

ESCOLA DE COMANDO E ESTADO-MAIOR DO EXÉRCITO  
ESCOLA MARECHAL CASTELLO BRANCO

MARCELO ANTONIO OSSLER **MALAGUTTI**

*Software Power as a Cyber-Dissuasion Tool  
for Non-Aggressive Nations*



Rio de Janeiro  
2021



Doutorando MARCELO ANTONIO OSSLER **MALAGUTTI**

***Software Power as a Cyber-Dissuasion Tool for Non-Aggressive Nations***

Thesis presented as a requirement for obtaining the title of PhD in Military Sciences by the Post-Graduation in Military Sciences Programme of the Brazilian Army Command and General Staff College (ECEME) – Major in Peace and War Studies (EPG).

Supervisor: Prof. Dr RICARDO BORGES GAMA NETO

Rio de Janeiro  
2021

M236s	Malagutti, Marcelo Antonio Osller
	Software Power as a Cyber-Dissuasion Tool for Non-Aggressive Nations. / Marcelo Antonio Osller Malagutti. —2021. 240 f.: il.; 30 cm.
	Orientação: Ricardo Borges Gama Neto. Tese (Doutorado em Ciências Militares) — Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2021. Bibliografia: f. 211-240.
	1. CYBER DISSUASION. 2. CYBER COERCION. 3. INSTITUTIONALISM. I. Título.
	CDD 003.5

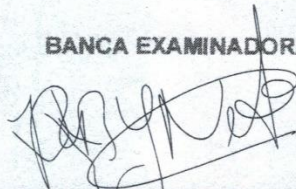
**MARCELO ANTÔNIO OSSLER MALAGUTTI**

**SOFTWARE POWER AS A CYBER DISSUASION TOOL FOR NON-AGGRESSIVE NATIONS.**

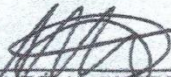
Tese apresentada à Escola de Comando e Estado-Maior do Exército, como requisito parcial para a obtenção do título de Doutor em Ciências Militares.

Aprovada em 10 de fevereiro de 2021.

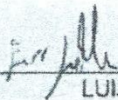
**BANCA EXAMINADORA**



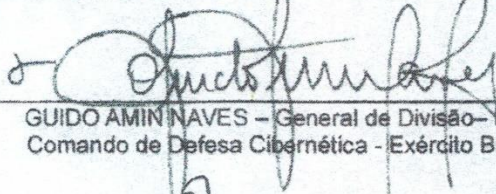
RICARDO BORGES GAMA NETO – Prof Dr – Presidente  
Escola de Comando e Estado-Maior do Exército - ECEME



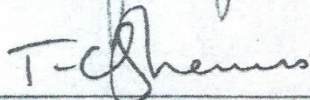
MARCOS AURÉLIO BUÉDES DE OLIVEIRA – Prof Dr – Membro  
Escola de Comando e Estado-Maior do Exército - ECEME



LUIZ ROGÉRIO FRANCO GOLDONI – Prof Dr – Membro  
Escola de Comando e Estado-Maior do Exército - ECEME



GUIDO AMIN NAVES – General de Divisão – Membro  
Comando de Defesa Cibernética - Exército Brasileiro



TIMOTHY CHARLES STEVENS – Prof Dr – Membro  
King's College London

Ciente



MARCELO ANTÔNIO OSSLER MALAGUTTI – Postulante  
Escola de Comando e Estado-Maior do Exército



## **ACKNOWLEDGEMENTS**

I am profoundly grateful:

To my wife Andrea and our daughters, Larissa and Leticia, for the understanding and permanent support provided during this work.

To my parents, Antonio (*in memoriam*) and Cecilia, for everything they have proportionated to me.

To my thesis Supervisor, Professor Dr Ricardo Borges Gama Neto, for his safe and smooth guidance, availability and permanent support throughout this journey.

To my professors and colleagues at Meira Mattos Institute, King's College London and Brazilian Cyber Defence Command, for their teachings, friendship, and healthy and fruitful coexistence.





*“Qui desiderat pacem, praeparet bellum (If you want peace, prepare for war).” (Flavius Vegetius)*

*We shall fight on the beaches; we shall fight on the landing grounds; we shall fight in the fields and in the streets; we shall fight in the hills; we shall never surrender.” (Winston Churchill)*



## **ABSTRACT**

Cyberattacks increasingly become an option in the “toolbox” of nation-states for the coercion of other nations. This determines the need to study the possibilities of deterrence and defence against this threat. While the mainstream of cyber-dissuasion literature extols Dissuasion by (fear of) Punishment, based on the threat of retaliation, it is unlikely to be successful for nations with a non-aggressive tradition. Hence, ineffective! It is necessary to evaluate other dissuasion alternatives for these nations. Thus, the evolution of deterrence (or dissuasion) theory is investigated in-depth, as well as its adaptation to the threats posed by cyberspace. Also examined are the characteristics of state-sponsored cyber-offences, the nature of defence strategies and defence and attack instruments, in addition to the economic impacts of both the adoption and non-adoption of dissuasive and defensive measures. While computers and components (hardware) have traditionally characterized the pursuit of military cyber power, modern cyber threats are mostly concentrated in software capabilities (‘Software Power’). It is concluded that the possibilities presented by the development of these capacities constitute a potential element to leverage the national power in its military, economic and scientific-technological expressions.

Keywords: Cyber Dissuasion; Cyber Coercion; Institutionalism.



## RESUMO

Ciberataques tornam-se crescentemente uma opção na “caixa de ferramentas” dos estados nacionais para a coerção de outras nações. Isso determina a necessidade de se estudar as possibilidades de dissuasão e defesa contra esta ameaça. Enquanto o *mainstream* da literatura sobre ciberdissuasão enaltece a Dissuasão por (medo de) Punição, com base na ameaça de retaliação, esta apresenta-se inverossímil para nações com tradição não-agressiva. Portanto, ineficaz! Faz-se necessário avaliar outras alternativas de dissuasão para essas nações. Assim, investiga-se em profundidade a evolução da teoria da dissuasão, bem como sua adequação às ameaças postas pelo ciberespaço. Investiga-se também as características das ciberofensas perpetradas por estados nacionais, a natureza das estratégias e instrumentos de defesa e ataque, além dos impactos econômicos tanto da adoção quanto da não adoção de medidas dissuasórias e defensivas. Conquanto computadores e componentes (hardware) tenham tradicionalmente caracterizado a busca do poder militar cibernético, as ciberameaças modernas concentram-se majoritariamente em capacidades de software (*Software Power*). Conclui-se que as possibilidades apresentadas pelo desenvolvimento dessas capacidades constituem elemento potencial para alavancagem do poder nacional em suas expressões militar, econômica e científico-tecnológica.

Palavras-chave: Ciberdissuasão; Cibercoerção; Institucionalismo.



## LIST OF FIGURES

Figure 1 – Graphical View of the Elements of Influence and Coercion Theories .....	74
Figure 2 – Graphical View of the Context of Causation .....	94
Figure 3 – Evolution of the Number of Publications on Cyber-Deterrence (sic).....	95
Figure 4 – Evolution of Brazilian Cyber Defence Budget .....	178
Figure 5 – World IT Market Distribution.....	201





## LIST OF TABLES

Table 1 – World’s Largest Supercomputers in November 2015.....	35
Table 2 – World’s Largest Supercomputers in November 2020.....	36
Table 3 – Computing Power of Folding@home Platform.....	39
Table 4 – Other Countries Largest Supercomputers in November 2020.....	40
Table 5 – Largest Supercomputers Power Consumption (in November 2020).....	41
Table 6 – Comparison Between Punishment and Denial.....	126
Table 7 – Comparison Among the Six Types of Cyber Dissuasion.....	127
Table 8 – Corpus Candidate Documents.....	133
Table 9 – Categories and Subcategories of NCSS Elements.....	138
Table 10 – Regexes per Type.....	142
Table 11 – Terms per Document.....	143
Table 12 – Frequency per Category.....	145
Table 13 – Frequency per Subcategory.....	146
Table 14 – Frequency per Category (adjusted DRTI).....	149
Table 15 – Frequency per Subcategory (adjusted DRTI).....	151
Table 16 – Top-5 Subcategories per Country.....	157
Table 17 – Top 5 Subcategories per “Aggressive” Nation.....	158
Table 18 – Top 5 Subcategories per “Non-Aggressive” Nation.....	158
Table 19 – Organisations of Cyber Defence and Security.....	179
Table 20 – Population, Military Personnel and GDP (PPP).....	183
Table 21 – Compared Cyber Defence and Defence Staff.....	184
Table 22 – Proposal of Evolution of ComDCiber Staff.....	185
Table 23 – Brazilian Military Officers Wages.....	187
Table 24 – Qualification Additional.....	187
Table 25 – Average Monthly Wage of Systems Analysts in Brazil.....	188
Table 26 – Dimensions & KPAs of the Oxford GCSCC Maturity Model.....	191
Table 27 – Areas per Stage in Brazilian Capacities.....	192
Table 28 – Areas per Stage in Brazilian and British Capacities (no Hybrid Stage).....	192
Table 29 – Score of Each Area of the Brazilian Capacities.....	193
Table 30 – Points of Each Area of the UK Capacities.....	193
Table 31 – U.S. Software Market Evolution between 2014 and 2018.....	199
Table 32 – E.U. Software Market Evolution between 2014 and 2016.....	200

Table 33 – Brazilian Software Market Evolution between 2015 and 2019 .....	201
Table 34 – Global Market of Software and Services in 2018 .....	202
Table 35 – Global Market of Software and Services in 2019 .....	203

## SUMMARY

<b>ACKNOWLEDGEMENTS</b>	<b>7</b>
<b>ABSTRACT</b>	<b>11</b>
<b>RESUMO</b>	<b>13</b>
<b>LIST OF FIGURES</b>	<b>15</b>
<b>LIST OF TABLES</b>	<b>17</b>
<b>SUMMARY</b>	<b>19</b>
<b>FORMATTING CONVENTIONS</b>	<b>23</b>
<b>1 PRELUDE</b>	<b>25</b>
<b>1.1 Introduction, Context and Motivation</b>	<b>25</b>
<b>1.2 The Research Question</b>	<b>27</b>
1.2.1 Support Questions	27
1.2.2 Objectives	28
1.2.3 Scope Delimitation	29
1.2.4 Contribution of the Research to the Military Sciences	29
<b>1.3 Theoretical and Methodologic Frameworks</b>	<b>29</b>
1.3.1 Theoretical Framework	29
1.3.2 Methodological Frameworks	29
1.3.3 Sources	29
<b>1.4 Limitations</b>	<b>30</b>
<b>1.5 Thesis Structure</b>	<b>30</b>
<b>2 SOFTWARE POWER</b>	<b>33</b>
<b>2.1 Introduction</b>	<b>33</b>
<b>2.2 Cyber Power</b>	<b>33</b>
<b>2.3 Hardware Power is not Unimportant</b>	<b>35</b>
<b>2.4 Why Focusing on Software Power?</b>	<b>37</b>
2.4.1 All Malware is Software!	37
2.4.2 Software ‘Animates’ Hardware!	37
2.4.3 Software Can Be Operated Remotely	38
2.4.4 Software Can Substitute Hardware	38
2.4.5 Hardware has a High Entry Barrier	39
2.4.6 Hardware Faces Export Restrictions	40
2.4.7 “Data Is the New Oil” (THE ECONOMIST, 2017)	42
<b>2.5 Conclusion</b>	<b>42</b>

<b>3</b>	<b>“NON-AGGRESSIVE” NATIONS</b>	<b>45</b>
<b>3.1</b>	<b>Introduction</b>	<b>45</b>
<b>3.2</b>	<b>The Relevance of Culture in Power Assessments</b>	<b>45</b>
<b>3.3</b>	<b>The Institutionalisation of Culture</b>	<b>51</b>
<b>3.4</b>	<b>Aggressive (and Non-Aggressive)</b>	<b>52</b>
<b>3.5</b>	<b>The “Brazilian-Way” (or <i>O Jeitinho Brasileiro</i>)</b>	<b>53</b>
<b>3.6</b>	<b>Conclusion</b>	<b>56</b>
<b>4</b>	<b>‘DETERRENCE THEORY’ FALLS SHORT</b>	<b>57</b>
<b>4.1</b>	<b>Introduction - The Hatcher of ‘Deterrence Theory’</b>	<b>57</b>
<b>4.2</b>	<b>On ‘Deterrence Theory’</b>	<b>58</b>
4.2.1	The Structural Elements of ‘Deterrence Theory’	60
4.2.2	Coercion & Strategy	70
<b>4.3</b>	<b>On ‘Influence Theory’</b>	<b>71</b>
4.3.1	Structural Elements of ‘Influence Theory’	71
<b>4.4</b>	<b>Comparing ‘Deterrence’ and ‘Influence’ Theories</b>	<b>73</b>
<b>4.5</b>	<b>The Pitfalls of Deterrence and Influence Theories</b>	<b>74</b>
4.5.1	The Limited Scope of ‘Deterrence’ (And ‘Coercion’)	74
4.5.2	The Problem of the Term ‘Influence’	75
<b>4.6</b>	<b>The Unfolding of ‘Dissuasion Theory’</b>	<b>76</b>
<b>4.7</b>	<b>Types of Dissuasion</b>	<b>78</b>
4.7.1	Dissuasion by Punishment	78
4.7.2	Dissuasion by Denial	80
4.7.3	Dissuasion by Futility	83
4.7.4	Dissuasion by Norms	84
4.7.5	Dissuasion by Entanglement	85
4.7.6	Dissuasion by Individualisation	86
<b>4.8</b>	<b>Dissuasion in the Russian and Chinese Doctrines</b>	<b>87</b>
<b>4.9</b>	<b>Dissuasion in the Brazilian Doctrine</b>	<b>89</b>
<b>4.10</b>	<b>The Blossom of ‘Causation Theory’</b>	<b>91</b>
<b>4.11</b>	<b>Conclusion</b>	<b>94</b>
<b>5</b>	<b>ON ‘CYBER-DISSUASION’</b>	<b>95</b>
<b>5.1</b>	<b>Introduction</b>	<b>95</b>
<b>5.2</b>	<b>The Need for Cyber-Dissuasion</b>	<b>96</b>

<b>5.3</b>	<b>National Security and Cyberspace</b>	<b>97</b>
<b>5.4</b>	<b>Cyber-Power and Causation Operations</b>	<b>99</b>
5.4.1	General Concepts	99
5.4.2	Causation Theory Concepts	106
<b>5.5</b>	<b>Types of Cyber Dissuasion</b>	<b>112</b>
5.5.1	Punishment	112
5.5.2	Denial	115
5.5.3	Futility	118
5.5.4	Norms	119
5.5.5	Entanglement	124
5.5.6	Individualisation	125
<b>5.6</b>	<b>A Comparison Among the Different Types of Dissuasion</b>	<b>126</b>
<b>5.7</b>	<b>Cyber-Dissuasion in the Brazilian Doctrine</b>	<b>128</b>
<b>5.8</b>	<b>Conclusion</b>	<b>128</b>
<b>6</b>	<b>COMPARED ANALYSIS OF CYBERSECURITY STRATEGIES</b>	<b>131</b>
<b>6.1</b>	<b>Introduction</b>	<b>131</b>
<b>6.2</b>	<b>Methodology</b>	<b>131</b>
6.2.1	The Pre-Analysis Phase	132
6.2.2	The Analysis Phase	140
<b>6.3</b>	<b>Validation of Gathered Data</b>	<b>142</b>
6.3.1	On the Number of Terms	142
6.3.2	On Categories	143
6.3.3	On Subcategories	144
<b>6.4</b>	<b>Computing the Degree of Relative Thematic Incidence (DRTI)</b>	<b>149</b>
6.4.1	Categories (adjusted by DRTI)	149
6.4.2	Subcategories (adjusted by DRTI)	150
<b>6.5</b>	<b>Analysis of the Outliers by Subcategories</b>	<b>154</b>
<b>6.6</b>	<b>Analysis by Country</b>	<b>156</b>
<b>6.7</b>	<b>Conclusion</b>	<b>159</b>
<b>7</b>	<b>WHEN TWO BECOME NONE</b>	<b>161</b>
<b>7.1</b>	<b>Introduction</b>	<b>161</b>
<b>7.2</b>	<b>On Security and Defence</b>	<b>162</b>
7.2.1	The Classic Distinction and the Securitization Merge	162
7.2.2	The Fusion of National Security and Defence in the Cold War	162
7.2.3	The Institutionalization of Defence and Security in Brazil	163
7.2.4	Post-Cold War Securitisation	164
<b>7.3</b>	<b>On Strategy and Strategic Communication</b>	<b>166</b>
<b>7.4</b>	<b>Impacts in Brazilian Cyber Defence and Cybersecurity</b>	<b>168</b>

<b>7.5</b>	<b>A ‘Brazilian-Way’ Cyber Strategy</b>	<b>169</b>
7.5.1	On Scope	169
7.5.2	On Objectivity, Verbal Moods and Language	171
7.5.3	On Document Structure	172
7.5.4	On References	173
<b>7.6</b>	<b>Conclusion</b>	<b>174</b>
<b>8</b>	<b>BRASILIAN CYBER CAPABILITIES</b>	<b>177</b>
<b>8.1</b>	<b>Introduction</b>	<b>177</b>
<b>8.2</b>	<b>Compared Analysis of Cyber Defence Structures</b>	<b>179</b>
<b>8.3</b>	<b>The Peculiar Organization of Brazilian Cyber Defence</b>	<b>180</b>
<b>8.4</b>	<b>The Need for Increasing the Staff of ComDCiber</b>	<b>182</b>
8.4.1	On the Size of an Adequate Staff	182
8.4.2	How Big Should ComDCiber Be, and How to Get There?	184
8.4.3	The Need for Civilian Staff	186
<b>8.5</b>	<b>Where to Locate ComDCiber in the Context of the Ministry of Defence?</b>	<b>189</b>
<b>8.6</b>	<b>The OAS and Oxford Report on Brazilian Cyber Capabilities</b>	<b>190</b>
<b>8.7</b>	<b>On the Good News</b>	<b>194</b>
<b>8.8</b>	<b>Conclusion</b>	<b>195</b>
<b>9</b>	<b>THE STRATEGIC OPPORTUNITY POSED BY SOFTWARE POWER</b>	<b>197</b>
<b>9.1</b>	<b>Introduction – “It’s the Economy, Stupid!”</b>	<b>197</b>
9.1.1	Cutting Costs	197
9.1.2	Increasing Revenue	198
<b>9.2</b>	<b>The Global Software Market</b>	<b>198</b>
9.2.1	The U.S.	199
9.2.2	Europe	199
9.2.3	Brazil	200
<b>9.3</b>	<b>Cyber Security and Defence Market</b>	<b>204</b>
<b>9.4</b>	<b>Strategic Opportunity</b>	<b>205</b>
<b>9.5</b>	<b>Conclusion</b>	<b>207</b>
<b>10</b>	<b>CONCLUSION</b>	<b>209</b>
<b>11</b>	<b>REFERENCES</b>	<b>211</b>

## FORMATTING CONVENTIONS

This thesis has been written under the Brazilian Technical Norms Association (ABNT) formatting and referencing specifications.

In-text citations, thus, appear as:

- At the end of the phrase: "... (SURNAME, YEAR)" or "... (SURNAME1; SURNAME2, YEAR)";
- At the beginning or the middle of a phrase: "Surname (YEAR)..." or "Surname1 and Surname2 (YEAR) ...".

Other typographic conventions may affect the understanding of the text, and be perceived as follows (MENDES; FORSTER JÚNIOR, 2018):

- ‘Single quotes’ are used in transcriptions, highlighting, or a quote within a quote.
- “Double quotes” mark the beginning and end of a quote that does not exceed three full lines; text citations in footnotes; vernacular expressions used only in a specific professional environment; relative terms, such as slang, nicknames or an ironic meaning; or conceptual definitions of terms.
- *Italics* highlight book titles, periodicals, plays, films, operas, music, paintings and sculptures. Scientific species names, words, expressions and phrases in other languages (including Latin) cited in the text to be emphasized may also be in italics.
- **Bold** highlights Chapter, Section and Subsection names, and letters or words when the use of any of the methods mentioned above is not possible.
- Underlined indicates Subsubsection names.

According with norm ABNT NBR 6024, progressive numbering is used for sections starting with level one (primary sections, or chapters) to level five (ex.: 1.1.1.1.1.).





## 1 PRELUDE

Might ‘Software Power’ be a tool of Cyber-Dissuasion for Non-Aggressive Nations? This is the question answered in this research, which has confirmed the hypothesis that software capabilities can have a deterrent/dissuasive effect against cyber-offenders, and that the development of such capabilities can represent a strategic opportunity for the desired international insertion of a country like Brazil. For explaining such conclusions, this work starts by presenting the context of the problem.

### 1.1 Introduction, Context and Motivation

In recent years it has become common sense to consider cyberspace as the fifth domain of war, after land, sea, air and outer space. In this fifth domain, the United States of America (USA or U.S.), as in all other domains, seeks to preserve its supremacy, maintaining the advantage gained with its historical control over the development of computers and the Internet, as well as in the production of software. Other "cyber powers", such as the United Kingdom (UK), France and Israel, also develop advanced offensive capabilities. Countries like China, Russia, North Korea and Iran also use cyberspace widely as a statecraft resource.

At the same time, North-American think tanks debate a new ‘grand strategy’ for the USA, in which it is necessary to decide between the limits of primacy and restraint (MAZARR, 2016). The restraint trend is evidenced by announcements of withdrawal or reduction of American military forces from Europe and Asia. It should force its European and Asian allies to invest more in their own defence and ease battered American coffers. This option also avoids ‘body-bags’ which, televised, generate enormous political “wear and tear”. Nevertheless, neither the prospect of restraint nor that of primacy indicates that the United States would reduce its presence or aggressiveness in cyberspace (GOMPERT; BINNENDIJK, 2016). Indeed, the option for a more limited global military presence would free up resources for an even more aggressive presence in cyberspace, which could compensate for the loss of global kinetic (or physical) presence. Moreover, the vast resources liberated by the option for restraint could also be applied by the USA in the ‘American Hemisphere’, aiming to increase its grasp on this area.

Besides, “software tools” have long been used for espionage, sabotage, crime or activism, sponsored or not by states. Among many examples, the Snowden case, in particular, revealed a massive state espionage operation. It involved political espionage, related to the personal communications of the German Chancellor, the presidents of Brazil and Mexico, and some of their ministers, as well as thousands of other people. Outside the political scope, Snowden also showed systematic spying on Petrobras, the Brazilian state oil company that had

announced the discovery of gigantic oil reserves in Brazilian jurisdictional waters a few years earlier.

Espionage, sabotage, crime and activism, in general, are related to security, and in themselves would justify nations to invest in their software power. However, before the Snowden Case, there has been one notably different case, named Stuxnet. Although Rid (2012) disagrees, for the first (known) time software was used by one nation-state to impose its political will on another, using violence, in the form of physical destruction of machinery, and even lethality, in the way of attacking a vital interest of a nation. It is known that “an act of force **to compel our enemy to do our will**” is an act of war (CLAUSEWITZ, 1976, p. 75, emphasis added). In Schelling’s (1990) terms, a clear example of compellence, where a rational actor is led to decide against his will. Stuxnet, therefore, was a ‘watershed’ when it introduced an even more fundamental reason for nations to pursue software power: defence!

In a more contemporary example, the American intelligence community attributed to Russia the attacks on the Democratic Party and the selective leaks of information contrary to the Democratic candidate and in favour of the Republican candidate, winner of the election, indicating that the Russians were trying to influence the 2016 North-American presidential elections (PALETTA, 2016). The following week, President Obama declared that the White House would be studying proportional responses, while Russian Chancellor Sergei Lavrov told CNN that Russia “does not deny”, but “we have not seen a single fact, a single proof”; “if they decide to do something, let them do it,” he said (KREVER; SMITH-SPARK, 2016).

Even though the U.S. always complains about the “aggressions” promoted by Chinese, Russians, North Koreans and Iranians to their cyberspace, there is a critical current that puts Americans themselves in the most aggressive pole of this space (AUSTIN, 2015; HARRIS, 2014a). Conceptually, the same cybernetic power that Americans would have used against Iran is now being used against them by the Russians, essentially for the same purpose: coercion by compulsion.

Schelling (1980, p. 194) determined that, in addition to capabilities, credibility was an essential element of deterrence by threat of punishment (or fear), associated mainly with the willingness to employ the available retaliatory means. This will would be related to the personality (face) of a country: its reputation for the action, the expectation that other countries have about its behaviour. After WWII, among the G-20 countries, only Brazil, Germany, Mexico and Japan did not engage in aggressive actions, as defined by the United Nations (U.N.) except in operations sanctioned by the U.N. itself or by regional multilateral entities where all of the countries involved were members. These four countries, therefore, have a ‘face’ of non-

aggressive nations. Even so, all have been spied on by the U.S. National Security Agency (NSA) and other members of Five-Eyes (the U.S., the United Kingdom, Canada, Australia and New Zealand intelligence communities) (GREENWALD, 2014). Additionally, they are also spied on by China and Russia, and possibly others (WAGSTYL, 2016).

