



PROFESSIONAL MASTER'S THESIS

**Key Factors for
a Cybersecurity and Cyberintelligence Policy
in Brazil**

Marcelo Garcia

Brasília, Junho de 2023

UNIVERSITY OF BRASILIA

Faculty of Technology
DEPARTMENT OF ELECTRICAL ENGINEERING

UNIVERSITY OF BRASILIA
Faculty of Technology

PROFESSIONAL MASTER'S THESIS

**Key Factors for
a Cybersecurity and Cyberintelligence Policy
in Brazil**

Marcelo Garcia

*Professional Master's Thesis submitted to the Department of Electrical
Engineering as a partial requirement to obtain
the degree of Master in Electrical Engineering*

Examination Board

Robson Albuquerque, Ph.D, FT/UnB
Advisor

João José Costa Gondim, Ph.D, FT/UnB
Internal Examiner

Luiz Octávio Gavião, Ph.D, Escola Superior de
Guerra
External Examiner

CATALOG SHEET

GARCIA, MARCELO

Key Factors for a Cybersecurity and Cyberintelligence Policy in Brazil [Federal District] 2023.

PPEE.MP.044, viii, 74 p., 210 x 297 mm (ENE/FT/UnB, Master, Electrical engineering, 2023).

Professional Master's Thesis - University of Brasilia, Faculty of Technology.

Department of Electrical Engineering

- | | |
|--------------------|--------------------------------|
| 1. Cybersecurity | 2. Cyberintelligence |
| 3. Public policies | 4. Public-private partnerships |
| I. ENE/FT/UnB | II. Título (série) |

BIBLIOGRAPHIC REFERENCE

GARCIA, M. (2023). *Key Factors for a Cybersecurity and Cyberintelligence Policy in Brazil*.

Professional Master's Thesis, Department of Electrical Engineering, University of Brasília, Brasília, DF, PPEE.MP.044, 74 p.

ASSIGNMENT OF RIGHTS

AUTHOR: Marcelo Garcia

TITLE: Key Factors for a Cybersecurity and Cyberintelligence Policy in Brazil.

GRADE: Master in Electrical Engineering YEAR: 2023

Permission is granted to the University of Brasilia to reproduce copies of The Professional Master's Thesis and loan or sell such copies for academic and scientific purposes only. The authors reserve other publication rights and no part of The Professional Master's Thesis may be reproduced without the written permission of the authors.

Marcelo Garcia

Dept. of Electrical Engineering (ENE) - FT

University of Brasilia (UnB)

Darcy Ribeiro Campus

CEP 70919-970 - Brasília - DF - Brazil

DEDICATION

I dedicate this work to the brave and free spirits

who take the courage to think;

to those who blaze trails and

are not ashamed to try,

since erring is human,

and success,

Divine.

To my children – whom I hope may be such men,

as never to trade freedom – nor relinquish pride.

ACKNOWLEDGMENTS

To my country, whom I chose to serve, and from the cradle has served me first; to all those who, in efforts thousand, till this point helped me so I can return a bit of what I have seen and learned with the privilege of researching on the nation's behalf.

To my advisor, Prof. Dr. Robson Albuquerque, for the steadfast support, precise remarks, and practical guidance, on whose behalf I also thank all Professors, teachers, and staff in the Post Graduation Program at the Electrical Engineering Faculty of the University of Brasília for the academic environment and efforts.

To Prof. Dr. Octavio Gavião for the support in the quantitative analysis and to all researchers, experts, and colleagues who graciously contributed to the survey whose data was processed and analyzed in this research.

To my wife and family, for their frequent patience and eternal love.

To my parents and those before them. That I may honor their toils.

ABSTRACT

This work aims to understand the current state of the Brazilian national cyber capability and identify promising avenues for its improvement by evaluating key success factors for a national Cybersecurity and Cyberintelligence policy in Brazil. We first seek to establish a reference framework for assessing national cyber capabilities, with a scale adequate to the still developing reality of Brazil in the area. We then employed the framework to compare Brazil and a country with a matching geopolitical scale – Spain, although more advanced in cyber capabilities, as found by the study. To identify avenues for improving the Brazilian situation, we collected the opinion of Brazilian specialists through interviews and questionnaires and processed their answers with the multi-criteria decision method of probabilistic preference composition. We analyzed the results and isolated a set of factors of ample preference and consensus among the interest groups involved, which could parameterize the first edition of the policy and elevate Brazil's cyber capability to an acceptably established level. We also identified factors significant to advancing national cyber capabilities in other countries but with little consensus among Brazilian interest groups, especially concerning funding and subsidies. These groups should discuss those factors in a public-private forum, harmonizing their demands and expectations and cooperating so that future policy editions further elevate Brazil's cyber capability to strategic and dynamic levels.

RESUMO

Este trabalho visa mapear as condições atuais da capacidade cibernética nacional brasileira e identificar vetores promissores para seu desenvolvimento, avaliando os principais fatores de sucesso para uma Política Nacional de Cibersegurança e Ciberinteligência no Brasil. Em primeiro lugar, buscamos estabelecer um quadro de referência para avaliar as capacidades cibernéticas nacionais, com escala adequada à realidade ainda em desenvolvimento do Brasil na área. Em seguida, empregamos o quadro de referência numa comparação entre o Brasil e a Espanha, um país com escala geopolítica similar ao Brasil, embora mais avançada em capacidades cibernéticas, conforme concluído pelo estudo. Para identificar os vetores de melhora, coletamos a opinião de especialistas brasileiros através de entrevistas e questionários, que foram processados com método de decisão multicritério por composição de preferências probabilísticas. Os resultados foram analisados, sendo possível identificar a partir deles um conjunto de fatores de amplo consenso e preferência entre os grupos de interesse envolvidos, que poderiam parametrizar uma primeira edição da política e elevar a capacidade cibernética do Brasil a um patamar aceitável. Também identificamos fatores significativos para o avanço das capacidades nacionais de outros países mas com pouco consenso entre os grupos de interesse brasileiros, especialmente em relação a financiamento e subsídios. Tais grupos devem discutir esses fatores em fórum público-privado, harmonizando suas demandas e expectativas e cooperando para que futuras edições da política elevem a capacidade cibernética do Brasil para patamares estratégicos e dinâmicos.

INDEX

1	INTRODUCTION	1
1.1	OBJECTIVE	2
1.2	RESEARCH DELIMITATION AND CONTRIBUTIONS	3
1.3	RESEARCH ORGANIZATION	4
2	LITERATURE REVIEW	5
3	METHODOLOGY	13
3.1	ASSESSMENT BUILDING AND COMPARISON WITH SPAIN.....	14
3.2	STAKEHOLDER GROUPS IDENTIFICATION	16
3.3	INTERVIEWS WITH SPECIALISTS AND IDENTIFICATION OF RELEVANT FACTORS	17
3.4	QUESTIONNAIRE PREPARATION AND SUBMISSION	20
3.5	ANSWER PROCESSING.....	23
4	RESULTS AND ANALYSIS	25
4.1	ASSESSMENT FRAMEWORK AND COMPARISON WITH SPAIN	25
4.2	COLLECTED SURVEY DATA	27
4.2.1	RESPONDENTS QUALIFICATION	27
4.2.2	ANSWERS TO THE QUESTIONNAIRE	29
4.2.3	SUBGROUP PREFERENCE DIFFERENCES	35
4.3	ANALYSIS.....	37
4.3.1	1ST-TIER: TOP-RATED FACTORS	37
4.3.2	2ND-TIER: FACTORS FAVORED BY MOST BUT WITH SIGNIFICANT DIFFERENCES BETWEEN STAKEHOLDER GROUPS	39
4.3.3	3RD-TIER: FACTORS PERCEIVED WITH LESSER RELEVANCE.....	41
4.3.4	4TH-TIER: FACTORS PERCEIVED AS LEAST RELEVANT	42
4.3.5	SPECIALISTS' SUGGESTED LOCATIONS FOR CYBER TECH HUBS IN BRAZIL	43
5	CONCLUSIONS	47
	REFERENCES	49
	APPENDICES	56
A	INTERVIEW SCRIPT	57
B	QUESTIONNAIRE	58
C	MATRICES	65
D	R CODE	69

List of Figures

1.1	Digital technologies already underlie practically all strategic, economic and industrial processes in society.....	1
2.1	Countries with documentation accessed by this research.....	10
3.1	General workflow performed in this research	13
3.2	The three core cyber disciplines	14
3.3	The Frameworks’s five disciplines	15
3.4	Stakeholder groups.....	17
4.1	Assessment Built and employed in comparison between Brazil and Spain.	25
4.2	Number and proportion of Respondents per Stakeholder Group.....	28
4.3	Respondents Education	28
4.4	Years of professional experience in Cybersecurity and Cyberintelligence	31
4.5	Years of professional experience in innovation and entrepreneurship	31
4.6	Years of professional experience in public policy formulation	31
4.7	Radial histogram with years of professional experience	32
4.8	Overall person-years of professional experience in cyber, business and public policy, accumulated by the set of specialists consulted in this research. Colors numbered from one to ten mean the amount of person-years coming from specialists with that many years of individual accumulated experience.....	32
4.9	Visual summary of answers to the questionnaire. Each chart presents the distribution of answers to its corresponding question, according to the Likert scale adopted, from “Totally agree” – in dark blue, to “Totally disagree”, in dark red.	33
4.10	Overall Probabilistic Preferences. Pareto threshold and gradient clines marked.....	34
4.11	Comparison of Composite Probabilistic Preferences (CPP) curves between the full set and different stakeholder groups.	35
4.12	Results diagram with the 8 essential factors found (blue: related to demand; red: related to market; yellow: related to intellectual capital and labour) and associated stakeholders (gray).	38
4.13	Votes on where to host Cyber Tech Hubs in Brazil.....	45
4.14	Cities with most votes: potential candidates for hubs of national scope. Circle size proportional to number of votes received.....	46
4.15	Other cities with relevant voting: potential candidates for regional or niche-specific hubs, in partnership with the State or Municipality. Circle size proportional to number of votes received.	46

List of Tables

2.1	Bibliographic References per Country	7
2.2	Critical aspects observed in the literature review	10
3.1	Assesment levels and respective meanings.	16
3.2	Interviewee demography.....	18
3.3	Critical aspects mentioned in the literature and in the interviews	19
3.4	Questionnaire.....	21
4.1	Ranked array of preference probabilities, as calculated by the CPP method over the questionnaire answers; and the accumulated preference probability up until each rank.	30
4.2	Rank differences between subgroups and full set. Particularly high rank (>5) differences between stakeholder groups emphasized in red (down) or blue (up). Four tiers of aspect preferences in marked in green, yellow, orange and red, from most to least preferred. Grayed lines are beyond the Pareto threshold.	36
C.1	Matrix of frequencies of Likert values in the answers to the questionnaire, for the full set of respondents and for the state agents and entrepreneur/specialist stakeholder groups: 5 - totally agree; 4 - agree in part; 3 - nor agree nor disagree; 2 - disagree in part; 1 - totally disagree.	66
C.2	Matrix of frequencies of Likert values in the answers to the questionnaire, for the Public Funding, Academia and Entrepreneur/Specialist stakeholder groups: 5 - totally agree; 4 - agree in part; 3 - nor agree nor disagree; 2 - disagree in part; 1 - totally disagree.	67
C.3	Matrix of composed preference probabilities calculated by the CPP method over the questionnaire answers, for the full set of respondents and for each subgroup.	68

1 INTRODUCTION

The object of this research impacts the maintenance of a secure society and its sovereign state. Digital technologies already underlie practically all strategic, economic, and industrial processes in society (see Fig. 1.1, demanding effective Cybersecurity to protect these processes and ensure its transactions and data are carried through wholly and safely [1]. The same reasoning applies to the state, with the additional caveat of its permanent need to know and understand its current and upcoming threats to counter and overcome them, hence the need for Cyberintelligence [2].

A thriving Cybersecurity market would also contribute to a more developed national economy and potentially induce innovation and growth in the country's extant markets. In a globally competitive market, it is even the case that Cybersecurity development is imperative because, with secure production chains and digital transformation processes, a nation will better retain industrial competitiveness in the coming decades [3].

One must also note that the state demands of Cybersecurity and Cyberintelligence are simultaneously an opportunity to be taken advantage of since this demand can foster national economic development, with incentives for entrepreneurs, dynamization of the economy, and increase of internal revenue and



Figure 1.1: Digital technologies already underlie practically all strategic, economic and industrial processes in society.

employment [4].

With that in mind, it is necessary to assess Brazil's current cyber capability, and it was only logical to do it against an objective framework. We realized, however, that it was necessary to build a framework of our own: the frameworks available in the literature, though competently made, would either focus on more technologically advanced countries [5, 6] or would compromise scale detail to include both advanced countries and those with still incipient cyber capabilities [7, 8, 9]. In this aspect, the framework we developed is novel among the internationally available frameworks. It provides a resolution scale of attributes relevant to countries like Brazil in the intermediate tier of national cyber capabilities. We then employed the framework in a national cyber capabilities comparison between Brazil and Spain [10].

We proceeded to the identification of promising avenues of improvement for Brazilian capabilities. It was clear in the revised literature that every country that developed its cyber capability did so with the concurrence of state action, especially through the evaluation, negotiation, and establishment of Policies and Strategies [11] targeted at assimilating risks and opportunities posed by the cyber technologies.

The assessment gave us a solid starting point. However, these risks and opportunities are part of a complex system with local peculiarities and multiple stakeholders who may have different viewpoints on similar issues and attribute different weights to distinct factors. It was imperative, therefore, to listen to Brazilian specialists operating in the field.

Therefore, we had the opportunity to draw from other countries' experiences and understand which aspects therein would be most promising in the Brazilian case, in the eyes of Brazilian specialists. For that, we relied on a survey among Brazilian specialists [12] from the many stakeholder groups involved in the theme.

The survey consulted specialists on the side of public demand (consolidated and organized by the policy) and on the side of private supply (directed and supported by the policy to meet public demand). The specialists representing public demand included members of Brazilian Federal and state Police bodies [13], the Armed Forces [14], and the Brazilian Intelligence System [15], which all have established competence and jurisdiction over the matter. We selected specialists from the supply side representing Academia, research centers, innovation centers, and technology venture capital.

The survey data included a multiple choice questionnaire constructed from the domain of information available in models already implemented in other countries in the cybernetic theme. The answers to the questionnaire were processed in their raw format with a multi-criteria decision method. With the results obtained, we analyzed, evaluated, and discussed the key success factors for a Cybersecurity and Cyberintelligence Policy in Brazil.

1.1 OBJECTIVE

This research aimed to identify key success factors for a national Cybersecurity and Cyberintelligence Policy that would optimally elevate Brazilian national cyber capability.

This objective unfolded itself in the following intermediate objectives:

I. Understand the current state of Brazilian national cyber capability:

- i) Revise literature referring to national cyber capabilities.
- ii) Build an assessment framework appropriate to the scale of Brazil and other countries still developing their cyber capabilities.
- iii) Employ the framework in a real-world comparison between Brazil and another country of similar geopolitical scale.

II. Identify promising avenues of improvement:

- i) Identify the stakeholder groups involved in building national cyber capability.
- ii) Interview key members of these stakeholder groups.
- iii) Identify relevant factors from the literature and the specialists' interviews.
- iv) Build a questionnaire for a survey onto an ampler base of specialists.
- v) Submit the questionnaire and receive the answers.
- vi) Process the answers to the questionnaire with a multi-criteria decision method.
- vii) Analyze the results.
- viii) Write the research results, analysis, and conclusion.

1.2 RESEARCH DELIMITATION AND CONTRIBUTIONS

The research considers the Brazilian political-strategic framework and, for exploratory and comparative purposes, that of some other countries. The choice of countries was limited to those with publicly available documentation and a democratic constitution, as the institutional dynamics of autocratic regimes would not apply to the Brazilian case.

To study private sector engagement models, we considered relevant strategies in pioneering and leading countries such as the United states [16] and Israel [17]; the United Kingdom, for presenting considerations on the degree of private engagement in the sector [11]; France [18], for the common condition with Brazil of the need to preserve sovereignty against the dominance of a foreign private sector; and Spain, for presenting excellent results in its initiatives with modest resources and strategic dimensions comparable to Brazil's [10]; besides other countries with a similar demand and possibilities.

The Spanish case was studied in greater detail and compared to Brazil, due to the mentioned similarities and for representing a feasible and rational model for Brazil to consider. This comparison used the assessment framework created and was published as an article in the 17th Iberian Conference on Information Systems and Technologies under the following information: *GARCIA, Marcelo; MENDONÇA, Fabio; ALBUQUERQUE, Robson. Assessments on National Cyber Capability: A Brazilian Perspective in a Comparison with Spain. In: 2022 17th Iberian Conference on Information Systems and Technologies (CISTI). Madrid: IEEE, 2022. p. 1-6 [10].*

1.3 RESEARCH ORGANIZATION

Chapter 1 contextualizes the theme, delineates the research problem, and enunciates the question that guides the present study, unfolding it into the final and intermediate objectives and identifying the constraints that delimit the research and the existing gaps in Brazilian policy that justify it.

Chapter 2 covers the available literature, using reviews by international organizations on the subject and studies focused on specific countries, from which common and differential factors emerge from the cases of key countries.

Chapter 3 describes the methodology, enumerating the steps taken to achieve the research objectives and detailing the specialists' demography, the questionnaire, the respondents, and the method for analyzing the responses.

Chapter 4 presents and applies the collected data to the proposed treatment, then analyzes the results and validates the developed decision support method.

Chapter 5 concludes the study, presenting a summary of the research, the method, and the result, emphasizing the delimitations of the research in terms of scope and depth, and offering an evaluation of the question that guided the work.

2 LITERATURE REVIEW

Setting political-strategic guidelines at the national level is seen globally as a condition for adequately addressing cyberspace risks [7]. For such guidelines, it is important, first of all, to assess a country's current capability through an objective framework so that it can inform policymakers and also serve as a comparison ground for evolution measurement.

Thus, many assessment frameworks were created in the last decade to analyze and compare national cyber capabilities. The European Cybersecurity Agency (ENISA) – which focuses on the harmonization of national Cybersecurity policies and strategies of its member countries [19]–, for example, created a comprehensive framework to evaluate European nations [6]. The International Telecommunications Union (ITU) [7] and the Potomac Institute [20] tried to abridge as many countries as possible globally; the Belfer Center's [8] included 30 countries in its top cyber capability ranking, focusing on 10 of those in last year's edition [9]; the Swiss Federal Institute of Technology's (ETH) [21] encompassed Switzerland, France, Germany, Italy, the Netherlands, Finland, and Israel; the Organization of American States (OAS) study [22] focused in the Americas; and the study from International Institute for Strategic Studies (IISS) [23] on geopolitical allies and adversaries of the US and China.

The assessments also differ in the criteria evaluated, with most institutions developing their criteria. OAS, in its turn, employed Oxford Global Security Capacity Centre's Cybersecurity Capacity Maturity Model (CMM) [24]. That model, however, places Cyberintelligence advice too late in the cybersecurity chain. It also presents it as an indicator rather than a requisite, which is a problem since it is easier to design reasonable Cybersecurity with Cyberintelligence informing it first [25].

The Belfer Center assessment presented an appealing visualization, similar to Gartner's "magic quadrant" [26]. It used, however, around 30 indicators mapped to 8 objectives, with multiple indicators connecting to multiple objectives. We believe this has the problematic potential to propagate eventual weight imbalance among the criteria, all the more so when some indicators are subjective ("global soft power") and might be considered only marginally related to cyber capability ("mobile speed" and generic "patent applications" for example) [8, 9]. Such imbalances might only be visible when comparing known countries pairwise: Brazil, for example, figured in the Belfer 2020 study [8] as more cyber-capable than Italy. We know that quite the opposite is true, which has been corrected in the 2022 edition [9].

Brazil figured in ITU's ranking, having jumped from 70th to 18th in its 2020 world rank. One must note, though, that ITU assesses governmental commitments rather than capabilities ([7], p. 130). Indeed, there was an acute improvement in the perception of the Brazilian commitment to the cyber agenda, but an official strategy still needs to be developed [27].

In Brazil, the cybernetic sector received special attention from the Armed Forces, being incorporated as an essential strategic technological sector in the National Defense Strategy since 2012 [28], establishing the elimination of national dependence on the sector as a goal for the Brazilian Army. This independence, however, is impossible to achieve to its fullest extent without mastering the semiconductor industry, which was — and still is — incipient in Brazil. Coincidentally, in the same year, the Brazilian state-owned

semiconductor company, CEITEC, was also created [29]). This company, however, almost went through liquidation due to accumulated losses over the years [30].

Without the industrial base of semiconductors, it remains for Brazil to operate Cybersecurity at the level of software and, eventually, firmware (software embedded in hardware). A much more modest but feasible goal would be the reduction of national dependence on foreign software technology. The Brazilian Army is, however, still extremely dependent on foreign technology for the operations and Cybersecurity of its own Cyber Defense Center – Centro de Defesa Cibernética – CDCiber [31], created in 2010 and integrated into the Joint Command of Cybernetic Defense in 2014 [32].

As for the legal framework for Security issues, there is a National Policy for Information Security [33], which has yet to expand or evolve into Cybersecurity. The National Intelligence Policy [15], in turn, confirms cyber attacks as one of the eleven priority threats to be faced by the country in the coming years and establishes the expansion of the operational capacity of intelligence in cyberspace as one of its ten guidelines, without however, specifying how to achieve it.

The National Cybersecurity Strategy, recently established [34], unfortunately also failed to fill this gap, being considered by some as “exceptionally vague” [27], and it is plausible that one of the reasons for this is precisely the fact of not having had a National Policy that preceded and adequately guided it.

Considering the Security, Defense, and Development triad essential to maintaining the state [35], evaluating the Development aspects linked to the cyber issue is also necessary. In Brazil, the National Strategy for Science, Technology, and Innovation [36] addresses the cyber issue, but in a still marginal way, diluted among several other themes and disconnected from objective demand (op. cit., p. 105), not least because its lack of association with a Policy or Strategy that orders the use of technology to be promoted and developed.

Meeting the state’s demand for Cybersecurity could hardly do without the private sector. In addition, coupling public demand with promoting private initiative has provided a competitive advantage in countries that emerged successfully and early in terms of the development of their national cyber capabilities [11, 4]. These countries generally implement this relationship through public-private partnerships, which assume various arrangements and strategies from case to case [37, 38, 39, 40]. In the US, for example, the public-private partnership materialized in the venture capital investment company In-Q-Tel [41, 42], created by the US Central Intelligence Agency (CIA) to obtain technology to supply the demand collected from the intelligence and national security community.

In Israel, partnerships materialize from the interaction between research laboratories of the armed forces and startups from those same laboratories, with veteran entrepreneurs serving as angel investors [43]. In Spain, state action on cyber issues only advanced more significantly after the creation of the National Council for Cyber Security [44], which began to organize the state’s cyber demands based on joint deliberations between all relevant state actors. The demand initially came from established companies, but currently, there is an emphasis on encouraging entrepreneurs from their initial stages. The same effort to connect public demand with the private market is also found in Asian countries, such as Japan [45], India [46], China [47, 48], and Taiwan [49].

Table 2.1 below presents a summary of the literature reviewed in this study, by country.

