2019, elaboração própria).

Tabela 10 - Data centers certificados por TIER dos países tratados na pesquisa

PAIS	TOTAL	TIER IV	TIER III	TIER II	PORCENTAGEM SEGUNDO SEU CONTINENTE
EEUU	93	8	79	6	34.96 %
CANADA	33	2	30	1	12.41 %
MEXICO	15	3	11	1	5.64 %
COLOMBIA	10	1	9	0	3.76 %
CHILE	19	3	16	0	7.14 %
ARGENTINA	4	0	3	1	1.50 %
PERU	9	0	9	0	3.38 %
BRASIL	41	2	38	1	15.41 %
TOTAL	224	19	195	10	84.21 %
Segundo sua categoria TIER no mundo		16.96 %	32.88 %	26.32 %	

Fonte: (Uptime Institute Tier Certification Map, 2019, elaboração própria).