In this geopolitical context, and considering Brazil's desire and need for international insertion, a "Brazilian look" on the cybernetic power of nation-states and its use as an instrument of coercion on the international stage becomes relevant to understand how they can affect our sovereignty. Indeed, the recent cases of cyber-offences made public internationally demonstrate that Brazil needs to be prepared to avoid becoming easy prey for nations interested in cyber-offences. The Snowden case, in particular, showed that the Americans carried out political and economic espionage operations that affected the country (GREENWALD, 2014). Before that, although not aimed to attack Brazil in particular, Stuxnet also infected critical Brazilian infrastructures that used industrial control systems provided by the German company Siemens (FALLIERE e colab., 2011). If Brazil were the target, it would undoubtedly have faced harmful and potentially catastrophic effects.

## **1.2 The Research Question**

The research's core consists of a quest to identify whether 'software power' can be an alternative for nations with institutional culture and tradition (or personality) of non-aggression to dissuade their peers from committing cyber-offences against them.

In particular, considering that the mainstream of the available literature on cyber-dissuasion (or cyber-deterrence), mostly from NATO member countries, indicates that deterrence by fear (or threat of punishment), with retaliation capabilities not necessarily "of the same nature" (in-kind), is the only economically viable alternative for cyber-dissuasion, given that deterrence by denial would be very expensive and that a "secure perimeter" cannot be established in cyber terms (NYE, 2015b).

### **1.2.1 Support Questions**

This research focused on the pursuit of "why" questions more than "how" or "what" ones. Despite, for answering the first type, it is necessary to answer some of the later types. Altogether, they constitute support questions that emerge from the context to guide the research. Ten of these questions are reproduced here since considered the more relevant ones during the research. Such questions cannot necessarily be answered in light of the public information made available. Still, they pointed out relevant traits, answered where and when possible:

- Can cyber power be an effective tool for geopolitics?

- Is the “culture” (*face*) of a “non-aggressive nation” a disadvantage in terms of cyber-dissuasion?
- Can non-aggressive nations develop effective cyber-dissuasion in the context of a highly aggressive cyber realm?
- Is *Software Power* a viable tool for cyber-dissuasion without the support of Hardware Power from supercomputers?
- How can nations develop their *Software Power*, reducing the existing gap with cyber superpowers?
- Is there a better type of dissuasion regarding cost and benefits?
- What about the other types of dissuasion?
- What would constitute an effective cyber-dissuasion?
- Is *Software Power* dependent on a nation’s economic power or a potential driver of that power?
- Can international norms provide adequate support against hostile cyber-peace?

## 1.2.2 Objectives

### 1.2.2.1 General

The possibilities of cyber-dissuasion for non-aggressive nations are critically analysed, in the light of: the original Deterrence Theory and its evolutions; the nature of state-sponsored cyber-offences; and the positions expressed by countries in their National Cyber Security Strategies (NCSSs). The research identifies distinct types of dissuasion that can be attempted, their structural elements, as well as ends, means, present and potential threats declared or implied by different countries.

### 1.2.2.2 Specific

The first specific objective was to identify why Software Power should receive particular attention from non-aggressive nations, particularly Brazil, in the formulation of public defence, security, and economic development policies.

The second, originally, consisted of identifying structural components of dissuasion theory on the National Cyber Defence Strategies of 8 (eight) countries: USA, UK, Germany, France, China, Russia, Israel and Italy. During the research, it became clear that there was not enough public information about Israel, whilst Brazil published its first NCSS. Thus, Israel was excluded from the list. Three more countries were added: Estonia and Australia, due to their increased participation in the international cyber stage, and Brazil, due to its relevance globally, although not as a cyber-power.

### **1.2.3 Scope Delimitation**

The research focused on concepts. However, it was necessary to implement a textual research tool based on regular expressions, described later, whose code and other generated artefacts were made available on GitHub, a repository of domain code and public access, and not attached to the thesis.

### **1.2.4 Contribution of the Research to the Military Sciences**

The work may constitute a reference for researchers and public policymakers interested in establishing and executing strategies focusing on cyber-dissuasion or the development of autonomous cyber defence capabilities that seek to make the country less susceptible to coercion by other nation-states.

## **1.3 Theoretical and Methodologic Frameworks**

This section presents the theoretical and methodological frameworks of the research.

### **1.3.1 Theoretical Framework**

Influence Theory, as originally described by Singer (1963) and revisited by Baldwin (1971), and its subset Deterrence Theory, well developed by the original work of Kaufmann (1954), Snyder (1959, 1960, 1961, 1970), Kahn (1960) and Schelling (1962, 1980, 2008), as well as the contributions of many others to those theories, constitute the theoretical foundation of this research.

### **1.3.2 Methodological Frameworks**

Different techniques and tools will be used in diverse parts of the work.

For defining “Software Power” and “Non-aggressive Nations”, descriptive analysis was the best-suited method (GERRING, 2012).

For the identification of structural elements of Influence Theory and Deterrence Theory, I have used qualitative content analysis (BARDIN, 2016).

With the elements above identified, the comparative analysis of NCSSs used quantitative content analysis (BARDIN, 2016). For achieving more precision on data collection, the research was automatized with a specific computer program that I developed based on the search of Regular Expressions, described in more detail in the corresponding chapter.

### **1.3.3 Sources**

Sources included official documents from several nations and multilateral agencies, books, reports, academic and news articles, videos, lecture and conference notes, in particular

those from the Brazilian War College (ESG), King's College London and the Brazilian Command and General Staff College (ECEME) PhD classes, seminars and debates, and international congresses and workshops. Additionally, technical visits and conversations with the personnel of the Brazilian Cyber Defence Command provided invaluable insights.

#### **1.4 Limitations**

This research considers a broad concept of non-aggressive nations, and has identified four of them in the G-20 countries: all of them have already published at least one National Cyber Security Strategy, and all of these documents have been considered in this research. Research also considered cultural aspects of them whenever possible. Despite, there is an emphasis in data from Brazil, mainly due to the fact that the researcher is Brazilian, developing his research in a Brazilian military school, financed by the Brazilian Ministry of Education, and on a subject defined as strategic to Brazilian defence by the Brazilian National Strategy of Defence. Nevertheless, both the theoretical framework and the empirical data collected indicate the concrete possibility of using inductive reasoning to conclude for the applicability of the premises to all of the other countries that constitute the group.

#### **1.5 Thesis Structure**

For better answering the research question, it is necessary to 'dissect the problem' and conceptualise its three foundational components. Thus, Chapter 2 describes the meaning of "Software Power", while Chapter 3 develops the idea of "Non-Aggressive nations", departing from the U.N.'s definition of aggression. It also develops on how 'traditions' are incorporated into national 'character' and 'culture' and shapes national character and behaviour. Chapter 4 digs into the origins, evolution and limits of 'Deterrence Theory' and even the broader 'Coercion Theory', and explains why a 'Causation Theory' shall be more adequate the contemporary context, detailing the fundamental elements of it.

Established the theoretical foundations, the next chapters use them to develop different types of analyses. Chapter 5 focuses on the applicability of dissuasion theory to cyberspace (or cyber-dissuasion theory), presenting the six types of dissuasion currently identified, and comparing them considering the relevance of the structural elements of Dissuasion. Chapter 6 presents a comparison of 14 National Cyber Security Strategies, considering a broad set of components, identifying their commonalities and idiosyncrasies. Chapter 7 analyses the Brazilian e-Ciber considering Brazilian culture's perspective as a determinant influencer of its shape and content. Chapter 8 draws on Brazilian Cyber Capabilities, again with a comparative perspective. Then, Chapter 9 presents the strategic opportunity posed by Software Power as an

instrument of international insertion and income generation. Finally, chapter 10 presents the research conclusions and points out its strengths and weaknesses, and possible future developments of it.





## 2 SOFTWARE POWER

This chapter explains the concept of Software Power, departing from the idea of cyber-power as having two constitutive parts: hardware power and software power.

### 2.1 Introduction

A well-accepted definition of Cyber Power states it as “the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power” (KUEHL, 2009, p. 38).

Nye (2004) defined soft power as the ability to attract and persuade, while hard power was that of coercing. Although playing with Nye’s terminology, it is essential to clarify that both hardware and software power, as defined here, are examples of ‘hard power’ in his original concept.

The concepts of cyber power, soft power and hard power presented above deal with many of the elements that constitute the foundation of Influence Theory: influence, persuasion and coercion. These, and their use in cyberspace, are an essential part of this work.

### 2.2 Cyber Power

“Might an army of software wizards use insidious electronic means to dislocate the support systems of modern societies, such as transport, banking and public health?” (FREEDMAN, 2015, p. 228). This question presents the two central elements of the so-called cyber power: software, whose “wizards” would use “insidious electronic means”, hardware, to achieve their goals.

Humans have a clear perception of the materiality of things. The same clarity exists concerning the concrete military artefacts of the industrial era: aircraft, armoured vehicles, missiles and armies. They are valued as symbols of power. In May 1935, the French Chancellor Laval interviewed Stalin to discuss a pact between France and the Soviet Union (USSR or S.U.). After three days debating the French army’s strength, Laval asked if Stalin could encourage religion and the Catholics in Russia, arguing that this could help with the Pope. Stalin answered: “Oho! The Pope! How many divisions has he got?” (CHURCHILL, 1986, p. 121). In cyber terms, Stalin’s question would correspond to “How many supercomputers has he got?”. Materiality corresponds to hardware.

It is much harder to realize the importance of knowledge, the fuel of the post-industrial era, which is immaterial, abstract: no form, colour, weight, smell; human senses cannot perceive it. In cyber terms, it is called software.

There are some compelling arguments for considering cyber power in its totality. For example, hardware and software depend upon one another; attacks from one side can affect the other (GAMA NETO; LOPES, 2014, p. 34). Besides, the U.S. Army works with the concept of Cyber Electromagnetic Activities (CEMA), defined “as a unified effort where cyberwar and electronic operations must be integrated and synchronized, perceived as a unique operational environment” (GAMA NETO, 2017, p. 212, free translation). Albeit, developing nations have difficulties with hardware development. Hence, software becomes more feasible for them. Brazil, for instance, is “deficient mainly in the hardware layer, due to a history of low investments in science and technology”, whilst, in software, “the country plays an important role and has positioned itself as one of the largest program producers in the world” (GUEDES DE OLIVEIRA; PORTELA, 2017, p. 77, free translation). More arguments that support focusing on Software Power, mainly when resources for hardware development are limited, are further discussed in detail.

The term cyber power, “part of a terminological lineage that includes ‘airpower’ and ‘seapower’ to describe the operations of national, principally military, coercive power in particular environmental domains” lacks clear and precise definitions (BETZ; STEVENS, 2011, p. 43).

To avoid such inaccuracy, the term Software Power was conceived to designate:

*Software tools used on behalf of a state to exploit, deny, degrade, disrupt, destroy or defend computer networks, its connected devices, and information systems or data resident on them* (MALAGUTTI, Marcelo, 2016b).

In practical terms, offensive and defensive software capabilities related to cyber-operations originated by states targeting other states.

This definition brings together the three subsets of Computer Network Operations (CNO): Computer Network Exploitation (CNE), Computer Network Attack (CNA), and Computer Network Defence (CND) (KLIMBURG; HELI TIRMAA-KLAAR, 2011, p. 7). It also extends such concepts to include not only ‘computer networks’, but also all devices connected to them, as well as systems and data residing on them (MALAGUTTI, Marcelo, 2016b). Finally, it specifies software used in ‘state-sponsored’ cyber operations, thus including Libicki’s already classic definition (LIBICKI, 2009, p. 23).

The given definition also excludes PsyOps (psychological operations) or the so-called Informational Warfare, the use of social networks, such as Twitter or Facebook as occurred during the Arab Spring or in recent elections in the U.S. and different countries in Europe. It also precludes fruitless discussions about cybernetics presenting ‘shading areas’ related to

electronic warfare. According to the definition used in this work, exploiting a network vulnerability through software, or remotely ‘hacking’ an unmanned aerial vehicle (drone) is a software power operation. The use of radio signals to interfere in the same drone’s communication and control capacity does not constitute this type of operation. The above definition also excludes operations not sponsored by states, whether or not motivated by political intentions (MALAGUTTI, Marcelo, 2016b).

### 2.3 Hardware Power is not Unimportant

The focus on ‘Software Power’ does not pretend that ‘Hardware Power’ is irrelevant.

Which country possesses the world’s fastest computer matters as much to policymakers now as which country possessed the fastest or longest-range aircraft in the interwar period, and for the same reason. They are thought to be indicative of military potential as well as prestige. (BETZ; STEVENS, 2011, p. 86)

The unit for measuring today’s supercomputers’ computational power is PFLOPS (PetaFLOPS), meaning  $1,000^5$  (one thousand elevated to the fifth power), which gives the greek prefix ‘peta’, a scale of 5, to this unit, corresponding to  $10^{15}$  Floating-point Operations Per Second. Table 1 shows the top five supercomputers in the world as in November 2015.

Table 1 – World’s Largest Supercomputers in November 2015.

Rank	Country	Computer	Capacity (PFLOPS)
1	China	Tianhe-2 (MilkyWay-2)	33,9
2	USA	Titan	17,6
3	USA	Sequoia	17,2
4	Japan	RIKEN	10,5
5	USA	Mira	8,6

Source: Compiled by the author with data from TOP500.org (2015).

In the subsequent update of the list, in June 2016, a new Chinese computer, the Sunway TaihuLight, was in the first position, with 93.0 PFLOPS of capacity, almost three times faster than its conational Tianhe-2 and five times faster than the North-American Titan (TOP500.ORG, 2016).

Despite the enormous processing power of TaihuLight, it was based on a 256-core processor designed and built in China (FU e colab., 2016). However, while the Chinese could and should be proud of their double achievement, the North-Americans also expanded theirs. That same June 2016, a U.S. university announced the creation of the first kilo-core processor (1024-core), four times larger than the recently launched Chinese processor (FELL; BASS, 2016).

It was only in June 2018 the North-Americans dethroned TaihuLight, with Summit. It had a quarter of the cores of its Chinese contender (“only” 2,282,544 cores against the opponent’s 10,649,600) and achieved impressive 122.3 PFLOPS of sustained capacity. The USA also presented a new supercomputer that assumed the third position in the ranking, Sierra, with 71.6 PFLOPS of sustained capacity.

The list did not change much until June 2020, when the Japanese computer Fugaku ‘cut the line’ and reached the first place, with more than three times the computing power of Summit, a position kept until now (indeed with a small increase in the sustained processing capacity in the recent list).

Table 2 presents the most recent top 500 list (November 2020).

Table 2 – World’s Largest Supercomputers in November 2020.

Rank	Country	Computer	Capacity (PFLOPS)
1	Japan	Fugaku	442,0
2	USA	Summit	148,6
3	USA	Sierra	94,6
4	China	TaihuLight	93,0
5	USA	Selene	63,5
6	China	Tianhe-2	61,4

Source: Compiled by the author with data from TOP500.org (2020).

Superior processing capabilities are essential for tasks of military and economic importance, such as cryptanalysis or accurate simulation of nuclear reactions or chemical reactions at the molecular level.

In 2017, the European Union (EU) listed some of its concerns about European participation in the international supercomputer, or high-performance computing (HPC), market: (1) the absence of supercomputers from nations in the European Union in the list of the ten largest supercomputers; (2) the need for greater computational power for advanced research; (3) the fact that Europeans participate with 5% of the world’s supercomputing resources, although consuming a third of that computational capacity; (4) The lack of a supply chain in the European industry capable of supplying the market competitively in relation to the USA, China and Japan; (5) the risk of being technologically deprived or lagging behind in know-how for innovation and competitiveness; (6) the risk of having data produced by EU researchers and industries processed elsewhere for lack of corresponding capacities in Europe (EUROPEAN COMMISSION, 2017b). This led the European Union to start the EuroHPC (European High-

Performance Computing Joint Undertaking) project, whose central objective is to foster European investments in the supercomputing segment by injecting approximately one billion euros in the 2018-2020 period (EUROPEAN COMMISSION, 2017a).

Moreover, expanding the current processing capabilities is a promise of the research into new quantum computers (BIERCUK; FONTAINE, 2017; FINANCIAL TIMES, 2017; OWEN; GORWA, 2016; THE ECONOMIST, 2016). The U.S. Government has just announced a new five-year funding plan for quantum computing research centres: USD 625 million from the Department of Energy and USD 300 million from the research centres themselves (WHITE HOUSE, 2020).

To measure the expected quantitative processing capacity leap, it is estimated that, in 2022, it will move from ‘petascale’ to ‘exascale’ ( $1,000^6$  FLOPS), corresponding to a thousand PFLOPS, or  $10^{18}$  FLOPS. Indeed, the Japanese supercomputer Fugaku, although not based on quantum technology, has already achieved 0.41 EFLOPS (ExaFLOPS).

## **2.4 Why Focusing on Software Power?**

Despite the importance of hardware, the emphasis on Software Power observed in this work is due to several objective reasons.

### **2.4.1 All Malware is Software!**

To date, all relevant cyber offences made public are related to software capabilities rather than those of hardware. In general, cyberattacks consist of the transmission of software or data to a target network for exploiting vulnerabilities or damaging the network itself or the systems or data on it (LUKASIK, 2010).

### **2.4.2 Software ‘Animates’ Hardware!**

As explained in the question posed by Sir Lawrence Freedman (presented at the beginning of this chapter), it is the ‘magic’ of software that controls hardware, at different levels.

Software is present in many different layers in any computing device: (1) in the context of applications (or Apps ) that perform the user’s end tasks, processing the data and presenting decision support information or controlling the flow of business processes; (2) in that of middleware, intermediate software that support applications, as in the case of web servers (Apache Tomcat, for example), application servers (.NET framework or JBoss, for instance) or database managers (mySQL or Oracle, to name a few), as well as distributed processing platforms such as Hadoop, Accumulo and BOINC, discussed below; (3) in the context of operating systems (for example Windows, Linux, Android or iOS) that manage hardware

resources, such as memory, processors and other devices, allocating them to the demands of applications and middleware; (4) within the scope of the drivers that connect the operating systems to the respective hardware devices, such as printers or uranium enrichment centrifuges at the Iranian nuclear power plant in Natanz, targeted by Stuxnet; (5) in the context of the firmware (microcode) executed on the electronic circuit board components themselves, which interact with the drivers.

### **2.4.3 Software Can Be Operated Remotely**

Although “hardware can be switched off or destroyed, deliberately or accidentally”, this requires a physical presence on the spot, while remotely “software can be altered, allowing actions that were once precluded or vice versa” (STEVENS; BETZ, 2013, p. 152).

### **2.4.4 Software Can Substitute Hardware**

In the process of technological evolution, just as electronics have replaced mechanics in a wide range of uses, similarly, software has been replacing hardware. Parallel computing algorithms implemented by software have made ordinary low-cost commercial computers, interconnected in clusters, capable of processing massive volumes of data at speeds previously unprecedented. The British signal intelligence agency GCHQ, for example, uses the open-source software platform Hadoop, inspired by Google’s MapReduce, to analyse electronic communications metadata (DEAN; GHEMAWAT, 2004). This platform was designed to provide “distributed processing of large data sets across clusters of computers using simple programming models” (APACHE SOFTWARE FOUNDATION, 2020b). “With hundreds of hard disks working simultaneously multiple gigabytes can be read per second. This allows the processing of the multi-terabyte datasets we intercept” (GCHQ, 2011, p. 60). In 2008, GCHQ’s American counterpart, the National Security Agency (NSA), developed the Accumulo platform, also based on Google technology (HARRIS, 2014a, p. 36; METZ, 2012). Subsequently, in 2011, the NSA made the Accumulo platform available as open-source (APACHE SOFTWARE FOUNDATION, 2020a).

While the above platforms are capable of handling large volumes of data for relatively simple processing needs, the SETI @ home experiment (Search for Extraterrestrial Intelligence at Home), managed by the University of Berkeley, produced the Berkeley Open Infrastructure for Network Computing (BOINC), voluntary cooperative distributed computing platform. The concept of “voluntary” is characterized by the fact that a computer user installs software that ‘shares’ available computing power. For example, when a personal computer enters ‘screen saver’ mode, its processor starts to perform processing tasks for the project using the BOINC

application. On August 27, 2020, the platform registered an average of 859,385 computers active, generating 26.0 PFLOPS (BOINC, [S.d.]). This computing power puts it as the 8<sup>th</sup> most potent ‘supercomputer’ in the world.

Another voluntary computing platform is that of Folding@home (or FAH), used for computing ‘protein folding’ in search for the cure of cancer, amyotrophic lateral sclerosis and, since January 2020, Covid-19. Besides using the regular CPUs processing power, it also uses the superior capabilities of Graphics Processing Units (GPUs) and gaming consoles (FOLDING@HOME, [S.d.]). On August 2020, the stats (statistics) page of this platform had reported, in 50 days, the performance data presented in Table 3.

Table 3 – Computing Power of Folding@home Platform.

OS	AMD GPUs	Nvidia GPUs	CPUs	CPU cores	PFLOPS
Linux	8,024	436,173	1,842,044	14,877,878	943.1
Windows	27,480	98,162	263,218	1,666,878	224.5
macOSX	10	0	36,787	153,748	1.7
<b>Totals</b>	<b>35,514</b>	<b>534,335</b>	<b>2,142,049</b>	<b>16,698,504</b>	<b>1,169.3</b>

Source: Compiled by the author with data from Folding@home stats (FOLDING@HOME, [S.d.]).

As reported, the 16.7 million cores volunteered were able to provide 1,169.3 PFLOPS (or 1.17 ExaFLOPS), almost three times the computing power of the mighty Fugaku. In other words, the first exascale computer appeared already in 2020 (not in 2022, as expected), and was provided by software.

#### 2.4.5 Hardware has a High Entry Barrier

Superior hardware capabilities present a high entry barrier, due not only to the cost of designing electronic components, but also to the cost of their production plants (factories and equipment), and the fact that their market is very limited. It shall also be noted that among the countries that figure as cyber-superpowers, and those that constitute large economies, the availability of expressive hardware-power is not significant, as seen in Table 4.

The first Russian supercomputer ranks 40<sup>th</sup>, while the largest UK one figures only in the 75<sup>th</sup> position. Israel does not have a single supercomputer listed among the top 500. Neither does North Korea. Thus, hardware-power is not determinant for achieving some advanced cyber capabilities.

Table 4 – Other Countries Largest Supercomputers in November 2020.

Rank	Country	Computer	Capacity (PFLOPS)
8	Italy	HPC-5	23.5
15	Germany	SuperMUC-NG	19.5
18	France	PANGEA III	17.9
27	Australia	Gadi	9.3
40	Russia	Christofari	6.7
63	India	Siddhi-AI	4.6
66	Brazil	Atlas	4.4
75	UK	Cray XC40	3.9

Source: Compiled by the author with data from TOP500.org (2020).

#### 2.4.6 Hardware Faces Export Restrictions

Importing supercomputers is a complex task, since hardware can fall under arms control restrictions (or controlled, or sensitive, products) for its exporters. Brazil, for example, has always had difficulty importing computers and other "sensitive materials", or even in purchasing equipment made in Brazil by North-American companies (ANGELO, 2007).

Importation restrictions are not only applied to complete computers but also to their components. The Chinese Tianhe-2, today the sixth most powerful supercomputer in the world, uses Intel (an American company) processors. In mid-2015, due to the alleged use of that computer for the simulation of nuclear reactions, North-American agencies restricted exports of these processors to China (CLARK, 2015). The Chinese response, obviously planned ahead, was the launch of TaihuLight, in 2016, built exclusively with Chinese processors, as already mentioned before.

Despite the enormous Chinese achievement, the processors' technological difference is reflected in the figures of After Huawei banned the use of North American components in 2019, the Chinese giant began to work to replace these components with Chinese versions (STRUMPF, 2020). Albeit, even that strategy was threatened when the U.S. Department of Commerce stepped up in May 2020 and banned component manufacturers from around the world, using U.S. technology, from selling products to Huawei (U.S. DEPT. OF COMMERCE, 2020). This new difficulty may lift the company out of its dominant position in the 5G race, and even hinder the maintenance of other generation telephone networks provided by the company and already in use in several countries (STRUMPF, 2020). The United States is still considering blocking the supply of U.S. technology to five Chinese video surveillance companies (SHIDONG, 2019).



Table 5. Column ‘PFLOPS per kCore’ shows how many PFLOPS are generated by 1,024 cores (one kCore), while ‘PFLOPS per MW’ indicates the number of PFLOPS generated by each megawatt of energy consumed. While the nominal PFLOP capacity of TaihuLight (China) is not significantly lower than that of Sierra (USA), its PFLOP rate per kCore is only 15% of the American, and its PFLOP rate per MW is 47%. The difference is larger when considering Fugaku (Japan) and Summit (USA).

After Huawei banned the use of North American components in 2019, the Chinese giant began to work to replace these components with Chinese versions (STRUMPF, 2020). Albeit, even that strategy was threatened when the U.S. Department of Commerce stepped up in May 2020 and banned component manufacturers from around the world, using U.S. technology, from selling products to Huawei (U.S. DEPT. OF COMMERCE, 2020). This new difficulty may lift the company out of its dominant position in the 5G race, and even hinder the maintenance of other generation telephone networks provided by the company and already in use in several countries (STRUMPF, 2020). The United States is still considering blocking the supply of U.S. technology to five Chinese video surveillance companies (SHIDONG, 2019).