Table 2.1: Bibliographic References per Country

Country	Reference	Article Title
United states	RATHJE 2019 [50]	Survive, But Not Thrive? The Constraining Influence of Government Funding on Technology startups
	AGGARWAL 2018 [51]	Comparative industrial policy and Cybersecurity: the US case
	ZHANG 2016 [52]	A Study on Cybersecurity Startups
	REINERT 2013 [41]	In-Q-Tel: The Central Intelligence Agency as Venture Capitalist.
	KENNEY 2011 [53]	How venture capital became a component of the US national system of innovation
	WEINGARTEN 2005 [54]	How Venture Capital Thwarts Innovation
	BELKO 2004 [42]	Government Venture Capital: a case study of the In-Q-Tel model.
	MOLZAHN 2003 [16]	The CIA's In-Q-Tel Model Its Applicability
	BENS 2001 [55]	Accelerating the Acquisition and Implementation of New Technologies for Intelligence: The Report of the Independent Panel on the Central Intelligence Agency In-Q-Tel Venture
Israel	SHULMAN 2021 [43]	Unit 81: The elite military unit that caused a big bang in the Israeli tech scene – Veterans of the IDF's secretive technological division are the entrepreneurs driving major changes across the industry
	DANINO 2017 [56]	Cyber Security Economics in Israel
	ADAMSKY 2017 [57]	Israeli Odyssey toward its National Cyber Security Strategy
France	D'ELIA 2018 [18]	Industrial policy: the holy grail of French Cybersecurity strategy?
	FRANCE 2017 [58]	Label France Cybersecurity – Catalogue 2017 des Offres Labelisées
Spain	GARCIA 2022 [10]	Assessments on National Cyber Capability — A Brazilian perspective in a comparison with Spain
	ESPAÑA 2018 [44]	Orden PRA/33/2018, Ministerio de la Presidencia
	INCIBE 2017 [59]	Key findings from the Catalog and knowledge map of R&D+i in Cybersecurity
United Kingdom	CASELLI 2021 [60]	The Cambridge Phenomenon; An Innovation System Built on Public Private Partnership
	CARR 2016 [11]	Public-private partnerships in national cyber-security strategies

Table 2.1 – *Continued from previous page*

Country	Reference	Article Title
Canada	BRANDER 2013 [61]	Government Sponsored versus Private Venture Capital — Canadian Evidence
European Union	OECD 2022 [3]	Cybersecurity Policy Making at a Turning Point. Analysing a new generation of national Cybersecurity strategies for the Internet economy
	BRANDAO 2021 [62]	Playing the Market Card: The Commission’s Strategy to Shape EU Cybersecurity Policy
	CALCARA & MARCHETTI 2021 [63]	State-industry relations and Cybersecurity governance in Europe
	GRUBER 2017 [64]	Innovation, skills and investment: a digital industrial policy for Europe
	ENISA 2017 [38]	Public Private Partnerships (PPP) Cooperative models
	EUROPE 2016 [65]	Commission signs agreement with industry on Cybersecurity and steps up efforts to tackle cyber-threats
India	KSHETRI 2015 [46]	India’s Cybersecurity Landscape: The Roles of the Private Sector and Public–Private Partnership
Japan	BARTLETT 2018 [45]	Government as facilitator: how Japan is building its Cybersecurity market
	AGGARWAL 2020 [66]	New Economic statecraft: Industrial Policy in an Era of Strategic Competition
Taiwan	HUANG 2018 [49]	A centralised Cybersecurity strategy for Taiwan
China	LIU 2021 [48]	Evaluating performances and importance of venture capitals: A complex network approach
	AUSTIN 2020 [67]	Five years of cyber security education reform in China
	AGGARWAL 2020 [66]	New Economic statecraft: Industrial Policy in an Era of Strategic Competition
	CHEUNG 2018 [68]	The rise of China as a Cybersecurity industrial power: balancing national security, geopolitical, and development priorities
	WANG 2013 [47]	How Government Venture Capital Guiding Funds Work in Financing High-Tech startups in China: A ‘Strategic Exchange’ Perspective
Brazil	GARCIA 2022 [10]	Assessments on National Cyber Capability — A Brazilian perspective in a comparison with Spain
	OAS 2020 [69]	OAS Cybersecurity Capacity Review – Federative Republic of Brazil
	BRASIL 2023 [70]	PNCiber – Apresentação do Projeto
	BRASIL 2020 [34]	Decreto nº 10.222, de 05 de fevereiro de 2020. Estratégia Nacional de Segurança Cibernética

Table 2.1 – *Continued from previous page*

Country	Reference	Article Title
	STRONNEL [27]	Brazil's cyber security strategy leaves much to be desired
	BRASIL 2019 [71]	Glossário de Segurança da Informação
	BRASIL 2018 [33]	Política Nacional de Segurança da Informação
	BRASIL 2016 [15]	Política Nacional de Inteligência
	BRASIL 2012 [13]	Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos
	BRASIL 2020 [72]	Estratégia Nacional de Defesa, 2020
	BRASIL 2020 [73]	Política Nacional de Defesa, 2020
	BRASIL 2016 [14]	Livro Branco de Defesa
	BRASIL 2014 [74]	Doutrina Militar de Defesa Cibernética
	BRASIL 2014 [32]	Portaria Nº 2.777/MD, de 27 de Outubro de 2014 - (Criação do Comando de Defesa Cibernética)
	BRASIL 2012 [28]	Estratégia Nacional de Defesa, 2012
	BRASIL 2010 [31]	Portaria nº 666, de 4 de agosto de 2010 - (Criação do Centro de Defesa Cibernética)
	BRASIL 2021 [75]	Lei Complementar nº 182, de 1º de junho de 2021 (Marco Legal das Startups)
	BRASIL 2018 [36]	Estratégia Nacional de Ciência, Tecnologia e Inovação
Comparatives	ITU 2021 [7]	Global Cybersecurity Index 2020
	ENISA 2020 [6]	European Union Agency for Network and Information Security – National Capabilities Assessment Framework 2020
	ENISA 2016 [19]	NCSS Good Practice Guide: Designing and Implementing National Cyber Security Strategies
	HATHAWAY 2015 [20]	Potomac Institute Cyber Readiness Index 2.0
	VOO 2022 [9]	Harvard Kennedy School, Belfer Center for Science and International Affairs – National Cyber Power Index 2022
	VOO 2020 [8]	Harvard Kennedy School, Belfer Center for Science and International Affairs – National Cyber Power Index 2020
	BAEZNER 2019 [21]	Swiss Federal Institute of Technology – National Cybersecurity Strategies in Comparison – Challenges for Switzerland
	OAS 2020a [22]	Cybersecurity risks, progress, and the way forward in Latin America and the Caribbean – 2020 Cybersecurity Report
	IISS 2021 [23]	Cyber Capabilities and National Power: A Net Assessment



Figure 2.1: Countries with documentation accessed by this research

We noticed common problems addressed by the literature covering different countries, as referenced in the Table 2.1 above. These problems could be classified into four broad categories:

- A. The demand
- B. Development and Venture Capital
- C. Market, Incentives and Risks
- D. Intellectual Capital and Labor

Table 2.2 presents, therefore, the revised literature and problems addressed by it according to the above categories.

Table 2.2: Critical aspects observed in the literature review

Category	Problem	References
A: state demand	Government technical lag	MOLZAHN 2003 [16]; CHRISTENSEN e PETERSEN 2017 [76]; ESPAÑA 2013 [77]; KSHETRI 2015 [46]; WANG 2013 [47]; LIU 2021 [48]; HUANG 2018 [49]; BELKO 2004 [42]; BENS 2001 [55]

Table 2.2 – *Continued from previous page*

Category	Problem	References
	Organization of governmental demand	WEINGARTEN 2005 [54]; WANG 2013 [47]; CARR 2016 [11]; BRANDER 2013 [61]; WEISS 2019 [37]; OECD 2012 [3]; SHORE 2011 [40]; CHRISTENSEN e PETERSEN 2017 [76]; AGGARWAL 2018 [51]
	Public contracting models	CARR 2016; CALCARA 2021 [63]; SHORE 2011 [40]; BRASIL 2021 [75]; INCIBE 2017 [59]
B: Subsidies and Venture Capital	Access to capital	KENNEY 2011 [53]; BELKO 2004 [42]; BENS 2001 [55]; CALCARA 2021 [63]; WANG 2013 [47]; AGGARWAL 2018 [51]; RIBEIRO NETO 2020 [78]
	Critical stage for startup support	WEINGARTEN 2005 [54]; BRANDER 2013, p. 276 [61]; ZHANG 2016, p.13 [52];
	Other support policies	BARTLETT 2018 p.11-12 [45]
	Venture capital investments	REINERT 2013 [41]; BELKO 2004 [42]; CARR 2016 [11]; WEINGARTEN 2005 [54]; WANG 2013 [47]; KENNEY 2011; SHULMAN 2021 [43]; DANINO 2017 [56]; D’ELIA 2018 p. 394 [18]; ZHANG 2016, p. 13 [52]
C: Market, Incentive and Risks	Market size and sustainability	D’ELIA 2018, pp. 392, 403 [18]; HUANG 2018 [49]; BARTLETT 2018 [45]; ZHANG 2016, pp. 12, 18; [52]; DANINO 2017 [56]; CALCARA 2021 p.5 [63]; [18]; GRUBER 2017 [64]; DANINO 2017 [56]; FRANCE 2017 [58]
	Association to security and intelligence	SHULMAN 2021 [43]; DYDUCH 2018 [79]; CHEUNG 2018 [68]; D’ELIA 2018 [18]; ZHANG 2018 [52], p. 15; CALCARA 2021 [63], p. 4;
	Legal and regulatory uncertainty	VIEIRA et al. 2019 [80]

Table 2.2 – *Continued from previous page*

Category	Problem	References
D: Intellectual Capital and Labour Force	Brain Drain	CARNEIRO 2020 [81]; NELSON 2015 [82]; AUSTIN and LU 2020 [67]; ZHANG 2016 [52]; AUSTIN and LU 2020 [67], pp. 173-193;
	Business education	MALACH-PINES 2002 [83]
	Technical workforce education	DANINO 2017 [56]; AUSTIN and LU 2020 [67], pp. 173-193; ZHANG 2016 [52], p. 13; ADAMSKY 2017 [57] p. 119; AUSTIN and LU 2020 [67]
	Technology Clusters	COHEN et al 2017 [4]; D’ELIA 2018 [18] pp 394, 402; ZHANG p. 37 [52]; ADAMSKY 2017 [57] p. 119; DANINO 2017 [56]

3 METHODOLOGY

The research intends to assess Brazil’s cyber capabilities and identify avenues for their improvement. Other countries and international organizations have performed national capability assessments in the last years to improve their condition or better understand their allies’ or adversaries’ condition. We revised the assessments available, observing their criteria and eventual motivation and critically evaluating their usefulness to the Brazilian reality, deriving our assessment framework adequate to the Brazilian scale. Many of the assessments mentioned included comparisons of national capabilities from different countries (Table 2.1, line "Comparatives"), so we also built and published a comparison based on the framework created [10].

This comparison allowed identifying areas where Brazilian cyber capability could be better formed and established. However, improving that capability was a complex problem, with many arrangements and models referred to by other countries and interest groups (see Table 2.1). It was thus advisable to listen to the opinion of specialists on the different possibilities for solving this problem. Since these specialists necessarily belong to groups that have a stake in the problem, this research qualifies as "action-research". As Vergara prescribes [84], the problem is "collective and in which researchers and participants representing the situation or problem are involved in a cooperative or participatory way."

We, therefore, partitioned the research into the intermediate objectives stated in section 1.1 and followed the workflow presented in Fig. 3.1. We further describe below the methodology for each objective.

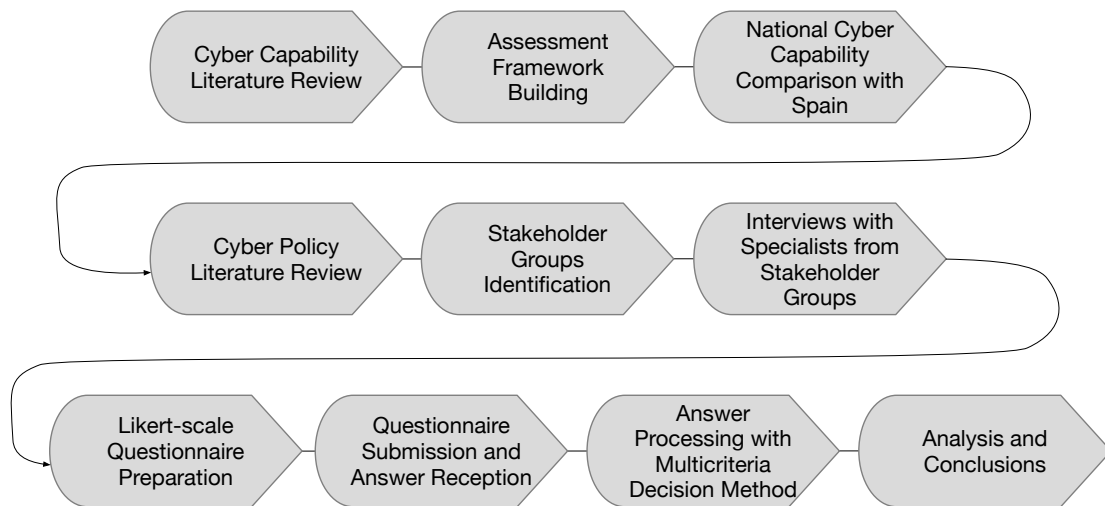


Figure 3.1: General workflow performed in this research

3.1 ASSESSMENT BUILDING AND COMPARISON WITH SPAIN

We have identified five disciplines – three technical and two organizational – around which it was possible to understand national cyber capabilities and build an assessment framework with resolution geared to orient countries at the formative stage of such capability [10]. The three technical disciplines – *Cyberintelligence*, *Cybersecurity*, and *Cyber Operations* – are the core disciplines of cyber, as can be immediately understood from the diagram presented in Fig. 3.2.

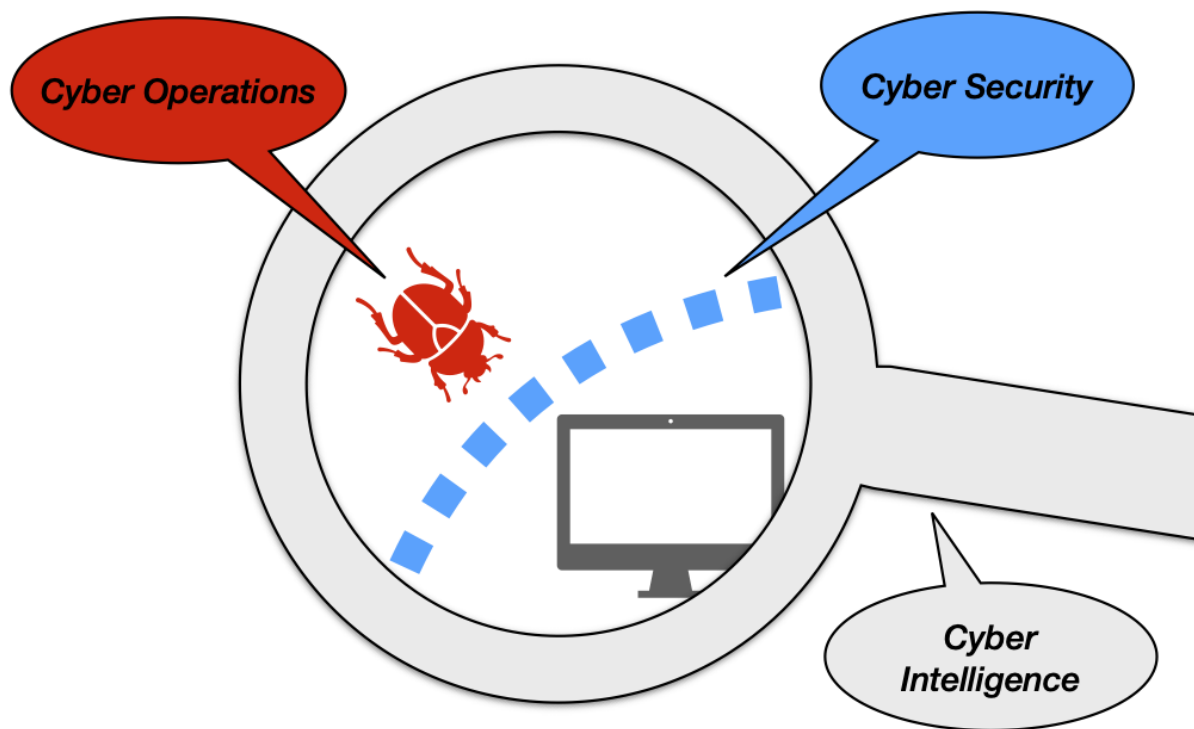


Figure 3.2: The three core cyber disciplines

As for the organizational disciplines, *institutional governance* deals with organizing the endeavors, resources, roles, and responsibilities in public and private institutions that act at any level of the three technical disciplines, whereas *synergy with society* deals with partnerships with other sectors of society, such as the scientific, financial and educational sectors, in order to further promote and leverage cyber capability. The diagram in Fig. 3.3 shows the disciplines and axes of the assessment framework.

The framework employs a scale based on the CMM model and used by ENISA [6], plus a preceding “Absent” level that we found necessary to distinguish from the “Initial” level in those models, resulting in the scale shown in Table 3.1. We used the framework in comparing Brazil and Spain, a country that has reached a satisfactory capability with resources within the Brazilian possibilities. Results are presented further in the Results chapter.

The framework is then revisited in the analysis to assess the improvement that could be attainable against the current scenario if the factors identified in the next section of the research – namely the survey and its processing – could leverage a successful policy. It must be noted that the Framework was not offered nor shown to the specialists consulted in the survey in order not to interfere in any way with their opinion



Figure 3.3: The Frameworks's five disciplines

since one of the main goals of this research was to collect information directly from those who are dealing in practice with cyber disciplines, be them technical or organizational, in the public or private sector and as users or providers.

We also noted that *Cyber Operations*, as defined in the assessment, are rarely mentioned in Policy documents, barred confidential pieces [9]. The reason for such is straightforward: Cyber Operations are deemed unlawful in most or all countries unless perpetrated by the state actor, in pursuance of lawful obligation, or by private entities thereby authorized, or still under the guise of research or national security [85]. Because of the strategic advantage it provides, it often falls under the realm of intelligence, military, or law enforcement authority, with details and methods protected by legal confidentiality or eventually abridged discretely under the label of either Cyberintelligence or cyber security. Therefore, although contemplating all core cyber disciplines in the assessment, this research explicitly investigated key success factors for a

Table 3.1: Assessment levels and respective meanings.

#	Level	Symbol	Meaning
0	<i>ABSENT</i>	(∅)	The assessed criterion is absent or has yet unknown initiatives.
1	<i>INITIAL</i>	(*)	The assessed criterion is in embryonic stage, with generic discussions and eventual isolated or uncoordinated actions.
2	<i>FORMATIVE</i>	(**)	There is consensus on general directions but specific plans are not in place yet. Some capacity has been demonstrated but mostly in ad-hoc or irregular fashion.
3	<i>ESTABLISHED</i>	(***)	Mission is defined and an action plan exists. Capacity is established, but still not in optimal relation to demand.
4	<i>STRATEGIC</i>	(****)	Capacity is established and satisfies demand in a dimension fit to the country's strategic imperatives.
5	<i>DYNAMIC</i>	(*****)	Capacity is advanced and able to absorb strategy changes without disruption, evolving and adapting to new circumstances, demands, and technologies.

Cyberintelligence and Cybersecurity Policy as per global parlance and practice for policy making in the area.

With the framework ready, the assessment of a country's national cyber capability becomes a matter of historical research, gathering the necessary data to assign a capability level to each of the 17 assessment criteria, according to the scale in Table 3.1. This data can be obtained and analyzed from policy documents, legislation, public records, specialized knowledge, and news records for Brazil and Spain and employed in comparing Brazil and Spain's national cyber capabilities. We chose Spain for the comparison with Brazil for having similar geopolitical interests and strategic dimensions and for having reached excellent results in its cyber initiatives yet with modest resources. The comparison results are described in an article published (10) and summarized in Results section 4.1.

3.2 STAKEHOLDER GROUPS IDENTIFICATION

First, we needed to identify the groups directly interested in the problem resolution by reasoning about the contemporary social actors involved in the process, as detailed below and represented in Fig. 3.4. The first group corresponds to the group of state agents with demands for cybernetic capacity. It is inherently important, thus, to consult experts from this group. The next group consists of those individuals who, within the national scenario, would have the potential capacity to meet the demands of the first, that is, technical specialists in cyber security and Cyberintelligence.

This workforce, in turn, has to be managed and organized. For this role, as is both tacit knowledge and noted by the available literature, most countries turn to the private sector, which is more dynamic and adaptable to new technologies, avoiding burdening the public service with personnel management and long-term pensions. In addition, this sourcing from the private sector also serves the State's objective of developing the nation's economy. Therefore, we also have entrepreneurs as a stakeholder group.

As this is a new market, still in formation, in which the government is interested in having access to its products and services as soon as possible, it is usual to establish public incentive policies to boost the

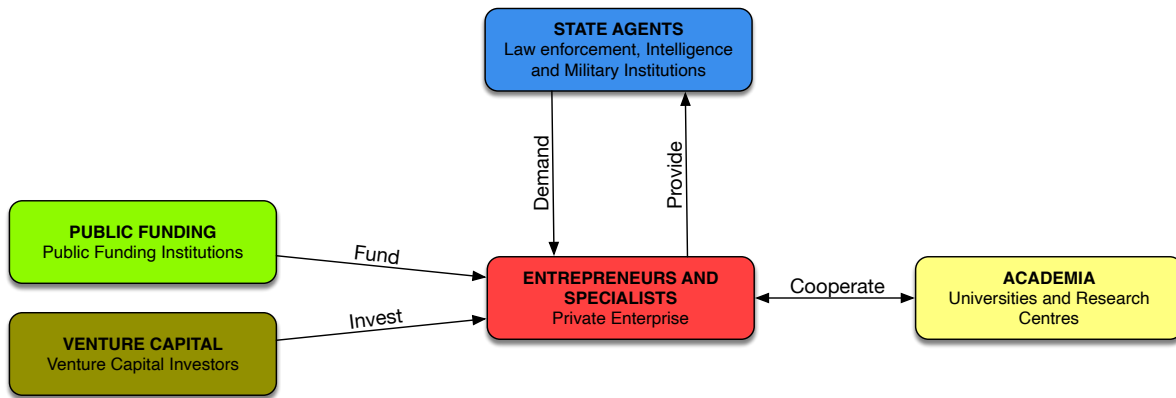


Figure 3.4: Stakeholder groups

sector. Therefore, we also have public development agencies as actors of interest in this process.

It is also observed, with the maturation and multiplication of private venture capital funds, the tendency of the private sector to join together with the public sector in the very allocation of capital in strategic sectors for the government. In this partnership, private capital seeks better rates of return for its portfolio while the government minimizes investment costs. This partnership was especially noticeable in the US and Israel, the two countries most recognized for their advanced cyber capabilities. Consequently, private venture capital managers are also stakeholders in the cyber issue.

Finally, the issue of building a state's cyber capability is a problem common to many countries. The groups identified here were also consistently discernible in the Literature (Table 2.1). Such consistency will allow the correlation between the literature and the interviewees' experience, as described in the next section.