Table 5 – Largest Supercomputers Power Consumption (in November 2020).

Rank	Country	Computer	Capacity (PFLOPS)	Cores	Power (MW)	PFLOPS per kCore	PFLOPS per MW
1	Japan	Fugaku	442,0	7.630.848	29,9	0,058	14,8
2	USA	Summit	148,6	2.414.592	10,1	0,062	14,7
3	USA	Sierra	94,6	1.572.480	7,4	0,060	12,8
4	China	TaihuLight	93,0	10.649.600	15,4	0,009	6,0
5	USA	Selene	63,5	555.520	2,7	0,114	23,5
6	China	Tianhe-2	61,4	4.981.760	18,5	0,012	3,3

Source: Compiled by the author with data from TOP500.org (2020).

Restrictions, of course, do not only apply to hardware, but also to software. The U.S. government’s ban on Huawei prevents Google from licensing the use of Android OS on company handsets (MOON, 2019). Although its core is open source, and so it can continue to be used by the Chinese company, several associated services are provided by Google and would no longer be available, limiting smartphone usefulness (MOON, 2019).

Amidst the U.S. embargo on supplying technology to China, Beijing has ordered all government offices and public institutions to remove foreign equipment and software by 2022 (YANG; LIU, 2019). The move is part of a campaign to reduce Chinese dependence on foreign technologies, is likely to have an effect of decoupling supply chains from the U.S. and China,

and could be a severe blow to U.S. companies (YANG; LIU, 2019). The new sanctions imposed added urgency to the project, unlike previous efforts for self-sufficiency in technology, the goal is that soon companies and the government will be free from U.S. threats (YANG; LIU, 2019).

Replacing U.S. hardware and software with Chinese equivalents also poses problems. China's Lenovo uses Intel's processors and hard drives made by South Korean Samsung (YANG; LIU, 2019). China lags the U.S. in some of the most advanced technologies, including chip design and manufacturing. Intel or Qualcomm manufactures the primary components used by some of the country's largest technology companies. The OS most used on Chinese made devices is Google Android, on smartphones and tablets, and Microsoft Windows, on computers (SHIDONG, 2019).

#### **2.4.7 “Data Is the New Oil” (THE ECONOMIST, 2017)**

Finally, but no less important, is the fact that in the creative economy of the post-industrial era, software becomes an increasingly relevant part of the scientific-technological, economic and military expressions of national power.

Alphabet (Google's parent company), Amazon, Apple, Facebook and Microsoft—look unstoppable. They are the five most valuable listed firms in the world. Their profits are surging: they collectively racked up over \$25bn in net profit in the first quarter of 2017. Amazon captures half of all dollars spent online in America. Google and Facebook accounted for almost all the revenue growth in digital advertising in America last year. (THE ECONOMIST, 2017)

Besides the aforementioned companies, others such as Uber and AirBnB, without having automobiles or apartments, raise money from software that allow them to act as brokers between owners and users, and make money from it. Other economic aspects of the software industry are debated in Chapter 9.

## **2.5 Conclusion**

There are various reasons why an aspiring cyber-power should focus on software power instead of on hardware power. Albeit, it is quite improbable that a country that plans to develop advanced cyber-capabilities might be able to do so at all layers of software, at least in the short term. For example, the firmware of many hardware devices may be inaccessible and the kernels of many commercial operating systems and middleware, software used as a foundation for building information systems, such as database managers, data and application servers. This can undoubtedly limit the possibility of achieving full control and auto sufficiency of the internal cyberspace or even software market. But there are alternatives, as the adoption of open-source software, which allow to shorten the process of assimilation of knowledge and to reduce

the risks of using 'black-box software' (as undocumented backdoors). Achieving advanced knowledge at least at the superior levels of the software used ensures a much smaller scale of cyber risk and a much smaller 'contact surface', at a much faster pace and lower cost than trying to compete at the hardware level.



### 3 “NON-AGGRESSIVE” NATIONS

This chapter examines the influence of ‘culture’, traditions and ‘institutions’ shaping the ‘character’, ‘personality’, ‘reputation’ or ‘face’ of countries and influencing their ‘perceptions’. It then draws on the concept of “non-aggressive nations”, as those that avoid using military power to defend their interests.

#### 3.1 Introduction

“Both men and societies are defined by their styles, their way of doing things”, and this defines their culture (DAMATTA, 1984, p. 12, free translation). This culture or tradition develops based on history and is marked both by routine (the usual) and extraordinary experiences (DAMATTA, 1984, p. 57).

As observed Morgenthau (1948) that the culture (character) is steady, consolidated, and hard to change. Differently from the Arabic idea expressed in the word *maktub* (it was written), connected with the concept of destiny, culture is not a ‘given thing’, something immutable.

#### 3.2 The Relevance of Culture in Power Assessments

National culture has long been considered an essential element of national power. Liddell Hart observed that the Comte of Guibert’s book on military tactics, used by Napoleon Bonaparte during his early campaigns, already considered that “each nations system of war should be based on its essential characteristics **fitted to the national character**” (LIDDELL HART, 1939, p. 107, emphasis added). In this respect, the head of the Operations Section of the German Supreme Command, Lieutenant Colonel Wetzell, in 1918 (actually in 1917<sup>1</sup>), would have claimed that German military actions “ought to be guided by the character of their respective opponents”: “The French are better in the attack and more skilful in the defence, but are not such good stayers as the British” (LIDDELL HART, 1939, p. 108). Liddell Hart also identified that, when designing a strategy intended to dislocate the opponent, the strategist has to study the physical aspect of the enemy, as well as the psychological one, and combine both (LIDDELL HART, 1941).

In a similar vein, although in a much more straightforward way, Morgenthau appointed eight National Power elements. Five more quantitative (or physical, as called by Liddell Hart): Geography, Natural Resources, Industrial Capacity, Military Preparedness and Population. And

---

<sup>1</sup> The evaluation actually would have occurred in December 12, 1917, and not in 1918 (GRIFFITHS, 1986, p. 205).

three more qualitative (or psychological, as Liddell Hart named): National Character, National Morale and The Quality of Diplomacy (MORGENTHAU, 1948, p. 80–109).

National Character and National Morale are elusive “from the point of view of rational prognosis” and have a “permanent and often decisive influence upon the weight” on the perceived power of nations (MORGENTHAU, 1948, p. 96). The Character is the set of “certain qualities of intellect and character occur more frequently and are more highly valued in one nation than in another”, which “set one nation apart from others” and presents “a high degree of resiliency to change” (MORGENTHAU, 1948, p. 96).

National character cannot fail to influence national power; for those who act for the nation in peace and war, formulate, execute, and support its policies, elect and are elected, mould public opinion, produce and consume – they all bear to a greater or lesser degree the imprint of those intellectual and moral qualities which make up the national character (MORGENTHAU, 1948, p. 98).

As examples of these ‘traits’ that define National Character and are perceived externally, Morgenthau cites the Russians' tenacity, the individual initiative and inventiveness of the Americans, the common sense of the British, the discipline and thoroughness of the Germans and the individualism of the French. These “are some of the qualities which will manifest themselves, for better or for worse, in all the individual and collective activities in which the members of a nation can engage” (MORGENTHAU, 1948, p. 98; 101).

The second qualitative element is National Morale, “the degree of determination with which a nation supports the foreign policies of its government in peace or war”, that albeit strongly influenced by National Character is “more elusive and less stable, but no less important than all other factors in its bearing upon national power” (MORGENTHAU, 1948, p. 100–1).

It permeates all activities of a nation, its agricultural and industrial production as well as its military establishment and diplomatic service. In the form of public opinion it provides an intangible factor without whose support no government, democratic or autocratic, is able to pursue its policies with full effectiveness, if it is able to pursue them at all (MORGENTHAU, 1948, p. 101).

In the quest for quantitative measurement of national power, Cline (1977) presented a formula based again on two sets of elements: one more concrete and the other more subjective. For the concrete elements, it was considered:

- 1) Critical Mass (C): comprehended the Territorial Area and the Population Size.
- 2) Economic Capacity (E): comprehended the Gross National Product (GNP), Energy Sources (oil, coal and nuclear energy), Critical Non-combustible Ore sources (iron ore, copper, chromite, bauxite and uranium), Industrial Production (steel and

aluminium), Food Production (wheat, corn and rice), and the Foreign Trade chain (sum of imports and exports).

- 3) Military Capacity (M): considered Conventional Military Capacity (conventional forces of land, sea and air) and Strategic Weapons (nuclear); bonuses were attributed on Strategic Reach due to geographic position and Military Effort for significant expenses that favoured military action.

Subjective factors were indicators constructed from psychosocial components:

- 1) National Will (W): assessed based on the National Integration Level (subdivided into Cultural Integration Level and Territorial Integration Level), National Leadership Strength (composed of Government Policy Capacity and Social Discipline Level) and on the Relevance of the Strategy for the National Interest.
- 2) National Strategy (S): would indicate how much each nation develops a truly global and integrated strategic concept in the conduct of its international affairs.

All considered, the final Cline's (1977) formula of Perceptible Power (Pp) was:

$$Pp = (C + E + M) \times (W + S)$$

It should be noted that the subjective components (W and S) were valued between 0 and 1, so that their sum could vary between 0 and 2. Thus, the result of the intangible component, being multiplied by that of the concrete element, can reduce or amplify the effect of this. In other words, the availability of resources does not, in itself, generate perceptible power, being dependent on cultural and moral factors.

Analysing Cline's formula, Meira Mattos noted the absence of another relevant 'subjective' element: "In our view, however, the second term lacks a factor [...] which today weighs substantially on the realization success of any enterprise - the power to persuade" (1977, p. 131, free translation). In his assessment, the U.S. had no problems with a lack of strategy (S) or will (W) in the Vietnam War. Their main concern would have been the lack of capacity to convince its internal public and its traditional allies of justice in its cause (MEIRA MATTOS, 1977, p. 132). Thus, Meira Mattos proposed the formula be changed to include 'persuasive power' (P) as follows:

$$Pp = (C + E + M) \times (W + S + P)$$

Regardless of the criticisms which might be made to the adequacy of the different proposed elements that constitute national power, the fact is that subjective factors related to the culture of a nation, often institutionalized in its society, will always have to be taken into

account in any power assessment or attempt to construe it (statecraft) as national strategies often sought to do.

Cultural and societal factors, political institutions, and pressure from the international arena all shape how a state uses its resources. They constitute the environment in which a state's military activities take place: for example, they influence how patterns and routines emerge and evolve for strategic and operational planning, selection of leaders, procurement of weapons, training of soldiers, and creation of doctrine. By influencing these activities, a state's society and its international environment affect how well it uses its material and human resources in the process of organizing and preparing for war and therefore its ability to create military power. (BROOKS, 2007, p. 1)

Albeit the realist grasp on International Relations, in particular Kenneth Waltz's seminal *Theory of International Politics* has provided a firm base for the field of national security studies, Waltz made it "very clear that the internal characteristics of states were irrelevant to his theory" (KATZENSTEIN, 1996, p. 3).

It is especially surprising that realists, with their natural focus on states, have not inquired more systematically into the effects of changes in state identity, for example from warfare state to welfare state in Western Europe, that have altered traditional conceptions and instruments of national security (KATZENSTEIN, 1996, p. 3).

By the end of the XIX century, warfare was still considered a "virtuous exercise of state power"; a century later, "changing international norms and domestic factors have 'tamed' the aggressive impulses of many states" (JEPPERSON e colab., 1996, p. 9). The realist view, with its rationalist and materialist perspective, considers only the "rational-state-as-actor model", and the implicit "bureaucratic routinization" of decision making, not considering the "cultural content of the environment", an element often questioned by critics of deterrence theory (JEPPERSON e colab., 1996, p. 15–6).

However, rationality might be impaired by cognitive and motivational biases "rooted not only in the information-processing proclivities of individuals but also in the operational codes, understandings, and worldviews shared by decision-makers and diffused throughout society" (JEPPERSON e colab., 1996, p. 16). In this view, the institutionalization of ideas, in research institutes, schools of thought, laws and government bureaucracies, is a crucial determinant of policy (JEPPERSON e colab., 1996, p. 16).

"Norms are collective expectations about proper behavior for a given identity" (JEPPERSON e colab., 1996, p. 18). They can create ("constitute") identities, generating expectations about the proper portfolio of identities for a given context, as well as "prescribe or



proscribe” (“regulate”) behaviours within shared identities; thus, “norms establish expectations about who the actors will be in a particular environment and about how these particular actors will behave” (JEPPERSON e colab., 1996, p. 19).

“Culture” “refers both to a set of evaluative standards, such as norms or values, and to cognitive standards, such as rules or models defining what entities and actors exist in a system and how they operate and interrelate” (JEPPERSON e colab., 1996, p. 20). Culture is a socially construed object, and can even achieve the level of “a ‘taken for granted’ image of social reality” (EYRE; SUCHMAN, 1996, p. 80).

Analysing the patterns of non-use of chemical and nuclear weapons, Price and Tannenwald (1996) observed that the use of these weapons, for different reasons, became a taboo. The taboo on chemical weapons, derived from the horrors of its use in WWI, originated mostly at the systemic level; the one on nuclear weapons emerged “principally (although not entirely) in the United States and was then diffused transnationally” (PRICE; TANNENWALD, 1996, p. 100). These weapons have not been used even when they were militarily justifiable and when the risk of retaliation or sanctions was practically non-existent.

To cite but one example, the U.S. did not employ gas warfare against the Japanese, even though there was no threat of retaliation and cw [chemical warfare] would have been enormously effective against Japanese forces entrenched in the tunnels and caves of the Pacific Islands (PRICE; TANNENWALD, 1996, p. 101).

On nuclear weapons, they observe that:

Likewise, a deterrence explanation cannot account for why nuclear weapons were not used by the United States during the first ten years of the nuclear era, when the U.S. possessed a virtual monopoly on nuclear weapons and fear of retaliation was not a dominant concern. In the late 1940s and early 1950s, the United States faced crises in Berlin, Korea, Quemoy and Matsu, and Dien Bien Phu. Yet, despite a perceived weakness in U.S. conventional military capabilities and a military strategy that relied increasingly upon nuclear weapons, U.S. leaders did not use nuclear weapons during these crises. (PRICE; TANNENWALD, 1996, p. 101)

At the beginning of the Eisenhower Administration, in 1953, with Dulles as Secretary of State, tactical nuclear weapons were qualitatively much better than the ‘strategic’ ones used against Japan in 1945, and when the USSR was not able to retaliate ‘in-kind’. Eisenhower and Dulles “actively sought to make these weapons ‘usable’, i.e., to make them like any other weapon” in the U.S. arsenal. But they faced “the normative stigma against nuclear weapons that was already beginning to emerge”, and realised they “were more preoccupied by the constraint

on nuclear use imposed by negative public opinion than by any more material concern” (PRICE; TANNENWALD, 1996, p. 112).

Domestic institutions are powerful determinants of military effectiveness among modern nation-states. The rules within which political contenders compete for leadership and delegate tasks to military organizations affect the strategies that politicians employ to affect military behavior and also, over time, the professional strength of military organizations and their preferences as embodied in organizational culture or bias. (AVANT, 2007, p. 80)

In other words, as the military is a segment of the society they are immersed in, military culture is influenced by national culture. And “what the military perceives to be in its interest is a function of its culture. In short, by accounting for policy makers’ cultural environment, we can better explain choices between offensive and defensive military doctrines” (KIER, 1996, p. 155).

As the political vision in the 1920s Paris establishment was that a long war of attrition with Germany “could only result in the eventual triumph of Germany’s superior economic strength and industrial mobilization”, the French military adopted an offensive posture: they had to strike decisively, winning a short war; the French weakness in the face of its most probable enemy required an offensive posture (KIER, 1996, p. 157). A decade later, the establishment identified that Germany was too strong to be beaten quickly. Hence, “France’s only hope, it was then argued, was that the initial resistance to a German offensive would provide the necessary time for the injection of allied assistance. France could only win a long war”, what required a defensive posture (KIER, 1996, p. 157).

In other words, France’s relative weakness led to support for an offensive orientation in the 1920s and a defensive doctrine in the 1930s. French policy makers were not misguided, nor did they misunderstand France’s strategic position. Either an offensive or a defensive posture is a sensible response to the systemic demands of a relatively weak state. (KIER, 1996, p. 157)

Since the military is often fundamental in the statecraft process, policymakers have an informed view of military policy, and “the creation or stabilization of every state requires that a bargain be struck over the control of the military” (KIER, 1996, p. 163). This internal bargain, more than the international system configuration, is institutionalised, thus, reflecting the military perceived interests, in a form that “cannot be disentangled from their country’s experience with the armed services and the role that it played in securing a particular distribution of power within the state” (KIER, 1996, p. 163–4).

After the end of WWII, Germany and Japan have deemphasized military power to pursue their national objectives, despite the increase of their relative strength, and even the significant changes in their regional (or even the global) security environments (BERGER, 1996, p. 261). Both countries have refused to assume a more assertive role in international security, a behaviour that cannot be explained with neorealist and neoliberalist views, which consider states as driven “by the rational responses of state actors to pressures emanating from their international environments” (BERGER, 1996, p. 261).

The history of Germany and Japan’s creation and consolidation as unified States show that the military played a crucial part, elevating their status as military powers to a central role in their national identities and self-understandings (BERGER, 1996, p. 268). When the military promised increased power to their empires, their nations agreed and engaged in the efforts. However, they have not been able to fulfil their promises, and the disastrous defeat, followed by a vexing occupation, made them lose their credibility and status, creating a strong anti-military sentiment, institutionalised in their political systems, that still reflect in their national identities (BERGER, 1996, p. 261–2).

War is generally unpopular in liberal democracies, but in no other country it is so despised, and there is such an intense antimilitarist sense, as in Japan and Germany (BERGER, 1996, p. 264).

National culture influences how a given society sees its national security, military institutions, and even the use of force to pursue its objectives (BERGER, 1996, p. 265). Thus, it shall be expected that members of different national cultures, if put in the same situation, might behave differently, since their cultural backgrounds are institutionalised with different values and norms regarding the military and the use of force (BERGER, 1996, p. 266).

The behaviour of a nation can significantly influence other countries' behaviour, having an impact at the system-level in the long run. The isolationist attitude of the U.S. and its resistance in entering WWII might have signalled to Germany and Japan “a window of opportunity in which the Axis powers could have achieved military victory” (BERGER, 1996, p. 267).

### **3.3 The Institutionalisation of Culture**

“Historical institutionalism” states that “institutions” “are the rules of the game in a society or, more formally, are the humanly devised constraints that shape human interaction” and that “institutional change shapes the way societies evolve through time and hence is the key to understanding historical change” (NORTH, 1990, p. 3).

Furthermore, institutions can be either formal, as acts and laws, or informal, as conventions and codes of behaviour, and can be created, as a new law, or evolve over time, as the common-law. And they can be written, such as rules and statutes, or unwritten, as the codes of conduct that often underlie and supplement them (NORTH, 1990, p. 4).

Institutions are distinct from organisations, although both have the intent of providing a framework for human interaction. Organisations are formal structures, and the way they are structured and evolve is strongly influenced by the institutional framework. And whilst formal rules can be changed quickly, “informal constraints embodied in customs, traditions, and codes of conduct are much more impervious to deliberate policies” (NORTH, 1990, p. 4; 6).

Throughout history, institutions have been devised to reduce uncertainty in exchange, creating order and offering a stable, although not necessarily efficient, structure for human interaction (NORTH, 1990, p. 6, 1991, p. 97).

Thus, the culture and traditions of a society gradually amalgamate in its institutional framework, written or not. And this institutional framework of a society reverberates in the way that community is perceived. They consolidate the expectation other States have about that country’s reputation for action, its ‘face’ (SCHELLING, 1980, p. 194).

### **3.4 Aggressive (and Non-Aggressive)**

For this work, the concept of non-aggressive nations is here developed as follows:

Non-aggressive nations are those that did not engage in aggressions between states since the end of World War II, except in peacekeeping or peacebuilding actions sanctioned by the United Nations (U.N.) or other multilateral organisations where all those engaged or affected are member states.

The concept of Aggression between states is that of the U.N.: the invasion or attack, any military occupation, however temporary, any annexation, bombing or blocking of ports, or the sending of bands, groups, irregulars or armed mercenaries, by or in the name of a state against another state (UN GENERAL ASSEMBLY, 1974).

Moreover, two relevant facts justify the temporal cut as starting after WWII: (1) it shaped the contemporary international system and the U.N. itself; (2) the origin of the first computers (and thus cyberspace) is linked to WWII (indeed, for military applications).

Finally, the last part of the concept is relevant for considering legitimate peacekeeping and peacebuilding operations. It is not plausible that a country can be subject to these operations if it is not a member of the organization that implements them. Thus, operations sanctioned by the North Atlantic Treaty Organisation (NATO) against (or in) non-member nations, as in the cases of Kosovo (against Serbia) and the Second Gulf War (against Iraq), are considered

aggressive, since they were not sanctioned by the U.N., an organisation which encompasses all involved nations, and Kosovo (or Serbia), in the first case, and Iraq, in the second, were not represented in the forum that ‘sanctioned’ those operations. Conversely, the intervention in Afghanistan (2002) was valid, since authorised by the U.N., which represented all the involved parties. Similarly, the Dominican Republic intervention (1960), determined by the Organisation of the American States, which also represented all involved nations, was valid as well.

It is worth to test the concept with a significant sample of nation-states. The G-20 is formed by the 19 countries with the world’s largest economies, plus the European Union: Argentina, Australia, Brazil, Canada, China, France, Germany, India, Indonesia, Italy, Japan, Mexico, Russia, Saudi Arabia, South Africa, South Korea, Turkey, United Kingdom, United States and the European Union. Using this sample of 19 countries and applying the ‘non-aggressive filter’ defined, only Brazil, Germany, Japan and Mexico would be regarded as non-aggressive.

Looking for their commonalities, all of them are relevant regional powers, none are in the same region (thus not competing directly), and all four are traditional Western (the U.S. and Western Europe) allies. Yet, all four have been victims of Five-Eyes espionage denounced by Edward Snowden (GREENWALD, 2014).

Furthermore, this characterisation as non-aggressive nations (and, by exclusion, the aggressive ones) reflects their strategic stance: their tradition, ‘face’ or Historical Institutionalism.

### **3.5 The “Brazilian-Way” (or *O Jeitinho Brasileiro*)**

As stated, culture is not a ‘given thing’. Albeit, in Brazil, not even the Military Regime (1964-1985) made significant changes in Brazilians’ behaviour in the long term. Despite the massive marketing campaigns based on catchy jingles like *Este é um país que vai prá frente* (“This is a country that goes ahead”) and *Povo desenvolvido é povo limpo* (“Developed people are clean people”), and the mandatory national flag-raising ceremonies, chanting the National Anthem and the Independence Anthem, and the also mandatory *Civic and Moral Education* classes.

It does not mean, however, that Brazilians do not care their symbols. The first part of the Brazilian National Anthem is quite longer than the 20 seconds reserved for national anthems at the beginning of international volleyball matches. And it is internationally known (and respected) that the National Team, when playing in Brazil, will have the public chanting it entirely, “a Capella” after the 20 seconds of music end. And volleyball is the second most

popular sport in the country. In a football match, however, it is almost impossible to hope for the majority of the public to stand still. Thus, it is a volleyball fans 'institution'.

Furthermore, a Gallup International poll conducted in 2015 showed that 48% of Brazilians said they would fight for their country. A small number compared to the Chinese (71%), Israeli (66%) or Russians (59%). Even so, significantly larger (9% in comparison) than North-Americans (44%), and much larger than Australians and French (29%), British (27%), Italians (20%), Germans (18%) and Dutch (15%) (GALLUP INTERNATIONAL, 2015, p. 284). Thus, if needed, Brazilians would fight in significant numbers. Albeit prefer not to go to war. It is not in the Brazilian culture, as will be shown.

Historically, Brazil does things differently. Often in a softer and more 'conversational' (less-confrontational) way. And slower. As a colony, it was the only in the Americas to host the capital of the empire it belonged to. Fleeing from Bonaparte, the Portuguese court settled in Brazil in 1808. Even with the French defeat in 1815, the King only returned to Portugal in 1821 (GOMES, 2007).

It was one of the latest countries in South America to become independent, in 1822. And the only one to do so by the hands of the crown prince of the metropolis. Independent, it was the only one to establish a monarchy. Not a monarchy: the Empire of Brazil (GOMES, 2010). Acclaimed Emperor, the former Prince Regent would abdicate the Brazilian crown nine years later (in favour of his five-year-old son) to be crowned King of Portugal.

The Brazilian War of Independence took between 2,000 and 3,000 lives among the country's 4.8 million inhabitants. A minimal number, compared to roughly 25,000 dead in the USA Independence, among the 2.5 million inhabitants they had (BRASIL-IBGE, 2000; GOMES, 2010, p. 163–4; US CENSUS BUREAU, 2016). The switch from Empire to Republic, in 1889, conducted by a cavalry Field Marshal close to the Emperor, had no further contestation (GOMES, 2013). Most of the more than 30 internal revolts involved a few hundred insurgents engaged in combat, with less than a handful exceeding 3,000 and only one surpassing 10,000.