3.3 INTERVIEWS WITH SPECIALISTS AND IDENTIFICATION OF RELEVANT FACTORS

After identifying the interested parties, we sought to select and interview at least one expert from each group, except for state agents, of which the author himself is a member. The interviewees were presented with the research goal to identify key factors to improve Brazilian national cyber capability and asked about their general perception of the matter.

Building on elements of their answer, they were progressively asked about their view on the categories and problems previously identified in the literature review (Table 2.2). The general script used as a basis for the interviews is annexed in Appendix A. However, the actual sequence and form of the questions varied greatly depending on the interviewee to accommodate for conversation fluidity. Table 3.2 presents the qualifications and experience of the specialists selected and interviewed.

Table 3.2: Interviewee demography

Interv.	Stakeholder group	Education and experience summary	Years of experience
IE1	Entrepreneur	PhD in Mathematics, M. Sc. in Computer Science and Baccalaureate in Electrical Engineering. Founder of high-tech startup and Coordinator of a R&D Center.	40 years
IE2	Entrepreneur	Cybersecurity specialist and Founder of Cybersecurity Startup.	24 years
IE3	Specialist	Senior engineer. Chief Cybersecurity Vulnerability Research.	24 years
IP1	Public funding	M. Sc. in Production Engineering, Baccalaureate in Mechanical Engineering, Business Administration and Military Engineer.	25 years
IP2	Public funding	Director of Entrepreneurship and Innovation; 5 years experience with innovation funding and 20 years as IT specialist.	25 years
IP3	Public funding	Mechanical Engineer. Manager with 25 years experience with innovation funding and technological qualification.	25 years
IV1	Venture capital	Director of Cybersecurity Strategy. M. Sc. in Computer Science. Founder of two tech startups. Corporate Venture manager.	26 years
IV2	Venture Capital	Angel Investor. Private Venture Capital Fund Manager. Director and Advisor in Startup Accelerators.	25 years
IA1	Academia	PhD in Electrical Engineering, M. Sc in Computer Science and Baccalaureate in Electrical Engineer. Professor in Federal University, with experience in Information Security and Cybersecurity.	38 years
IA2	Academia	PhD and M. Sc. in Electrical Engineering and Baccalaureate in Computer Science. More than 20 years of experience in Cyber Security.	21 years
IA3	Academia	PhD, M. Sc. and Baccalaureate in in Electrical Engineering. Professor in Federal University, experienced in support to entrepreneurship.	47 years

During the interviews, we took notes on the main comments and observations made by the interviewees. Crossing these comments and observations against the revised literature made it possible to compile a preliminary matrix of such factors evidencing their mentions in the literature and by the interviewees, as presented in Table 3.3 below.

Table 3.3: Critical aspects mentioned in the literature and in the interviews

Critical Aspect / Interviewee	IE1	IE2	IE3	IP1	IP2	IP3	IV1	IV2	IA1	IA2	IA3
A1: Demand meeting by the private sector	X	X	X								
A2: Dialogue forum between government and private sector			X								
A3: Dedicated authority to Cybersecurity and Cyberintelligence	X	X									
A4: Contracting models that encourage the private sector to provide to the government	X	X									
A5: Legal framework to facilitate the contracting of startups by the government					X	X					
B1: Venture capital market	X	X			X	X					
B2: Sector subsidy policies	X	X	X		X	X					
B3: Continuity of subsidy programmes	X			X							
B4a: Early stage startups (seed capital for prototypes and business plans)			X	X	X	X					
B4b: First customers stage (Series A)			X	X							
B4c: Scale-up stage (series B and beyond)			X	X							
B5: Tax incentives	X										
B6: Startup contracting by the government reduces risk for the private sector		X			X						
B7: Public-private partnership models for venture capital investment	X										
B8: Startup incubators and accelerators						X					X
B9: Corporate venture							X				
C1: National demand sustainability	X	X	X								
C2: Dual use (civil and state – law-enforcement, military and intelligence) of cyber security and Cyberintelligence technologies		X									
C3: Market dominance by foreign companies	X	X	X								
C4: Access to regional market (e.g.: Am. Latina)	X	X	X								
C5: Global market niches	X	X	X								
C6a: Positive impact due to the association with technical competence		X									

Table 3.3 – *Continued from previous page*

Critical Aspect / Interviewee	IE1	IE2	IE3	IP1	IP2	IP3	IV1	IV2	IA1	IA2	IA3
C6b: Negative impact due to association with electronic surveillance	X										
C7: Government dependency as only or main client	X	X									
C8: The level of juridical and regulatory uncertainty discourages the creation of startups in the country		X									
D1: Growing and lasting country brain drain		X									
D2: Programs for repatriation of intellectual capital and technical workforce	X	X	X					X			
D3: Business management experience			X								X
D4: Teaching computer programming at fundamental school (K-12)			X							X	
D5: Lines of research and courses in Graduation and Post-graduation							X	X	X	X	
D6: Cyber technology clusters to catalyze industry growth						X					

3.4 QUESTIONNAIRE PREPARATION AND SUBMISSION

The revised literature and the interviews with Brazilian specialists offered an initial point of view for creating a questionnaire that permeates the critical aspects of the problem. We could forward this questionnaire to a broader group of specialists whose position might clarify the relevant factors for solving the problem within a national frame of reference.

The questionnaire begins with a qualification section with five questions to record and assess the level of experience of the respondents in their areas of expertise, followed by 30 subject-matter questions. We divided these questions across four sections corresponding to the identified categories of problems and critical aspects. The division serves primarily for the respondents' readability, visualization convenience, and manipulation of the form by the respondent (Table 3.4).

We implemented and distributed the questionnaire in a Google Form – see Appendix B for its English translation. We wrote the questions in a way as to provoke and collect the experts' opinions regarding the critical aspect or factor addressed, that is, how much the specialist considers that factor or aspect addressed is key to solving the problem. The response scale follows a Likert scale [86], with five possible alternatives for all responses:

- 1) Totally agree

- 2) I agree in part
- 3) I do not agree nor disagree
- 4) I disagree in part
- 5) Totally disagree

We opted for a single scale for all questions for the convenience of the respondents and to avoid disengagement, given the relatively high number of questions, the respondents' high qualification level, and the valuable time they were already giving to answer the questionnaire. For the same reason, we opted for the scale with only five levels instead of 7 or 9, as the five-level scale already provides a relevant distinction between opinions.

The question related to the critical aspect C8 – juridical and regulatory insecurity – was dropped from the questionnaire in order to limit the questionnaire to 30 questions, but also because it is mostly out of reach by the executive branch of the government, depending on slow-changing civil law and affecting all Brazilian business in general.

We invited specialists and authorities from each stakeholder group identified in Section 3.2. On the public side, we counted on competent authorities, area specialists, and academics from bodies that deal with Cybersecurity, Cyberintelligence, or Cyber Operations. In the private sector, we selected and invited entrepreneurs, experts, executives, and professionals from startups and technology companies, business accelerators and incubators, and venture capital and corporate venture managers.

All survey participants received questions from all sections, as it was relevant to know whether there were statistically significant differences depending on the expert's interest group. All in all, the questionnaire was submitted to around 90 specialists, being fully responded to by 59 of them – *i.e.*, two-thirds – a high engagement rate, for which we highly appreciate the respondents' efforts.

Table 3.4: Questionnaire

#	Question
A1	Does the organization of government cyber demands and their forwarding to the private sector tend to accelerate the incorporation of technological innovations for the country's intelligence and public security agencies?
A2	Would the existence of a forum for dialogue between government and entrepreneurs be important for the market's understanding of the government's demands for security and cybernetic intelligence?
A3	Would the existence of an authority dedicated to Cybersecurity and Cyberintelligence issues in Brazil be important to guide the private sector on the subject?
A4	Do public procurement models discourage the private sector from providing products and services to the government?
A5	Does the Legal Framework for Startups (Law 182/2019, in force since Sep. 2021) facilitate the hiring of innovative technologies by the public sector?

Table 3.4 – *Continued from previous page*

#	Question
B1	Is it easy for Brazilian technology startups to access and obtain venture capital?
B2	Would public policies to encourage national entrepreneurship be decisive for the development of a cyber industry in Brazil?
B3	Is the discontinuity of Brazilian development programs throughout successive governments an impediment to the development of a cyber industry in Brazil?
B4a	Should public subsidy policies in the cyber area prioritize entrepreneurs in search of seed capital ("seed capital") to validate their idea/prototype in the market?
B4b	Should public subsidy policies in the cyber area prioritize startups that already have a working prototype and business plan but need to obtain their first customers? ("Series A")
B4c	Should public subsidy policies in the cyber area prioritize startups that already have a product developed and initial customers but need capital to acquire scale and increase the customer base? ("Series B")
B5	Would tax incentives for the cyber sector be a success factor for the development of the cyber industry in the country?
B6	Does government hiring startups make them more attractive to private venture capital managers?
B7	Is the venture capital investment model in partnership between government and private capital viable and advantageous in Brazil for the parties involved (entrepreneur, government and private capital)?
B8	Would Business incubators and accelerators be a fundamental success factor for the development of a cyber industry in Brazil?
B9	Would Cyber startups incubated or accelerated by large companies ("corporate venture") have a better chance of success than the others?
C1	Is there enough demand (including government and private initiative) to sustain a cyber industry in the country?
C2	Can security technologies and cybernetic intelligence developed for State institutions also generate dual solutions for civil and commercial use?
C3	Is the dominance of foreign companies in the cyber market in Brazil an impediment to the flourishing of a local industry?
C4	Do Brazilian cyber startups have a better chance of success targeting the regional Latin American market in addition to the national market?
C5	Are there niches in the global cyber market in which Brazil could successfully establish itself?
C6a	Would the involvement of a startup in government intelligence and Cybersecurity projects reflect positively on the company's image by associating it with the ideas of technical competence and Law and Order?
C6b	Would a startup's involvement in government intelligence and Cybersecurity projects provoke unwanted stigma by associating it with the idea of electronic surveillance?
C7	Is there a risk for cyber startups to develop dependence on the government as their sole or main customer?

Table 3.4 – *Continued from previous page*

#	Question
D1	Is the brain drain problem in Brazil an impediment to the establishment of a national cyber industry?
D2	Would the creation of an incentive program for the repatriation of intellectual capital and technical labor be important for the development of a national cyber industry?
D3	Does the Brazilian innovation entrepreneur have enough management skills to thrive?
D4	Is the inclusion of computer programming in basic and fundamental education important for the formation of a technologically skilled workforce in Brazil?
D5	Would the creation of lines of research in Cybersecurity in Undergraduate and Postgraduate courses be important for the development of the cyber industry in Brazil?
D6	Is establishing technological hubs that bring together and catalyze cyber research and development together with other pre-existing industries important for the development of a cyber industry in the country?

3.5 ANSWER PROCESSING

The questions in the survey aimed at identifying, from the plethora of issues debated in the literature and mentioned in the interviews, which were the most relevant to the Brazilian case and, therefore, most likely to produce a positive impact if properly addressed by policy. The answers to the questionnaire were processed in their raw format with a multi-criteria decision method to obtain an objective evaluation of the relevance of the criteria associated with the questions. The method chosen was the Composition of Probabilistic Preferences – CPP [87] due to its adequacy in dealing with preferences manifested over a Likert scale [88], which is precisely the case of our specialists' answers to the questionnaire [89].

For convenience, the answers dataset was processed with the R software [90], using the publicly available CPP R package implemented by Gavião *et al.* [91]. The method calculates the joint probabilities of alternatives maximizing and minimizing their preferences in a criterion. In our dataset, the alternatives are the factors addressed in each question, and the criterion is their perceived relevance to improving Brazil's national cyber capability.

For this dataset, we needed to use only the CPP maximizing function (PMax) since we formulated almost all of the questions considering the importance of a given factor in the respondents' eyes. Two questions (B1 and D3) had been inadvertently formulated in an inverted semantics and, for that reason, had their Likert scale mirrored to be properly consumed by the maximizing function.

Question A4, in its turn, was removed from the dataset and disregarded in the analysis, as it contained a typo that led to ambiguous and opposite interpretations (as in "encourage" versus "discourage"). Although corrected shortly after being warned by one of the first respondents, the formulation of the question in the negative form (discouraged), unlike all other questions, may have misled other respondents.

The CPP maximization function uses the measures of the problem's decision matrix as input, which in our case were the frequencies of responses to the Likert scale values collected by the questionnaire.

Such frequencies were readily available from the answers spreadsheet associated with the questionnaire's Google Form. We then transposed these frequencies to a separate working spreadsheet for ease of access and manipulation and to prepare the input matrices to the CPP R function. The input matrices prepared are in Appendix C in Tables C.1 and C.2 .

The output of this process was a ranked list of preference probabilities among the full set of questions. We ran the process for the entire dataset and each stakeholder group subset to further compare the groups' differential preferences. The output was collected and added to a matrix for the analysis and can be found in the Table C.3 in the Appendix C.

In this probability matrix, each probability represents, from the CPP methodology, the chance that the aspect addressed in that alternative is preferred, to all others in the set, by the group of respondents considered.

Since these probabilities are additive within their set, it follows that, for any given subset, the sum of its individual CPP probabilities is the probability that the group of specialists considered prefers it to any other subset.

Furthermore, since probabilities are also ordinal, if we take an ordered subset, starting with the aspect of highest probability of preference and progressing sequentially until the n^{th} -ranked aspect, it follows that this very subset of size n is the one with the highest probability of being preferred to all others the same size, by the set of respondents considered.

Therefore, through this process, we have objectively reduced the problem of deciding which of the many factors or aspects are perceived to be of greater relevance (preference) to the analysis of the ordered set of aspects and the decision of how many of them should proceed to further appreciation of policymakers.

Two considerations came into play for analyzing how many ordered factors to choose. One of them is the Pareto principle [92, 93]. By applying the Pareto principle, we can choose an initial subset of size n , such that the accumulated probability of the n highest-ranked alternatives reaches 80%, meaning that the resulting subset of alternatives has an 80% probability of being the optimal one and that no smaller subset is probabilistic superior to it. Reversely, it also means that the alternatives excluded by the Pareto cut represent less than a 20% chance of being preferred by the respondents.

Additionally, clines in the overall ordered set (also equivalent to the inflection points in the curve of the plotted set) are obvious cleavage points for determining subsets and were analyzed within the Pareto subset, in order to provide options for further optimizing it.

The overall results were analyzed to identify which set of factors of a National Policy on Cybersecurity and Cyberintelligence would generate the most favorable scenario for entrepreneurship and the development of a national industry in the sector, given the Brazilian actors, possibilities, and constraints.

4 RESULTS AND ANALYSIS

4.1 ASSESSMENT FRAMEWORK AND COMPARISON WITH SPAIN

We generated the assessment framework (Fig. 3.3) according to the methodology previously described and employed it in comparing Brazil’s and Spain’s national cyber capabilities. The comparison results can be found in full in the article published by this author and collaborators [10]. In summary, the framework allowed the comparison of the cyber capabilities of Brazil and Spain based on a set of criteria across five disciplines, as presented below in Fig. 4.1.











A. INSTITUTIONAL GOVERNANCE				
	1) Clearly defined institutional leadership over Cyber Intelligence	2) Established military Cyber Command and Doctrine	3) Legal mandate for Cybersecurity	4) Well-defined roles and responsibilities for all government institutions with Cyber mandates
 BR	★★	★★★★★	★	★★
 ES	★★★★★	★★★	★★★★★	★★★★★
B. CYBER INTELLIGENCE CAPABILITIES				
	1) Autochthonous cryptography and cryptanalysis	2) Large scale collection capacity	3) International cooperation	4) Analytical and attributional capability
 BR	★★★	∅	★★★	★★
 ES	★★★★★	★★★★★	★★★★★	★★★
C. CYBER OPERATIONS CAPABILITIES				
	1) Short missions	2) Sistematic operations	3) Complex operations	
 BR	★★★	★★	∅	
 ES	★★★★★	★★★★★	★★★[★?]	
D. CYBER SECURITY CAPABILITIES				
	1) Cyber Security strategy	2) Incident response capability	3) Critical infrasctrure protection capability	
 BR	★	★★	★★	
 ES	★★★★★	★★★★★	★★[★?]	
E. SYNERGY WITH SOCIETY				
	1) Partnership with Academia and Research Centers	2) Partnership with high-tech entrepreneurship and Venture Capital	3) Access to local Cybersecurity workforce	
 BR	★	★	★★★	
 ES	★★★★★	★★★★★	★★★★★	

Figure 4.1: Assessment Built and employed in comparison between Brazil and Spain.

In terms of Institutional Governance, Brazil is in a formative stage, while Spain is considered dynamic since its Cyberintelligence systems are present in most government areas and even in the private sector [94]. Both countries have established military cyber commands and doctrines, but Spain’s doctrine is still under development [74, 95]. Regarding legal mandates for Cybersecurity, Brazil lacks statutory power and coordination among different actors, placing it in an initial stage, while Spain has a legally mandated and evolving Cybersecurity framework, earning it a dynamic assessment [96]. Spain also managed a

dynamic review in its definition of roles and responsibilities due to its National Cybersecurity Council [44], while Brazil could benefit from further descriptions for its Cybersecurity and Cyberintelligence roles and responsibilities.

In terms of Cyberintelligence capabilities, Brazil's cryptography capability is established, but its capacity has stagnated, while Spain maintains a strategic stance [77]. Spain also has a large-scale collection capacity [97] while Brazil does not. In terms of international cooperation, Brazil is open to collaboration but has a scarce workforce, while Spain has strategic cooperation with European and Ibero-American countries. Brazil has an effective capacity for forensic analysis but relies on outsourced solutions for threat intelligence, while Spain has deployed sensors for threat intelligence [98] and likely attribution analysis [99].

Regarding Cyber Operations, Brazil has established short-mission capabilities across the board and technical ability for systematic operations in many institutions. However, most of them need to implement and structure this ability formally. Conversely, Spain likely develops systematic operations at a strategic level and has some capacity for complex operations. As foreseen, the need for more documents in this area prevents a more precise picture.

Regarding Cybersecurity capabilities, Brazil's Cybersecurity strategy is at an initial level, lacking concrete instruments for implementation [34, 27], while Spain's strategy is dynamic and has undergone evolution [100]. Spain has mature incident response [94, 96] while Brazil's capabilities are in the formative stage. Still, both countries would benefit from more integration and awareness of Cybersecurity into their Critical Infrastructure.

In terms of Synergy with Society, Brazil has few partnerships with Academia and research centers, while Spain has a strategic initiative to support and coordinate Cybersecurity research [59]. Spain also has partnerships with high-tech entrepreneurship and venture capital, while Brazil's efforts in this area are still in the initial stage [36]. Both countries face challenges with access to a local Cybersecurity workforce, with talent often moving abroad [81, 82], but Spain has strategic plans to address this issue [96].

Overall, Spain demonstrates more advanced cyber capabilities compared to Brazil across various criteria assessed. Spain had earlier, steadier, and more coordinated efforts from governmental structures, which likely contributed to these results. In addition to that, three aspects seem to have strongly favoured success in Spain's cyber policymaking: being well-informed by Cyberintelligence from early stages; establishing a multi-institutional forum to deliberate on Cybersecurity policy and roles and responsibilities; and resolutely promoting private sector capacity development through Academia and entrepreneurship.

It was possible to identify the cyber disciplines in which Brazilian national cyber capability has yet to establish itself yet at a minimum acceptable level (level 3 – *ESTABLISHED*, as described in Table 3.1). If we aim to elevate the overall Brazilian national cyber capability to that level, we would be looking for the improvement of the following conditions:

A. Institutional Governance:

- Clearly define institutional leadership over Cyberintelligence;
- Define legal mandate over Cybersecurity;

- Define roles and responsibilities for all government institutions with Cyber mandates;

B. Cyberintelligence Capabilities:

- Initiate efforts for large-scale collection capacity;
- Increase and improve analytical and attributional capability;

C. Cyber Operations Capabilities

- Establish capacity for systematic operations;
- Initiate efforts for forming complex operations capability;

D. Cyber Security Capabilities

- (Re-)define and implement a Cybersecurity strategy;
- Organize and formalize incident response capacity;
- Define and establish capacity for critical infrastructure protection;

E. Synergy with Society

- Devise and establish a long-term Program for partnership with Academia and Research Centers;
- Initiate efforts for partnerships with business and venture capital communities.

The attainment of these 12 goals would remove the main deficiencies currently existing in Brazilian national cyber capability and elevate it to an overall ESTABLISHED level.

4.2 COLLECTED SURVEY DATA

In this section, we present the data collected in the survey, which consisted of the respondents' qualifications and the questionnaire answers. A field for free commentary was also available to the specialists at the end of the questionnaire. Eventual comments were collected and stored for further consideration in future research and surveys.

4.2.1 Respondents Qualification

The survey had 59 respondents in all. The group with the highest representation was that of state agents who deal with cyber security and intelligence, equivalent to 60% of respondents (Fig. 4.2). We already expected this predominance since it was the group most directly accessible from the author.

The groups representing Academia (Professors and Researchers) and the private sector (Entrepreneurs and Specialists) follow with equal representation, with ten respondents — 16.7% of the total each. Note: one of the respondents categorized himself as "Others: Private Initiative"; for processing purposes in this work, we computed his responses in the category "Entrepreneurs and specialists."

We then had four managers and specialists in government funding, all in senior management positions in funding policies and public resources at the Ministry of Science, Technology, and Innovation.

Finally, the group of venture capital investors had three participants in the survey, of which only one was available to answer the questionnaire, with the other two participating via interview. In this author’s perception, these professionals deal with a high volume of contacts and interactions, preferring verbal interaction — in which they also have the chance to clarify ad hoc doubts and exchange information — rather than filling out the written form, even if the interviews are longer. (30 to 90 minutes) than filling (10 to 20 minutes).

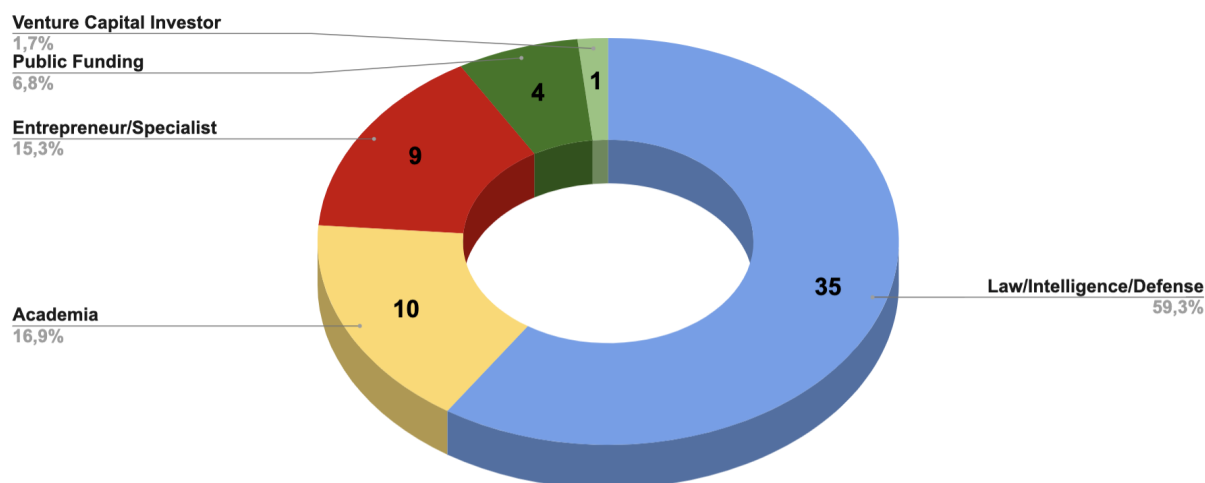


Figure 4.2: Number and proportion of Respondents per Stakeholder Group.