Its Military Regime (1964-1985) was 'softer' than those of other countries in the region. Congress (and opposition) operated for almost the entire period. Presidents changed regularly and periodically. The number of dead and missing was considerably smaller than in neighbour countries. And much lower as a percentage of respective populations.

Brazilian diplomacy often presents Brazil as a 'peaceful country' (AMORIM, 2012; GIRALDI, 2012). It is a tradition of which the country is proud of, that concerns external armed conflicts. Since its independence, Brazil wielded weapons only three times in interstate wars. The first, Platine War (August 1851-February 1852), was in response to the Argentine invasion

of southern Brazil. The second was the War of the Triple Alliance (1864-1870), when Paraguay invaded portions of Brazil and Argentina, making these and their ally Uruguay to retaliate. Without a large professional army, it took two years before Brazil could assume the offensive (DORATIOTO, 2002).

WWII was the third. As in the previous case, Brazil entered into the conflict in a very 'Brazilian-Way'. In 1941, before both countries joined the war, Brazil granted the USA the use of an area near Natal (Brazil), Americas' nearest point to Africa. There, Parnamirim Airbase was built, becoming a central element for sending aircraft lend-leased by the British and to the allied offensive in North-Africa. In return, Brazil received financing and technology for its first steel plant. In February 1942, with the USA already at war, German and Italian submarines began sinking Brazilian merchant ships. After 21 sunk ships, in August, Brazil declared war on them. Militarily unprepared, it postponed its entry into active combat. In January 1943, returning from Casablanca, in Natal, Roosevelt promised support for preparing a Brazilian contingent of 100,000 men to be sent to Europe. In July 1944, almost two years after the declaration of war, Brazil sent a single division to Italy. Just over 25,000 men, whose weapons and doctrine were provided by the Americans. Less than nine months later, the war in Europe would end. Parnamirim airbase returned to Brazil in 1946 (BARONE, 2013; RUIZ, 2019; THE NEW YORK TIMES, 1946).

Subsequently, the country engaged in dozens of peacekeeping missions, always under the auspices of the United Nations, as in Suez, Congo, Haiti, and Lebanon or of the Organisation of American States, as in the Dominican Republic, to name just a few (BRASIL-MD, [S.d.]).

This non-aggressive stance in the context of international conflicts is found in the Federal Constitution, already in its Preamble, and also in the Fundamental Principles, Article 4, Item VII (BRASIL-CN, 1988). It was also repeatedly expressed in the National Defence Policy and the National Defence Strategy until 2016, always in the form of a preference for the peaceful resolution of disputes (BRASIL-MD, 2016, p. 6;11;16-17;23-24).

Since the beginning of my Doctorate studies at ECEME, I have consistently criticized the insistence on repeating this "mantra" in official documents. As will be seen, this posture is a very relevant limitation for the implementation of deterrence by fear (or threat of retaliation or punishment), since it has as structural elements the capacity (means) and credibility (tradition or willingness to use these means) to retaliate and instil fear. Coincidence or not, in this year's proposed update of the National Defence Policy and the National Defence Strategy, this Brazilian preference has been reduced to two single manifestations.

### 3.6 Conclusion

For different reasons, Brazil, Germany, and Japan (as well as Mexico) have institutionalised severe restrictions on the use of military force, even in the pursuit of their national interests. In the cases of Japan and Germany, although the military had been influential in their consolidation as modern nations, the fiasco caused by the defeat in WWII made them be considered hazardous to their countries. In the Mexican case, due to the loss in the Mexican-American war, the country lost half of its territory after Mexico City felt hostage of the U.S. Army. In Brazil, due to a long history of military involvement in internal affairs, resulting in a historical unpreparedness of the military for external confrontations, and ultimately with the political consequences of the Military Regime that ruled the country between 1964 and 1985, creating a historical diffidence on the military which makes it hard to obtain the resources needed to keep pace with the modern military technology available to those nations with a more 'aggressive' culture, amplifying the existing gap.

As a result, these nations tend to define their 'grand strategies' without considering military force as a coercive power, opting for emphasising different elements of national power. This 'anti-military-force-usage' is already crystallised in their institutions, and any change is destined to occur only in the long-run, forcing them to adopt strategic postures that reflect this situation.



## 4 'DETERRENCE THEORY' FALLS SHORT

This chapter analyses the evolution and concepts related to 'Deterrence Theory' and the broader 'Influence Theory', arguing that they do not appropriately accommodate the vast body of knowledge developed for describing interstate causal influence. A descriptive methodology is used for analysing the involved concepts and their relationship within the core of those theories (GERRING, 2012). It is shown that 'Deterrence Theory', its superset 'Coercion Theory' and even the broader 'Influence Theory' are inappropriate for different reasons. A better concept would be 'Causation Theory'.

### 4.1 Introduction - The Hatcher of 'Deterrence Theory'

Deterrence Theory was born in a specific context, with limited scope and objectives. However, many of its basic concepts are still relevant today and can integrate more extensive views and theories, if considered under the right perspectives. For better understanding the theory and its concepts, it is better to acknowledge where it was born, and the problems it intended to solve.

In August 1945, WWII had already finished in Europe (May), and the U.N. had been founded at the San Francisco Conference (June). Victory over an exhausted, but still obstinate, Japan was granted, albeit it should yet cost thousands of lives to the allies. This was the justification the U.S. used for detonating two atomic bombs over the industrial cities of Hiroshima and Nagasaki. It is mostly accepted that these bombings were militarily not significant; their target was political. "The bomb that hit Hiroshima was a threat aimed at all Japan. The political target of the bomb was not the dead of Hiroshima or the factories they worked in, but the survivors in Tokyo" (SCHELLING, 2008, p. 17). It is also believed that the political message had one other intended audience: their anti-Hitler allies, the Soviet Union (USSR or S.U.) (HOBSBAWM, 1995, p. 27). The Soviets knew they would have to coexist with a long hegemony of the U.S., which wealth and power increased enormously during WWII and were prominent, with its economy totalling more than the rest of the world combined (HOBSBAWM, 1995, p. 232). Hence, the USSR, afraid of being targeted by the North-Americans, adopted a posture much more defensive than offensive at that time. Indeed, the U.S. had 12 available nuclear devices, and the S.U. had none. Moreover, although the Soviets did not know at that time, despite not disposing of long-range bombers to launch those artifacts inside the Soviet Union until December 1947, the U.S. Joint Chiefs of Staff made plans for atom-bombing the 20 largest Soviet cities (HOBSBAWM, 1995, p. 234-5).

In August 1949, just four years after the U.S. show-off of nuclear weapons, and quite earlier than North-American strategists expected, the USSR exploded its first fission (atom) bomb (HOBSBAWM, 1995, p. 229). In 1952, the British, trying to reduce their dependence on U.S. protection, tested their first atomic device (HOBSBAWM, 1995, p. 235). Then, in 1954, nine months after the U.S., the S.U. detonated its first fusion (Hydrogen) bomb (HOBSBAWM, 1995, p. 229). Having the artefacts was only half of the threat, however, and the U.S. could still count on the lack of Soviet vectors to deliver those artefacts on American soil. Nevertheless, in June 1955, in the Aviation Day parade in Moscow, the S.U. “ostensibly demonstrated the capability of delivering repeated inter-continental attacks against American industrial and population centers” (ZAGARE; KILGOUR, 2004, p. 180).

In 1960, it was the French turn, and in 1964, that of the People’s Republic of China (PRC), detonate their first nuclear artefacts; both countries handled their capabilities as strategic assets, independent from both the U.S. and the S.U. international policies (HOBSBAWM, 1995, p. 236). It was in this context that the core of ‘Deterrence Theory’ was developed.

Being “largely a by-product of the Cold War era”, not surprisingly classical deterrence theory “has been inordinately influenced by the hostile relationship of the United States and the Soviet Union and by the haunting specter of nuclear weapons” (ZAGARE; KILGOUR, 2004, p. xix).

## 4.2 On ‘Deterrence Theory’

‘Deterrence Theory’ has a well-developed body of knowledge, consolidated for decades, “one that has advanced the field of national security by illuminating the logic that underlies threats, violence, and war” (BIDDLE, 2020, p. 95). Its spinal cord was, as the name indicates, connected with the meaning of the verb ‘deter’: “Discourage (someone) from doing something by instilling doubt or fear of the consequences” (OXFORD DICTIONARY, [S.d.]).

Its context was that of avoiding possible USSR territorial expansion, threatening to respond it with nuclear bombardment. Back in November 1954, when only the U.S., the S.U., and the UK had atomic devices at hand, Kaufmann wrote an influential piece where he presented the flaws of what was then called “doctrine of massive retaliation” and established many of the concepts of what would be “a policy of deterrence” (KAUFMANN, 1954, p. 1). While the doctrine of massive retaliation was entirely reactive, ‘deterrence’, he argued, could help “preventing certain types of contingencies from arising”.

Deterrence would be a type of “bargain” between the two involved parts: “deterrence policy thus constitutes a special kind of forecast: a forecast about the costs and risks that will

be run by the party to be deterred, if certain actions are taken, and about the advantages that he will gain if those actions are avoided” (KAUFMANN, 1954, p. 4). “It is possible to deter an antagonist from taking inimical action by the offer of a better prospect than the one he presently enjoys” (KAUFMANN, 1954, p. 14).

Kaufmann also established the foundations of many structural aspects of deterrence (explained ahead), as the need to know the enemy for designing tailored threats, and the need for credibility and will (what he called ‘intent’) to fulfil the threats made.

Kaufmann, moreover, argued that a deterrence policy would require the reduction of the dependence on strategic (nuclear) forces: conventional military defences would add significant deterrent value, as well as other measures.

Similarly, the support of allied forces, military institutions, and economies can hardly be relaxed. Offshore purchases, a continuing supply of military end items, economic assistance to ease the burden of large military establishments, the liberalisation of trade if only to prevent the allied nations from becoming attached to the markets of the Soviet bloc - all this and much more will have to be continued. It would seem desirable, too, for American troops to remain in areas of the world like Korea even if those areas are not ones that we would attempt to hold in the event of a general war. (KAUFMANN, 1954, p. 15)

Indeed, in 1959, Snyder proposed the concept of “deterrence by denial” as a complement to the original idea of “deterrence by [threat of] punishment” (SNYDER, 1959). In simple terms, he proposed that war was a decision based in the calculus of gains, costs and probabilities (risk) and that the alternatives presented in each case would lead to a different calculus. In certain instances, the likelihood of a massive retaliation (punishment) due to an attack of a particular target could be low, raising the possibilities of a significant gain for the attacker. However, in case there were conventional defences in the area, they would ‘deny’ gains to the attacker, and the probability of their engagement was relatively high. The engagement would also raise the likelihood of an escalation of the conflict, thus increasing the perspectives of massive retaliation. And this would constitute a deterrent value (hence the name of “deterrence by denial”). This consideration, indeed, provided the substance for the ‘doubt’ part of the meaning of the verb ‘deter’.

Singer (1963) proposed a model for what he called inter-nations ‘influence’. He defined “power” “as the capacity to influence” actions of other nations (SINGER, 1963, p. 420). Influence, for him, would be exerted in two ways. “Dissuasion” was the “negative” one, since inducing the target ‘not to act’. “Persuasion” was the “positive” one, since causing the target ‘to act’. Both could be achieved by “threat” and “punishment” or by “promise” and “reward”.

In 1966, Schelling systematised what came to be known as ‘Deterrence Theory’ (SCHELLING, 2008). He rearranged the many concepts presented by Kaufmann, Snyder and others, focusing on the use of force, “the power to hurt”, or “coercion”, and its use for influencing other nations. Thus, he dismissed the terms ‘persuasion’ and ‘dissuasion’ proposed by Singer, since these were not necessarily connected with the use of force. Since military power is not necessarily the best way of avoiding a conflict nowadays, we will return to ‘Influence Theory’ later.

#### **4.2.1 The Structural Elements of ‘Deterrence Theory’**

Terminological precision and semantics uniformity are relevant to avoid ambiguity and misunderstandings regarding any theory. And semantics frequently depends on the specific context of the application of a theory. Schelling devoted a lot of effort to both context and semantics when systematising the body of knowledge on ‘coercion’.

The apparent lack of understanding of at least some of these concepts may explain the incorrect use of terms like deterrence, coercion, compellence and even threats. Moreover, as it is not possible to understand Relativity or Quantum Mechanics without understanding Classical Mechanics, before going ahead, it is necessary to understand the fundamental concepts of ‘Coercion Theory’ and its subset ‘Deterrence Theory’.

##### **4.2.1.1 Coercion**

The first fundamental concept is that of “coercion”: “the potential or actual application of force to influence the action of a voluntary agent” (FREEDMAN, 1998). The need for force differentiates coercion from “consent”, where it is unnecessary, and from “control”, where its application is such that no option is available to the opponent. The idea of a “voluntary agent” relates to its ability to make “critical choices throughout the course of a conflict” (FREEDMAN, 2004, p. 26).

Thus, for coercion to be possible, the target, the ‘voluntary agent’, has to be a rational actor. For our purposes, a rational actor is one who, when confronted with alternatives resulting in different outcomes, choose the one yielding the “more preferred” one (ZAGARE; KILGOUR, 2004, p. 39).

On context (or scope) of coercion, Schelling left clear his focus on the use of military force, the “power to hurt”. For ‘coercion theory’, the “power to hurt” or “cause harm”, is quintessential. “The power to hurt – the sheer unacquisitive, unproductive power to destroy things that somebody treasures, to inflict pain and grief – is a kind of bargaining power, not easy to use but used often” (SCHELLING, 2008, p. xxi). “The power to hurt is bargaining

power. To exploit it is diplomacy – vicious diplomacy, but diplomacy” (SCHELLING, 2008, p. 2).

The power to hurt something valued by the opponent, causing suffering, and its value as an element of bargaining is the core of deterrence theory. But there is a notable difference between the power to hurt, the threat of pain, and brute force. While the first can be used to influence, the latter “tries to overcome his [the opponent’s] strength” (SCHELLING, 2008, p. 3). And hurting, unlike brute force, concerns the interests of others. “It is measured in the suffering it can cause and the victims’ motivation to avoid it” (SCHELLING, 2008, p. 2).

The power to hurt (coercive violence), starts after the ‘surrender’ of opponent forces. And surrender comes after (not before) the ‘military victory’ or when opposing forces are too weak, or unwilling to engage (SCHELLING, 2008, p. 14). If there is no hurting after the ‘surrender’, it is due to a bargain, with concessions made by the defeated for averting the prospect of harm (SCHELLING, 2008, p. 30).

To be effective, hurting must threaten something treasured by the opponent, and thus it is necessary to know what each opponent values. These are what will be taken as ‘hostages’. If the opponent is persuaded that these hostages are under real threat, he might be open for bargaining. Instead, “[t]he prospect of certain death may stun him, but it gives him no choice” (SCHELLING, 2008, p. 3–4). Hostages, for Schelling, “represent the power to hurt in its purest form” (SCHELLING, 2008, p. 6).

It is the power to hurt, not military strength in the traditional sense, that inheres in our most impressive military capabilities at the present time. We have a Department of Defense, but emphasise retaliation – “to return evil for evil” (synonyms: requital, reprisal, revenge, vengeance, retribution). And is pain and violence, not force in the traditional sense, that inheres also in some of the least impressive military capabilities of the present time. (SCHELLING, 2008, p. 7)

Military professionals, in general, are not familiar with ‘Coercion Theory’; when they know it, they are often uncomfortable with the term ‘coercion’, with the idea of using violence as bargaining power, or with that of bargaining with enemies (BIDDLE, 2020, p. 95). However, this bargaining power is a central issue for coercion (both deterrence and compellence), ultimately establishing its dependence on the cooperation of the threatened party (BIDDLE, 2020, p. 98).

Coercion can be divided into two kinds of actions: one intended “to make an adversary *do* something (or cease doing something)”, a call to action, named “compellence”, and one meant “to keep him from starting something”, a call to inaction, named “deterrence”

(SCHELLING, 1980, p. 195). Schelling established that both depend on threats of (or actual) use of force to be implemented.

The basis of coercion consists in convincing the target state that resistance brings suffering while conceding does not; “if it suffers either way, or if it has already suffered all it can, then it will not concede and coercion will fail” (BIDDLE, 2020, p. 103). Moreover, for coercion to be feasible, the interests of the deterrer and the deterred (or target) must not be completely opposed. “Coercion requires finding a bargain, arranging for him to be better off doing what we want – worse off not doing what we want – when he takes the threatened penalty into account” (SCHELLING, 2008, p. 4).

Without the threat of hurting something valued by the coerced, it is not possible to talk about deterrence or compellence.

#### 4.2.1.2 Deterrence

‘Deterrence’ came as the first part of coercion, defined as the use of threats to avoid an action that an opponent would instead do. Using Singer’s (1963) notation, it was the ‘negative’ aspect of coercion, since intending to ‘avert’ a possible undesired action.

When describing his search for a specific term for this negative side, Schelling wrote:

I had to coin a term. “Deterrence” was well understood. To “deter” was, as one dictionary said, to “prevent or discourage from acting by means of fear, doubt, or the like,” and in the words of another, “to turn aside or discourage through fear; hence, to prevent from acting by fear of consequences,” from the Latin to “frighten from”. Deterrence was in popular usage not just in military strategy but also in criminal law. It was complimentary to “containment,” the basis of our American policy toward the Soviet bloc. (SCHELLING, 2008, p. xviii)

This specific focus on containment hints on why the name ‘Deterrence Theory’ gained traction, instead of ‘Coercion Theory’.

Deterrence is about estimating enemies’ intentions *and* influencing them (SCHELLING, 2008, p. 35). Moreover, deterrence aims Dissuasion *ex-ante*, not revenge *ex-post* (SCHELLING, 1980, p. 187). Consequently, it involves “setting the stage”, by communicating (signalling) the threat and demonstrating will and capabilities, then waiting, usually indefinitely. Action (or, more accurately, inaction) depends on the opponent. “The stage-setting can be often nonintrusive, nonhostile, nonprovocative. The act that is intrusive, hostile or provocative is usually the one to be deterred; the deterrent threat only changes the consequences *if* the act in question – the one to be deterred – is taken.” (SCHELLING, 2008, p. 71–2)

“Deterrence, in one sense, is simply the negative aspect of political power; it is the power to dissuade as opposed to the power to coerce or compel” (SNYDER, 1961, p. 9). Alternatively, it can be said that “deterrence is the use of threats to protect the status quo” (LINDSAY; GARTZKE, 2019, p. 14).

#### 4.2.1.3 Compellence

For the positive side of coercion, that of using threats to ‘induce’ the opponent to do something he would instead not do, Schelling coined the noun “compellence”. The term relates to the meaning of the verb ‘to compel’: “Force or oblige (someone) to do something” or “Bring about (something) by the use of force or pressure” (OXFORD DICTIONARY, [S.d.]).

We have come to use “defense” as a euphemism for “military”, and have a Defense Department, a defense budget, a defense program, and a defense establishment; if we need the other word, though, the English language provides it easily. It is “offense”. We have no such obvious counterpart to “deterrence”. “Coercion” covers the meaning but unfortunately includes “deterrent” as well as “compellent” intentions. “Intimidation” is insufficiently focused on the particular behavior desired. “Compulsion” is all right but its adjective is “compulsive”, and that has come to carry quite a different meaning. “Compellence” is the best I can do. (SCHELLING, 2008, p. 71)

A compellence threat often requires that the punishment be administered until the target acts (SCHELLING, 2008, p. 70). Thus, compellence “involves *initiating* an action that can cease, or become harmless, only if the opponent responds”. Differently from the case of deterrence, the first step must be from the side that makes the compellent threat (SCHELLING, 2008, p. 72).

Compellence also has to be definite in time. “There has to be a deadline; otherwise tomorrow never comes. If the action carries no deadline, it is only a posture, or a ceremony with no consequences” (SCHELLING, 2008, p. 72).

Thus, the compellent threat, to be credible, has to be communicated (signalled) by the coercer, and perceived (and believed) by the coerced, and then the latter needs to have some time to act. If the time given is too short, compliance becomes unattainable; instead, if it is too long, compliance becomes unnecessary (BIDDLE, 2020, p. 99). Compellence, empirically, has been demonstrated to work only in circa one-third of the time (BIDDLE, 2020, p. 99). Opposingly to ‘deterrence’, “its offensive twin, compellence, is the use of threats to change (or restore) the status quo” (LINDSAY; GARTZKE, 2019, p. 14).

#### 4.2.1.4 Capabilities

Capabilities relate to the ‘means’ (or resources) aspect of coercion. In coercion by threat of punishment, making credible threats relies on making the opponent believe (or perceive) that the deterrer can implement them. The same applies to ‘deterrence by denial’ since an opponent will only be dissuaded if he believes that strong defending forces or resilience capabilities will deny his gains.

The primary element the attacker has to consider in deterrence by denial is the defender’s capabilities, while intent is more relevant in deterrence by punishment. In the first case, the attacker has to evaluate how much damage he is going to face; in the second, he can assume that damage is granted if the threat is fulfilled (SNYDER, 1961, p. 15). Thus, there is uncertainty in both cases, but the consequences of a miscalculation can be more severe in the second case than in the first.

It is relevant that Snyder also included considerations regarding ‘morale’ as an aspect of military capability.

While there are some aspects of military capability, such as morale, which can hardly be appraised with any reliability short of the ultimate test of battle, military capabilities in general are composed of rather concrete elements which an efficient intelligence system can assess with some confidence. (SNYDER, 1959, p. 5)

#### 4.2.1.5 Will

In his in-depth knowledge of Clausewitz’s work, Sir Michael Howard highlighted that two qualities of a strategist caught the Prussian’s attention. One was the *coup d’oeil*, the “capacity to discern through the fog of war what was happening and what needed to be done”, focusing on the essentials and avoiding “the elaborate process of calculations of possibilities and probabilities that would paralyse the decisions of a lesser man”. The other was “the capacity, having taken a decision, to stick to it: determination”, despite everything that would conspire to convince him that his decision had been wrong (HOWARD, 2002, p. 28).

This second quality is also a fundamental element of Coercion Theory. Once a threat is made, the target has to believe that the coercer has the determination (or will, intent or commitment) to fulfil the threatened harm.

On the question of ‘intention’, Kaufmann observed that an opponent might use “three main sources of information about the intentions of a country”: “its record of performance in comparable contingencies during the recent past; the statements and behavior of its government; and the attitudes of public opinion, both domestic and allied” (KAUFMANN, 1954, p. 6). Thus, reputation, character, and morale. “A policy of deterrence consistent with the country’s recent



behavior in the international arena is likely to seem much more plausible than one which constitutes a sharp break with tradition” (KAUFMANN, 1954, p. 6). “Finally, and perhaps most importantly in the realm of intentions, a policy of deterrence will seem credible only to the extent that important segments of public opinion in domestic and allied countries support it” (KAUFMANN, 1954, p. 6). Here, he drew on what Meira Mattos later called ‘persuasion’.

In the early stages of the Cold War, U.S. President Eisenhower and Secretary of State Dulles stated their Massive Retaliation Strategy, noting that any misbehaviour of the ‘communists’ (USSR and People’s Republic of China – PRC) would be answered with nuclear weapons. Even before the USSR had strategic bombers at hand for threatening to bomb the U.S. soil, critics like Kaufmann questioned the Americans' will in fulfilling this threat. It was evident that an attack to the American soil could unleash nuclear retaliation; but was it credible that the U.S. could retaliate in the same way an attack against a small country in Asia? (KAUFMANN, 1954). After it became clear that the Soviets were capable of Mutually Assured Destruction (MAD) against the U.S., even European leaders started to question if the U.S. would ensure their protection in case of a conventional (non-nuclear) Soviet attack.

Kaufmann, indeed, argued for the presence of American troops placed in allied countries, so that in case of an attack, they would be engaged (KAUFMANN, 1954). As Snyder claimed, Deterrence by Denial is maximised if there are forces deployed on the threatened territory, particularly in its boundaries, since such deployments signal a clear determination to fight (SNYDER, 1959, p. 35).

Will, capabilities and credibility are factors that often go together. However, if the coerced perceives the lack of any of these factors, deterrence shall fail. “At times a coercer may have preponderant power in a general sense but lack specific means to influence an adversary” (BYMAN; WAXMAN, 2002, p. 18). Opposingly, “the mere presence of will in the absence of capability is nothing more than bluster” (BRANTLY, 2020, p. 211).

Thus, “war is a contest of wills as much as it is a contest of instruments and materiel” (BIDDLE, 2020, p. 106).

#### 4.2.1.6 Credibility

Focused on ‘deterrence by punishment’ Kaufmann established the need for credibility regarding the threats made.

The risk is that, despite our best efforts, the antagonist will challenge us to make good on our threat. If we do so, we will have to accept the consequences of executing our threatened action. If we back down and let the challenge go unheeded, we will suffer losses of prestige, we will decrease our capacity for instituting effective deterrence

policies in the future, and we will encourage the opponent to take further actions of a detrimental character. (KAUFMANN, 1954, p. 5)

Going further on the question of credibility, he divided the concept into three parts: (a) the need of persuading the ‘enemy’ that there is the ‘capability’ to act; (b) that in acting, the inflicted ‘costs’ could be greater than the ‘gains’ he could achieve; (c) the ‘intention’ on using that ‘capability’ and incurring in its ‘costs’ (KAUFMANN, 1954, p. 5–6).