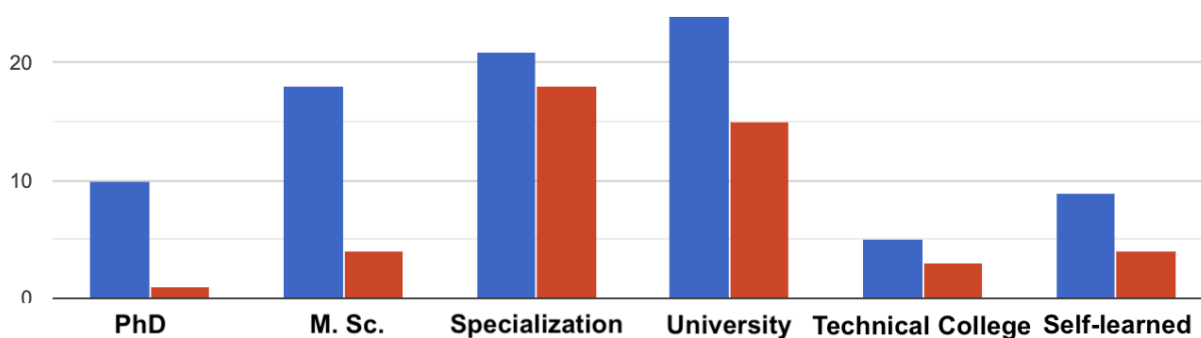


Figure 4.3: Respondents Education

As for the academic background of the respondents, most have a degree or specialization in a technical area or not, whereas the Masters and Doctorates concentrate in technical areas (Computer, Electrical Engineering, etc.) – Fig. 4.3. On the other hand, some acquired their expertise at a Technical High-school or are even self-taught, which is common among professionals in the field.

As for the time of experience of the response as a whole, 58% of respondents have ten years or more of experience in security or Cyberintelligence, with only 10% having less than two years of experience in

the area, even including non-technical professionals (Fig. 4.4). For entrepreneurship and innovation, 39% of the total have ten years or more of experience, against 21% with less than two years of experience (Fig. 4.5); and for public policies, 48% of respondents had ten years or more of experience; and 20% with less than two years (Fig. 4.6). For comparison purposes, the Fig. 4.7 presents a radial histogram with all three vectors included.

The numbers indicate that, as a whole, the respondents have a significant experience in their cyber security and intelligence, innovation and entrepreneurship, and public policies experience vectors. That warranted this research access to more than 300 person-years of accumulated experience in any of the three said vectors 4.8.

4.2.2 Answers to the Questionnaire

Figure 4.9 below provides an overview of the specialists' opinions as per their answers, with pie charts summarizing the overall proportion of choices for each alternative in the Likert scale for each question.

As explained in the methodology chapter, these answers were further processed with a multi-criteria decision method (composition of probability preferences) to estimate which questions – and, therefore, which critical aspects for a successful national cyber policy – were favored by the specialists as most relevant, resulting in a ranked array of preference probabilities.

This array and the critical aspects addressed in the respective questions are in Table 4.1, together with the critical aspects addressed in the questions. The table also indicates the accumulated preference probability up until that rank. The Pareto threshold for the accumulated preference probability is reached at rank 16, meaning that the set of aspects from C2 to D1 in the ranked list has more than 80% probability of being the most relevant to the specialists.

Indeed, the chart in Fig. 4.10 presents the curve of preference probabilities, from the most (C2) to the least (B1) favored question in the list, also evidencing the Pareto threshold and the gradient descents that can be useful to delimit the set further within that threshold.

Table 4.1: Ranked array of preference probabilities, as calculated by the CPP method over the questionnaire answers; and the accumulated preference probability up until each rank.

Q#	Rank	Preference Probability	Accum. P. P.	Critical Aspect
C2	1	0,070231476	7,0%	Dual solutions for state and civil/commercial use
D5	2	0,065186514	13,5%	Cybersecurity lines of research in Undergraduate and Graduate Courses
A3	3	0,065106215	20,1%	Authority dedicated to Cybersecurity and Cyber intelligence
A2	4	0,061909753	26,2%	Forum for dialogue between government and entrepreneurs
D6	5	0,060235614	32,3%	Establishing cyber technology hubs in the country
C5	6	0,057209561	38,0%	Niches to be explored in the global cyber market
C1	7	0,055114282	43,5%	Domestic market sufficiency
D4	8	0,049331547	48,4%	Inclusion of computer programming in basic school curriculum (K-12)
D2	9	0,047401407	53,2%	Program for repatriation of intellectual capital and technical workforce
B2	10	0,045857435	57,8%	Public policies for encouraging national entrepreneurship
B8	11	0,04539398	62,3%	Business incubators and accelerators
C4	12	0,040396195	66,3%	Latin America as a target market
B3	13	0,039195062	70,3%	Discontinuity of Brazilian development programs
C6a	14	0,038653779	74,1%	Contracts with government seen as sign of technical competence
B5	15	0,03597455	77,7%	Tax incentives for the sector
D1	16	0,027508091	80,5%	Brain drain problem
B9	17	0,027366337	83,2%	Corporate venture as better chance of success
A1	18	0,025776655	85,8%	Organizing and sourcing government cyber demands to private sector
B6	19	0,024307544	88,2%	Government-contracted startups' attractiveness to venture capital
B7	20	0,02198846	90,4%	Viability and advantage of public-private partnerships in venture capital in Brazil
B4a	21	0,018735539	92,3%	Public subsidy policies for very early-stage startups (seed capital)
B4b	22	0,017584593	94,0%	Public subsidy policies for early-stage startups (series A)
B4c	23	0,015546754	95,6%	Public subsidy policies for scale-up startups (series B+)
A5	24	0,014069562	97,0%	Startups contracting facilitated by 2019 Startups Law
C3	25	0,008584175	97,9%	Dominance of foreign companies stifles local development
C7	26	0,006714885	98,5%	Risk of dependence on government as sole or main customer
C6b	27	0,006412128	99,2%	Risk of image association with electronic surveillance
D3	28	0,005134911	99,7%	Brazilian entrepreneurs business preparedness
B1	29	0,003047712	100,0%	Accessibility to venture capital

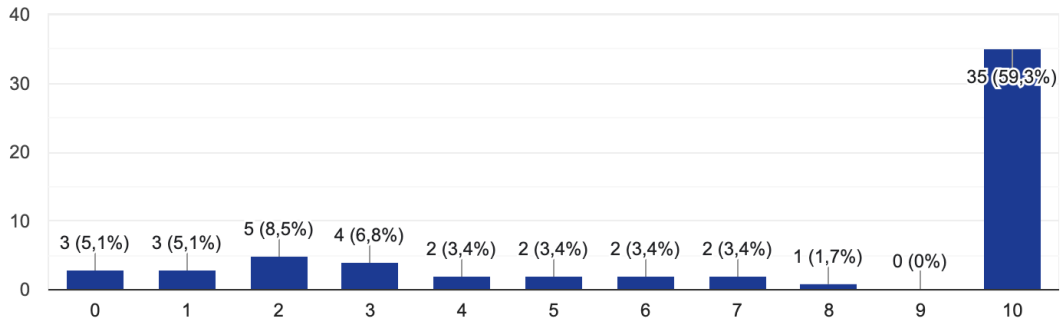


Figure 4.4: Years of professional experience in Cybersecurity and Cyberintelligence

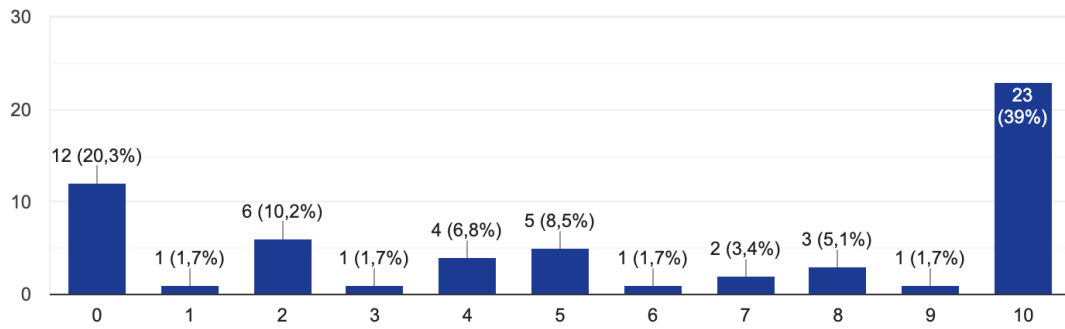


Figure 4.5: Years of professional experience in innovation and entrepreneurship

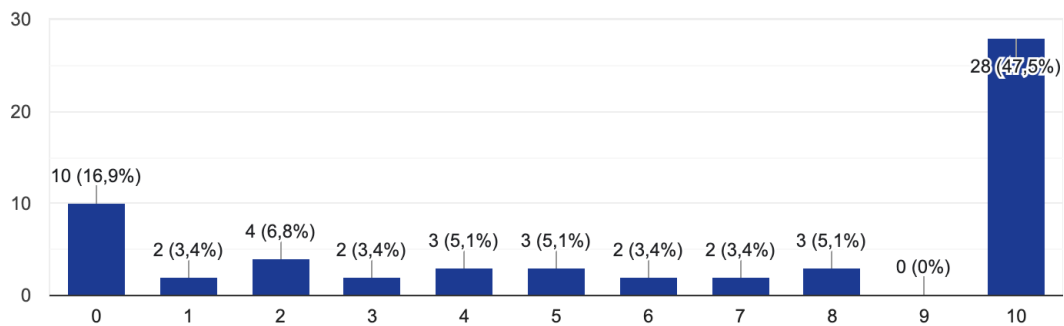


Figure 4.6: Years of professional experience in public policy formulation

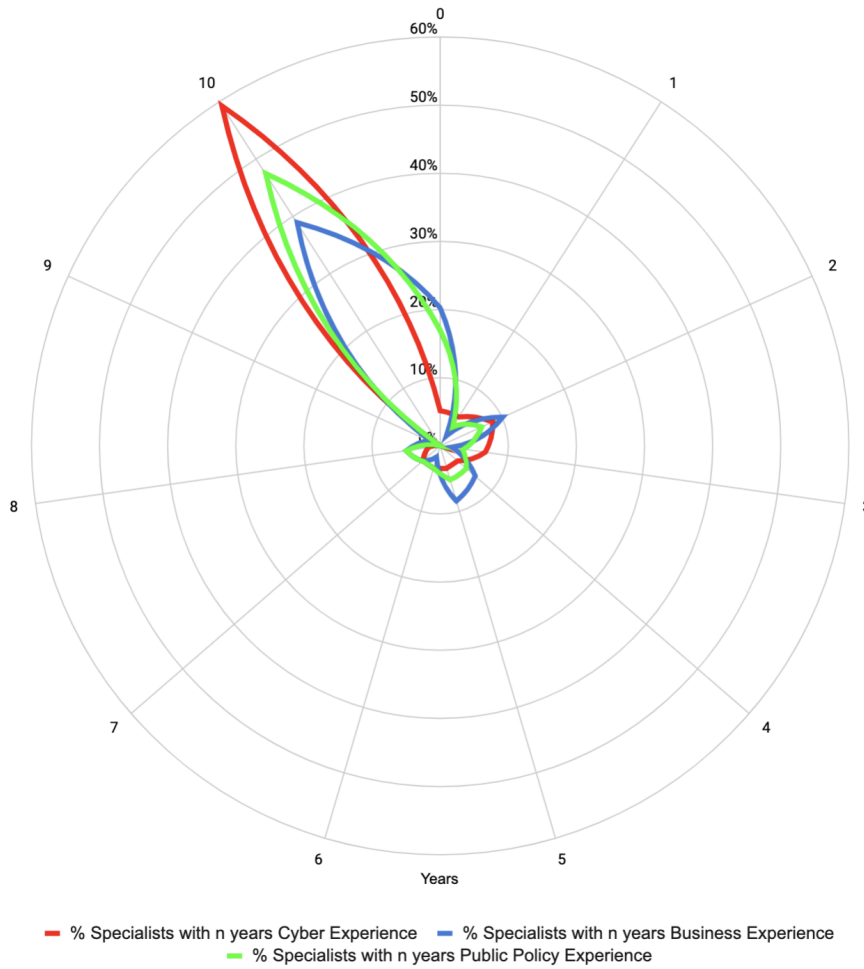


Figure 4.7: Radial histogram with years of professional experience

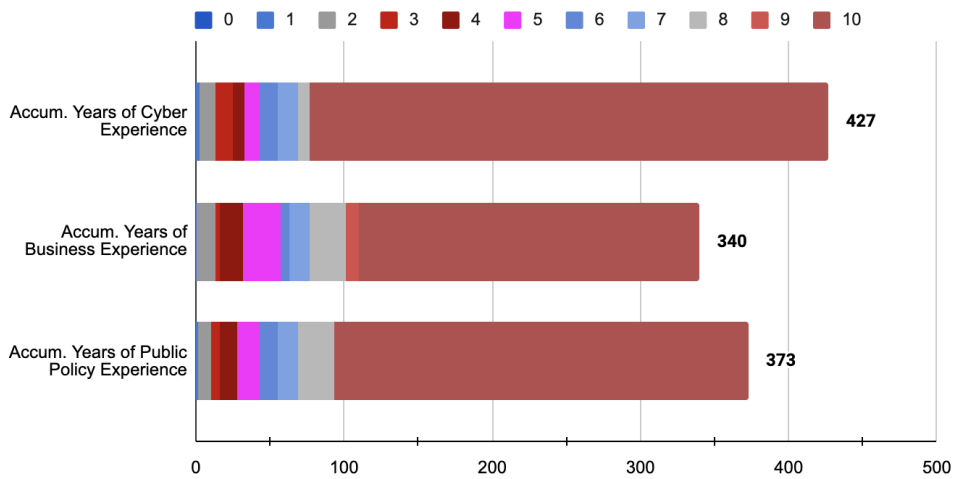


Figure 4.8: Overall person-years of professional experience in cyber, business and public policy, accumulated by the set of specialists consulted in this research. Colors numbered from one to ten mean the amount of person-years coming from specialists with that many years of individual accumulated experience.

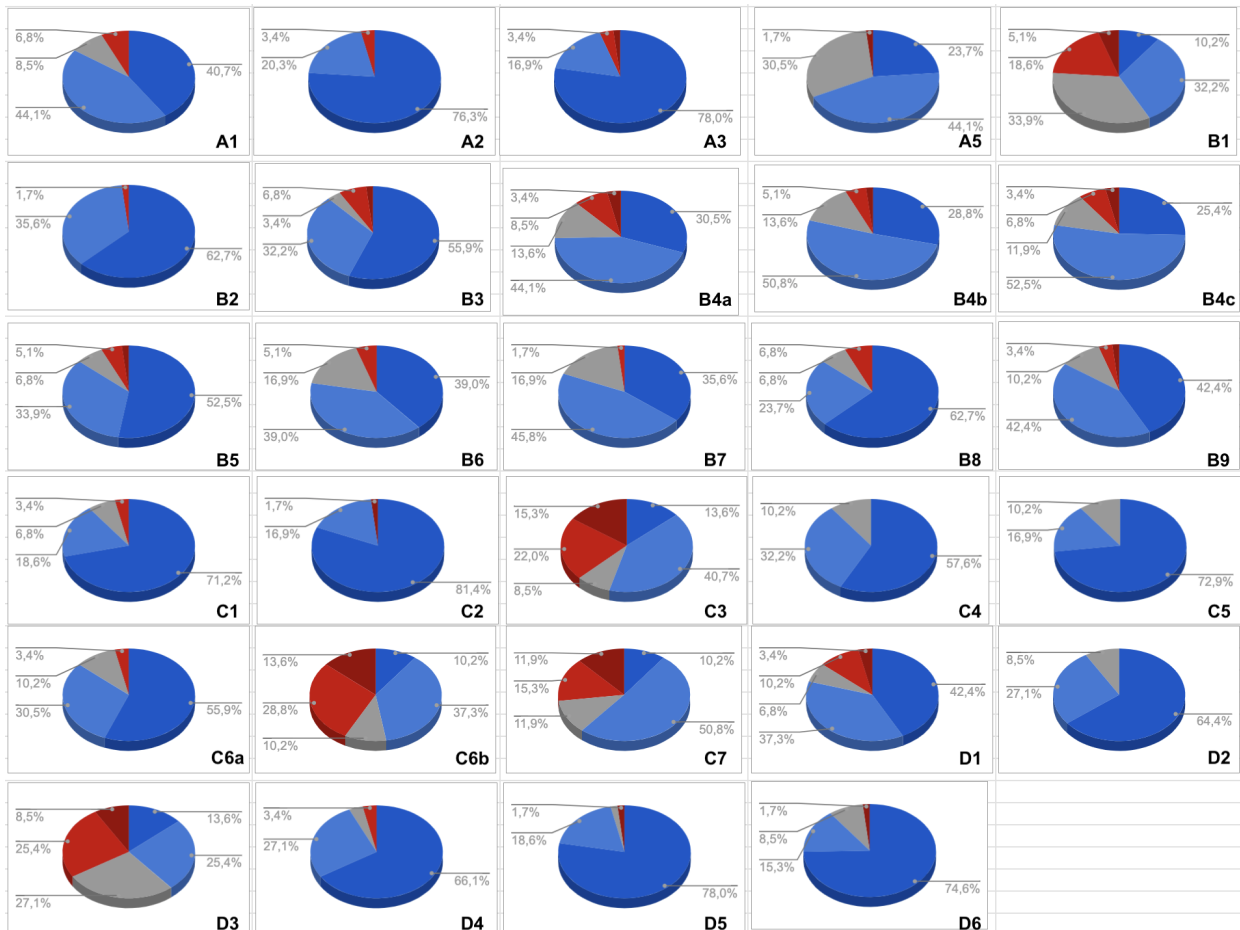


Figure 4.9: Visual summary of answers to the questionnaire. Each chart presents the distribution of answers to its corresponding question, according to the Likert scale adopted, from “Totally agree” – in dark blue, to “Totally disagree”, in dark red.

Probabilistic Composition of Preferences

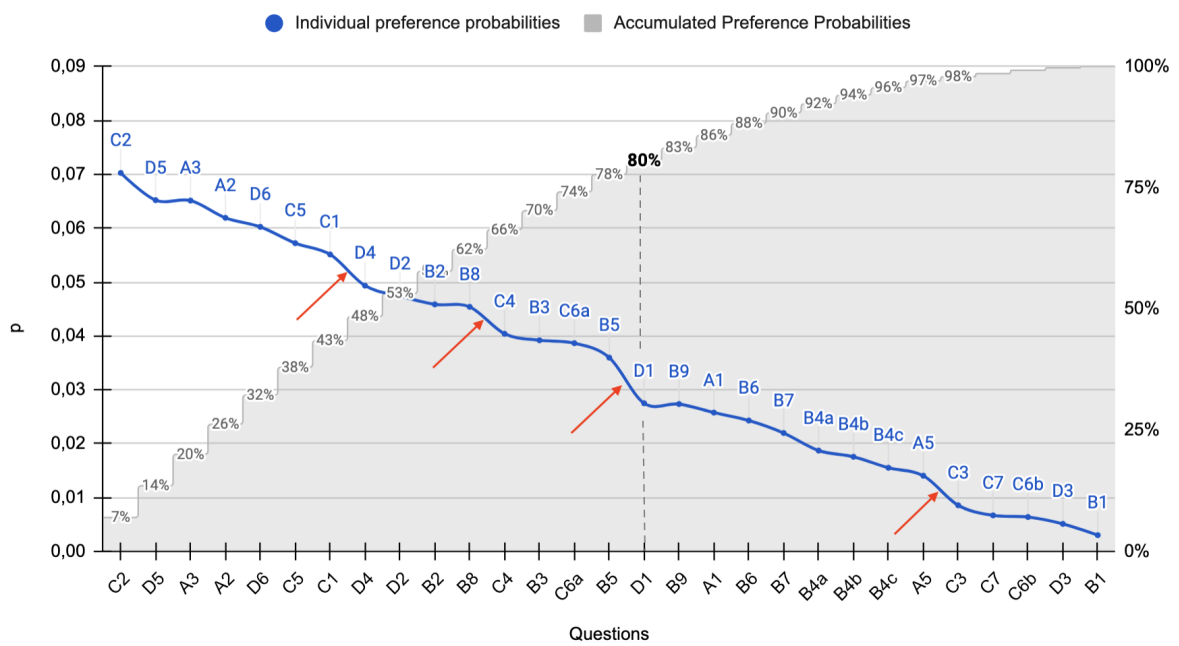


Figure 4.10: Overall Probabilistic Preferences. Pareto threshold and gradient clines marked.

4.2.3 Subgroup preference differences

We also ran the process and extracted the preference arrays from the stakeholder subgroups to identify significant subgroup preference differences in particular questions. The matrix containing all the generated arrays, ordered by the full set rank, can be found in Appendix C, Table C.3.

This matrix was used to plot the chart in Fig. 4.11, with the main curve (the ranked probability preferences from the full dataset) accompanied by the curves for each of the stakeholder subgroups, keeping, however, the question order from the full dataset rank.

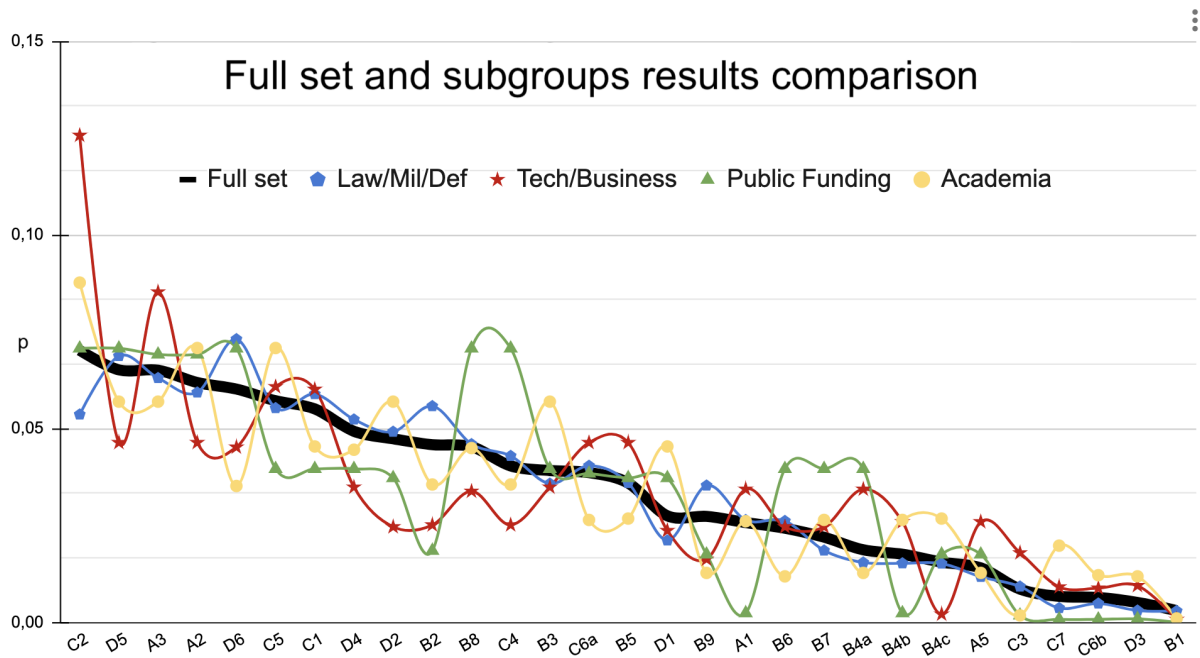


Figure 4.11: Comparison of Composite Probabilistic Preferences (CPP) curves between the full set and different stakeholder groups.