Credibility stands on the ‘reputation’ or ‘face’ of a nation. It is thus based on how past commitments have been honoured. It is determinant for the opponent to believe whether or not perceived (or communicated) threats are to be enforced, what is usually linked to whether the issues at stake are worth the effort. It can also be assumed to be related to the quality of the enforcement options [capabilities] and the opponent’s ability to resist enforcement and retaliate in kind (FREEDMAN, 2004, p. 36).

In principle, every act of foreign policy has some significance for the creation of expectations of future performance. Compliance may be a form of humiliation and an acknowledgement of submission. This can have long-term consequences. How one deters now will have an impact on how much one might have to deter in the future. (FREEDMAN, 2004, p. 52)

Credibility deserves “special attention because it is in terms of this component that the risk calculus of the aggressor ‘interlocks’ with that of the deterrer” (SNYDER, 1961, p. 12). Credibility stands for the probability of the various possible responses available to the deterrer (SNYDER, 1961, p. 13). Thus, it is neither unvarying nor permanent (BIDDLE, 2020, p. 104). Albeit, it is attached to legal, moral and ethical (therefore cultural and institutional) aspects at the time of the influence attempt, which tend to be consolidated (and somehow crystalised) over time.

“A persuasive threat of war may deter an aggressor; the problem is to make it persuasive, to keep it from sounding like a bluff” (SCHELLING, 2008, p. 35). Occasionally recurring to war can be an element for creating a reputation that offers a dissuasive effect on foes, as might be Israel’s case (FREEDMAN, 2004, p. 38). However, “force demonstrations, when used to indicate intent, differ from the effects of verbal threats in various ways”, and “cannot be as explicit as threats [since] they are inherently somewhat ambiguous and diffuse” (SNYDER, 1961, p. 254).

The ability to increase resource allocation is an essential element of credibility. In particular, the ability to rapidly spend large sums of money (KAHN, 1960, p. 37). “In June, 1950, the United States was engaged in a great debate on whether the defense budget should be

14, 15, or 16 billion dollars. Along came Korea. Congress quickly authorised 60 billion dollars, an increase by a factor of four!” (KAHN, 1960, p. 35). Kahn also states that particularly valuable is the existence of civil defence plans (thus resilience) and limited conflict capabilities (KAHN, 1960, p. 37).

‘Appeasement’, which relies on removing the causes of conflict, opposes the concept of dissuasion. It shall not work if war is in the opponents’ plans, as in the case of Hitler at Munich in 1938. But it might work “when threats of force are instrumental and the inducements on offer have some appeal” (FREEDMAN, 2004, p. 53). Nations must “make it risky for the enemy to force [them] into situations in which we must choose between fighting and appeasing, presenting an “alternative to peace”, which must include at least a limited-war capability (KAHN, 1960, p. 39, 40).

#### 4.2.1.7 Costs

The concept of “costs” is central to coercion (and indeed influence), as in its basic formulation: “a deterrence policy thus constitutes a special kind of forecast: a forecast about the costs and risks that will be run by the party to be deterred, if certain actions are taken, and about the advantages that he will gain if those actions are avoided” (KAUFMANN, 1954, p. 6).

However, the fact that different types of costs shall be considered is often unnoticed. Already in 1939, Liddell Hart stated that when enemy attack meets defence it tends to “weaken the will of the enemy people, and foster unrest among them”; “this state of mind, and loss of spirit, will develop all the sooner if the offensive campaign produces no results comparable with its cost” (LIDDELL HART, 1939, p. 124). He also observed that there are different types of costs, that concern to values: first, the attacker shall face ‘moral expenses’ related to the rightful ownership of the attacked land, as he is the aggressor; second, “there is nothing more demoralising to troops than to see the corpses of their comrades piled up in front of an unbroken defence, and that impression soon filters back to the people at home” (LIDDELL HART, 1939, p. 124). Thus, moral costs add up to the analysis of cost and benefits.

Snyder straightforwardly worked on cost as a marginal utility.

The rule of minimising “expected cost plus preparedness cost” could be expressed in terms of the familiar economic principle of marginal utility. This principle simply says that in any allocation of scarce resources among competing uses, when each use is subject to diminishing marginal returns as additional resources are applied to it, no increment should be given to any one use when it would yield a greater return in some alternative use. In the optimal allocation, the “last” or marginal increment to each use would yield a return exactly equivalent to its marginal cost, with marginal cost defined as the utility which could have been gained by applying the increment to other

alternatives. When this condition holds, the maximum total utility is being obtained with the available resources. (SNYDER, 1961, p. 275)

“Preparedness cost” consists in the resources consumption in peacetime, while “expected cost” consists in two items: reducing the risk of war (dissuasion); and minimising costs and losses in case of war (defence) (SNYDER, 1961, p. 266).

Furthermore, as he observed, “one does not usually risk much to obtain little”; thus, it is not a simple question of gains being greater than losses, being “more common to risk much to gain much” (SNYDER, 1959, p. 31).

Snyder also observed that defending forces might be predisposed to suffer higher costs when intending to dissuade the enemy, showing their willingness to suffer increased costs in the future (SNYDER, 1961, p. 38). Thus, the construction of credibility may impose higher costs than typical defence would justify. This disposition elevates what he called ‘deterrent value’. If, on the contrary, the defender fails to fight or to carry out a threat, it loses deterrent value (SNYDER, 1961, p. 40).

#### 4.2.1.8 Signalling

“Signalling” refers to ‘communicating’ the limits of tolerated enemy actions. It is often associated with ‘red-lines’ or the ‘threshold’ to escalation. The use of “occasional wars” to communicate resolve and limits, reinforcing credibility, although “uncomfortable”, fits in with the notion of a “costly signal”.

As Schelling observed, “the objective is often communicated by the very preparations that make the threat credible”; compelling threats “tend to communicate only the general direction of compliance, and are less likely to be self-limiting, less likely to communicate in the very design of the threat just what, or how much, is demanded” (SCHELLING, 2008, p. 73).

Having an “adequate denial capability, preferably one situated near or in a threatened area, is the surest sign we can make to the enemy that the area is valued highly” (SNYDER, 1959, p. 5).

Communicating deterrence by denial requires a demonstration of capability, presenting a particular problem: showing defensive capabilities to a potential aggressor may provide him with the information needed for side-stepping defences (FREEDMAN, 2004, p. 38).

Conversely, the communication of threats in deterrence by punishment involves exploiting the capacity “for hurting and inflicting damage one needs to know what an adversary treasures and what scares him”. Besides, the threatened “pain and suffering have to appear contingent on his behavior [...] that he can avoid the pain or loss if he does comply”; “the

prospect of certain death may stun him, but it gives him no choice” (SCHELLING, 2008, p. 3, 4).

#### 4.2.1.9 Perception

Perception is the way that someone sees or understands something. In his seminal work, Kaufmann described the “quite obvious” need of knowing the opponent to make the policy meaningful to him (know his values) and the need for ‘communicating’ the threat to the opponent (KAUFMANN, 1954, p. 5). Jervis put it differently:

If a policy is to have the desired impact on its target, it must be perceived as it is intended; if the other’s behavior is to be anticipated and the state’s policy is a major influence on it, then the state must try to determine how its actions are being perceived. (JERVIS, 1982, p. 4)

“Perceptions are the dominant variable in deterrence success or failure” (MAZARR, 2018, p. 7). For coercion to succeed, it is necessary to exhibit such a commitment to create, on the target, a subjective perception of risk (or cost) that supersedes the perceived return of being non-compliant (MAZARR, 2018, p. 7).

Perceptions are influenced by information as well as by heuristics, biases, values and personality (DAVIS, 2014, p. 9). They are also greatly influenced by reputation and past behaviour. An actor often “ignores statements and other signals that can be easily manipulated and looks only at whether the other stood firm, compromised, or retreated in the past, irrespective of what he [the opponent] said he would do” (JERVIS, 1982, p. 12).

Moreover, people usually attach new information to their “pre-existing beliefs”. “Ambiguous or even discrepant information is ignored, misperceived, or reinterpreted so that it does minimum damage to what the person already believes (JERVIS, 1982, p. 24). Hence, influence strategies that are more likely to be successful must be tailored to the other’s pre-existing beliefs and images; since these are different for distinct actors, what may work for one actor shall fail to another (JERVIS, 1982, p. 27; MAZARR, 2018, p. 8). In other words, perceptions are deeply affected by ‘culture’.

#### 4.2.1.10 Resilience

NATO defines resilience as “a society’s ability to resist and recover easily and quickly from shocks [natural disaster, failure of critical infrastructure, or a hybrid or armed attack] and combines both civil preparedness and military capacity” (NATO, 2020).

In a similar mood, the U.S. Department of Homeland Security states that resilience “includes the ability to withstand and recover rapidly from deliberate attacks, accidents, natural disasters, as well as unconventional stresses, shocks and threats to our economy and democratic

system”, included in the U.S. national doctrine in the 2017 National Security Strategy (US-DHS, [S.d.]).

Although these definitions are relatively new, during the Cold War, Brodie, one of the major American strategists, spent a lot of effort arguing for the need of “civilian protection” in the event of a nuclear war. His efforts focused on the necessity of preserving the American economy and the capabilities of continuing to function as a State (BRODIE, 1959a, p. 173–222).

In defining the importance of defence as a dissuading element, Snyder established that “defense value is denial capability plus capacity to alleviate war damage” (SNYDER, 1961, p. 4). The capacity to alleviate war damage corresponds to ‘resilience’. In simpler terms, he stated that

$$\text{Defence} = \text{Denial} + \text{Resilience}$$

#### 4.2.2 Coercion & Strategy

National security practitioners, strategists and warfighters (both military and civilian) need to have a grasp of the logic and concepts underneath Coercion Theory; if they don’t, they may not be able “to understand the ways that their enemies may resist and thwart them, even when those enemies are materially weaker” (BIDDLE, 2020, p. 96).

In May 2019 the U.S. Joint Chiefs of Staff established six “special areas of emphasis” (SAEs) for the Joint Professional Military Education: (1) The Return to Great Power Competition; (2) Globally Integrated Operations in the Information Environment; (3) *Strategic Deterrence in the 21st Century*; (4) Modern Electromagnetic Spectrum Battlefield; (5) Space as a Warfighting Domain; (6) Ability to Write Clear and Concise Military Advice Recommendations (DUNFORD, 2019, emphasis added). The two pages that detail the intended syllabus of Strategic Deterrence is still mostly connected with nuclear deterrence. Although, its last item states the following:

(4) Contemporary Deterrence Challenges

(a) Deterrence in U.S. national and defense strategy.

(b) *Adversary doctrine and perceptions.*

(c) *Tailored deterrence strategies for specific adversaries.*

(d) Extended nuclear deterrence and assurance of allies.

(e) *“Integrated deterrence” approaches to account for all elements of national power, the spectrum of conflict, and emergent capabilities (e.g., cyber, space, conventional precision strike, missile defense).*

- (f) Deterrence messaging in the modern information environment.
- (g) Conventional-nuclear planning integration.
- (h) Conventional campaigns in the “nuclear shadow.”
- (i) Challenges to the legitimacy of nuclear deterrence. (DUNFORD, 2019, p. 4, emphasis added)

Naming it Strategic Deterrence and considering it an SAE, at least theoretically, reinserts deterrence at the strategic level for the U.S. military. And the inclusion of “contemporary deterrence challenges” clearly indicates the interest in expanding its scope. Items (b), (c) and (e) illustrate the importance of culture (doctrine and perceptions), which influence “tailored deterrence strategies” involving “all elements of national power” (not only military power) in their design and application.

### 4.3 On ‘Influence Theory’

Three years before Schelling’s seminal work, Singer (1963) proposed his *Inter-nation Influence: A Formal Model*. The “capacity to influence” actions of other nations would define the influencer’s power (SINGER, 1963, p. 420). Influence would be exerted in two ways. “Dissuasion” was the “negative” one, since inducing the target ‘not to act’, while “Persuasion” was the “positive” one.

Threat and punishment and promise and reward go together, but the distinction must be constantly kept in mind. Threat and promise refer to nothing but contingent, probable future events, while punishment and reward are concrete acts that already have taken, or are in the process of taking, place. (SINGER, 1963, p. 427)

These three concepts do not oppose to those of ‘Coercion Theory’. Instead, they are complementary, as supersets of the original ones.

#### 4.3.1 Structural Elements of ‘Influence Theory’

##### 4.3.1.1 Influence

As Singer (1963) stated, when a nation (the influencer) exerts an “influence attempt”, it tries to conduct the actions of another nation (the influenced<sup>2</sup>). Influence efforts are always future-oriented and uncertain regarding their results. One invests its resources now expecting for an outcome that can or cannot be achieved in the future. Moreover, influence efforts are based on the influenced past and present behaviour, as the influencer perceives them. Furthermore, influence is not a “one-way affair”; if the influencer is attempting to modify an

---

<sup>2</sup> Singer called it “influencee”, but in this work I prefer using the name influenced.

influenced behaviour, it is because the actions of the latter affect the interests of the first (SINGER, 1963, p. 420–1).

Influence operations depend on three fundamental aspects: the predicted outcome; the desired one; and the resources available for influencing (SINGER, 1963, p. 422). This last aspect is relevant; since resources are limited, influence attempts must be prioritised. In general, they tend to be concentrated in influence attempts targeting nations with “competitive and conflictful relationships”, with far fewer resources applied on those “either friendly or negligible” (SINGER, 1963, p. 423).

Influence can be used for two types of outcomes: “persuasion” is the one that ‘induces’ an act (the “positive” one); “dissuasion” is the one that ‘averts’ an action (the “negative” one).

Both types of influence operations can use the same techniques: threat of punishment and promise of reward. And both can be used “either to modify or to reinforce” a behaviour (SINGER, 1963, p. 426). Threats and promises constitute “probable future events”, while punishment and reward are concrete events related to the consequences of the threats and promises. So, rewards and punishments shall “be devoted, among other aims, to increasing the credibility of the promises and threats” made (SINGER, 1963, p. 427).

The combination of the pairs (Persuasion, Dissuasion) and (threat of punishment, promise of reward) results in four attempt types, with specific desired outcomes from the influenced part.

- a) If you do this, I will punish you in this way (dissuasive threat);
- b) If you do not do this, I will reward you in this way (dissuasive promise);
- c) If you do this, I will reward you in this way (persuasive promise);
- d) If you do not do this, I will punish you in this way (persuasive threat).

#### 4.3.1.2 Dissuasion

‘Dissuasion’, as seen, constitutes an attempt to make the influenced not to do (or stop doing) something undesired by the influencer.

Among the possible outcomes listed above, Dissuasion constitutes the two first options (items ‘a’ and ‘b’). Both options can have two different forms each, albeit preserving the same intent of averting (or stopping) an undesired action.

For dissuasive threats, these forms are:

- a) If you do this, I will punish you in this way;
- a’) If you continue doing this, I will punish you in this way.

For dissuasive promises, these forms are:

- b) If you do not do this, I will reward you in this way;



b') If you stop doing this, I will reward you in this way.

Two things might be already evident. First, that 'dissuasive threats' contain (or include), using 'Set Theory' terminology, the concept of 'deterrence'. Second, that 'dissuasive promises' are not contained (or not included) in Coercion Theory, since not related to threats of punishment. Thus, Dissuasion contains Deterrence (dissuasive threats) and dissuasive promises.

#### 4.3.1.3 Persuasion

'Persuasion', conversely, constitutes an attempt to make the influenced do (or continue doing) something desired by the influencer, corresponding to options 'c' and 'd' of the list of influence types.

Moreover, as in the case of Dissuasion, each type of Persuasion can have two different forms, albeit preserving the same intent of inducing (or continuing) a desired action.

For persuasive promises, these forms are:

c) If you do this, I will reward you in this way;

c') If you continue doing this, I will reward you in this way.

For persuasive threats, these forms are:

d) If you do not do this, I will punish you in this way;

d') If you stop doing this, I will punish you in this way.

As in the case of Dissuasion, it might be clear that persuasive threats contain the concept of 'compellence'. 'Persuasive promises' are not included on Coercion Theory, since not related to threats of punishment. In other words, Persuasion contains Compellence (persuasive threats) and 'persuasive promises'.

## 4.4 Comparing 'Deterrence' and 'Influence' Theories

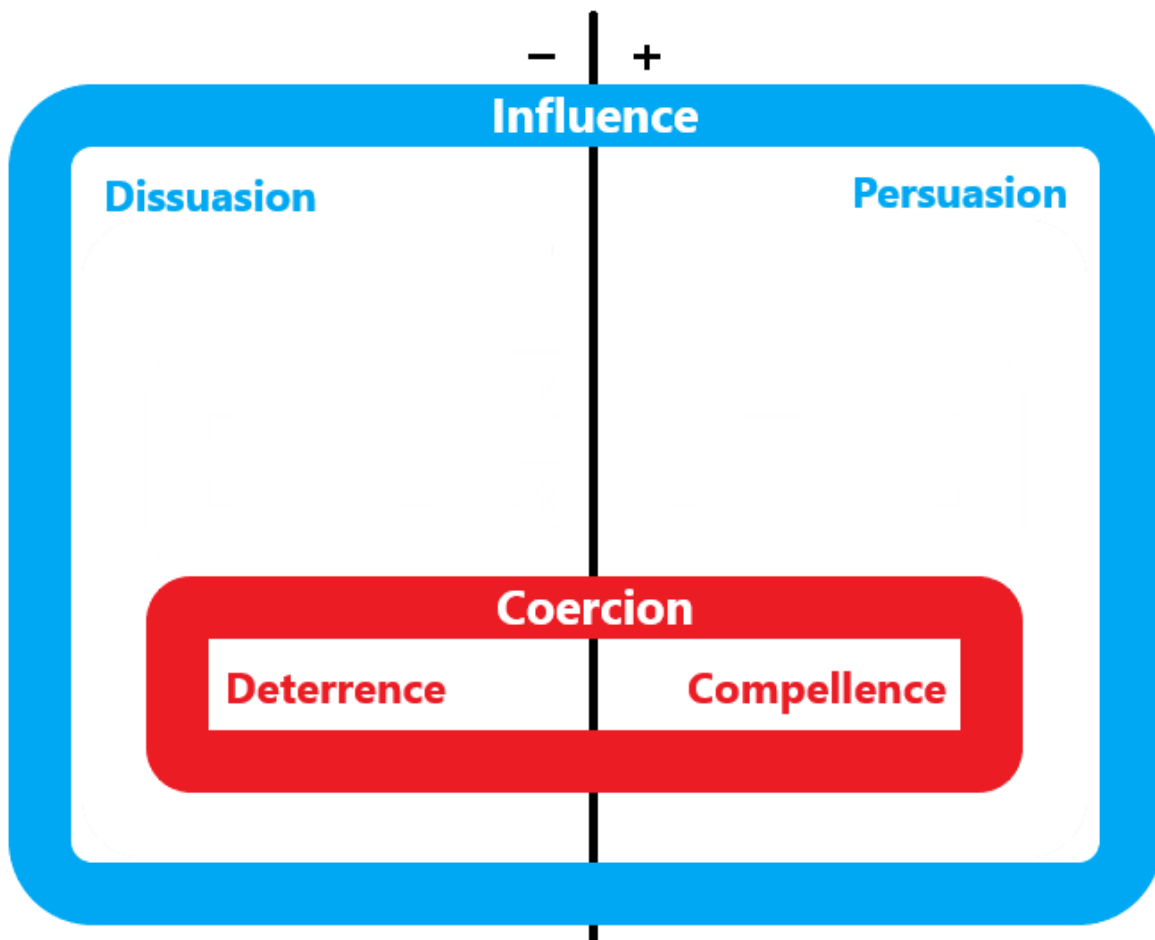
Interestingly, while Schelling denotes a great deal of preoccupation with precise terminology, he acknowledges that the use of the term 'deterrence' was inaccurate for describing the whole of coercive postures. Still, he accepts it as a "restrictive euphemism" for 'coercion':

Among the reasons why coercive warfare has not figured much in our theoretical discussions or our military plans, one is that we have been mainly concerned with "deterrence", and deterrence is comparatively simple. Partly, our aim has indeed been deterrence; partly deterrence has been a euphemism for the broader concept of "coercion", as "defense" has replaced words like "war" and "military" in our official terminology. It is a restrictive euphemism if it keeps us from recognising that there is a real difference between deterrence and what, in Chapter 2, I had to call

“compellence”, that is, a real difference between inducing inaction and making somebody perform. (SCHELLING, 2008, p. 174)

With that in mind, the concepts proposed by Singer and Schelling are graphically represented in Figure 1. The minus signal indicates the ‘negative’ side, while the plus sign represents the ‘positive’ one. The blue area (Influence) shows Singer’s concepts, while the red one (coercion) indicates those of Schelling. Since ‘coercion’ was ‘influence’ made by the threat of force, it constitutes a subset of influence.

Figure 1 – Graphical View of the Elements of Influence and Coercion Theories



Source: Compiled by the author

#### 4.5 The Pitfalls of Deterrence and Influence Theories

Although Influence Theory contains Deterrence Theory, it still leaves some uncovered areas.

##### 4.5.1 The Limited Scope of ‘Deterrence’ (And ‘Coercion’)

When considering Singer’s concepts and terminology, and his distinction between the positive and negative sides, Schelling wrote:

J. David Singer has used a nice pair of nouns, “persuasion” and “dissuasion” to make the same distinction. It is the adjectives that cause trouble; “persuasive” is bound to suggest the adequacy or credibility of a threat, not the character of its objective. Furthermore, “deterrent” is here to stay, at least in the English language. Singer’s breakdown goes beyond these two words and is a useful one; he distinguishes whether *the subject is desired to act or abstain*, whether or not he is presently acting or abstaining, and whether he is likely (in the absence of threats and offers) to go on acting or abstaining. (If he is behaving, and is likely – but not certain – to go on behaving, there can still be reason to “reinforce” his motivation to behave.) Singer distinguishes also “rewards” and “penalties” as threats and offers; while the rewards and “penalties” can be the consequences of threats and offers, they can also be gratuitous, helping to communicate pervasively some new and continuing threat or offer. (SCHELLING, 2008, p. 71, emphasis added)

The passage shows that he was interested in the meaning of both the nouns and their respective adjectives. In the excerpt, indeed, albeit recognising many merits of Singer’s work, he dismisses Singer’s terminology because it worked for a broader field of ‘influence’ than that of the use of force, thus out of Schelling’s focus (*Arms and Influence* was the name of his book!).

For the last two decades, it has been already noticed that deterrence is not enough to describe intended causality outcomes that result from the application of different elements of power than that which can “hurt” or “threaten hostages”. Yet, many authors insist on using the wrong terminology to describe and analyse these ‘new phenomena’.

#### **4.5.2 The Problem of the Term ‘Influence’**

Schelling observed that Singer was also focused on “causation”, as indicated in the emphasised part of the excerpt above. Thus, both deterrence, coercion and influence theories focused on studying relations of the type “do as I say”.

Interestingly, Schelling “flies by” a significant point when he does not observe that, differently than proposed by Singer, ‘influence’ is broader than ‘persuasion + dissuasion’.

A better noun for the name of the intended theory, instead of ‘influence’, would be “causation”, which means “the causing or producing an effect” (OXFORD DICTIONARY, 1992, p. 179).

The problem lies in the meaning of “influence”: “the power to affect somebody’s *actions, character or beliefs* through example, fear, admiration, etc.”(OXFORD DICTIONARY, 1992, p. 641, emphasis added). Thus, influence goes well beyond just affecting

actions, touching “character or beliefs” as well. This could be irrelevant, at first sight. But a more in-depth consideration reveals that it is not.

In the international system, a form of behaviour commonly observed is “mimicry”, by which a state behaves like one that is admired, believing that “good people do X” (FINNEMORE; HOLLIS, 2016, p. 451; RISSE, 2000, p. 4–5). Consequently, ‘influence’ can lead to situations that fit in the “do as I say, not as I do”.

#### 4.6 The Unfolding of ‘Dissuasion Theory’

After decades with a narrow focus on deterrence, it was perceived that a broader spectre of options for changing opponents’ behaviour was available. In September 2001, the U.S. DoD published the Quadrennial Defense Review, where ‘dissuasion’ appeared as one of four strategic goals:

- Assuring allies and friends;
- *Dissuading* future military competition;
- Deterring threats and Coercion against U.S. interests; and
- If deterrence fails, decisively defeating any adversary. (U.S. DOD, 2001, p. 11, emphasis added)

Rumsfeld later explained the concept:

Just as the existence of the U.S. Navy dissuades others from investing in competing navies – because it would cost them a fortune and would not provide them a margin of military advantage – we must develop new assets, the mere possession of which discourages adversaries from competing. For example, deployment of effective missile defenses may dissuade others from spending to obtain ballistic missiles, because missiles will not provide them what they want: the power to hold U.S. and allied cities hostage to nuclear blackmail. (RUMSFELD, 2002, p. 27)

As Yost (2003) observed, there was a recognition that ‘deterrence’ was not enough anymore. Indeed, albeit all the examples cited by Rumsfeld involved militaria (the strategic DoD goal itself is focused in military competition), the concept is not anymore related to the threat of use of force: neither for punishment nor for denial. It relates to the economic idea of ‘utility’, linked to ‘return on investment’. Hence, it does not any longer fit neither in the scope of the narrow ‘Deterrence Theory’ nor in that of the broader ‘Coercion Theory’. Instead, it stands in the broader arena of ‘Dissuasion’, while still working with the negative side, or the even more comprehensive ‘Influence Theory’.