The chart hints at differences of preference among the stakeholder groups. However, to objectively assess the significance of an eventual opinion difference from a particular subgroup, we used the ranks instead of comparing the probabilities across groups since they were calculated jointly in complement only to probabilities from within that subgroup. It did not seem rigorous to compare them across groups directly. It wouldn't either be appropriate to compare them against those of the full set since the full set abridges them.

The ranks, on the other hand, are, by definition, comparable between groups. Although on a coarser scale than the probabilities, this coarseness reflects the reality of an objective consolidation of the underlying data – the probabilities – unto a discrete and finite dimension adequate to the reality of decision-making.

Table 4.2 presents then the ranks of the questions according to their preference probability in each of the stakeholders' groups, together with their difference Δ from that question's rank in the full data set. This way, for a given question i :

$$\Delta_{SubgroupDataset} = Rank_{[i,FullDataset]} - Rank_{[i,SubgroupDataset]}$$

The rank differences bigger than five positions up or down are emphasized in the table and painted as blue or red cells: a blue delta means that, for that subgroup, that aspect is perceived as more relevant – so much as to be Δ positions higher in their rank than in the general rank; and a red delta means that the aspect is perceived as quite less relevant to the group than to the full set of respondents, so much as to be Δ positions lower. We chose five as a delta sufficient to slide a question across one of the four clines in the main probability curve (see Fig. 4.10).

Table 4.2: Rank differences between subgroups and full set. Particularly high rank (>5) differences between stakeholder groups emphasized in red (down) or blue (up). Four tiers of aspect preferences in marked in green, yellow, orange and red, from most to least preferred. Grayed lines are beyond the Pareto threshold.

Q#	R	Law/I/M		Entr./Tech		Publ. Fund.		Academia		Critical Aspect
		R'	Δ	R'	Δ	R'	Δ	R'	Δ	
C2	1	8	-7	1	0	3	-2	1	0	Dual solutions for state and civil/commercial use
D5	2	2	0	6,5	-4,5	3	-1	5,5	-3,5	Cybersecurity lines of research in grad. and undergrad. courses
A3	3	3	0	2	1	6,5	-3,5	5,5	-2,5	Authority dedicated to Cybersecurity and Cyberintelligence
A2	4	4	0	6,5	-2,5	6,5	-2,5	2,5	1,5	Forum for dialogue between government and entrepreneurs
D6	5	1	4	9	-4	3	2	14	-9	Establishing cyber technology hubs in the country
C5	6	7	-1	3	3	11	-5	2,5	3,5	Niches to be explored in the global cyber market
C1	7	5	2	4	3	11	-4	8,5	-1,5	Domestic market sufficiency
D4	8	9	-1	10	-2	11	-3	11	-3	Inclusion of computer programming in basic school (K-12)
D2	9	10	-1	20	-11	17	-8	5,5	3,5	Program for repatriation of intellectual capital and tech workers
B2	10	6	4	18	-8	19	-9	12,5	-2,5	Public policies for encouraging national entrepreneurship
B8	11	11	0	14	-3	3	8	10	1	Business incubators and accelerators
C4	12	12	0	17	-5	3	9	12,5	-0,5	Latin America as a target market
B3	13	15	-2	11	2	11	2	5,5	7,5	Discontinuity of Brazilian development programs
C6a	14	13	1	6,5	7,5	15	-1	19	-5	Contracts with government seen as sign of technical competence
B5	15	14	1	6,5	8,5	17	-2	16	-1	Tax incentives for the sector
D1	16	19	-3	22	-6	17	-1	8,5	7,5	Brain drain problem
B9	17	16	1	24	-7	20,5	-3,5	23	-6	Corporate venture as better chance of success
A1	18	17	1	12,5	5,5	23,5	-5,5	20	-2	Organizing and sourcing gov. cyber demands to private sector
B6	19	18	1	20	-1	11	8	26	-7	Government-contracted startups' attractiveness to venture capital
B7	20	20	0	20	0	11	9	17,5	2,5	Viability of public-private partnerships in venture capital in Brazil
B4a	21	21	0	12,5	8,5	11	10	23	-2	Public subsidy policies for very early-stage startups (seed capital)
B4b	22	22	0	15	7	23,5	-1,5	17,5	4,5	Public subsidy policies for early-stage startups (series A)
B4c	23	23	0	28	-5	22	1	15	8	Public subsidy policies for scale-up startups (series B+)
A5	24	24	0	16	8	20,5	3,5	23	1	Startups contracting facilitated by 2019 Startups Law
C3	25	25	0	23	2	25	0	28	-3	Dominance of foreign companies stifles local development
C7	26	27	-1	26	0	27	-1	21	5	Risk of dependence on government as sole or main customer
C6b	27	26	1	27	0	28	-1	25	2	Risk of image association with electronic surveillance
D3	28	28	0	25	3	26	2	27	1	Brazilian entrepreneurs business preparedness
B1	29	29	0	29	0	29	0	29	0	Accessibility to venture capital

In Fig. 4.10, the Pareto threshold divides our group of critical aspects in two. The results in the rank differences between subgroups allow us to subdivide each of the two further, leaving our questions divided in four very distinct tiers:

- 1st-tier: Set of aspects perceived as most relevant by the full set of respondents with high consensus among all stakeholder groups.
- 2nd-tier: Set of aspects perceived as relevant by the majority of respondents (80% probability of composing the preferred set of alternatives following the 1st-tier), but with marked preference differences in some stakeholder groups.

- 3rd-tier: Aspects outside the Pareto threshold – *i.e.*, with less than 20% overall probability of being preferred by the respondents – and with marked preference differences between respondent groups.
- 4th-tier: Aspects that were not considered most relevant by any subgroup (less than 3% of preference probability), as seen in Table 4.1).

Considering those results, we proceeded to the analysis of the preferred critical aspects.

4.3 ANALYSIS

4.3.1 1st-Tier: Top-Rated Factors

The set of practically unanimous consensus factors in the specialists' perception provides an accurate view of Brazil's most acute problems involving cyber issues. Consequently, it also provides an important basis for designing lines of action to develop a cyber industry in Brazil.

These aspects were the ones identified in the 1st-tier of the results presented; they are marked in green in Table 4.2 and are listed hereunder:

C2 – Dual solutions for state and civil/commercial use

D5 – Lines of research for Cybersecurity in graduate and undergraduate courses

A3 – Authority dedicated to Cybersecurity and Cyberintelligence

A2 – Forum for dialogue between government and entrepreneurs

D6 – Establishing cyber technology hubs in the country

C5 – Niches to be explored in the global cyber market

C1 – Domestic market sufficiency

D4 – Inclusion of computer programming in the basic school curriculum (K-12)

The diagram in Fig. 4.12 shows the interplay between those aspects and the stakeholders involved.

The first one (C2) reflects the confidence of virtually all specialists that the cyber sector accommodates the development of dual solutions, that is, solutions that serve the government in its defense, security, and intelligence functions and, with pertinent modifications and adjustments, also to the civil sector. This factor also allows companies that supply these technologies to earn revenue from the civil sector, reducing their dependence on the government and boosting their growth [63, 56]. The emphatic confidence of all expert groups in this factor was a surprise in this survey and indicated the importance for public policies to channel rather than obstruct the potential for dual solutions.

Secondly, the specialists also understood that creating Undergraduate and Graduate courses specialized in Cybersecurity and structuring lines of research (D5) would be an essential factor for leveraging national

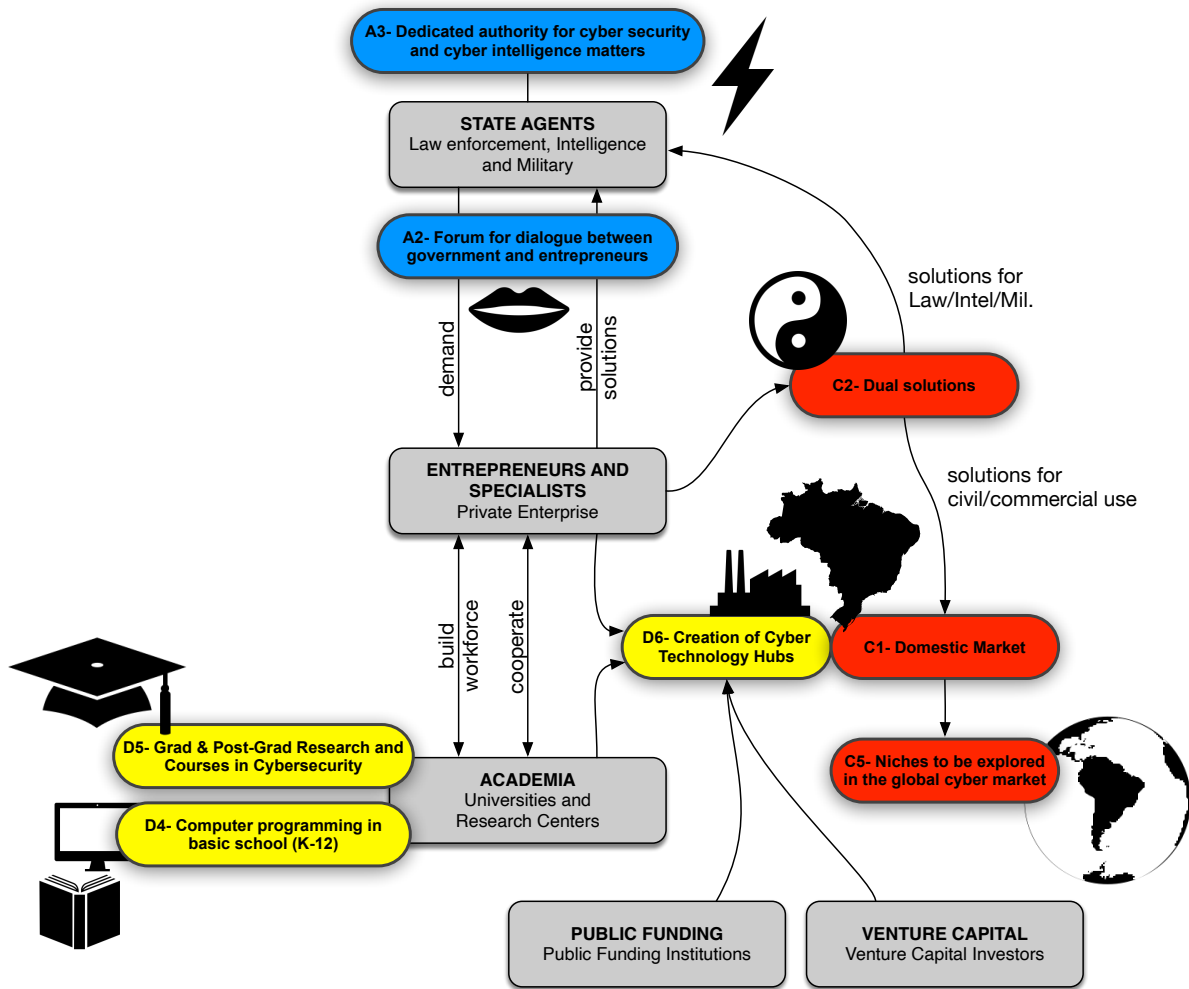


Figure 4.12: Results diagram with the 8 essential factors found (blue: related to demand; red: related to market; yellow: related to intellectual capital and labour) and associated stakeholders (gray).

cyber capacity. As commented by one of the interviewees, it would be urgent to increase the offer of cyber courses in graduation, given that there would be, according to his perception, 400,000 vacancies in the sector in Brazil. Postgraduate courses would also cooperate directly to fill these vacancies by offering the possibility of retraining professionals already trained in other areas, a widespread and well-received practice in the market.

The third aspect in the preference list points to the organizing role of the state in unlocking civil society’s potential for action and innovation in the area. The question of a Cybersecurity authority in Brazil is long overdue, with many initiatives that still need to progress past the initial talks. Very recently, the Institutional Security Cabinet (Gabinete de Segurança Institucional – GSI, a Ministry in the Executive Federal Government) proposed to create a Cybersecurity National Agency under its auspices [70], along the lines of a regulatory Agency, like the Regulatory Agency for Health and Sanitation or the Regulatory Agency for Telecommunications, for example. This proposal is under initial public consultation in Congress and has received criticism from bodies with legal mandates over cyber-related issues not contemplated in the proposal.

The fourth aspect (A2) relates to the government's ability to organize, consolidate and communicate its technological demands in cyber security and intelligence. This capacity is fundamental for leveraging the sector, a condition confirmed by the history of cyber development in other countries, according to references [37, 51, 76, 11, 61, 47, 3, 40, 54].

The following aspect, D6, relates to creating cyber technology hubs to catalyze development in the area. This strategy is one of the most traditional ones national states employ to promote development in a specific area. We will address it in more detail in a section by itself 4.3.5, using the poll realized in the survey about the most appropriate cities for harboring such cyber hubs in Brazil. We noted that among all other aspects in the 1st tier, this was the only one with some particular difference regarding stakeholder groups since, for Academia specialists alone, it would appear in the 2nd tier of aspects rather than in the 1st.

Next in the sequence come items C5 and C1, which relate to market conditions in the cyber industry. The results were surprising, as they unveiled the solid confidence of all specialists in the sufficiency of the internal (national) demand for cyber and the viability of exploring internationally competitive niches.

Finally, the D4 factor – teaching computer programming since elementary school – may not have an immediate impact, but it is still strategic since computer literacy is increasingly necessary for most future occupations. The goal of preparing every Brazilian child for a world that is undergoing digital transformation seems not only imperative but also attainable.

These eight factors compose a common ground of wide acceptability among all stakeholder groups on the issue of cyber.

4.3.2 2nd-Tier: Factors favored by most but with significant differences between stakeholder groups

Following the 1st-tier of preferred factors, the 2nd-tier comprises elements that were generally well ranked but with significant differences according to the stakeholder group. This condition suggests that the responses while confirming the importance of such factors as predicted in the literature and interviews, point to the need to investigate in greater detail the possible causes of reservations on the part of some stakeholder groups. The factors are:

D2 - Program for repatriation of intellectual capital and technical workforce

B2 - Public policies for encouraging national entrepreneurship

B8 - Business incubators and accelerators

C4 - Latin America as a target market

B3 - Discontinuity of Brazilian development programs

C6a- Contracts with the government seen as a sign of technical competence

B5 - Tax incentives for the sector

D1 - Brain drain problem

The first and last factors in this group deal with the issue of the country's brain drain. The first one (D2) suggests the importance of considering strategies that encourage the repatriation of intellectual capital and technical workforce. The latter (D1) assesses how much of an impediment the brain drain problem is to develop a cyber industry in the country.

First of all, it must be said, in the perception of the interviewees, the primary reason for the brain drain is not specifically the search for higher wages but a combination of better living conditions (especially public safety and education for children) with the possibility of professional fulfillment in a career with challenges for technicians at the height of their capacity.

These factors were of much higher concern from the academic group than the entrepreneurs or public funding groups. It seems, according to the interviews, that Brazilian entrepreneurs and specialists, although resenting the scarcity of highly skilled labor, eventually worked around it with strategies such as building teams with a large base of entry-level professionals led by very few senior professionals that would also act as mentors of the novices, somehow forming their skills internally, even facing high turnover rates.

Additionally, entrepreneurs firmly believed that an increase in the academic sector's offering and scale of technical courses could attenuate the brain drain problem (D1) over the years. However, Academia's situation is more heartfelt (see lines D2 and D1 in the Academia column in Table 4.2, compared to the entrepreneurs and specialists). That becomes a greater concern since entrepreneurs' main hope for more technical labor relies 100% upon Academia, which suffers from an even more acute brain drain. That might signal a race condition deserving a closer look and a more detailed investigation to be effectively solved. It bears mention that the creation of technology hubs itself (factor D6) might be a strategy to overcome that race condition.

The next factor (B2) concerns the importance perceived by all interest groups on the government's role as a first-rate promoter of cyber innovation and entrepreneurship. Some say this would be an implicit necessity since the government holds strategic interests and prerogatives of exclusive employment [11] in the area (such as interception technologies, state encryption, and others). Others, that the capital market does not know the technical demand as well as the State and ends up selecting poorly [54] or even giving up investing [51]. Entrepreneurs and public funding groups (public and private) do not prize government direct involvement in the matter with the same regard as state actors and Academia. Since they would be the main beneficiary of this government assistance, their skepticism should be better heard and understood. They manifest ample criticism towards the poor quality of many government programs, inadequate selection criteria, and absence of program follow-up. Due to these marked differences of understanding, factor B2 could benefit from being more deeply discussed in the forum suggested by factor A2 instead of being implemented without consensus among the stakeholders.

Factor C4 points to the possibility of also exploring the regional Latin American market — besides the national market and eventual global niches of Brazilian competitiveness, which the specialists already considered in higher priority. The Brazilian economy is well-positioned in the continent, and many industries in Brazil explore this natural proximity to increase scale. We conjecture the specialists did not appreciate

this factor more because the cyber sector in Brazil is still trying to establish itself rather than looking for scale. Still, that time may come if the first policies be successful.

Factor B3 alludes to the problem of discontinuity of Brazilian development programs, an unfortunate Brazilian tradition tied to the ebbs and flows of domestic politics and cabinet changes that occur every four years in government. Academia seemed, once more, more concerned than the other sectors, maybe for being effectively more affected by this transience. Properly implementing a State agency dedicated to the matter (factor A3) and the dialogue forum (factor A2) could remedy much of this impermanence for cyber-related programs.

Finally, sector-specific tax incentives is one of the tools considered for leveraging development in the area, as employed, for instance, in Japan [45]. As expected, this factor received a much higher rank from the entrepreneurs' group than the others. It is nevertheless clearly an accessory tool in the whole set that can be better discussed after higher priority factors are achieved.

4.3.3 3rd-Tier: Factors perceived with lesser relevance

The factors in this tier have a less than 20% probability of being preferred to the ones already mentioned in the previous levels.

B9 - Corporate venture as a better chance of success

A1 - Organizing and sourcing government cyber demands to the private sector

B6 - Government-contracted startups' attractiveness to venture capital

B7 - Viability of public-private partnerships in venture capital in Brazil

B4a- Public subsidy policies for very early-stage startups

B4b- Public subsidy policies for early-stage startups

B4a- Public subsidy policies for scaling startups

A5- Government contracting of Startups facilitated by the 2019 Startups Law

Coincidentally or not, all the factors in this tier deal with funding (B9, B7, B4a, B4b, B4c) and contracting (A1, B6, A6) startups. Corporate venture (B9) is not seen as an advantageous factor and is even more disfavored by entrepreneurs and Academia subgroups, which bears meaning. Public-private partnerships in venture capital (B7) were also not considered highly. Although found in other countries, like the United States [42, 41, 52], this kind of partnership does not exist in Brazil, to the extent of our knowledge.

It also bears consideration that the Brazilian legal framework might not favor this kind of partnership. Upon hearing how such partnerships happened in the United States and Israel [41, 43], one of the Public Funding interviewees said that had that happened in Brazil, the officers involved would have already been accused and indicted for conflict of interests.

The rank sequence curiously clumped factors regarding the preferred stage for subsidizing startups (B4a, B4b, and B4c). However, there were differences of opinion among the stakeholder groups about which startup stage would better benefit from the subsidies. Entrepreneurs and public funding agents preferred subsidizing seed capital to very early-stage startups, with entrepreneurs also supporting financing early-stage startups. Conversely, academics preferred to fund scaling startups rather than earlier-stage startups. The differences are significant and hard to peer into.

Also, curiously, the organization and sourcing of governmental cyber demands to the private sector (A1) were reasonably regarded by entrepreneurs rather than the other groups. That might signal a greater desire in the private sector to meet government demand than a willingness of the public sector to organize and outsource part of its demand. Since it is implausible that the public sector will be able to meet its demands solely by itself and its internal personnel, this result points to the necessity of elevating this discussion at public governance levels and advancing talks on how to meet the existing demand. Creating a central authority for cyber (A3) and a forum for dialogue between government and entrepreneurs (A2) might significantly change the general stance on this item.

As for the factor B6, earning contracts with the government was a key difference for cyber startups in the United States and Israel [41, 43] and is well regarded by public funding and venture capital specialists (it diminishes risk for the capitalist), but not by most respondents from other groups. This might signal an aspect of venture capital culture still unfamiliar to Brazil.

Accordingly, the facilitation of government agencies to contract startups, as promoted in 2019's Startups Law (A5), received many neutral votes from the survey. However, that may also result from the fact the law is recent and, therefore, still not widely known.

Overall, the healthy controversies raised on these factors regarding funding and contracting cyber startups signal these aspects need to be further investigated in more detail and preferably also discussed with the participation of all stakeholder groups involved.

4.3.4 4th-Tier: Factors perceived as least relevant

As shown in the results, factors addressed in the questions were not perceived by most specialists as fundamental in current Brazilian conditions. Those would be:

C3 - Predominance of foreign companies

C7 - Dependence on the government as the only or main customer

C6b- Negative association with the idea of electronic surveillance

D3 - Business preparedness of the Brazilian entrepreneur

B1 - Access to Venture Capital

The predominance of foreign companies in the local market (C3) is surprisingly not seen by most Brazilian specialists as a great risk, despite appearing in the literature as a formidable obstacle to developing

a national industry by stifling local innovation with products subsidized and designed in their countries of origin. Interestingly, especially in the groups of entrepreneurs, specialists, public funding, and venture capital managers, a great portion disagrees with the thesis that foreign dominance is an obstacle to Brazilian development, indicating that Brazilian entrepreneurs do not fear competition with foreigners and appear to be acutely aware of strategic advantages and disadvantages vis-à-vis foreigners.

Dependence on the government as the only or main customer (C7) also appeared to be of little concern to many specialists consulted. However, the revised literature does see it as a risk and a problem for even developed countries like France [18] and Japan [45]. Two of the factors that might have downplayed this factor are the strong confidence manifested by the specialists in the duality of cyber tools (C2 – *i.e.*, tools developed for the state could be modified and adapted for civil and commercial use) and the sufficiency of the domestic market (C1). Therefore, market regulations must preserve national sovereignty without curbing dual development.

Another factor that was not regarded as much concern by the specialists, although much present in public lore and press, is the risk of associating cyber startups with the negative image of electronic surveillance. On the contrary, most specialists considered that the startup would instead benefit from the image of technical competence by being contracted by government agencies (C6a).

Finally, the business administration preparedness of the Brazilian innovation entrepreneur (D3) was also not lacking as a first-order problem. It did appear as a concern in an interview with an academic Professor with extensive experience supporting entrepreneurship but did not reverberate in the survey.

Likewise, the accessibility to venture capital (B1) was not considered a pressing issue. No interviewee felt that access to capital is difficult in Brazil. It was clear from the interviews that capital exists, be it from public subsidies, the nascent venture capital market in Brazil, or the international venture capital market. What came into question was the effectiveness and efficiency of the channels to catalyze the encounter of capital and enterprise.

4.3.5 Specialists' suggested locations for Cyber Tech Hubs in Brazil

Creating technological hubs for industry sectors is a traditional development resource and has been considered an important factor for the cyber industry (4, 18, 52, 57). The so-called hubs aim to make the sector more competitive, concentrating specialized labor and lowering infrastructure costs.

In the questionnaire, we asked respondents to indicate up to 3 cities that should, in their opinion, host cyber technology hubs. Twenty-eight different cities received mentions. However, only 15 of those cities received at least two votes each. Of these 15, some are quite close to each other (São Paulo, Campinas, and São José dos Campos, no Estado de São Paulo; Florianópolis, Joinville and Jaraguá do Sul, no Estado de Santa Catarina; and Porto Alegre, Torres e Osório, no Estado do Rio Grande do Sul), which led us to merge their votes as into a single hub covering the region they comprise.

In the case of São Paulo, for instance, the triangle between São Paulo, Campinas, and São José dos Campos is already the most industrialized in the country and also the one with the largest number of teaching and technical training institutions, and is, therefore, a natural and expected hub location option.

Within the scope of those three cities, the secondary industrial centers of Campinas and São José dos Campos may be more interesting than the city of São Paulo itself because while still neighbor to it and its huge industrial park, they present far lesser urban and populational challenges, beyond already having centers of excellence in Computing of their own (like the State University of Campinas — UNICAMP and Instituto Tecnológico da Aeronáutica — ITA, respectively).

After the São Paulo triad, Brasília followed in second place. This may well be an artifact because most of the respondents were in the Security/Intelligence/Defense group, with many of them working for the federal government and the armed forces, whose command centers are in Brasília. Despite this, Brasília still does not have significant economic activity or any industrial specialization in particular. A cyber hub in Brasília would bring supply closer to a demand center that is still predominantly governmental, a situation of potential dependency that, in principle, one wants to avoid [(18), (52, p. 15), (63, p. 4)]; moreover, proximity could eventually even accentuate the exodus of good government professionals to the private sector. The option for Brasília, therefore, deserves a separate investigation, given the special interest of the respondents.

In third place comes Recife, a city that established itself as a regional center in Computing for the entire Northeast region, with the Federal University of Pernambuco always placed among the main ones in the country, especially in Computer Science. The city is also known for its Porto Digital (*Digital Harbor* – [101]) and its Centro de Estudos e Sistemas Avançados do Recife (CESAR – Center of Studies and Advanced Systems in Recife – [102]), which support local and regional tech entrepreneurship. The city, therefore, seems prepared and is a promising location to become a cyber hub, which would also meet the regional development objectives of the Northeastern region of Brazil and the distribution of national economic activity across the country.

Rio de Janeiro comes next in the list, in fourth place. Rio has a vigorous Oil and Gas industry and nuclear sectors that need critical infrastructure protection. The city was once a financial center in the country, with its own stock exchange. Some believe this condition should return [103], for the sake of Rio's development and for the country to have recourse to redundancy in case of obstruction or attack on the main financial center — São Paulo. It is worth noting that the City of Rio has an initiative dubbed “Porto Maravalley”, which aims to attract and facilitate high-tech startups to be hosted in the city and foster local economic development, with the participation of IMPA – the Federal Institute for Pure and Applied Mathematics [104]. The city also recently added the WebSummit event to its annual calendar for the coming years – a famed yearly fair that brings together venture capitalists and tech entrepreneurs from around the globe [105] in order to leverage and showcase new businesses.

The capitals of the states of Santa Catarina (Florianópolis–SC), Rio Grande do Sul (Porto Alegre–RS), Minas Gerais (Belo Horizonte–MG), Amazonas (Manaus–AM), Ceará (Fortaleza–CE) and Paraná (Curitiba–PR) come further in the sequence of the respondents' preference, with 5% or less of votes each. In the case of Florianópolis and Porto Alegre, we fused the votes for close-by cities, as we did in the case of São Paulo. While these cities may not yet have national centers of excellence in Computing, they have an expanding industrial activity and the state government's interest in developing their local economy. They could, therefore, house regional cyber hubs in partnership or coordination with state governments, especially in areas linked to economic activities important for their regions, such as cybernetic security

of manufacturing processes and industrial control processes in Santa Catarina and Rio Grande do Sul; telecommunications in Minas Gerais; biodiversity and microelectronics in the Amazon; and agroindustry and smart cities in Paraná.

The creation of cyber technological hubs in the country appears to be a relevant and important tool for national development, potentially combining national centers of excellence with regional centers specialized in the local economic matrix, aiming at the development of the country, taking advantage of regional opportunities and harmonious balance of national integration.

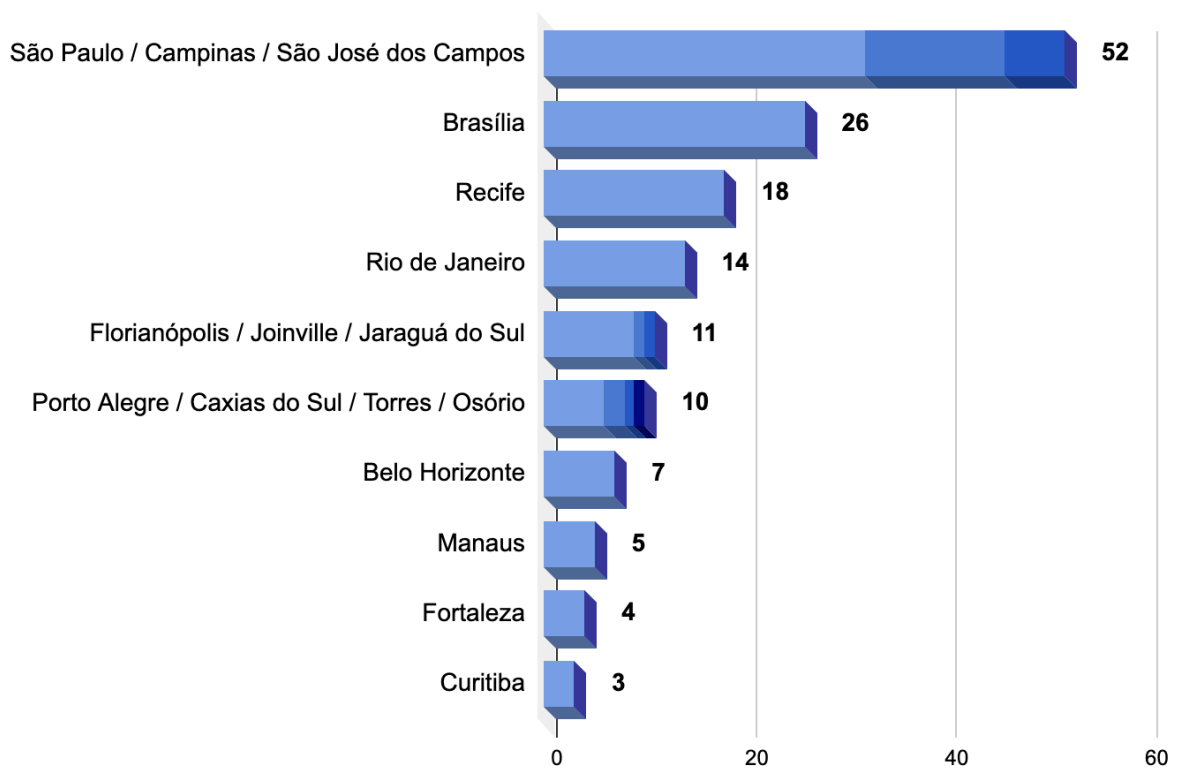


Figure 4.13: Votes on where to host Cyber Tech Hubs in Brazil.



Figure 4.14: Cities with most votes: potential candidates for hubs of national scope. Circle size proportional to number of votes received.



Figure 4.15: Other cities with relevant voting: potential candidates for regional or niche-specific hubs, in partnership with the State or Municipality. Circle size proportional to number of votes received.

5 CONCLUSIONS

The results suggest it is possible to parameterize a Cybersecurity and Cyberintelligence national policy that circumvents existing obstacles and strengthens a Brazil's Cybersecurity and Cyberintelligence industry. The research segregated 30 initial factors adapted to a Likert scale questionnaire and submitted it to specialists. From the processing of the answers through the multi-criteria decision method of preference probability composition [87, 88], it was possible to isolate eight out of the initial 30 factors to compose the starting core of a successful Cybersecurity and Cyberintelligence policy, and another eight that are deemed important but are not in agreement from all stakeholder groups and would therefore benefit from greater dialogue and convergence among these groups, prior to implementation.

This scenario indicates that an optimal strategy for Brazil would be implementing the Cybersecurity and Cyberintelligence policy in at least two phases. The first phase could approach the top-rated factors in this research (Fig. 4.12), which carry ample consensus from the entire stakeholder landscape – state agencies, businesses, and technical communities and the academy –, increasing thus the odds of its political acceptability, an important factor when launching a new policy. Addressing those top-rated factors would already yield a sizable and substantial edition of the policy, involving establishing a public authority and a public-private forum, new educational and research programs, adjustments in market regulation, and eventual incentives.

A second phase could address the remaining preferred factors, especially those deemed relevant but not in full accordance among different stakeholder groups. For that, it is important that the public-private dialogue forum for Cybersecurity – one of the top-rated factors – was established and successfully employed to progressively harmonize demands and expectations among the stakeholder groups. This second phase could also address the implementation of cyber technology hubs in Brazil. Although this was a top-rated factor, the choice of locations would necessarily engage regional politics, which might generate premature and unwanted attrition for the first edition of the policy.

Such technological hubs aims to catalyze development policy in key chosen regions and create critical mass for the rest of the country [18, 4, 57, 56, 52]. There are several viable candidates in Brazil, as indicated by the poll among the specialists (Fig. 4.13). Such hubs can also be conceived in different and overlapping scales (national – Fig. 4.14 and state or regional – Fig. 4.15) to accommodate for the realities of the vast Brazilian geography, regional politics, and economic sense since hubs should preferably have strong synergy with the economy of their surroundings.

Other factors that would benefit from further dialogue in the public-private forum are the ones in the “Subsidies and Venture Capital” category. None of these factors reached a consensus among the stakeholder groups in this research. Surprisingly, half of those factors – specifically those dealing with the funding and contracting of startups – haven't even made it to the 2nd-tier in the specialists' perception. That does not indicate, however, that we could give up further analysis on those since multiple causes could have influenced this result.

Availability of capital, for example, was the least concern among all factors assessed. Another fact

is that the venture capital group was sub-represented in the survey, and its culture and possibilities might need to be more well-known among the other groups since it is relatively young in Brazil. Yet another is actual differences of opinion between public and private sectors about what roles government should play and which ones it should avoid, and likewise for private capital and private enterprise. All these transpired to be at play.

It is important, therefore, that the public-private forum suggested for the first phase discuss these factors more deeply. This research also observed, in the interviews and through the answers to the questionnaire, the resilience and self-confidence of the Brazilian entrepreneur who, even in adverse conditions, circumvents obstacles of all kinds and is capable of rationally seeking niche opportunities in the local, regional, and international markets. It sounds important, therefore, that the public-private dialogue forum appropriates this experience. Moreover, capital may not be as abundant in the years to come as it was in the past decades, and venture capital is bound to look for higher quality and safety when allocating resources as it grows more mature. Public and private sectors are bound to mutually benefit from better understanding each other demands and claims.

Especially, public-private partnerships in venture capital investments in technology were deemed crucial to the development of national cyber capabilities in leading countries in the area, such as the USA [41, 53, 54], Israel [43, 56], and the United Kingdom [60]. The same approach has been tried in others, such as Spain [10, 59]. These partnerships are complex instruments and depend on local features of institutional arrangement, innovation ecosystem, venture capital market, entrepreneurship culture, business and legal environment, and regulatory framework. For this reason, the experiences of other countries with these models, however positive, are not immediately transferable to Brazil but point to more in-depth studies, which is one of the possibilities for extending this research.

All in all, the specialist opinion indicates that despite all hardships, Brazil can establish a robust Cybersecurity and Cyberintelligence industry, supplying the pent-up State demand and leveraging opportunities for the exploration of niches in the international market. As shown in the diagram in Fig. 4.12, the key factors for that policy would be the creation of a dedicated authority for Cybersecurity and Cyberintelligence; a forum for dialogue between government and entrepreneurs; proper regulation allowing for the commercialization of dual solutions in the domestic market; abundant technical workforce continuously formed by Academia in graduate and undergraduate courses; the teaching of computer programming in elementary schools; and the creation of cyber tech hubs in the country.

Finally, to project and measure advancements, it is important to use a framework with the appropriate scale for a country in its formative stages of national cyber capability, like the one produced in this research and used to assess Brazil's present situation [10]. This approach would favor commonsensical and effective capacity-building instead of dependence on grand top-down models disconnected from the country's reality and organically evolved field experience.

Future work may address the factors in this research that had a marked difference of opinion between distinct stakeholder groups; industry regulatory mechanisms for dual solutions for state and civil use; parameters for establishing cyber technological hubs in Brazil; the issue of public-private partnerships in venture capital investments in the cyber industry; and the inclusion of other countries in the assessment, eventually including a summarized quantitative index in the framework.

REFERENCES

- 1 DREYER, P.; JONES, T.; KLIMA, K.; AL. et. *Estimating the Global Cost of Cyber Risk: Methodology and Examples*. Santa Monica, CA, 2018.
- 2 BONFANTI, M. E. Cyber intelligence: in pursuit of a better understanding for an emerging practice. *Inss.Org.II*, v. 2, n. 1, 2018.
- 3 Organisation for Economic Co-operation and Development. *Cybersecurity Policy Making at a Turning Point. Analysing a new generation of national cybersecurity strategies for the Internet economy*. 2012. Disponível em: <<http://www.oecd.org/sti/ieconomy/cybersecurity/%20policy/%20making.pdf>>.
- 4 COHEN, N.; HULVEY, R.; MONGKOLNCHAIARUNYA, J. e. a. *Cybersecurity as an engine for growth*. 2017. Washington, DC: New America Foundation. Disponível em: <https://d1y8sb8igg2f8e.cloudfront.net/documents/FINAL_Clusters.pdf>.
- 5 The International Institute for Strategic Studies. *CYBER Capabilities and National Power: A Net Assessment*. 2021. <<https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power>>. [Online]. Accessed on: Apr. 8, 2022.
- 6 European Union Agency for Network and Information Security. *National Capabilities Assessment Framework*. Attiki: [s.n.], 2020. <<https://www.enisa.europa.eu/publications/national-capabilities-assessment-framework>>. Accessed on 8 Apr. 2022.
- 7 International Telecommunication Union. *Global Cybersecurity Index 2020*. Geneva, 2021. Accessed on 8 Apr. 2022.
- 8 VOO, J.; HEMANI, I.; JONES, S.; DESOMBRE, W.; CASSIDY, D. *National Cyber Power Index 2020*. Cambridge, EUA, 2020.
- 9 VOO, J.; HEMANI, I.; CASSIDY, D. *National Cyber Power Index 2022*. Cambridge, EUA, 2022.
- 10 GARCIA, M.; MENDONÇA, F.; ALBUQUERQUE, R. de O. Assessments on national cyber capability: a Brazilian perspective in a comparison with Spain. In: *Proceedings of the 17th Iberian Conference on Information Systems and Technologies*. Madrid: CISTI, 2022. p. 1–6.
- 11 CARR, M. Public-private partnerships in national cyber-security strategies. *International Affairs*, v. 92, n. 1, p. 190–209, 2016. Disponível em: <https://www.chathamhouse.org/sites/default/files/publications/ia/INTA92_1_03_Carr.pdf>.
- 12 Escola Superior de Guerra (Brasil). *Trabalhos de Conclusão de Curso*. Rio de Janeiro: ESG, 2022. Unpublished.
- 13 BRASIL. *Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos [...]*. 2012. <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112737.htm>. Accessed: April 8, 2022.
- 14 BRASIL, Ministério da Defesa. *Livro Branco de Defesa Nacional*. Brasília, DF, 2016. Versão sob apreciação do Congresso Nacional (Lei Complementar 97/1999, art. 9º, § 3º). Disponível em: <<http://www.defesa.gov.br/arquivos/2017/mes03/livro-branco-de-defesa-nacional-consulta-publica-12122017.pdf>>.
- 15 BRASIL. *Política Nacional de Inteligência*. 2016. Presidência da República. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8793.htm>.

- 16 MOLZAHN, W. *The CIA's In-Q-Tel Model Its Applicability*. [S.l.], 2003.
- 17 AVNIMELECH, G.; TEUBAL, M. Creating venture capital industries that co-evolve with high tech: insights from an extended industry life cycle perspective of the israeli experience. *Research Policy*, v. 35, n. 10, p. 1477–1498, 2006.
- 18 D'ELIA, D. Industrial Policy: The Holy Grail of French Cybersecurity Strategy? *Journal of Cyber Policy*, v. 3, n. 3, p. 385–406, 2018.
- 19 European Union Agency for Network and Information Security. *NCSS Good Practice Guide: Designing and Implementing National Cyber Security Strategies*. Attiki: [s.n.], 2016. <https://www.enisa.europa.eu/publications/ncss-good-practice-guide/at_download/fullReport>. Accessed on 8 Apr. 2022.
- 20 HATHAWAY, M.; DEMCHAK, C.; KERBEN, J.; MCARDLE, J.; SPIDALIERI, F. *Cyber Readiness Index 2.0*. [S.l.]: Potomac Institute, 2015.
- 21 BAEZNER, M.; CORDEY, S. *National Cybersecurity Strategies in Comparison – Challenges for Switzerland*. [S.l.], 2019.
- 22 OAS. *Cybersecurity risks, progress, and the way forward in Latin America and the Caribbean – 2020 Cybersecurity Report*. [S.l.], 2020. Disponível em: <<http://dx.doi.org/10.18235/0002513>>.
- 23 IISS. *Cyber Capabilities and National Power: A Net Assessment*. 2021. [Online]. Disponível em: <<https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power>>.
- 24 CENTRE, G. C. S. C. *Cybersecurity Capacity Maturity Model for Nations (CMM)*. [S.l.], 2021. Disponível em: <<https://gcsc.ox.ac.uk/files/cmm2021editiondocpdf>>.
- 25 SILVA, A. de Melo e; GONDIM, J. J. C.; ALBUQUERQUE, R. de O.; VILLALBA, L. J. G. A methodology to evaluate standards and platforms within cyber threat intelligence. *Future Internet*, MDPI, v. 12, n. 6, p. 108, 2020.
- 26 GROUP, G. *Gartner Magic Quadrant - Positioning technology players within a specific market*. [Online]. Accessed on Feb 16, 2022. Disponível em: <<https://www.gartner.com/en/research/methodologies/magic-quadrants-research>>.
- 27 STRONNEL, A. Brazil's cyber security strategy leaves much to be desired. *IISS Analysis*, Sept 2020. Disponível em: <<https://www.iiss.org/blogs/analysis/2020/09/csfc-brazils-cyber-security-strategy>>.
- 28 BRASIL, Ministério da Defesa. *Estratégia Nacional de Defesa*. Brasília, DF, 2012. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/END-PNDa_Optimized.pdf>.
- 29 BRASIL. *Lei nº 11.759, de 31 de julho de 2008. Autoriza a criação da empresa pública Centro Nacional de Tecnologia Eletrônica Avançada S.A. - CEITEC e dá outras providências*. 2008. <http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/11759.htm>. Accessed: April 8, 2022.
- 30 BRASIL, Ministério da Ciência, Tecnologia e Inovação. *Ato nº 15, de 26 de julho de 2021*. 2021. <<https://www.in.gov.br/en/web/dou/-/ato-n-15-de-26-de-julho-de-2021-334314032>>. Accessed: April 8, 2022.
- 31 BRASIL, Exército. *Portaria nº 666, de 4 de agosto de 2010*. 2010. Boletim do Exército, Brasília, DF, n. 31, 6 ago. 2010.
- 32 BRASIL, Ministério da Defesa. *Portaria Nº 2.777/MD, de 27 de Outubro de 2014*. Brasília, DF, 2014.

- 33 BRASIL. *Política Nacional de Segurança da Informação*. 2018. Casa Civil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm>.
- 34 BRASIL. *Decreto nº 10.222, de 05 de fevereiro de 2020. Estratégia Nacional de Segurança Cibernética*. 2020. <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm>. Accessed: April 8, 2022.
- 35 Escola Superior de Guerra (Brasil). *Fundamentos do Poder Nacional*. Rio de Janeiro: ESG, 2022.
- 36 BRASIL, Ministério da Ciência, Tecnologia, Inovação e Comunicações. *Estratégia Nacional de Ciência, Tecnologia e Inovação*. 2018. <http://www.finep.gov.br/images/a-finep/Politica/16_03_2018_Estrategia_Nacional_de_Ciencia_Tecnologia_e_Inovacao_2016_2022.pdf>. Accessed: April 8, 2022.
- 37 WEISS, M.; JANKAUSKAS, V. Securing cyberspace: how states design governance arrangements. *Governance*, v. 32, n. 2, p. 259–275, 2019.
- 38 European Union Agency for Network and Information Security. *Public Private Partnerships (PPP) Cooperative models*. Attiki: [s.n.], 2017. <<https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models/@@download/fullReport>>. Accessed on 8 Apr. 2022.
- 39 MANLEY, M. Cyberspace’s dynamic duo: Forging a cybersecurity public-private partnership. *Journal of Strategic Security*, v. 8, n. 5, p. 85–98, 2015.
- 40 SHORE, M.; DU, Y.; ZEADALLY, S. A Public-Private Partnership Model for National Cybersecurity. *Policy & Internet*, v. 3, n. 2, p. 168–190, 2011.
- 41 REINERT, J. T. In-Q-Tel: The Central Intelligence Agency as Venture Capitalist. *Northwestern Journal of International Law & Business*, v. 33, n. 3, p. 677–709, 2013.
- 42 BELKO, M. E. *Government venture capital: a case study of the In-Q-Tel model*. Ohio: US Air Force Institute of Technology, 2004.
- 43 SHULMAN, S. *Unit 81: The elite military unit that caused a big bang in the Israeli tech scene - Veterans of the IDF’s secretive technological division are the entrepreneurs driving major changes across the industry*. 2021. CTECH. Disponível em: <<https://www.calcalistech.com/ctech/articles/0,7340,L-3886512,00.html>>.
- 44 ESPAÑA, Ministerio de la Presidencia. *Orden PRA/33/2018*. 2018. 8186 p. <<https://www.boe.es/eli/es/o/2018/01/22/pra33>>. [Online]. Accessed on: Apr. 8, 2022.
- 45 BARTLETT, B. Government as facilitator: how japan is building its cybersecurity market. *Journal of Cyber Policy*, v. 3, n. 3, p. 327–343, 2018.
- 46 KSHETRI, N. India’s Cybersecurity Landscape: The Roles of the Private Sector and Public-Private Partnership. *IEEE Security and Privacy*, v. 13, n. 3, p. 16–23, 2015.
- 47 WANG, J. et al. How government venture capital guiding funds work in financing high-tech start-ups in china: A ‘strategic exchange’ perspective. *Strategic Change*, v. 22, n. 7/8, p. 417–429, 2013.
- 48 LIU, J.; LU, Y.; ZHOU, M.; WU, J.; WU, Y.; ZHU, S. Evaluating performances and importance of venture capitals: A complex network approach. *IEEE Transactions on Circuits and Systems I: Regular Papers*, v. 68, n. 5, p. 2060–2068, 2021.
- 49 HUANG, H.; LI, T.-S. A centralised cybersecurity strategy for Taiwan. *Journal of Cyber Policy*, v. 3, n. 3, p. 344–362, Sept. 2 2018.