Moreover, Davis (2015) suggested using ‘deter’ only in the classic sense, involving a threat of punishment. Even ‘deterrence by denial’, he suggested, should be referred as ‘dissuasion by denial’, and defined as: “dissuading an action by having the adversary see a

credible capability to prevent him from achieving potential gains adequate to motivate the action” (DAVIS, 2015, p. 5). Moreover, “‘dissuasion by futility’ should be added to the vocabulary”, Davis argued. He also observed that deterrence is “merely one element along a spectrum of influences”, and that “the notion that adversaries can be persuaded not to do something by deterrent threats alone is naïve” (DAVIS, 2015, p. 20).

I endorse Davis’ suggestions regarding the use of the term dissuasion instead of deterrence. Besides, as already evidenced, dissuasion constitutes a superset that contains deterrence. Thus, it is better to adopt dissuasion in all of the cases for maintaining the taxonomic uniformity. So, starting now, ‘deterrence by [the threat of] punishment’ is renamed ‘dissuasion by [the threat of] punishment’, the first type of dissuasion; ‘deterrence by denial’ is renamed ‘dissuasion by denial’, the second type; and ‘dissuasion by futility’ constitutes the third type.

Elsewhere, as part of the findings of my Masters’ research at King’s College London, I had already made an incursion on the necessity of distinguishing deterrence from dissuasion, and unifying the naming convention under the general class of “dissuasion” (MALAGUTTI, Marcelo, 2016a). In the present work, however, the theoretical foundations supporting this claim are much more robust and elaborated.

It shall be noted that Nye (2017, p. 52–5) devotes some effort to “equalise” deterrence and dissuasion. His claim has a questionable substance. First, a single Schelling’s phrase picked from an entire book committed to explaining the need for violence, “the power to hurt”, “taking hostages” and so on for coercion, deterrence and compellence. Second, another single phrase from Snyder in the book that draws the concept of ‘deterrence by denial’ relying on military capabilities. Finally, when presenting what Nye called “means of deterrence and dissuasion”, he argues:

For purists who object to “concept-stretching,” only the first (or first two) constitute deterrence, but the latter two mechanisms are also important in preventing hostile acts. Whether one chooses to incorporate them in a broader definition of deterrence or just describe them as additional means of dissuasion is mainly a semantic question. The important issue is to understand the general principles of causation. (NYE, 2017, p. 55)

As a “concept-stretcher” he names all of the identified “means of deterrence and dissuasion” (in this research called ‘types’) naming them “deterrence”.

The growth of cyber-threats brought renewed interest in ‘deterrence’ and ‘dissuasion’ possibilities. Stevens (2012, p. 155), studying *Deterrence and Norms in Cyberspace*, observed that both Lewis (2010) and Nye (2010) had considered that norms could reinforce deterrence

of cyber-offences, whilst none had “explicitly categorize[d] norms as a form of deterrence”. It was only in 2017 that Nye named it ‘Deterrence by Norms’, making it the fourth type of dissuasion (NYE, 2017).

The fifth type of dissuasion proposed was that of ‘deterrence [sic] by entanglement’. Albeit frequently credited to Nye (2017), it was first considered by Denning:

“Well-tempered statecraft can deter aggressive state behavior in all domains of warfare. Also, to the extent that the affairs of states are intertwined, especially economically, there is some deterrence [sic] by interdependency or entanglement; if one state harms another, it will also harm itself.” (DENNING, 2015, p. 13)

Finally, a sixth type, from now on named ‘dissuasion by individualisation’, seems to gather momentum in the international stage, based on making the individual perpetrators of attacks held responsible for their acts and prosecuting them, instead of their countries or organisations (BRAW; BROWN, 2020).

These six types of dissuasion are detailed in the next section.

## **4.7 Types of Dissuasion**

Albeit having already recurrently insisted on the impossibility of naming ‘deterrence’ anything other than ‘deterrence by punishment’, the term is still largely used by many as if interchangeable with dissuasion. Consequently, it will appear in citations from other authors. Thus, regrettably, in these cases, it shall be considered a synonym of dissuasion.

### **4.7.1 Dissuasion by Punishment**

“Dissuasion by [threat of] Punishment” (DbP) relies on the threat that an attack will be retaliated with so much force that the costs can become unsurmountable to the attacker. The origins of the concept go back to Thucydides, who argued: “when there is mutual fear, men think twice before they make aggressions upon one another” (JOWETT, 1900, p. 46, book 4, paragraph 62). Although ‘passive’, in the way of being a reaction to an aggression, it rests on offensive capabilities, or more precisely in the defender’s capacity (the deterrer) to project power over something that the attacker (the deterred) values. In political science and military jargon, power projection consists of applying force out of national boundaries, in a remote conflict area. Traditional military examples include aircraft carriers, ballistic missiles and, more recently, drones.

The combination of nuclear weapons and airpower significantly increased the perception of a prospective cost of punishment that could be imposed, thus elevating its importance as a dissuasive or deterrent factor (SNYDER, 1959, p. 1–2). It had a significant side effect, however.

The association of the concept of deterrence with air-nuclear technology has fostered the notion that deterrence is accomplished primarily, if not exclusively, by threatening the enemy of overwhelming punishment for his aggression, or at least with costs greater than the value he attaches to his strategic objective. (SNYDER, 1959, p. 1)

The fear of these terrible costs would stimulate prudence upon the enemy, although there was uncertainty connected with the threats. “Even though he [the enemy] thinks there is little chance of our punishment threat being carried out, he can never be sure”, and even a threat with very low credibility would still have some deterrent effect due to this uncertainty (SNYDER, 1959, p. 6).

Notwithstanding, the use of ‘Punishment’ by nuclear retaliation as the main element of ‘Deterrence Theory’ has been questioned since its early stages (BRODIE, 1959b; KAUFMANN, 1954). As stated, there were the moral and ethical issues of the use of ‘nukes’ to retaliate ‘any’ communist aggression in a remote place in Asia. Furthermore, knowing that a Soviet counter-strike would destroy the U.S., raised many concerns regarding these threats' credibility.

One other issue regarded the paradox posed by nuclear weapons as dissuaders. To be meaningful, they demanded not to be used at all. But to ensure their effectiveness, they required their “capacity to function to be “maintained at a very high level and constantly refined”, at a high cost. “In other words, expecting the system to be constantly perfected while going permanently unused. Surely we must concede that there is something unreal about it all” (BRODIE, 1959b, p. 175).

There was a “special significance” involving the idea of “surprise attack” and the vulnerability of retaliatory forces themselves. Both sides considered that their retaliatory means could survive a massive first strike; but they believed they could not ensure that the other side could not strike back. Thus, “there would be no powerful temptation to strike first” and “there would be less need to react quickly to what might prove to be a false alarm” (SCHELLING, 1980, p. 233).

The association of ‘Deterrence Theory’, particularly ‘Deterrence by Fear’, with nuclear weapons, and the Cold War, made the theory less pervasive to many countries. Only a bunch of countries had ‘nukes’. And only two with vectors that could deliver them worldwide. Did it mean that ‘Deterrence by Fear’ concepts were not valid for nations without those means? The answer is no! Countries with only conventional weapons could instil fear in their peers. Thus, having (and showing) advanced conventional weapons capabilities is still a form of dissuasion. It had been so before the advent of nuclear weapons, and it shall continue to be valid for nations

without them. All of the concepts associated with ‘Deterrence Theory’ (capabilities, will and credibility, risks and costs, and so on) are applicable.

A significative change, however, was included in the ‘cost x benefit’ calculus of conflicts. Having nuclear capabilities and launching vectors would make it possible for nations with lower conventional capabilities to instil fear in countries with stronger conventional forces (SNYDER, 1961, p. 8). Indeed, this possibility was masterfully depicted in the movie *The Mouse that Roared* (ARNOLD, 1959).

DbP is hard to implement in the military realm in the absence of attribution; one needs to know who did the wrongdoing to be able to punish him (FINNEMORE; HOLLIS, 2016, p. 458). Nevertheless, the international arena is political, and not necessarily a legal one. Thus, attribution becomes a matter of degree, with each specific political moment demanding more or less evidence. If the *cui bono* (who benefits) test points to an opponent and there are widely deemed credible rumours to support this argument, then the international community will likely sustain the claim of attribution without concrete evidence (HARE, 2012; NYE, 2013).

#### 4.7.2 Dissuasion by Denial

“Dissuasion by Denial” (DbD) was first defined as “deterrence achieved by the capability to deny the other party any gains from the move which is to be deterred” (SNYDER, 1960, p. 163). More recently, a refined definition, more adequate to the idea of dissuasion as more than deterrence alone, was proposed: “dissuasion by denial [...] is deterring an action by having the adversary see a credible capability to prevent him from achieving potential gains adequate to motivate the action” (DAVIS, 2014, p. 1).

Thus, DbD is based on the idea that defending forces (of the deterrer) can make the intended attacker (the deterred) consider that the gains of his attack will be denied, or will have cost close or larger than the benefits of that attack. The idea of dissuading an enemy denying gains was not new, however.

It is important to realise that this new-old and strength-conserving strategy of Imperial defence does not imply a purely passive resistance, Its aim is to convince the enemy that he has nothing to gain and much to lose by pursuing a war. Its guiding principle is to eschew the vain pursuit of a decision by the offensive on our own part. Its method is not merely to parry, but to make the enemy pay as heavily as possible for, his offensive efforts. (LIDDELL HART, 1939, p. 121, emphasis added)

In opposition to DbP, DbD rests on defensive capabilities, and relates to the military concept of ‘area denial’. This concept is based on denying the adversary the ability to bring into (or freely using within) the contested region its operational capabilities (RUSSELL, 2015).



Traditional examples are barb-wired fences, minefields, caltrops or the dragon teeth used on the famous Siegfried Line, the chain of fortifications know as Maginot Line and the Finnish resistance against the Soviet invasion of 1939.

The cost of the threat of DbD is more straightforward to estimate than that of DbP (SNYDER, 1959, p. 5). Besides, the capacity of denying territory (or gains) to the aggressor by conventional means is usually more effective than threats of punishment in deterring more traditional forms of aggression (SNYDER, 1959, p. 32). Since it does not involve offensive (out of borders) operations, it does not require formal accountability or attribution; defending forces just prevent losses as a result of the aggression (SNYDER, 1959, p. 32).

Usually, the attacker has low uncertainty regarding the will of the defender in engaging its forces, and that these forces can be effective in blocking his gains; the downside is that the costs imposed to the attacker are proportionally lower than those of nuclear punishment. All summed up, “denial capability is more useful than the threat of punishment in deterring and dealing with ambiguous forms of aggression” (SNYDER, 1959, p. 38).

It is important to observe, however, that the deterrent value of a denial force is different from, and must be added to, its defence value, “its utility in blocking the enemy’s assault and preserving territorial values for the defender should deterrence fail” (SNYDER, 1959, p. 38). Exemplifying, the presence of small contingents of U.S. troops in Western Europe has little defence value. Still, it has a considerable dissuasive value since, presumably, the U.S. shall respond with a more extensive engagement of its means once they are attacked. Thus, the utility of defence for “detering major aggression must be looked for not in its direct denial capability, but rather in its indirect complementary effects” (SNYDER, 1959, p. 9).

Deterrence, as seen, is *ex-ante* and passive. Once the threat is posed, the deterrer just stands still and waits. If the deterred chooses to attack, he faces progressive resistance, increasing the costs of his actions. “If he expected no opposition, encountering some may cause him to change his mind” (SCHELLING, 2008, p. 78).

Traditionally, the same military forces provided defence if dissuasion failed. The need to choose between dissuasion and defence was, mostly, due to the development of long-range airpower and, later, nuclear weapons. Before these developments, the same weapons provided the three primary functions of military force: to punish the enemy (power projection), to deny him territory or to take it from him (area denial), and the mitigation of damage to oneself (resilience) (SNYDER, 1961, p. 8).

Long-range airpower partially separated the function of punishment from that of denial by making it possible to hit targets far from the frontlines (SNYDER, 1961, p. 8). And the Battle

of Britain offers an excellent example of the different deterrent and defensive values of airpower. Based on the premise of the dissuasive effect of long-range airpower, the Royal Air Force (RAF) had more long-range bombers than fighters in the prelude of war. As a matter of fact, RAF bombers had a relevant value in avoiding the UK invasion by sea, since the Germans were afraid of losing their troops and ships in the Channel. But the Germans did not consider the threat of having their fatherland bombed costly enough, and started the ‘Blitz’ attacking the UK with mid-range air bombing. Indeed, the RAF immediately started the counter-strike with its long-range bombers, but could not defend appropriately for a long time and reached the brink of defeat.

The example illustrates the distinction between “forcible defence” and “defensive action intended to deter”. Actions taken to ensure “that the enemy *cannot* succeed even if he tries” characterise forcible defence. Action taken “to *induce* him not to proceed, by making his encroachment painful or costly” illustrate “‘coercive’ or ‘deterrent’ defence” (SCHELLING, 2008, p. 78).

The language is clumsy but the distinction is valid. Resistance that might otherwise seem futile can be worthwhile if, though incapable of blocking aggression, it can nevertheless threaten to make cost too high. This is “active” or “dynamic” deterrence, deterrence in which the threat is communicated by progressive fulfillment. At the other extreme is forcible defense with good prospect of blocking the opponent but little promise of hurting; this would be purely defensive. (SCHELLING, 2008, p. 79)

It is possible to argue that denial has coercive elements, although tending towards control, meaning controlling the situation sufficiently to deny the foe strategic options. Thus, the opponent would have to consider those that would be incurred in the battle for control. Conversely, DbP “was pure coercion, in that the opponent was not denied choice, but was given powerful incentives to choose in a particular way” (FREEDMAN, 2004, p. 37).

Capable defensive means also increase the uncertainty perceived by the adversary on the likelihood of success on beating the defenders under the estimated costs; in time, this persistent uncertainty can make people not dissuadable at the beginning of the conflict become so at later stages of it (DAVIS, 2014, p. 5–7). There is, however, a “certain disadvantage to the defending side in the relative certainty of the denial calculus”; if the opponent knows that the defensive capabilities are not strong enough, these capabilities will have little dissuasive value, “even though such value will rise steeply once our denial forces become large enough to become effective” (SNYDER, 1959, p. 6).

Regarding the costs of denial strategies, from the dissuader's point of view, it has been observed that these tend to stay constant or to increase during a conflict (BRANTLY, 2020, p. 214).

### 4.7.3 Dissuasion by Futility

The concept of 'futility' stands in opposition to that of 'utility'. In 1949, in the U.S., there was an intense debate regarding the acquisition of aircraft carriers, intended by the U.S. Navy, and ballistic missiles, desired by the U.S. Air Force. Analysing the arguments from both sides, Brodie (1949) observed that "current trends, technological and otherwise" can affect costs circumstances and that "costs can be compared only where functions [of compared items] are comparable"; thus, "the real issue is utility, and since every military unit or weapon is expendable in war, the question of relative vulnerability is significant only because it affects utility" (BRODIE, 1949, p. 481).

What we need to know is the circumstances under which aircraft carriers have succeeded in their missions in the past and those under which they have failed, either through their own destruction or otherwise. (BRODIE, 1949, p. 481)

For example, during 1944 the Navy severely cut back its production of submarines not because those in service in the Pacific had failed but because they had been too successful. They had sunk so many Japanese ships that they were having difficulties finding new targets. (BRODIE, 1949, p. 482)

"Dissuasion by Futility" (DbF) would be achieved by convincing the adversary of the futility of competition, that his means are not going to be enough to reach eventual goals; thus it is better to allocate his resources elsewhere (YOST, 2003). Moreover, as it is possible to combine DbP and DbD, it is also possible to combine DbF. "If missile defences do not discourage an enemy from acquiring missiles (the goal of dissuasion [by futility]), they might discourage him from using them (the goal of deterrence [sic] by denial)" (YOST, 2003).

'Dissuasion by Futility' has also been described as below:

A third, broader way of approaching deterrence is to understand the idea of discouraging unwanted actions as including means beyond threats—to think of deterrence as only one part of a larger process of *dissuading* an actor. The goal of dissuasion is to convince a potential attacker that the cost-benefit calculus of aggression is unfavorable, partly through emphasising the costs of aggression but also through offering reassurances and benefits that make a world without aggression more attractive. (MAZARR, 2018, p. 4–5)

#### 4.7.4 Dissuasion by Norms

“Dissuasion by Norms” is based on the principle that laws, social or moral rules, or international norms might restrain the behaviour of a possible attacker. “Attitudes and norms arguably have more potential than laws per se, but they can be mutually reinforcing” (DAVIS, 2015, p. 20). “Crimes committed by nonstate actors have been deterred traditionally through norms via religious and moral teachings as well as crime statutes” (DENNING, 2015, p. 14).

For having this dissuasive (or possibly persuasive) effect on behaviour, “norms-based approach requires reinforcing certain values to the point where it is well understood that they must not be violated” (FREEDMAN, 2004, p. 4). “This involves deterrence, in that part of this exercise may be punishing or threatening to punish violations, although the process of establishing norms takes in all elements of foreign policy” (FREEDMAN, 2004, p. 4). The recognition that compliance with norms goes beyond punishment makes it clear that it is not only a matter of coercion, but involves a broader view of influence. Besides, Sir Freedman also recognises that the critical element for compliance is their legitimacy, rather than their enforcement (FREEDMAN, 2004, p. 72).

One more characteristic put apart norms from the limited scope of deterrence. In establishing norms, many actors try to “do the right thing” instead of just trying to maximise their preferences and gains. This differentiation has causal effects, while also defining social identities like “good people do X” (RISSE, 2000, p. 4–5; STEVENS, 2012, p. 156).

Altogether, there are three ways in which norms influence actions: “inducement and coercion; moral pressure and persuasion; and social learning and habit” (STEVENS, 2012, p. 156).

Non-compliance with norms can damage reputations and affect the attacker’s soft power, imposing costs that might exceed (or severely alleviate) the gains derived from the attack (NYE, 2017, p. 60).

Norms can impose costs added to other dissuasion types, or even in their absence, but, differently from entanglement, require some degree of attribution for working (NYE, 2017, p. 60). This, however, only applies when intended to be used for sanctioning (punishing) an attacker not restrained by moral questions attached to the infringed norms. Besides, again, attribution is political.

#### 4.7.5 Dissuasion by Entanglement

“Dissuasion by Entanglement” (DbE) occurs when the would-be attacker gives up the action because he perceives that his relationship with the target is so entangled, that the reflexes of an attack can have a serious repercussion on himself.

The idea was first described by Denning (2015, p. 13) as “to the extent that the affairs of states are intertwined, especially economically, there is some deterrence [sic] by interdependency or entanglement; if one state harms another, it will also harm itself”. Later, it was adopted by Nye (2016, 2017, p. 58) as “Entanglement refers to the existence of interdependences which makes a successful attack simultaneously impose serious costs on the attacker as well as the victim”. Another definition is given by Brantly (2020, p. 211): “At its most basic entanglement is the involvement of adversaries and allies in complicated patterns of behavior and interaction (a relationship) from which it is difficult to escape or alter without incurring substantial costs”.

While Entanglement makes much sense considering intertwined economies like those of the U.S. and the EU or China, it shall “not create significant costs for a state like North Korea which has a low degree of interdependence with the international economic system” (NYE, 2016). But even North Korea can be entangled indirectly, via ‘proxy entanglements’ with China, if this is entangled by the aspiring dissuader (BRANTLY, 2020, p. 228).

Fear of losing the benefits of entanglement shall discourage defection (BRANTLY, 2020, p. 226). Despite, even with the highly integrated political-economic relationship between the UK and the EU, the British people decided for Brexit, perceiving that the gains would exceed the costs.

Interestingly, Brantly considered that Entanglement would fill in the “gap” between ‘Punishment’ and ‘Denial’ (BRANTLY, 2020, p. 214). It only makes sense if one considers that all dissuasion types can always be applied to the same dissuaded, which often does not happen. Punishment and Denial were modelled for fighting the Soviets. There was not much integration between the U.S. and the S.U., and the previously existing one vanished after Stalin rebutted the Marshall Plan in 1947. Thus, it would not be possible to think of Entanglement as between Punishment and Denial in the USSR case. Instead, Entanglement is one more tool, which, as any of the others, can or cannot be used according to each specific case.

Multilateral military and intelligence organisations like NATO and Five-Eyes often foster the cooperation and increase the entanglement among their participating states and help mitigate tensions in times of crisis (BRANTLY, 2020, p. 222–3). Political and economic regional organisations as the EU, ASEAN and MERCOSUL also contribute to reducing the

probability of conflict among their member-states. Entanglement is fostered by promoting continuous interactions and dialogue, increased interdependence through heterogeneous markets, and increased prospects of economic gains and market growth (BRANTLY, 2020, p. 223–4). Entanglement can also be increased by the presence of multinational companies (NYE, 2016).

There is also a ‘group effect’ regarding entanglement: all members have an incentive to dissuade (or even persuade) third parties; the alliance raises the costs for non-members to act against the block; and entanglements within one group can enforce compliance within other groups, even among adversaries (BRANTLY, 2020, p. 217–226).

Nye (2017, p. 59) appoints that DbE could sometimes be “called ‘self-deterrence’ and treated as a case of misperception” since the dissuaded would be deciding based on his perception of things that might not be there. “But all deterrence is self-deterrence in that it ultimately depends on the calculations made by the deterred, whatever the quality of the threats being made by the deterrer” (FREEDMAN, 2004, p. 30). And projecting a desired perception on the opponent is one of the main objectives of any dissuasion policy: “the art of policy is to create a calculation of the risks and rewards that affect the adversary’s calculations” (KISSINGER, 1994, p. 481).

#### **4.7.6 Dissuasion by Individualisation**

“Dissuasion by Individualisation” (DbI) comes from making individuals nominally (thus personally) accountable for offences, even if they might be military or government employees in active duty. It has been called initially “Personalized Deterrence” (BRAW; BROWN, 2020). Nevertheless, there are good reasons for changing its denomination. Again, it is not the case of calling it deterrence since not connected to the use of force. Then, all types of dissuasion (or deterrence) were named as “dissuasion by <noun>”, where <noun> was one of the following: (threat of) punishment (or fear), denial, futility, norms and entanglement. There is no motive for abandoning this standard.

Naming it “dissuasion (or deterrence) by personalisation” would solve the above issue. However, the term personalisation carries two problems. First, “personalise”, the verb from which it derives, is usually connected with the idea of customising something to a specific individual (e.g. tailoring it for that person), which is not the case. Second, it derives from “person”, and could also refer to “legal person” (a company or organisation), thus escaping from the concept of the individual that is to be held accountable for his acts. Therefore, it is more precise to name the concept as ‘Dissuasion by Individualisation’.

The main motives for focusing on the individuals instead of their governments are two. One is the fact that individuals ponder costs and benefits differently than states (BRAW; BROWN, 2020, p. 52). The other is its lower potential for escalation regarding ‘naming and shaming’ of governments or States. “With less explosive consequences in the case of error, [it] also allows states to avoid the sticky attribution problem that sponsoring states have used to their advantage for the past two decades” (BRAW; BROWN, 2020, p. 54).

It shall be observed that attributing attacks to individuals does not require less evidence than naming States. It might even incur in requiring more substantial proof, since developed legal systems usually require striking evidence from the prosecutors (the State) against the individual, while in the international arena attribution can be mostly political. Besides, for nominating and indicting the perpetrator, it might require even more advanced intelligence capabilities than for naming a State and ‘burn’ intelligence sources. Thus, the investigation process might even be lengthier.

Interestingly, when a country’s military or intelligence officer is indicted to an offence, it should be easy to attach his State to his actions. But recently (after 2015), at least regarding cyber-offences, the preference goes to suing the individuals.

DbI presents explicit signalling that actions do not go unpunished, and that the personal life of the accused individual is going to be affected. If he “may have ambitions to travel or study abroad, or to hold international financial assets, the possibility of forfeiting such opportunities as a result of an employment choice may give them pause” (BRAW; BROWN, 2020, p. 52).

“Although it does not replace other methods of deterrence [sic], it supplements them effectively” (BRAW; BROWN, 2020, p. 54).

#### **4.8 Dissuasion in the Russian and Chinese Doctrines**

Russian dissuasion doctrine is relatively new, and still has at least three different phases: first, between 1991 (the collapse of the USSR) and 2006, where it was based on nuclear retaliation against any threat to Russia; second, from 2006 to 2014, where conventional military forces were added to it; and third when non-military forms of coercion were included (ADAMSKY, 2018; VEN BRUUSGAARD, 2016).

Russian military–theoretical texts indicate a concept like ‘strategic deterrence’ (*strategicheskoe sderzhivanie*), broader than the “traditional Western concept of deterrence”. The word “*sderzhivanie* (literally, ‘restraining’, ‘keeping out’ or ‘holding back’)", indeed, is

used to express a concept that “includes all activities aimed at war prevention, including what in the Western lexicon is called ‘containment’” (VEN BRUUSGAARD, 2016, p. 7–8).

It complies two goals – “prevention of war (in peacetime) and de-escalation of conflict (in wartime)” – to be achieved by “forceful (military and non-military) means (political-diplomatic, legal, economic, informational-psychological and spiritual-moral)” (ADAMSKY, 2018, p. 43). Thus, it presupposes its use either in peacetime and at war, resembling, “to Western eyes, a combined strategy of containment, deterrence and coercion” using any available means available to deter or dominate conflict (VEN BRUUSGAARD, 2016, p. 7).

It is considered innovative in Russian doctrine, since it breaks with traditional ideas of brute force and contrasts to “traditional massive use of force”, aiming at manipulating “the adversary’s perception, decision-making and behaviour” (ADAMSKY, 2018, p. 48).

Chinese dissuasion doctrine uses the term *weishe*, often translated in English as “deterrence”. It is defined by *The Science of Strategy*, published by the Chinese Academy of Military Science, as “a country or a political organization using the display of the intent to use force or the display of the intent to prepare to use force to force an opponent to yield to its will so that it does not dare conduct operations or escalate its military posture”, having two basic applications: preventing an enemy from taking an action (deterrence) and forcing an enemy to take an action (compellence); hence, *weishe* is better translated as coercion (POLLPETER, 2015, p. 147). There is also a suggestion for replacing coercion with a strategy of influence, seeking “to both deter an enemy and dispel its concerns by convincing other countries that China does not plan to violate their major interests” and seeking “to establish mutual benefit for all parties concerned through political mutual trust, economic cooperation, dialogue, and military exchanges” (POLLPETER, 2015, p. 148).

Chinese military strategy is primarily offensive, and the People’s Liberation Army (PLA) guideline favours ‘active defence’ “best thought of as a politically defensive, but operationally offensive strategy in which China will rhetorically maintain a defensive posture up until the time it decides to attack” (POLLPETER, 2015, p. 141). Accordingly, for “protecting China’s interests”, “the full range of offensive actions, including pre-emptive strikes, is permissible” (POLLPETER, 2015, p. 141). Besides, “operations should involve the strongest first strikes possible against key targets”, “to counter a future enemy that is predicted to be stronger than the PLA” like the USA, “achieving victory through surprise by striking at an unexpected time and place” (POLLPETER, 2015, p. 142). Thus, a very aggressive posture.



Moreover, as in the Western approach to coercion, Chinese analysts also consider capability, will, and signalling as elements of it, from which “capability and will are the most important and are described as the two ‘wings’ of coercion” (POLLPETER, 2015, p. 148).

#### **4.9 Dissuasion in the Brazilian Doctrine**

Schelling claimed that “A difficulty with our [the U.S.] being an unaggressive nation, one whose announced aim has usually been to contain rather than to roll back, is that we have not settled on any conventional terminology for the more active kind of threat” (SCHELLING, 2008, p. 71).

When considering the U.S. an “unaggressive nation” he was referring to the use of military force for conquering territorial gains, precisely what his ‘Coercion Theory’ intend to avert in the case of the USSR. Interestingly, Schelling mentions that the Mexicans conceded Texas, California and New Mexico the U.S. after Mexico City was held hostage in the hands of the Americans in 1848, in the Mexican-American War (SCHELLING, 2008, p. 32). Not surprisingly, he did not mention that Texas, California and New Mexico are the names the Mexicans used for their provinces, which correspond to the U.S. states of Texas, California, New Mexico, Arizona, Nevada, Utah and large parts of Colorado and Wyoming. Schelling also did not mention that while the three Mexican provinces corresponded to almost half of Mexico, historians argue that the treaty of Guadalupe-Hidalgo, which officially ended that war, was delayed by a long discussion in the U.S. Congress on the possibility of the “all-Mexico” annexation (NUGENT, 2009, p. 187–220).

Schelling also disregarded the Spanish cession of Puerto Rico and Guam, as well as the transfer of Cuba and Philippines’ sovereignty to the U.S. after the Spanish-American War in 1898 (NUGENT, 2009, p. 283–295).

Nevertheless, suppose this curriculum qualifies a nation as unaggressive and justifies the problem of having “not settled on any conventional terminology for the more active kind of threat”. In that case, the situation is even worse in the case of non-aggressive nations like Brazil.

Coercion has not a well-established and uniform body in the Brazilian military doctrine. There are just a few sparse definitions that conflict among them and with the international literature on the subject. Brazilian top-level defence documents are National Policy of Defence (PND) and National Strategy of Defence (END). In Brazil, due to political and historical reasons, National has to be the Policy or the Strategy, not the defence (MALAGUTTI, Marcelo, 2021). PND and END mention ‘dissuasion’ twenty times, ‘dissuasive’ and ‘dissuade’ once more each. Not a single reference to compellence can be found.

The National Strategy of Defence<sup>3</sup> (END) defines “dissuasion” as follows

DISSUASION - Strategic attitude that, through means of any nature, including the military, aims to advise or divert opponents, real or potential, from possible or presumed warlike purposes. Same as DETERRENCE. (BRASIL-MD, 2020b, p. 76)

It shall be noticeable that the Portuguese language does not have a word for deterrence, which is translated as *dissuasão* (as well as dissuasion). So, the text implements a neologism (*deterrença*). Albeit, this attempt fails conceptually, since the idea of “advise or divert” “through means of any nature, including military” characterises, indeed, dissuasion, and not deterrence. Thus, the equivalence is unnecessary and imprecise.

Interestingly, END also defines “dissuasion capability” as “an essential factor for National Security, as it aims to discourage possible aggressions. It is supported by the conditions that the Nation has to gather and apply its Capacities of Protection and Prompt Response, in the case of possible hostile actions against the sovereignty and legitimate interests of Brazil” (BRASIL-MD, 2020b, p. 75, free translation). Here it is clear that the meaning of dissuasion is that of deterrence, since connected to Protection and Prompt Response of military nature. Thus, there is either ambiguity or confusion concerning the concepts.

The Brazilian Army *Strategy Manual* considers that States have three forms of conflict resolution: persuasion, dissuasion and coercion (BRASIL-EB, 2001, p. 2–5). Persuasion is considered “a non-violent form that uses processes and techniques inherent to diplomatic, legal and political means” (BRASIL-EB, 2001, p. 2–5, free translation). The long list of diplomatic, legal and political means indicates ‘negative’ influence, in the sense of averting an action, thus ‘dissuasion’, and not ‘persuasion’. Then, it states:

Dissuasion - It is an intermediate form between Persuasion and Coercion, which has been present since peacetime, consisting of measures of a military nature, which will discourage the opponent from taking actions that lead to an escalation of the crisis. The following examples can be cited: deployment of military units, military manoeuvres, increased military presence in the area where the crisis occurs. (BRASIL-EB, 2001, p. 2–5, free translation)

This definition differs from that stated by the END, even though END already used that definition since at least 2016. Besides, all examples cited refer to the classic concept of preparation for ‘deterrence by denial’ or, as already demonstrated, ‘dissuasion by denial’.

---

<sup>3</sup> In Brazil the name denotes that national is the strategy, not the defence, in opposition to the case of the U.S., where it is named National Security Strategy.

Finally, ‘coercion’ is defined as “a violent form of conflict resolution, through the use, at a varying level, of the national power to coerce” (Brasil-EB 2001, 2–5). Besides, it states that any form of power available can be used, and cites examples of coercive actions out of the military spectrum: “the expulsion of diplomatic agents; the rupture of diplomatic relations; the ban on the use of air, sea or land space; embargoes and boycotts; freezing of assets; international campaigns, etc.” (BRASIL-EB, 2001, p. 2–5, free translation). Hence, it includes non-military (non-use-of-force) alternatives, thus escaping from the concept of Coercion Theory.

Besides, another concept is presented:

Direct Threat - Applies when one of the opponents has considerable superiority of means over the other (or can achieve it through alliances) and the objective pursued is modest (of no strategic value or little importance to the opponent or its allies). In this case, the simple threat of using military power can lead the opponent to accept the conditions imposed on him or to renounce his pretensions. It is the basis of deterrence/dissuasion. (BRASIL-EB, 2001, p. 2–6, free translation)

The described scenario points to ‘coercion’ (as compellence + deterrence), as denoted in the passage “the simple threat of using military power can lead the opponent to accept the conditions imposed on him or to renounce his pretensions”. However, it points to using it only when there is enough superiority or when objectives are modest. A clear signal of low interest in military engagement, thus with low credibility.

The manual also describes what it calls ‘Dissuasion/Deterrence Strategy’. The description is focused on the availability of enough “powerful military means, ready for immediate engagement, capable of countering any threat” (BRASIL-EB, 2001, p. 3–11). Such a ‘strategy’ is virtually impossible, since resources are, inevitably, scarce for such a challenge. The description briefly, and correctly, also describes deterrence as based on credibility and communication (signalling), and that “dissuasion/deterrence cannot be a bluff”. Nonetheless, there is no description of any of these concepts. Moreover, it poses three other ideas: “defensive dissuasion”, related to defence, resilience, and counter-strike; “offensive dissuasion”, as having powerful enough forces to dissuade the enemy of attacking; and “irregular warfare” capabilities in the long-term as also exerting a dissuasive effect. All three cases connect only with ‘deterrence by denial’ at best. Finally, it states that “whatever the nature of dissuasion, it is intended to avoid armed conflict” (BRASIL-EB, 2001, p. 3–11).

#### **4.10 The Blossom of ‘Causation Theory’**

As exposed, ‘Deterrence’ cannot describe all of the available dissuasive tools and must be replaced by the broader concept of ‘dissuasion’. Moreover, ‘Influence’ is more general than

‘Causation’, the subject of dissuasion (and thus deterrence, as dissuasive threats) and Persuasion (including Compellence, as persuasive threats).

If one is interested in just averting undesired actions, ‘Dissuasion Theory’ would, apparently, be enough. However, Dissuasion by Entanglement demands the existence of a previously built entanglement, while Dissuasion by Norms requires norms to be beforehand construed among States.

Therefore, a long-term strategy of dissuasion may depend on a previous work of Persuasion. And it would be naïve to believe that this would be exclusively based on persuasive threats (Compellence). Above and beyond, Article 52 of the 1969 Vienna Convention on the Law of Treaties expressly states that treaties made under coercion are void (UNITED NATIONS, 1969).

Realists tend to belittle norms saying that they “merely prohibit what states did not want to do anyway” (PRICE; TANNENWALD, 1996, p. 115). The reality, nevertheless, is much more complicated.

The 2001 Convention on Cybercrime (the Budapest Convention) reached 64 ratifications. Excluding Russia, Ireland and Sweden, all other 44 members of the Council of Europe (EC) acceded it, plus non-EC member countries as the USA, Canada, Japan, Australia and Argentina (COUNCIL OF EUROPE, 2019).

None of the BRICS has yet joined the Budapest Convention (South Africa signed, but not ratified). Brazil has been plagued for cybercrime for years (BRASIL-GSI, 2019). Despite, it was only in December 2019 that Brazil announced it started its accession to the Convention (BRASIL-MRE; BRASIL-MJSP, 2019). Historically, Brazil used two arguments to justify not joining the Convention. First, that “Brazilian foreign policy privileges agreements whose drafting Brazil participated in, to place our brand, our interest” (VITAL, 2008, free translation). This reflects a legitimate concern with the dominance of the great powers in the debate, which is explicit in the statement by the then-Secretary for Combating Transnational Offenses of the Brazilian Ministry of Foreign Affairs:

In a way, there is a democracy of vulnerability. Both developed and developing countries are in the same pattern. In this sense, Brazil intends not only to react, but to make its own proposals, so that more technologically developed countries do not dominate the debate. (BOL, 2011)

This argument is consistent with the notion that treaties are ‘one’, and not ‘the’ product of international negotiations; another product is the negotiation process itself; “The journey matters as much as the destination” (FINNEMORE; HOLLIS, 2016, p. 429). In this process, several components take part: “incentives”, such as favourable trade agreements; “coercion”,

in the form of bribes or threats; “persuasion”, in the search for changing attitudes; and “socialisation”, when countries with asymmetric capacities are considered as equals whose opinion has value (FINNEMORE; HOLLIS, 2016, p. 447–51). In other words, some countries intend to become ‘norm-makers’ instead of only ‘norm-takers’ (REILLY, 2012).

The second argument was that “what matters primarily is our internal legal system” (VITAL, 2008, free translation). It reflects a concern with the internal stabilisation of cybercrime before acceding international conventions or recognising their validity, probably related to formal accountability or designation as a ‘sanctuary’. The official note itself nods in this direction when declaring that “Brazilian accession initiative to the Budapest Convention comes in addition to Law 12,965/2014, named *Marco Civil da Internet*, for the criminal prosecution of cybercrimes” (BRASIL-MRE; BRASIL-MJSP, 2019).

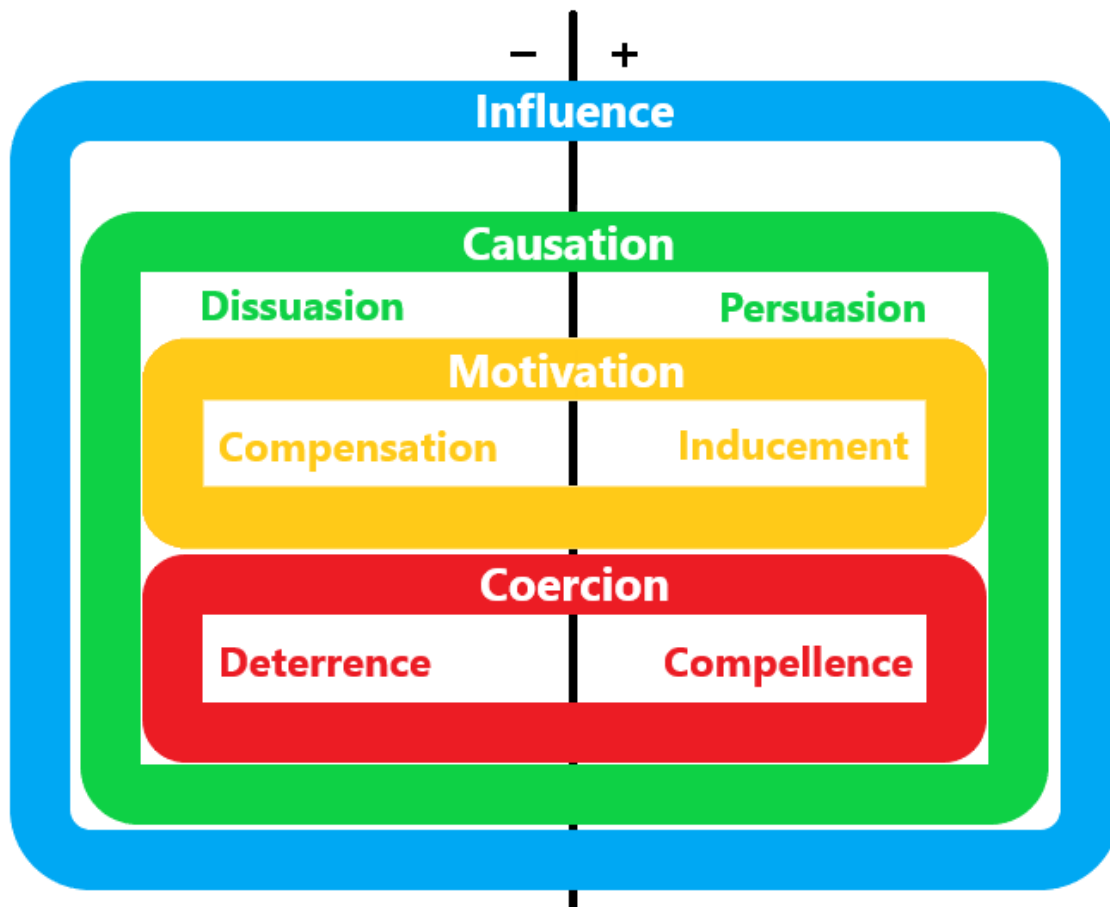
There were no known threats involved in promoting the accession of Brazil. Oppositely, there was fear of acceding and ‘then’ incurring in accountability. Besides, persuasive attempts were made from both sides. And there was a clear claim for ‘socialisation’. Therefore, a typical constructivist approach, rather than a realist one. The above is but one example, among many possible ones.

It is somewhat revealing that only the coercive part of influence (based on threats of use of force) has been named and became internationally well known, discussed and formalised. To fill the gap, for influence based on promises I propose the use of the term “Motivation”, since ‘to motivate’ means “be the reason for somebody’s action; stimulate the interest of somebody” (OXFORD DICTIONARY, 1992, p. 808). Its positive part (persuasive promise) shall be called “Inducement”, meaning “to do something that which persuades; incentive”, and derived from the verb ‘to induce’: “persuade or influence somebody to do something” (OXFORD DICTIONARY, 1992, p. 636). The negative part of ‘Motivation’ (dissuasive promise) is harder to name adequately with a single word. Nonetheless, “Compensation” seems a good option, since connected with the verb ‘to compensate’, which means “give somebody something good to balance or lessen the bad effect of damage, loss, injury, etc; recompense” (OXFORD DICTIONARY, 1992, p. 235). In this case, the influenced would be compensated for not doing something he would rather do.

Figure 2 provides a graphical view of the inter-relation among the different sets of instruments that constitute the influence toolbox.

In this work, the positive side of Causation will not be considered from now on. The focus will be on its negative part, dissuasion, comprehending deterrence and compensation.

Figure 2 – Graphical View of the Context of Causation



Source: Compiled by the author

#### 4.11 Conclusion

Coercion Theory (or Deterrence Theory) is not adequately applicable to the post-Cold War context, since centred exclusively on the use of military might for influencing nations. A broader theory is necessary, considering the more general spectre of types of dissuasion available to countries. Conversely, Influence Theory has an excessively larger amplitude. In this Chapter, I have planted the seeds for a debate regarding the prospects of what I called Causation Theory, standing between Coercion Theory and Influence Theory, whilst focused on inducing or averting ‘actions’, not behaviours. It could, indeed, be the case of using the neologism ‘Causaction’ for naming it. Nevertheless, any attempt to influence actions causing the desired action must consider both positive and negative causation. This is particularly relevant when considering dissuasion in cyberspace, as it is discussed in Chapter 5.

## 5 ON ‘CYBER-DISSUASION’

This chapter analyses the application, cyberspace, of the different dissuasion types identified in Chapter 4. Their constituent elements are studied in light of the different views that permeate the current debate in the international academic environment, considering the technical, political and economic difficulties of implementing each of these various forms of dissuasion.

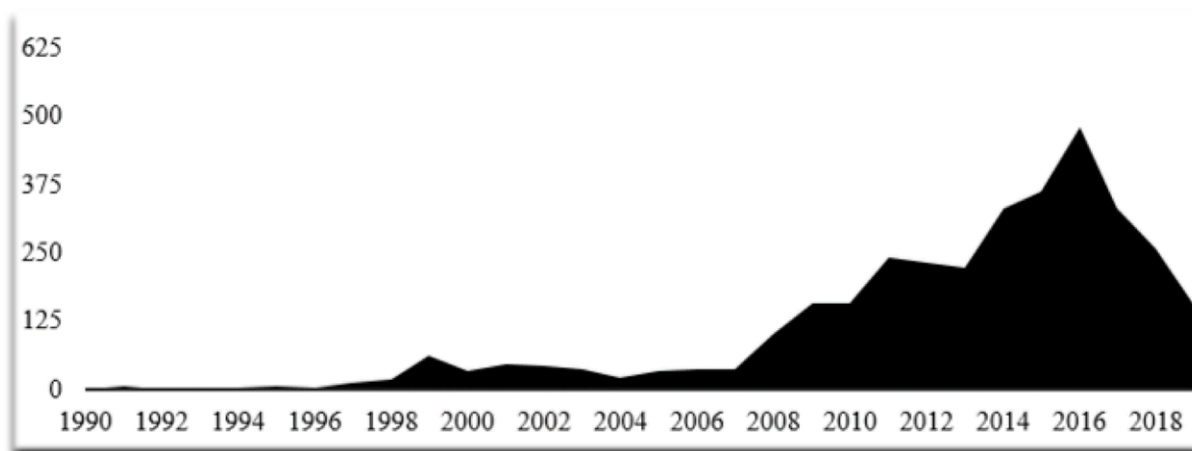
### 5.1 Introduction

Analysing ‘Deterrence Theory’ writings, Jervis (1979) identified three waves of deterrence theory.

Although the first wave, which came and went in the early years of the nuclear era, had little impact, the ideas of the second wave, which crested in the late 1950’s, soon became conventional wisdom even though there was little evidence for the validity of the propositions. Indeed, until the third wave, in the 1970’s, there were few calls for verification. (JERVIS, 1979, p. 289)

In comparison, Nye claimed that “theorising about deterrence in the cyber era is emerging from only its first wave” (NYE, 2017, p. 46). Research on ‘cyber-deterrence’ started as early as in the 1990s, “nurtured by the U.S. Department of Defense in numerous wargaming exercises” (SMEETS; SOESANTO, 2020). From 2008 to 2016 the theme grew on academic interest, but then this interest seemed to evaporate. Difficulties in applying the traditional deterrence elements, vastly presented in the available literature, helped make the concept fall “out of fashion” (SMEETS; SOESANTO, 2020).

Figure 3 – Evolution of the Number of Publications on Cyber-Deterrence (sic)



Source: Smeets and Soesanto (2020)

Many E.U. member-states adhered to the U.S. characterisation of cyberspace as a war domain that need cyber-dissuasion. Albeit, they have two large concerns regarding the U.S. concept of persistent engagement. First, they perceive it as “overly aggressive”; second, they think it is quite improbable that European military cyber organisations could have the resources it demands (SMEETS; SOESANTO, 2020). Due to these limitations, the authors claim that “E.U. member states will have to fill this strategic vacuum with creative conceptual thinking” (SMEETS; SOESANTO, 2020).

The authors’ “Eurocentric” finding can be replicated for all non-European middle powers. Still, it will demand even more creativity from those with a non-aggressive tradition, since, without being able to resort to the use of force due to their cultural limitations, they have to give up the ‘threat of retaliation’, the basis of most writings on cyber deterrence.

Dissuasion in the cyber realm differs from nuclear deterrence in some aspects; cyber “demands a focus on actors, rather than weapons/capabilities alone; hence prioritising these actors according to the scope, scale, and nature of the threat that they pose is critical” (CILLUFFO e colab., 2012, p. 5, 6)

## 5.2 The Need for Cyber-Dissuasion

The fall of the Berlin Wall (1989) and the end of the Soviet Union (1991) marked the end of the Cold War. With it, the fear of nuclear war has decreased significantly. Just two years later, Arquilla e Ronfeldt (1993) declared “Cyber War is Coming!”. Since then, the fear of “cyberwar” takes on more and more space every day in the popular imagination, in the media, in policymaking and academia, concerning what would be a cyberwar and if it would occur (CLARKE; KNAKE, 2010; STONE, 2013) or not (RID, 2012).

Meanwhile, post-industrial society’s advancement has accelerated digital inclusion (BELL, 1976; TOFFLER, Alvin, 1980). The rapid expansion of the Internet worldwide, making computers more and more pervasive and ubiquitous has created a new space: cyberspace. It also generated a *Powershift* in societies worldwide and a *Revolutionary Wealth*, with new means of producing goods and services (TOFFLER, Alvin, 1991; TOFFLER, Heidi; TOFFLER, 2006).

At first, the advance of cyberspace seemed to indicate that national borders could “blur”, as well as the idea of national sovereignty. This perception was reinforced by the globalisation of financial operations, with trillions of dollars flowing through computer networks daily, from one ‘corner’ of the world to another. However, in recent years, the development of cyber power and its use now suggests that it is becoming “just” one more statecraft tool, with extensive



potential use for inter-state influence and coercion. Thus, it presents itself as an object of study of geopolitics, in the sense of “the study of the spatialisation of international politics by core powers and hegemonic states” (TUATHAIL; AGNEW, 1992, p. 192).

Therefore, cyberspace influence operations demand attention from academia, policymakers, and society in general. However, research is still in its infancy, as well as the collection of empirical evidence regarding cyber-conflicts and influence attempts. Thus, “the answer to the question of whether deterrence works in cyberspace is ‘it depends on how, who, and what’” (NYE, 2017, p. 68). “Ironically, deterring major states like China from acts of force may be easier than deterring nonstate actors from actions that do not rise to the level of force” (NYE, 2016).

### **5.3 National Security and Cyberspace**

Communications intelligence has always played an essential role in security and defence issues. Signals Intelligence (SIGINT) has become increasingly relevant with the popularisation of telecommunications, and even more critical for the military. At Bletchley Park, in 1941, Alan Turing and his team created “the Bombe”, the first computer in history. Albeit electromechanical, it helped to decipher the Enigma code used by Nazi armed forces. Just two years later, at the same location, Tommy Flowers’ team created Colossus Mark I, the first electronic computer, which cracked the top-secret Lorenz code. Both were essential assets for allied victory in World War II (GCHQ, 2016).

Besides its use for SIGINT, automated information processing was also relevant for other military activities. Also in 1943, the American army commissioned the University of Pennsylvania to develop a machine capable of computing ballistic targets, resulting in the development of ENIAC, the first programmable electronic computer, delivered in 1946 (RID, 2016, p. 114–115).