- 50 RATHJE, J. Survive, but not thrive? the constraining influence of government funding on technology start-ups. In: *ANNUAL ACQUISITION RESEARCH SYMPOSIUM*. Monterey, CA: Naval Postgraduate school, 2019.
- 51 AGGARWAL, V. K.; REDDIE, A. W. Comparative industrial policy and cybersecurity: the us case. *Journal of Cyber Policy*, v. 3, n. 3, p. 445–466, 2018. Disponível em: <<https://doi.org/10.1080/23738871.2018.1551910>>.
- 52 ZHANG, C. *A Study on Cybersecurity Startups*. 1–195 p. Tese (Doutorado) — MIT Sloan School of Management, 2016.
- 53 KENNEY, M. How venture capital became a component of the US national system of innovation. *Industrial and Corporate Change*, v. 20, n. 6, p. 1677–1723, Dec. 2011.
- 54 WEINGARTEN, M. How venture capital thwarts innovation. *IEEE Spectrum*, n. April, 2005.
- 55 Business Executives for National Security. *The Report of the Independent Panel on the Central Intelligence Agency In-Q-Tel Venture*. Washington, DC: BENS, 2001.
- 56 DANINO, O. *Cybersecurity Economics in Israel*. 2017. <https://www.chaire-cyber.fr/IMG/pdf/2017_o_danino_1_economie_de_la_cybersecurite_en_israel_march_2017_-_article_iii.29.pdf>. [Online]. Accessed on: Apr. 8, 2022.
- 57 ADAMSKY, D. The israeli odyssey toward its national cyber security strategy. *Washington Quarterly*, v. 40, n. 2, p. 113–127, 2017. Disponível em: <<https://doi.org/10.1080/0163660X.2017.132892>>.
- 58 Label France Cybersecurity. *Catalogue 2017 des offres labélisées*. [Paris]: [s.n.], 2017.
- 59 Instituto Nacional de Ciberseguridad. *Key findings from the Catalog and knowledge map of R&D+i in cybersecurity*. España: [s.n.], 2017. <https://www.incibe.es/sites/default/files/paginas/red-excelencia/estudios-caracterizacion/catalog_infographic.jpg>. Accessed on 8 Apr. 2022.
- 60 CASELLI, G. et al. The cambridge phenomenon; an innovation system built on public private partnership. In: *Open innovation project @UK innovation research centre View project cross border acquisitions View projectthe-cambridge-phenomenon-an-innovation-system-built-on-public-priv*. [S.l.: s.n.], 2021. p. 1–30.
- 61 BRANDER, J. A.; EGAN, E. J.; HELLMANN, T. F. Government sponsored versus private venture capital: Canadian evidence. In: LERNER, J.; SCHOAR, A. (Ed.). *International Differences in Entrepreneurship*. University of Chicago Press, 2013. Disponível em: <<http://www.nber.org/chapters/c8226>>.
- 62 BRANDÃO, A. P.; CAMISÃO, I. Playing the market card: The commission’s strategy to shape eu cybersecurity policy. *Journal of Common Market Studies*, p. 1–21, 2021.
- 63 CALACARA, A.; MARCHETTI, R. State-industry relations and cybersecurity governance in europe. *Review of International Political Economy*, p. 1237–1262, 2021. Disponível em: <<https://doi.org/10.1080/09692290.2021.1913438>>.
- 64 GRUBER, H. Innovation, skills and investment: a digital industrial policy for Europe. *Economia e Politica Industriale*, v. 44, n. 3, p. 327–343, 2017.
- 65 European Commission. *Commission Signs Agreement with Industry on Cybersecurity and Steps Up Efforts to Tackle Cyber-Threats*. 2016. <<https://ec.europa.eu/digital-single-market/en/news/commission-signs-agreement-industry-cybersecurity-and-steps-efforts-tackle-cyber-threats>>. [Online]. Accessed on: Apr. 8, 2022.

- 66 AGGARWAL, V. K.; REDDIE, A. W. New economic statecraft: Industrial policy in an era of strategic competition. *Issues and Studies*, v. 56, n. 2, p. 1–30, 2020.
- 67 AUSTIN, G.; WENZE, L. Five years of cyber security education reform in china. In: BATES, J.; HARTLEY, T. (Ed.). *CYBER Security Education: principles and policies*. London: Routledge, 2020. cap. 11.
- 68 CHEUNG, T. M. The rise of china as a cybersecurity industrial power: balancing national security, geopolitical, and development priorities. *Journal of Cyber Policy*, v. 3, n. 3, p. 306–326, 2018. Disponível em: <<https://doi.org/10.1080/23738871.2018.1556720>>.
- 69 OAS. *Cybersecurity Capacity Review, Federative Republic of Brazil*. [S.l.], 2020. Disponível em: <<https://www.oas.org/en/sms/cicte/docs/ENG-CYBERSECURITY-CAPACITY-REVIEW-BRAZIL.pdf>>.
- 70 BRASIL, Gabinete de Segurança Institucional da Presidência da República. *PNCiber – Apresentação do Projeto*. 2023. Apresentação do Projeto, Exposição de Motivos, Minuta do Anteprojeto de Lei, Minuta de Decreto e Nota Técnica do GSI. Disponível em: <<https://www.gov.br/gsi/pt-br/composicao/SSIC/dsic/audiencia-publica/PNCiberAudienciaPublicaProjetoBase.pdf>>.
- 71 BRASIL, Presidência da República. *Glossário de Segurança da Informação*. Brasília, DF, 2019. Portaria. Disponível em: <<https://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663>>.
- 72 BRASIL, Ministério da Defesa. *Estratégia Nacional de Defesa*. Brasília, DF, 2020. Versão sob apreciação do Congresso Nacional (Lei Complementar 97/1999, art. 9º, § 3º). Disponível em: <https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_congresso_1.pdf>.
- 73 BRASIL, Ministério da Defesa. *Política Nacional de Defesa*. Brasília, DF, 2020. Versão sob apreciação do Congresso Nacional (Lei Complementar 97/1999, art. 9º, § 3º). Disponível em: <https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_congresso_.pdf>.
- 74 BRASIL, Ministério da Defesa. *Doutrina Militar de Defesa Cibernética*. Brasília, DF, 2014.
- 75 BRASIL. *Lei Complementar nº 182, de 1º de junho de 2021*. 2021. Institui o marco legal das startups e do empreendedorismo inovador; e altera a Lei nº 6.404, de 15 de dezembro de 1976, e a Lei Complementar nº 123, de 14 de dezembro de 2006. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/LCP/Lcp182.htm>.
- 76 CHRISTENSEN, K. K.; PETERSEN, K. L. Public-private partnerships on cyber security: A practice of loyalty. *International Affairs*, v. 93, n. 6, p. 1435–1452, 2017.
- 77 ESPAÑA. *Boletines Informativos*. 2021. [Online]. Disponível em: <<https://www.ccn.cni.es/index.php/es/menu-pytec-es/boletines-informativos-pytec>>.
- 78 NETO, R. R. *Desafios na contratação de startups pela administração pública*. 2020. Itsrio.Org. Disponível em: <https://itsrio.org/wp-content/uploads/2020/10/Desafios-na-contrataçãode-startups_Rafael_Ribeiro_Neto.pdf>.
- 79 DYDUCH, J.; OLSZEWSKA, K. Israeli innovation policy: an important instrument of perusing political interest at the global stage. *Polish Political Science Yearbook*, Wydawnictwo Adam Marszałek, v. 2, 2018.
- 80 VIEIRA, J. N. d. S.; GOMES, R. C.; FILHO, E. R. G. Reforma regulatória e estímulos à entrada de empreendedores privados no brasil. *Revista Economia & Gestão*, v. 19, n. 54, p. 6–22, set./dez. 2019. Disponível em: <<http://periodicos.pucminas.br/index.php/economiaegestao/article/view/20802>>.

- 81 CARNEIRO, A.; GIMENEZ, A.; GRANJA, C.; BALBACHEVSKY, E.; CONSONI, F.; ANDRETTA, V. Diáspora brasileira de ciência, tecnologia e inovação: panorama, iniciativas auto-organizadas e políticas de engajamento. *Ideias*, v. 11, p. e020010, 2020. Disponível em: <<https://doi.org/10.20396/ideias.v11i0.8658500>>.
- 82 NELSON, O. *The Social Effects of the Spanish Brain Drain*. Pennsylvania, 2015. (Social Impact Research Experience (SIRE), 35). Disponível em: <<https://repository.upenn.edu/cgi/viewcontent.cgi?article=1041>>.
- 83 MALACH-PINES, A.; KEINAN, G.; GILAT, I. Entrepreneurs and managers: Similar yet different. *The International Journal of Organizational Analysis*, v. 10, n. 2, p. 172–190, 2002. Disponível em: <<https://doi.org/10.1108/eb028949>>.
- 84 VERGARA, S. C. *Projetos e relatórios de Pesquisa em Administração*. 7. ed. São Paulo: Atlas, 2007.
- 85 MALAGUTTI, M. A. State-sponsored cyber-offences. *Revista da Escola de Guerra Naval*, Escola de Guerra Naval, Programa de Pós-Graduação em Estudos Marítimos, v. 22, n. 2, p. 261, 2016.
- 86 LIKERT, R. A technique for the measurement of attitudes. *Archives of psychology*, 1932.
- 87 SANT'ANNA, A. P. *Probabilistic Composition of Preferences, Theory and Applications*. 1. ed. Springer Cham, 2015. VII, 141 p. (Decision Engineering). ISBN 978-3-319-11276-3. Disponível em: <<https://doi.org/10.1007/978-3-319-11277-0>>.
- 88 GAVIAO, L. O.; LIMA, G. B. A.; SANT'ANNA, A. P.; MACIEL, G. F. S. V. Composition of probabilistic preferences with an empirical approach in multi-criteria problems. *Gestão & Produção*, v. 26, n. 2, p. e2802, 2019. Disponível em: <<https://doi.org/10.1590/0104-530X-2802>>.
- 89 ALLEN, I. E.; SEAMAN, C. A. Likert scales and data analyses. *Quality progress*, v. 40, n. 7, p. 64–65, 2007.
- 90 R Core Team. *R: A Language and Environment for Statistical Computing*. Vienna, Austria, 2023. Disponível em: <<https://www.R-project.org/>>.
- 91 GAVIAO, L. O.; SANT'ANNA, A. P.; LIMA, G. B. A.; GARCIA, P. A. de A. *Probabilistic preferences of Likert scale data by empirical distributions*. 2023. Disponível em: <<https://doi.org/10.5281/zenodo.7950538>>.
- 92 BACKHAUS, J. The pareto principle. *Analyse & Kritik*, v. 2, n. 2, p. 146–171, 1980. Disponível em: <<https://doi.org/10.1515/auk-1980-0203>>.
- 93 PIERRE, J.; PETERS, B. G. Handbook of public policy. *Handbook of Public Policy*, Sage, p. 1–528, 2006.
- 94 CCN-CERT. *Contención frente a los ciberataques*. [Online]. Disponível em: <<https://www.ccn-cert.cni.es/documentos-publicos/3480-Catalogo-Servicios-Empresas/file.html>>.
- 95 ESPAÑA, Ministerio de Defensa. *Real Decreto 521/2020, de 19 de mayo, por el que se establece la organización básica de las Fuerzas Armadas*. 2020. Disponível em: <<https://www.boe.es/eli/es/rd/2020/05/19/521/con>>.
- 96 ESPAÑA, Ministerio de la Presidencia. *Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información*. 2021.

- 97 Revista Española de Control Externo. La ciberseguridad y su relevancia en el sector público. XXII, p. 83, January 2020. Disponível em: <https://www.tcu.es/repositorio/ae417da8-201f-4da8-b2e9-0d498a774157/R64_ART\%204\%20CCN-CERT.pdf>.
- 98 NACIONAL, C. C. *Oferta Formativa 2022*. 2022. [Online]. Disponível em: <<https://angeles.ccn-cert.cni.es/index.php/es/docman/documentos-publicos/38-plan-de-formacion-ccn/file>>.
- 99 CCN. *Cyber threats and Trends 2019*. 2019. [Online]. Disponível em: <<https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4041-ccn-cert-ia-13-19-threats-and-trends-report-executive-summary/file.html>>.
- 100 ESPAÑA, Dept. de Seguridad Nacional. *National Cyber Security Strategy*. [S.l.], 2019. Disponível em: <<https://www.ccn-cert.cni.es/en/pdf/documentos-publicos/3812-national-cybersecurity-strategy-2019/file.html>>.
- 101 Porto Digital. *Porto Digital*. 2023. [Online]. Accessed on May 2023. Disponível em: <<https://www.portodigital.org/>>.
- 102 Exame. *Cesar anuncia abertura de operação em Portugal sobre educação e inovação*. 2023. [Online]. Accessed on May 2023. Disponível em: <<https://exame.com/bussola/cesar-anuncia-abertura-de-operacao-em-portugal-sobre-educacao-e-inovacao/>>.
- 103 COVA, C. *Uma história ilustrada do mercado de capitais no Brasil*. Rio de Janeiro: Ed. Andrea Jakobsson, 2021.
- 104 IMPA. *IMPA vai conduzir projeto de educação no Porto Maravalley*. 2022. [Online]. Accessed on Apr. 2022. Disponível em: <<https://impa.br/noticias/impa-vai-conduzir-projeto-de-educacao-no-porto-maravalley/>>.
- 105 Prefeitura do Rio de Janeiro. *Rio recebe, a partir de segunda-feira, o Web Summit, maior evento de tecnologia do mundo*. 2023. [Online]. Accessed on May 2023. Disponível em: <<https://prefeitura.rio/desenvolvimento-economico-inovacao-simplificacao/rio-recebe-a-partir-de-segunda-feira-o-web-summit-maior-evento-de-tecnologia-do-mundo/>>.

Appendices

A. INTERVIEW SCRIPT

Script used as basis for the interviews with stakeholder group representative specialists.

1. “Good morning. First of all, thank you very much for your time. The goal of this research is to try and identify key success factors for a Cybersecurity and Cyberintelligence Policy that aims to elevate Brazilian national cyber capability. What is your general perception on the matter?”
2. “What’s your view on the State demand of cybersecurity and cyberintelligence, especially on how to cope with the Government’s technical lag in relation to the private sector; on how to better organize governmental demands; and on the existing public contracting models?”
3. “In regard to funding, please provide your views about public subsidies and venture capital investment for the cyber industry: is there reasonable access to capital? Which is the startup stage where it needs external support the most? Any other support policies that would be helpful?”
4. “About the market risks and incentives, what are your comments about the size and sustainability of the market in Brazil, Latin America and globally? Do you see the association with national security and intelligence as a positive or negative factor? and do you see risks of legal or regulatory nature in this market?”
5. “Please provide your comments on the intellectual capital and labour force availability in the industry: do you see a brain drain problem and how do you cope with it? What do you think of the business preparedness of the Brazilian entrepreneur? What are your views on Brazilian technical workforce education? And do you think cyber technology clusters would be helpful?”

B. QUESTIONNAIRE

SURVEY -

Cybersecurity, Cyberintelligence and High-tech Entrepreneurship in Brazil

This form is part of a Research Project conducted by Marcelo Garcia within the scope of the Advanced Studies in Politics and Strategy Course (CAEPE 2022) of the Superior School of War of the Brazilian Ministry of Defense.

The research aims to gather specialists' opinions about the **governmental demand in cybernetic security and intelligence** and its supply by **Brazilian entrepreneurship**, with **State support** and/or private **venture capital**, aiming at the establishment of a Brazilian cyber industry.

This form is being sent to managers of the armed forces, federal and state intelligence and public security agencies, other member agencies of SISBIN — Brazilian Intelligence System —, prominent Brazilian entrepreneurs and specialists, researchers and academics, specialists in public development and Brazilian venture capital investors.

The questionnaire contains 4 sections of about 7 questions each, with a total estimated completion time of about 14 minutes. The email address is requested below to facilitate communication with respondents and will not be published.

Any questions, please contact :

Marcelo Garcia
marcelo.garcia.inbox@gmail.com

Q- SPECIALIST QUALIFICATION DATA

The qualification data below is requested for the proper processing of responses within the stakeholder categories of the survey.

Q1- Check the option that best corresponds to the role you currently play:

- Government - Law enforcement/Intelligence/Defense
- Government - Public Susidies
- Private Venture Capital
- Entrepreneur
- Specialist
- Researcher / Academic Professor
- Other: _____

Q2- Academic background in technology areas related to the subject ("Computer, Electrical Engineering, etc.") and other areas ("Others").

	Computer, Electrical Engineering, etc.	Others
Doctorate degree	<input type="checkbox"/>	<input type="checkbox"/>
Master´s degree	<input type="checkbox"/>	<input type="checkbox"/>
Specialization	<input type="checkbox"/>	<input type="checkbox"/>
Undergraduation	<input type="checkbox"/>	<input type="checkbox"/>
Technical High School	<input type="checkbox"/>	<input type="checkbox"/>
Self-taught	<input type="checkbox"/>	<input type="checkbox"/>

Q3- Time of professional experience (years) with matters related to security and cyber intelligence.

- 0 1 2 3 4 5 6 7 8 9 10 or more

Q4- Time of professional experience (years) with subjects related to innovation and entrepreneurship.

- 0 1 2 3 4 5 6 7 8 9 10 or more

Q5- Time of professional experience (years) with matters related to public policies and their management/legislation.

- 0 1 2 3 4 5 6 7 8 9 10 or more

A - DEMAND

Brazilian federal and state agencies have demands for cyber security and intelligence in order to fulfill their legally established missions. The Brazilian Intelligence System -- SISBIN, for example, brings together more than 40 bodies responsible for matters of intelligence and security of the State and society defined in Law 9,883/1999, in the National Intelligence Policy (PNI - Decree 8,793/2016) and in the National Intelligence Strategy (ENINT - Decree 14.503/2017), under the coordination of the Brazilian Intelligence Agency -- ABIN, subordinated to the Institutional Security Office -- GSI.

A1 - Does organizing the government's cyber demands and forwarding them to the private sector tend to accelerate the incorporation of technological innovations for the country's intelligence and public security bodies?

- Totally agree
- I agree in part
- Don't agree nor disagree
- Disagree in part
- Totally disagree

Obs.: The same Likert scale applies to all subsequent questions until D6.

A2- Would the existence of a forum for dialogue between government and entrepreneurs be important for the understanding, by the market, of the government's demands for security and cybernetic intelligence?

A3- Would the existence of an authority dedicated to cybersecurity and intelligence issues in Brazil be important to guide the private sector on the subject?

A4- Do public procurement models discourage the private sector from providing products and services to the government?

A5- Does the Legal Framework for Startups (Law 182/2019, in force since Sep. 2021) facilitate the hiring of innovative technologies by the public sector?

B- PUBLIC SUBSIDIES AND VENTURE CAPITAL

B1- Is it easy for Brazilian technology startups to access and obtain venture capital?

B2- Would public promotion policies for national entrepreneurship be decisive for the development of a cyber industry in Brazil?

B3- Is the discontinuity of Brazilian development programs throughout successive governments an impediment to the development of a cyber industry in Brazil?

B4a- Should public subsidy policies in the cyber area prioritize entrepreneurs in search of seed capital to validate their idea/prototype in the market?

B4b- Should public subsidy policies in the cyber area prioritize startups that already have a functional prototype and business plan but need to obtain their first customers? ("series A")

B4b- Should public subsidy policies in the cyber area prioritize startups that already have a functional prototype and business plan but need to obtain their first customers? ("series A")

B4c- Should public subsidy policies in the cyber area prioritize startups that already have a product developed and initial customers but need capital to acquire scale and increase the customer base? ("series B")

B5- Would tax incentives for the cyber sector be a success factor for the development of the cyber industry in the country?

B6- Does hiring startups by the government make them more attractive to private venture capital managers?

B6- Does hiring startups by the government make them more attractive to private venture capital managers?

B7- Is the venture capital investment model in partnership between government and private capital viable and advantageous in Brazil for the parties involved (entrepreneur, government and private capital)?

B8- Would business incubators and accelerators be a key success factor for the development of a cyber industry in Brazil?

B8- Would business incubators and accelerators be a key success factor for the development of a cyber industry in Brazil?

B8- Would business incubators and accelerators be a key success factor for the development of a cyber industry in Brazil?

B9- Would cyber startups incubated or accelerated by large companies ("corporate venture") have a better chance of success than the others?

C- MARKET, INCENTIVE AND RISKS

C1- Is there enough demand (including government and private initiative) to sustain a cyber industry in the country?

C1- Is there enough demand (including government and private initiative) to sustain a cyber industry in the country?

C2- Can security technologies and cybernetic intelligence developed for State institutions also generate dual solutions for civil and commercial use?

C3- Is the dominance of foreign companies in the cyber market in Brazil an impediment to the flourishing of a local industry?

C4- Would Brazilian cyber startups have a better chance of success targeting the regional Latin American market in addition to the domestic market?

C5- Are there niches in the global cyber market in which Brazil could successfully establish itself?

C6a- Would the involvement of a startup in government intelligence and cybersecurity projects reflect positively on the company's image by associating it with the ideas of technical competence and Law and Order?

C6b- Would the involvement of a startup in government intelligence and cybersecurity projects cause unwanted stigma by associating it with the idea of electronic surveillance?

C7- Is there a risk that startups in the cybernetic sector develop dependence on the government as their only or main customer?

D- INTELLECTUAL CAPITAL AND LABOR

D1 - Is the problem of brain drain in Brazil an impediment to the establishment of a national cyber industry?

D2- Would the creation of an incentive program for the repatriation of intellectual capital and technical labor be important for the development of a national cyber industry?

D3- Does the Brazilian innovation entrepreneur have enough management skills to prosper?

D4- Is the inclusion of computer programming in basic and fundamental education important for the formation of a technologically qualified workforce in Brazil?

D5- Would the creation of lines of research in cybersecurity in Undergraduate and Graduate courses be important for the development of the cyber industry in Brazil?

D6- Is establishing technological hubs to catalyze cyber research and development in pre-existing industries an important factor for the development of a cyber industry in the country?

D7- If yes in the previous question, name up to three cities, in order of priority, where it would be beneficial for Brazil to house cyber technological hubs.

E- FINAL CONSIDERATIONS

E1- Please, leave below your considerations and perceptions on the subject, as well as any comments about the research.

C. MATRICES

Table C.1: Matrix of frequencies of Likert values in the answers to the questionnaire, for the full set of respondents and for the state agents and entrepreneur/specialist stakeholder groups: 5 - totally agree; 4 - agree in part; 3 - nor agree nor disagree; 2 - disagree in part; 1 - totally disagree.

Q#	Full set					Law/Intel./Mil					Entrepr./Specialist				
	5	4	3	2	1	5	4	3	2	1	5	4	3	2	1
A1	24	26	5	4	0	16	16	2	1	0	4	3	0	2	0
A2	45	12	0	2	0	28	7	0	0	0	5	3	0	1	0
A3	46	10	0	2	1	29	6	0	0	0	7	1	0	0	1
A5	14	26	18	0	1	8	15	12	0	0	3	3	2	0	1
B1	6	19	20	11	3	5	9	14	5	2	1	5	1	2	0
B2	37	21	0	1	0	27	8	0	0	0	3	5	0	1	0
B3	33	19	2	4	1	20	9	2	3	1	4	4	0	1	0
B4a	18	26	8	5	2	10	14	6	3	2	4	3	0	2	0
B4b	17	30	8	3	1	10	19	4	2	0	3	3	1	1	1
B4c	15	31	7	4	2	10	18	5	2	0	0	5	1	1	2
B5	31	20	4	3	1	20	11	1	2	1	5	3	1	0	0
B6	23	23	10	3	0	16	13	5	1	0	3	4	1	1	0
B7	21	27	10	1	0	12	16	6	1	0	3	4	2	0	0
B8	37	14	4	4	0	24	8	2	1	0	4	2	1	2	0
B9	25	25	6	2	1	20	12	3	0	0	2	5	0	2	0
C1	42	11	4	2	0	28	3	3	1	0	6	2	0	1	0
C2	48	10	0	0	1	26	8	0	0	1	9	0	0	0	0
C3	8	24	5	13	9	6	14	4	7	4	2	1	1	2	3
C4	34	19	6	0	0	23	7	5	0	0	3	5	1	0	0
C5	43	10	6	0	0	27	3	5	0	0	6	3	0	0	0
C6a	33	18	6	2	0	22	10	3	0	0	5	3	1	0	0
C6b	6	22	6	17	8	3	14	4	9	5	1	3	1	2	2
C7	6	30	7	9	7	2	17	4	6	6	1	5	0	2	1
D1	25	22	4	6	2	13	16	1	3	2	3	2	1	3	0
D2	38	16	5	0	0	25	9	1	0	0	3	4	2	0	0
D3	8	15	16	15	5	4	9	12	8	2	3	2	0	3	1
D4	39	16	2	2	0	26	8	0	1	0	4	4	1	0	0
D5	46	11	1	0	1	30	4	0	0	1	5	3	1	0	0
D6	44	9	5	0	1	31	3	0	0	1	5	1	3	0	0

Table C.2: Matrix of frequencies of Likert values in the answers to the questionnaire, for the Public Funding, Academia and Entrepreneur/Specialist stakeholder groups: 5 - totally agree; 4 - agree in part; 3 - nor agree nor disagree; 2 - disagree in part; 1 - totally disagree.

Q#	Public Funding					Academia					Venture Capital				
	5	4	3	2	1	5	4	3	2	1	5	4	3	2	1
A1	0	3	1	0	0	4	3	2	1	0	0	1	0	0	0
A2	3	0	0	1	0	8	2	0	0	0	1	0	0	0	0
A3	3	0	0	1	0	7	3	0	0	0	0	0	0	1	0
A5	1	2	1	0	0	2	6	2	0	0	0	0	1	0	0
B1	0	3	1	0	0	0	2	4	4	0	0	0	0	0	1
B2	1	3	0	0	0	5	5	0	0	0	1	0	0	0	0
B3	2	2	0	0	0	7	3	0	0	0	0	1	0	0	0
B4a	2	2	0	0	0	2	6	2	0	0	0	1	0	0	0
B4b	0	3	1	0	0	4	4	2	0	0	0	1	0	0	0
B4c	1	2	0	1	0	4	5	1	0	0	0	1	0	0	0
B5	2	0	2	0	0	4	5	0	1	0	0	1	0	0	0
B6	2	2	0	0	0	2	3	4	1	0	0	1	0	0	0
B7	2	2	0	0	0	4	4	2	0	0	0	1	0	0	0
B8	3	1	0	0	0	6	3	1	0	0	0	0	0	1	0
B9	1	2	1	0	0	2	6	2	0	0	0	0	0	0	1
C1	2	2	0	0	0	6	4	0	0	0	0	0	1	0	0
C2	3	1	0	0	0	9	1	0	0	0	1	0	0	0	0
C3	0	2	0	1	1	0	7	0	3	0	0	0	0	0	1
C4	3	1	0	0	0	5	5	0	0	0	0	1	0	0	0
C5	2	2	0	0	0	8	2	0	0	0	0	0	1	0	0
C6a	2	1	1	0	0	4	4	1	1	0	0	0	0	1	0
C6b	0	1	0	3	0	2	4	1	3	0	0	0	0	0	1
C7	0	1	2	1	0	3	7	0	0	0	0	0	1	0	0
D1	2	0	2	0	0	6	4	0	0	0	1	0	0	0	0
D2	2	0	2	0	0	7	3	0	0	0	1	0	0	0	0
D3	1	1	1	1	0	0	2	3	3	2	0	1	0	0	0
D4	2	2	0	0	0	6	2	1	1	0	1	0	0	0	0
D5	3	1	0	0	0	7	3	0	0	0	1	0	0	0	0
D6	3	1	0	0	0	5	4	1	0	0	0	0	1	0	0

Table C.3: Matrix of composed preference probabilities calculated by the CPP method over the questionnaire answers, for the full set of respondents and for each subgroup.

Q#	Full Set		Law/Intel./Mil.		Entrepreneur/Specialist		Public Funding		Academia	
	Rank	Pref. Probab.	Rank	Pref. Probab.	Rank	Pref. Probab.	Rank	Pref. Probab.	Rank	Pref. Probab.
C2	1	0,070231476	8	0,053671356	1	0,1257290195	3	0,0707346	1	0,087713415
D5	2	0,065186514	2	0,068757304	6	0,0464190825	3	0,0707346	5	0,056980666
A3	3	0,065106215	3	0,063081813	2	0,0852985515	6	0,0691798	5	0,056980666
A2	4	0,061909753	4	0,059354042	6	0,0464190825	6	0,0691798	2	0,070826042
D6	5	0,060235614	1	0,073112405	9	0,0452373547	3	0,0707346	14	0,03520946
C5	6	0,057209561	7	0,055321435	3	0,0608350759	11	0,0396340	2	0,070826042
C1	7	0,055114282	5	0,058935773	4	0,0601646529	11	0,0396340	8	0,045410267
D4	8	0,049331547	9	0,052384333	10	0,0349190071	11	0,0396340	11	0,044573094
D2	9	0,047401407	10	0,049212904	20	0,0246664042	17	0,0372789	5	0,056980666
B2	10	0,045857435	6	0,055826282	18	0,0251498042	19	0,0185074	12	0,035589678
B8	11	0,04539398	11	0,046014785	14	0,0338565318	3	0,0707346	10	0,044991136
C4	12	0,040396195	12	0,042972962	17	0,0251498042	3	0,0707346	12	0,035589678
B3	13	0,039195062	15	0,035826061	11	0,0349190071	11	0,0396340	5	0,056980666
C6a	14	0,038653779	13	0,040421009	6	0,0464190825	15	0,0384522	19	0,026450461
B5	15	0,03597455	14	0,035992878	6	0,0464190825	17	0,0372789	16	0,026797791
D1	16	0,027508091	19	0,021157614	22	0,0237036114	17	0,0372789	8	0,045410267
B9	17	0,027366337	16	0,035328592	24	0,0163015843	20	0,0175520	23	0,012769517
A1	18	0,025776655	17	0,026398154	12	0,0343869338	23	0,0023868	20	0,026103831
B6	19	0,024307544	18	0,026177366	20	0,0246664042	11	0,0396340	26	0,01188046
B7	20	0,02198846	20	0,018552429	20	0,0246664042	11	0,0396340	17	0,026450461
B4a	21	0,018735539	21	0,015455834	12	0,0343869338	11	0,0396340	23	0,012769517
B4b	22	0,017584593	22	0,015253361	15	0,0259572116	23	0,0023868	17	0,026450461
B4c	23	0,015546754	23	0,015189196	28	0,002115933	22	0,0175520	15	0,026797791
A5	24	0,014069562	24	0,01175461	16	0,0259572116	20	0,0175520	23	0,012769517
C3	25	0,008584175	25	0,009258278	23	0,0179542274	25	0,0018157	28	0,001807698
C7	26	0,006714885	27	0,0037008	26	0,009152079	27	0,0007924	21	0,019805726
C6b	27	0,006412128	26	0,004871571	27	0,0088449231	28	0,0007924	25	0,012176325
D3	28	0,005134911	28	0,003062792	25	0,0094832286	26	0,0009059	27	0,01188046
B1	29	0,003047712	29	0,002934901	29	0,0007940086	29	0,0000000	29	0,001030829

D. R CODE

```
#####  
### Probabilistic Preferences in Likert Scales #####  
#####  
#  
# Source: Zenodo.org  
#  
# This R-code is intended for multicriteria decision support problems solved by the  
# Composition of Probabilistic Preferences (CPP).  
#  
# The two functions calculate the joint probabilities of alternatives maximizing (PMax)  
# and minimizing (PMin) their preferences in a criterion.  
#  
# The measures of the problem's decision matrix are the frequencies of responses to the  
# Likert scale values used in the questionnaires.  
#####  
  
### Joint probabilities of an alternative maximize preferences by criterion  
  
PMax.Emp.Likert = function (values,probs) {  
  require(mc2d)  
  
  PMax = rep(0,nrow(probs))  
  
  for (i in 1:nrow(probs))  
  {  
    PMax[i] = (integrate (  
      Vectorize (  
        function(x) {  
          prod( pempiricalC( x, min(values), max(values), values, prob=probs[-i,]) )  
          * dempiricalC(x, min(values), max(values), values, prob=probs[i,])  
        }  
      ), min(values)-3, max(values)+3 )  
    )$value  
  }  
  PMax  
  r = rank(-PMax)  
  
  Result = list(PMax=PMax, Rank=r)  
  Result  
}  
  
### Joint probabilities of an alternative minimize preferences by criterion  
  
PMin.Emp.Likert = function (values,probs) {  
  require(mc2d)  
  
  PMin = rep(0,nrow(probs))  
  
  for (i in 1:nrow(probs))  
  {  
    PMin[i] = (integrate (  
      Vectorize (  

```

```

        function(x) {
            prod(1-pempiricalC(x,min(values),max(values),values,prob=probs[-i,]))
            * dempiricalC(x,min(values),max(values),values,prob=probs[i,])
        }
    ), min(values)-3, max(values)+3)
) $value
}
PMin
r = rank(-PMin)

Result = list(PMin=PMin, Rank=r)
Result
}

#-----
#
# LOCAL PROCESSING - MARCELO
#
# . May, 2023
#
# change decimal separator in output
options(OutDec=",")
#setwd('~/Documents/Agencia/MESTRADO/DISSERTACAO/Analise quantitativa')

# Likert scale
values = 1:5 # equidistant values of the Likert scale, used to evaluate alternatives

#-----
# NOTE - ADJUSTMENTS
# please note that:
# - A4 was correctly removed before processing
# - B1 and D3 were scale-mirrored because their questions were formulated with inverted semantics

questions = c('A1', 'A2', 'A3', 'A5', 'B1', 'B2', 'B3', 'B4a', 'B4b', 'B4c', 'B5', 'B6', 'B7', 'B8',
              'B9', 'C1', 'C2', 'C3', 'C4', 'C5', 'C6a', 'C6b', 'C7', 'D1', 'D2', 'D3', 'D4', 'D5', 'D6')

#-----
# ALL SUBGROUPS - entire dataset
#
probFull.A1=c(0,4,5,26,24)
probFull.A2=c(0,2,0,12,45)
probFull.A3=c(1,2,0,10,46)
probFull.A5=c(1,0,18,26,14)
#probFull.B1=c(3,11,20,19,6)
probFull.B1=c(6,19,20,11,3)
probFull.B2=c(0,1,0,21,37)
probFull.B3=c(1,4,2,19,33)
probFull.B4a=c(2,5,8,26,18)
probFull.B4b=c(1,3,8,30,17)
probFull.B4c=c(2,4,7,31,15)
probFull.B5=c(1,3,4,20,31)
probFull.B6=c(0,3,10,23,23)
probFull.B7=c(0,1,10,27,21)
probFull.B8=c(0,4,4,14,37)
probFull.B9=c(1,2,6,25,25)
probFull.C1=c(0,2,4,11,42)
probFull.C2=c(1,0,0,10,48)
probFull.C3=c(9,13,5,24,8)
probFull.C4=c(0,0,6,19,34)
probFull.C5=c(0,0,6,10,43)

```

```

probFull.C6a=c(0,2,6,18,33)
probFull.C6b=c(8,17,6,22,6)
probFull.C7=c(7,9,7,30,6)
probFull.D1=c(2,6,4,22,25)
probFull.D2=c(0,0,5,16,38)
#probFull.D3=c(5,15,16,15,8)
probFull.D3=c(8,15,16,15,5) # sufficiency
probFull.D4=c(0,2,2,16,39)
probFull.D5=c(1,0,1,11,46)
probFull.D6=c(1,0,5,9,44)
probs.Full = rbind(probFull.A1, probFull.A2, probFull.A3, probFull.A5, probFull.B1, probFull.B2,
  probFull.B3, probFull.B4a, probFull.B4b, probFull.B4c, probFull.B5, probFull.B6, probFull.B7,
  probFull.B8, probFull.B9, probFull.C1, probFull.C2, probFull.C3, probFull.C4, probFull.C5,
  probFull.C6a, probFull.C6b, probFull.C7, probFull.D1, probFull.D2, probFull.D3, probFull.D4,
  probFull.D5, probFull.D6)

# function processing time
#ptm = proc.time()
#result.Full = PMax.Emp.Likert(values,probs) # min(values)-3, max(values)+3
#proc.time() - ptm

result.Full = PMax.Emp.Likert(values, probs.Full)
sum(result.Full$PMax)

#-----
# Law Enforcement, Intelligence, Defense subgroup
probLaw.A1=c(0,1,2,16,16)
probLaw.A2=c(0,0,0,7,28)
probLaw.A3=c(0,0,0,6,29)
probLaw.A5=c(0,0,12,15,8)
#probLaw.B1=c(2,5,14,9,5)
probLaw.B1=c(5,9,14,5,2)
probLaw.B2=c(0,0,0,8,27)
probLaw.B3=c(1,3,2,9,20)
probLaw.B4a=c(2,3,6,14,10)
probLaw.B4b=c(0,2,4,19,10)
probLaw.B4c=c(0,2,5,18,10)
probLaw.B5=c(1,2,1,11,20)
probLaw.B6=c(0,1,5,13,16)
probLaw.B7=c(0,1,6,16,12)
probLaw.B8=c(0,1,2,8,24)
probLaw.B9=c(0,0,3,12,20)
probLaw.C1=c(0,1,3,3,28)
probLaw.C2=c(1,0,0,8,26)
probLaw.C3=c(4,7,4,14,6)
probLaw.C4=c(0,0,5,7,23)
probLaw.C5=c(0,0,5,3,27)
probLaw.C6a=c(0,0,3,10,22)
probLaw.C6b=c(5,9,4,14,3)
probLaw.C7=c(6,6,4,17,2)
probLaw.D1=c(2,3,1,16,13)
probLaw.D2=c(0,0,1,9,25)
#probLaw.D3=c(2,8,12,9,4)
probLaw.D3=c(4,9,12,8,2)
probLaw.D4=c(0,1,0,8,26)
probLaw.D5=c(1,0,0,4,30)
probLaw.D6=c(1,0,0,3,31)
probs.Law = rbind(probLaw.A1, probLaw.A2, probLaw.A3, probLaw.A5, probLaw.B1, probLaw.B2,
  probLaw.B3, probLaw.B4a, probLaw.B4b, probLaw.B4c, probLaw.B5, probLaw.B6, probLaw.B7,
  probLaw.B8, probLaw.B9, probLaw.C1, probLaw.C2, probLaw.C3, probLaw.C4, probLaw.C5,

```



```

    probLaw.C6a, probLaw.C6b, probLaw.C7, probLaw.D1, probLaw.D2, probLaw.D3, probLaw.D4,
    probLaw.D5, probLaw.D6)

result.Law = PMax.Emp.Likert(values,probs.Law)
sum(result.Law$PMax)

#-----
# Entrepreneur and Specialists subgroup

probTec.A1=c(0,2,0,3,4)
probTec.A2=c(0,1,0,3,5)
probTec.A3=c(1,0,0,1,7)
probTec.A5=c(1,0,2,3,3)
#probTec.B1=c(0,2,1,5,1)
probTec.B1=c(1,5,1,2,0)
probTec.B2=c(0,1,0,5,3)
probTec.B3=c(0,1,0,4,4)
probTec.B4a=c(0,2,0,3,4)
probTec.B4b=c(1,1,1,3,3)
probTec.B4c=c(2,1,1,5,0)
probTec.B5=c(0,0,1,3,5)
probTec.B6=c(0,1,1,4,3)
probTec.B7=c(0,0,2,4,3)
probTec.B8=c(0,2,1,2,4)
probTec.B9=c(0,2,0,5,2)
probTec.C1=c(0,1,0,2,6)
probTec.C2=c(0,0,0,0,9)
probTec.C3=c(3,2,1,1,2)
probTec.C4=c(0,0,1,5,3)
probTec.C5=c(0,0,0,3,6)
probTec.C6a=c(0,0,1,3,5)
probTec.C6b=c(2,2,1,3,1)
probTec.C7=c(1,2,0,5,1)
probTec.D1=c(0,3,1,2,3)
probTec.D2=c(0,0,2,4,3)
#probTec.D3=c(1,3,0,2,3)
probTec.D3=c(3,2,0,3,1)
probTec.D4=c(0,0,1,4,4)
probTec.D5=c(0,0,1,3,5)
probTec.D6=c(0,0,3,1,5)
probs.Tec = rbind(probTec.A1, probTec.A2, probTec.A3, probTec.A5, probTec.B1, probTec.B2,
    probTec.B3, probTec.B4a, probTec.B4b, probTec.B4c, probTec.B5, probTec.B6, probTec.B7,
    probTec.B8, probTec.B9, probTec.C1, probTec.C2, probTec.C3, probTec.C4, probTec.C5,
    probTec.C6a, probTec.C6b, probTec.C7, probTec.D1, probTec.D2, probTec.D3, probTec.D4,
    probTec.D5, probTec.D6)

result.Tec = PMax.Emp.Likert(values,probs.Tec)
sum(result.Tec$PMax)

#-----
# Public Funding subgroup

probFun.A1=c(0,0,1,3,0)
probFun.A2=c(0,1,0,0,3)
probFun.A3=c(0,1,0,0,3)
probFun.A5=c(0,0,1,2,1)
#probFun.B1=c(0,0,1,3,0)
probFun.B1=c(0,3,1,0,0)
probFun.B2=c(0,0,0,3,1)

```

```

probFun.B3=c(0,0,0,2,2)
probFun.B4a=c(0,0,0,2,2)
probFun.B4b=c(0,0,1,3,0)
probFun.B4c=c(0,1,0,2,1)
probFun.B5=c(0,0,2,0,2)
probFun.B6=c(0,0,0,2,2)
probFun.B7=c(0,0,0,2,2)
probFun.B8=c(0,0,0,1,3)
probFun.B9=c(0,0,1,2,1)
probFun.C1=c(0,0,0,2,2)
probFun.C2=c(0,0,0,1,3)
probFun.C3=c(1,1,0,2,0)
probFun.C4=c(0,0,0,1,3)
probFun.C5=c(0,0,0,2,2)
probFun.C6a=c(0,0,1,1,2)
probFun.C6b=c(0,3,0,1,0)
probFun.C7=c(0,1,2,1,0)
probFun.D1=c(0,0,2,0,2)
probFun.D2=c(0,0,2,0,2)
#probFun.D3=c(0,1,1,1,1)
probFun.D3=c(1,1,1,1,0)
probFun.D4=c(0,0,0,2,2)
probFun.D5=c(0,0,0,1,3)
probFun.D6=c(0,0,0,1,3)
probs.Fun = rbind(probFun.A1, probFun.A2, probFun.A3, probFun.A5, probFun.B1, probFun.B2,
  probFun.B3, probFun.B4a, probFun.B4b, probFun.B4c, probFun.B5, probFun.B6, probFun.B7,
  probFun.B8, probFun.B9, probFun.C1, probFun.C2, probFun.C3, probFun.C4, probFun.C5,
  probFun.C6a, probFun.C6b, probFun.C7, probFun.D1, probFun.D2, probFun.D3, probFun.D4,
  probFun.D5, probFun.D6)

result.Fun = PMax.Emp.Likert(values,probs.Fun)
sum(result.Fun$PMax)

#-----
# Academia subgroup

probAcad.A1=c(0,1,2,3,4)
probAcad.A2=c(0,0,0,2,8)
probAcad.A3=c(0,0,0,3,7)
probAcad.A5=c(0,0,2,6,2)
#probAcad.B1=c(0,4,4,2,0)
probAcad.B1=c(0,2,4,4,0)
probAcad.B2=c(0,0,0,5,5)
probAcad.B3=c(0,0,0,3,7)
probAcad.B4a=c(0,0,2,6,2)
probAcad.B4b=c(0,0,2,4,4)
probAcad.B4c=c(0,0,1,5,4)
probAcad.B5=c(0,1,0,5,4)
probAcad.B6=c(0,1,4,3,2)
probAcad.B7=c(0,0,2,4,4)
probAcad.B8=c(0,0,1,3,6)
probAcad.B9=c(0,0,2,6,2)
probAcad.C1=c(0,0,0,4,6)
probAcad.C2=c(0,0,0,1,9)
probAcad.C3=c(0,3,0,7,0)
probAcad.C4=c(0,0,0,5,5)
probAcad.C5=c(0,0,0,2,8)
probAcad.C6a=c(0,1,1,4,4)
probAcad.C6b=c(0,3,1,4,2)
probAcad.C7=c(0,0,0,7,3)

```

```

probAcid.D1=c(0,0,0,4,6)
probAcid.D2=c(0,0,0,3,7)
#probAcid.D3=c(2,3,3,2,0)
probAcid.D3=c(0,2,3,3,2)
probAcid.D4=c(0,1,1,2,6)
probAcid.D5=c(0,0,0,3,7)
probAcid.D6=c(0,0,1,4,5)
probs.Acd = rbind(probAcid.A1, probAcid.A2, probAcid.A3, probAcid.A5, probAcid.B1, probAcid.B2,
  probAcid.B3, probAcid.B4a, probAcid.B4b, probAcid.B4c, probAcid.B5, probAcid.B6, probAcid.B7,
  probAcid.B8, probAcid.B9, probAcid.C1, probAcid.C2, probAcid.C3, probAcid.C4, probAcid.C5,
  probAcid.C6a, probAcid.C6b, probAcid.C7, probAcid.D1, probAcid.D2, probAcid.D3, probAcid.D4,
  probAcid.D5, probAcid.D6)

result.Acd = PMax.Emp.Likert(values,probs.Acd)
sum(result.Acd$PMax)

#-----
# FINAL: join all results into a single dataframe
#
df <- data.frame(questions, result.Full$Rank, result.Full$PMax,
  result.Law$Rank, result.Law$PMax,
  result.Tec$Rank, result.Tec$PMax,
  result.Fun$Rank, result.Fun$PMax,
  result.Acd$Rank, result.Acd$PMax)
df

```