The fear of a repetition of the Blitz (London bombing during WWII) in North-American territory led to the creation of the Semi-Automatic Ground Environment (SAGE), integrating hundreds of radar stations with processing in 23 supercomputers distributed throughout the USA, whose prototype was demonstrated as early as 1951 (RID, 2016, p. 76–77). The system was contracted to IBM and used commercial communication lines from AT&T to integrate the entire network, at the total cost (in 15 years), of more than 500 billion dollars in current values. In 1958, SAGE was centralised in the mythical North-American Air Defence Command (NORAD) in Colorado (RID, 2016, p. 76–77). Similarly, through the Advanced Research Projects Agency (ARPA), the Pentagon funded the development of ARPANET, the “famous

precursor to the Internet” (RID, 2016, p. 111). The goal was to improve military command and control systems and provide route redundancy in the event of a network node failure (RID, 2016, p. 147).

In Brazil, the development of information technology was also linked to military interests. It was under the influence of the ideas of Lieutenant Commander Geraldo Maia, who had returned from the USA, that the National Development Council of President Kubitscheck’s Administration proposed creating a group to evaluate the use of computers in the country (MOREIRA, 1995, p. 24). The following year, the team became the Executive Group for the Application of Electronic Computers (GEACE) and authorised the import of the first three Brazilian computers: one for the Pontifical Catholic University of Rio de Janeiro; one for the Brazilian Institute of Geography and Statistics (IBGE); and one for the company *Listas Telefônicas Brasileiras* (Brazilian Telephone Lists) (MOREIRA, 1995, p. 23).

In 1972 the Coordination of Activities for Electronic Data Processing (CAPRE) was created, under Ministry of Planning (FIGUEIREDO, 1986, p. 288; MOREIRA, 1995, p. 24; TONOOKA, 1992, p. 274–276). CAPRE was given responsibility for developing a national I.T. policy, and one of its first determinations was the restriction on the import of foreign hardware by governmental institutions (FIGUEIREDO, 1986; MOREIRA, 1995; TONOOKA, 1992, p. 274–278). A 20-year market reserve had started. In 1979 CAPRE was replaced by the Special Secretariat of Informatics (SEI), then under the National Security Council, and strongly influenced by the National Information Service (SNI), Brazilian intelligence agency at that time (MOREIRA, 1995, p. 28–29; TONOOKA, 1992).

In 1984, the Informatics Law (Lei de Informática)<sup>4</sup> was approved. It established the National Informatics Policy, by which only hardware and software products Made in Brazil (or authorised foreign ones) could be marketed (similar to the “Buy American Act”, but exclusively for the I.T. market). The idea was to create a market aimed at developing a national industry that could be internationally competitive. The model adopted was based on three pillars: staff training; stimulating private investment; and a state-owned company, *Computadores Brasileiros* (COBRA). However, such efforts were unsuccessful, and even counterproductive, given that they submitted the country to a considerable delay in the adoption of new technologies that quickly emerged in the foreign market, but that did not enter Brazil, and the high values that national users paid for products compared to international prices (MOREIRA,

---

<sup>4</sup> Law 7,232/1984.

1995; TONOOKA, 1992). In 1993, with the end of the market reserve, Brazilian companies opted for the licensing of foreign products.

#### **5.4 Cyber-Power and Causation Operations**

The concept of power in inter-nation politics and strategy is one of influence (including coercion) for changing others' behaviour and actions (BETZ; STEVENS, 2011, p. 42; SINGER, 1963, p. 420). 'Cyber War' (or cyberwar), is a catchy term, and has become popular, sometimes used even by the Secretary-General of the U.N. (GUTERRES, 2018; KHALIP, 2018). Nonetheless, characterising cyberattacks as acts of war is almost impossible in light of current concepts and cases. Most of the state-sponsored cyberattacks depicted in the media are, in fact, influence attempts carried by nations against their peers, contemporarily classified as grey-zone operations, designed for causation (persuasion or dissuasion), below the threshold of war.

To better understand these operations, it is necessary to know how some fundamental concepts apply (or are applied) in cyberspace. The first group of them is not inherent to Causation Theory but affects States' behaviour in cyberspace. The second group is that of Causation Theory concepts.

##### **5.4.1 General Concepts**

###### **5.4.1.1 Sovereignty**

The fast expansion of cyberspace brought with it a perception of freedom and spatial proximity never before experienced. It is almost instantly possible to visit a museum in France and a library in Italy, watch a popular festival in India, and buy books in the U.S. or electronic goods in China. The Internet, conceived as a resilient communications alternative in case of nuclear attacks, was thought to make communication untraceable, and thus beyond state control or censorship. The use of 'avatars' (virtual images and id's) would hide users identities, providing a sense of anonymity (and impunity from wrongdoings). "Somewhat romantic e-libertarians suggested cyberspace would allow users to stay away from the real-world dystopia, which imprisons and oppresses everyone. It seemed to offer a quasi-utopia, the unachievable perfect world" (MALAGUTTI, Marcelo, 2017b, p. 10). Cyberspace would be entirely disconnected from the real world, whose norms would not apply there. When President Bill Clinton Administration sanctioned the Telecommunications Act of 1996, John Perry Barlow reacted publishing his iconic *A Declaration of the Independence of Cyberspace* (BARLOW, 1996; RID, 2016, p. 244–245). "For the most part, though, this notion is a myth. States can and do control cyberspace when it suits them, often with a heavy hand (FINNEMORE; HOLLIS, 2016, p. 459–60).

The concept of sovereignty is well defined in international law since the Island of Palmas Case, in 1928: “Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State” (HUBER, 1928, p. 838). One of the “functions of a State” expressly manifest is that of the application of the law.

“The fact that the regulations for Tabukan are, by an express provision, declared applicable to the “islands of Nanusa and Meamgy thereunder included” proves that an island of the later name was known and deliberately treated as belonging to the vassal State of Tabukan” (HUBER, 1928, p. 863).

The application of the concept of sovereignty regarding cyberspace has different interpretations. While the United Kingdom disregards the nature of sovereignty in cyberspace, France defined it clearly considering that any attack to hardware, software or data resident in French territory is an attempt against their sovereignty (MINISTÈRE DES ARMÉES, 2019, p. 6–7; WRIGHT, 2018). The Netherlands goes with Rule 4 of the Tallinn Manual: “a violation of sovereignty is deemed to occur if there is 1) infringement upon the target State’s territorial integrity; and 2) there has been an interference with or usurpation of inherently governmental functions of another state” (MINISTRY OF FOREIGN AFFAIRS OF THE KINGDOM OF THE NETHERLANDS, 2019, p. 64). Australia advocates for sovereignty over information and communication devices located within its territory, and claims that these shall not be used to violate the rights and obligations of another nation, even for attacks passing thru it (DEPARTMENT OF FOREIGN AFFAIRS AND TRADE, 2017, p. 91).

U.S. positions are somewhat controversial. In 2012, the Department of State Legal Advisor Harold Koh claimed that “states conducting activities in cyberspace must take into account the sovereignty of other States, including outside the context of armed conflict”. Moreover, the “physical infrastructure that supports the internet and cyber activities are generally located in sovereign territory and subject to the jurisdiction of the territorial State”. Conversely, in 2016, his successor, Brian Egan said that “remote cyber operations involving computers or other networked devices located in another State’s territory do not constitute a *per se* violation of international law” Furthermore, “any regulation by a State of matters within its territory, including use of and access to the internet, must comply with that State’s applicable obligations under international human rights law”. Accordingly, the engagement in espionage acts is not considered a violation of sovereignty. (MALAGUTTI, Larissa, 2020, p. 22)

Schmitt (2019) argues that the U.K. “will presumably proffer a relatively low threshold for what constitutes coercion, as it must to compensate for its dismissal of sovereignty as a primary rule of international law” regarding cyberspace.

#### 5.4.1.2 Weapons

Cyber-weapons present a distinctive characteristic compared to conventional weaponry. For the other domains of war (land, air, sea and space) the distinction between offensive or defensive armaments is practically non-existent. In general, when defensive capabilities develop, offensive ones also develop. For example, an armoured vehicle, a combat aircraft, or a submarine can be used for both defence or offence.

In cyberspace, however, the distinction between an offensive or defensive weapon is often quite striking. Indeed, these mostly “mainly software” weapons, “though at times hardware as well”, can be divided into three groups (TABANSKY, 2011, p. 80):

- a. Unequivocally offensive weapons: different types of malware (viruses, worms, Trojan horses, logic bombs, and the like); denial of service actions.
  - b. Dual-use tools: network monitoring; vulnerability scanning; penetration testing; encryption; and camouflage of content of communications.
  - c. Unequivocally defensive tools: firewall, disaster recovery systems.
- (TABANSKY, 2011, p. 80)

Hence, a “cyberweapon” like Stuxnet will always be offensive, never defensive. Conversely, an intrusion detection system (IDS) or anti-virus will always be defensive, never offensive. Even the development of defensive systems does not demand the development of offensive capabilities to test them, since it is possible to use the already existing and documented threats to test defensive systems.

There is a fanciful claim that “in the cyber realm, the difference between a weapon and a nonweapon may come down to a single line of code, or simply the intent of a computer program’s user” (NYE, 2019). Albeit, there is no evidence to support it. It does not apply even to the “dual-use” group proposed by Tabansky, since they are ready to be used, and do not need to have their code altered a single line to be used for their purposes.

One could argue that a small change in a defensive tool like an anti-virus or IDS, inserting a backdoor, could facilitate offensive operations, diluting the distinction between offensive and defensive weapons. However, such a backdoor is just a vulnerability, not a weapon in itself. It makes exploitation and attacks feasible, but does not constitute them. In the kinetic world, it is the equivalent to the knowledge of a vulnerability in a defensive fortification or radar system, which to be explored will require specific offensive capabilities and preparation. For example, Eben-Emael, the formidable Belgian fortress, was considered virtually impregnable from an external frontal attack, but it was vulnerable to an attack from “above”. Thus, the Germans used airborne assault troops as an “offensive weapon” to exploit

that vulnerability, silently invading it from above and dominating it from within, on a mission designed and trained specifically for that purpose. Similarly, only an attack tool explicitly intended as an offensive weapon can exploit a specific vulnerability. In other words

Once in, you need a tailored tool to create the desired effects. Very often this has to be a handcrafted tool for the specific target. It is not the same as cranking out five-hundred-pound bombs and putting them on the shelf with their laser guidance kits. (HAYDEN, 2016, p. 145)

Moreover, offensive software ‘weapons’ (malware) involve thousands of lines of code designed to reach specific purposes and exploit particular vulnerabilities. And the number of lines of code is growing with their greater complexity. Until 2005, “most samples contain several thousand SLOCs [source lines of code]”, with a few over a dozen thousand; from 2007, counts are in the range of tens of thousands: GhostRAT (33,170), Zeus (61,752), KINS (89,460), Pony2 (89,758), or SpyNet (179,682). Most samples correspond to moderately complex malware (CALLEJA e colab., 2016, p. 10–11). Even the upgrades from one version to another can reach 4,600-9,000 lines (LINDORFER e colab., 2012, p. 9). Stuxnet was estimated having circa 15,000 lines of code, mostly written in C++, for exploiting five 0-day and one non-0-day vulnerability (FALCO, 2012, p. 7;20).

As for defensive software weapons (anti-virus, IDS, firewalls, etc.), they also constitute complex software projects, and it is not reasonable to suppose their size would be smaller. But instead of exploiting vulnerabilities, they search for patterns and control access to resources. Hence, it is not plausible to suppose that, changing “one single line of code” would alter their nature. In fact, even a direct and straightforward backdoor, easily identifiable, cannot be implemented with one single line of code. And it does not configure a change of behaviour. It merely opens a vulnerability.

Similarly, one line of code can cause an error, and this might (or might not) be discovered and used as a vulnerability. To be exploited, such vulnerabilities demand complex software, probably with thousands of lines of code, which might address their specific characteristics. Moreover, the opposite logic, e.g., transforming a malware in defensive software, is even harder to imagine feasible altering a single line.

Cyber-weapons also have an “ephemeral nature” (MALAGUTTI, Marcelo, 2016c, p. 278–9). A brief and simple explanation can be as follows:

To attack a target, you first have to penetrate it. Access bought with months, if not years, of effort can be lost with a casual upgrade of the targeted system, not even one designed to improve defenses, but merely an administrative upgrade from something 2.0 to something 3.0. (HAYDEN, 2016, p. 145)

Another problem lies in the “normalisation” of some practices in the cyber context that are contrary to international custom regarding armed conflicts (LIBICKI, 2019). Literature is full of different threat names: viruses, worms, botnets, Trojan Horses, malware, ‘rogue code’, logic bombs, and so on. But they all have two things in common: they consist of software, and they need to be “implanted” (installed) in advance on the target networks. Generally, malware implantation takes weeks, even months, in advance for a relevant cyberattack to be successful.

In June 2019, an international crisis was unfolded when Iran seized a British oil tanker in the Persian Gulf. The Royal Navy immediately sent a war vessel to prevent subsequent seizures of British ships, in an attitude easily characterised as self-defence under current international norms. Subsequently, it was revealed that the USA carried out cyberattacks that damaged the database used by the Iranians to carry out the arrests, even though no USA vessel had been affected (BARNES, 2019). The database hack itself configures a preventive action. And it probably demanded the use of implants deployed long before.

#### 5.4.1.3 Anonymity & Attribution

It is relatively easy to attribute a military operation to a particular country and then to initiate a counter strike, and having enough power, eventually overwhelm and defeat the attacker. Albeit nuclear attribution is imperfect, just a few states have nuclear weapons, their isotopic identifiers are relatively well known, and non-state actors face high entry barriers (NYE, 2015a).

However, precise attribution in cyberattacks is not easy (BUCHANAN; RID, 2014; CARR, 2015). The higher the quality demanded, the longer it takes and costly it becomes. As forensics technology improves, governments increase their attribution capabilities, but the most accurate attributions seem to come from private security companies. Possibly because in this way governments do not have to ‘burn’ intelligence sources. In the Sony case of 2014, U.S. officials quickly attributed it to North Korea, with widespread scepticism, until weeks later a press leak revealed that the U.S. had access to North Korean networks (NYE, 2015a; U.S. WHITE HOUSE, 2015).

One of the problems of attribution is that hackers usually protect their identities using deception techniques and by mimicking tools and even the *modus operandi* of other hackers, thus making believe a different group or country made the attack, what is often named ‘false flag’ (BUCHANAN; RID, 2014, p. 19; CARR, 2015). Moreover, with a ‘false flag’ covering the actual origin of attacks, retaliation could be triggered against an innocent country.

Nevertheless, the international arena is political, not a legal one. Thus, attribution becomes a matter of degree, with each specific political moment demanding more or less

evidence. If the *cui bono* (who benefits) test points to an opponent and there are widely deemed credible rumours to support this claim, then the international community will likely support the claim of attribution, with reputational damage to the ‘attacker’ without concrete evidence (HARE, 2012; NYE, 2013). Besides, neither theory nor past practice indicates that retaliation must be applied against an attack’s actual perpetrator (MORGAN, Patrick M, 2010, p. 68–69).

As in the case of general dissuasion theory, attribution can be more or less relevant according to the specific case of attack and momentary political situation, giving some latitude to the dissuader.

While accurate attribution of the ultimate source of a cyberattack is sometimes difficult, the determination does not have to be airtight. To the extent that false flags are imperfect and rumors of the source of an attack are widely deemed credible (though not legally probative), reputational damage to an attacker’s soft power may contribute to deterrence. (NYE, 2013)

#### 5.4.1.4 Asymmetry<sup>5</sup>

‘Asymmetrical warfare’ is a term sometimes used to characterise “countering an adversary’s strengths by focusing on its weaknesses” (ADAMS, 2001, p. 98–99). The concept fits well in the idea of “no forced entry in cyberspace”, but merely the exploitation of enemy’s vulnerabilities (LIBICKI, 2009, p. iii; xiv). Despite, focusing on an opponent’s weaknesses would be wise in any conflict, not only in asymmetrical ones. The best definition, so, is that which considers ‘asymmetry’ as the disparity between contenders’ means.

The costs of developing conventional or nuclear forces exert a dissuasive effect, by the futility of competing with the U.S. Navy in constructing carrier task forces and submarine fleets, for instance (NYE, 2012b; RUMSFELD, 2002). The same idea applies to the development of missile defences. Entry barriers are high and demand a large spectrum of technologies, as special alloys, fuels and explosives, as well as components needed for the production and operation of small nuclear reactors for carriers and submarines.

It is easy to imagine a Stuxnet-like tool being used to disable missile defences of the U.S., Russia, China, India, or Pakistan. As Stuxnet damaged rotating mechanical parts of the Iranian centrifuges, a similar effect could disrupt the steam turbines of nuclear subs, or perhaps damage a component of difficult replacement of missiles’ launching platforms. Hence, hypothetically, a software tool whose cost would be in the tenths of millions could disabled missile defences worth billions of dollars. Perhaps not even such an “expensive” worm would

---

<sup>5</sup> Adapted and revised from (MALAGUTTI, Marcelo, 2016c, p. 277–278).



be necessary; just a simple backdoor could be used to cripple missile alert or launching systems for, say, half an hour.

The above scenario is usually associated with the concept of asymmetry related to Software Power, since entry barriers in the cyber domain are so low that become accessible to non-state actors and small states, allowing them to play a significant role at relatively low cost (NYE, 2012a).

The asymmetry is also created by the imbalance of attack space – larger, technologically dependent nations possess a larger network space with a greater number of weak spots vulnerable to attacks, while the smaller nation has a smaller network surface to protect (ARENG, 2014, p. 6).

Consequently, even though great powers make larger investments in the development of cyber capabilities, small states still have more opportunity to compete in this domain than in traditional warfare, because “in modern warfare, ‘mass’ is no longer a decisive factor”, and “asymmetric warfare dilute the traditional power and dominance logic” (ARENG, 2014, p. 11).

More to the point, it is precisely because others suffer inferiority in conventional conflict that they feel driven to emphasise cyberattacks as a way to even the score. Thus, the United States, for all its advantages, might suffer more than adversaries would if retaliation begets counterretaliation. (LIBICKI, 2009, p. 32)

Software power, so, offers means for “Lilliputian States” (as also non-state actors) to develop their capabilities and face opponents that otherwise could not be confronted (ARENG, 2014).

The asymmetry provided by cyber-capabilities, and its proliferation, might even create scenarios that “provide conventionally weaker powers with a stronger deterrent against their stronger adversaries” (LIFF, 2012, p. 411). This context could lead to a situation where, instead of war, there would be a negotiated resolution of conflicts, with stronger states offering to their adversaries a better bargain than they would otherwise have (LIFF, 2012, p. 411). To avert this possibility, and keep their advantage, stronger conventional forces invest in keeping their advantage. However, nations as Iran and North Korea have been appointed as having relevant cyber capabilities, capable of creating problems to the USA and the U.K.

#### 5.4.1.5 Culture

Dissuasion is based on the calculation of risks (costs) and gains (benefits) of attacks. These calculations are affected by perceptions. And these perceptions vary: “different parts of complex organisations (whether private bureaucracies or governments) often perceive the same

actions (and the associated costs and benefits) from very different perspectives” (NYE, 2017, p. 57, 58).

“Strategic culture”, “the contemporary organisational, ideological and political culture of a country as it affects war planning” affect the way countries “see or feel cyberspace”. Many do not do it “in the same way as the United States or even each other”. Considering these different strategic cultures, “as opposed to a near exclusive focus on their hard political objectives”, might result in a fruitful cooperative military restraint in cyberspace (AUSTIN, 2016b).

Norms and taboos can restrain behaviour in cyberspace “by imposing reputational costs that can damage an actor’s soft power beyond the value gained from a given attack” (NYE, 2017, p. 60). A possible approach to arms control in the cyber realm would be to “develop a taboo not against types of weapons but against certain types of targets” (NYE, 2017, p. 61).

Cascading cyberattacks on the national communications infrastructure during a war or in preparation for it could affect the relationship between a government and its citizens degrade the target country’s war effort in ways not yet well understood (AUSTIN, 2016b).

An essential cost, often not considered, relates to cultural values: attack tools go against the institutionalised culture of non-aggressive states. Non-aggressive states will not probably have the will, or the legal framework, to support the development, acquisition or deployment of attack tools.

## **5.4.2 Causation Theory Concepts**

### **5.4.2.1 Coercion**

Clausewitz wrote that “war is an act of force to compel the enemy to do our will” (CLAUSEWITZ, 1976, p. 75). “Coercion” is an act of force to compel the enemy to do our will by threatening war.

Although cyberattacks are not expected (at least for now) to cause massive casualties, they could still be effective means of political coercion at different levels. From a strategic perspective, they can be used to paralyse critical infrastructures, while from a tactical one, they can be used to damage or incapacitate military and intelligence systems (LIFF, 2012, p. 403). From an operational point of view, the U.S. Defense Logistics Agency established that cybersecurity constitutes a significant risk that imposes severe challenges on military supply chains at all times (DEFENSE LOGISTICS AGENCY, 2015, p. 7).

There are various illustrative cases of cyber-fuelled coercion. Distributed Denial of Service (DDoS) attacks, attributed to Russia, were carried out against Estonia in 2007 and

against Georgia in 2008. In the Estonian case, attacks initiated when the Estonian government decided to move a statue representing the Soviet Soldiers dead for freeing Estonia from Nazi domination from the central area of Tallinn to the city's outskirts. In Georgia's case, the defence command and control system was closed, and the military forces of that country could not even react to the Russian kinetic military invasion of its territory (CLARKE; KNAKE, 2010).

In 2010, the Stuxnet malware, allegedly developed by the U.S. and Israel, damaged the cascade of centrifuges for uranium enrichment at the Natanz Nuclear Plant in Iran, allegedly delaying that country's nuclear program by years and coercing it to accept an agreement for international supervision of that program (FALLIERE e colab., 2011; TED, 2011; ZETTER, 2014).

In December 2015, in the middle of European winter, Ukrainian power companies suffered a cyberattack that caused the interruption of energy supply in much of that country (AUCHARD; FINKLE, 2016; DRAGOS, 2017; ZETTER, 2016).

One of the difficulties in cyberspace influence operations resides in determining if an attempt produced the desired results (LIBICKI, 2009, p. 54). Except in Stuxnet's case, there are no indications that the other cited cases resulted in the desired actions.

#### 5.4.2.2 Resilience

Resilience, in cyberspace, consists of actions aimed at increasing the capacity to resist the attacker's advance in the defended cyberspace. It stems from the understanding of the impossibility of guaranteeing total effectiveness in protection actions. One of the central objectives of resilience is to keep attacked systems operating, even if degraded. Another one aims the recovery of affected systems in the shortest possible time. Often these objectives conflict with each other, since the restoration of the system's normal condition may imply the temporary suspension of its degraded operation during the process of its restoration (AMIN NAVES; MALAGUTTI, [S.d.]).

Examples of actions for increasing cyber-resilience include classic file backups, network and server redundancy and replication, virtualisation of servers, processing and network load balancing, monitoring and restoration of settings and applications altered without proper authorisation, and the use of "cloud" based services (AMIN NAVES; MALAGUTTI, [S.d.]).

Libicki (2009, p. xv) stated that when systems are attacked, revealed vulnerabilities are repaired or circumvented, becoming more secure and resilient, culminating in a society more resistant to future coercion attempts. Albeit, this is true only if the attack is discovered.

#### 5.4.2.3 Signalling

Dissuasion depends on the perceptions of both the dissuader and the dissuaded and the ability to clearly communicate these perceptions (NYE, 2017, p. 53). The U.S., for example, declared it intends to use “a nuanced and graduated declaratory policy and strategic communications” to highlight its “commitment to using its capabilities to defend against cyberattacks”, while remaining “ambiguous on thresholds for response and consequences to discourage pre-emption or malicious cyber activities just below the threshold for response” (U.S. WHITE HOUSE, 2015, p. 13). This declaratory policy “has made clear that deterrence is not limited to cyber against cyber (though that is possible), but can be cross-domain or cross-sector with any weapons of its choice, including naming and shaming, economic sanctions, and nuclear weapons” (NYE, 2017, p. 63).

In the realm of conventional capabilities, a military parade provides the opponents with a reasonable understanding of the power of offensive and defence means. Considering the long lifecycle of weapons, they shall still present dissuasive value for two or three decades. Positioning these means provide some insight regarding ‘will’ and ‘resolve’. And historic behaviour provides for credibility.

It is much more complex in cyberspace. As immaterial means, cyber-resources cannot be shown openly. Using offensive capabilities will almost surely turn them obsolete in a question of weeks, or months at most.

In contrast, the adversary will have far less evidence of the extent and effectiveness of U.S. offensive cyber capabilities. Not only are they entirely invisible, but they may be untested against adversary systems, leaving the adversary with some doubt about the effectiveness of U.S. capabilities, and in turn about the credibility of its threats (FARRELL; GLASER, 2017, p. 9)

Moreover, establishing the so-called ‘red lines’, the limits that indicate that an undesired action will trigger a response, is also complicated in cyberspace. The difficulty comes from the “lack a discrete metric for cyberwar”, making it hard to evaluate the effects either on a first-strike or a retaliatory one (LIBICKI, 2010, p. 133). In other words, as a direct consequence of the ‘unpredictable’ and ‘uncontrollable’ propagation nature of cyber weapons, practical battle damage assessment (BDA) is virtually impossible (MALAGUTTI, Marcelo, 2016c, p. 279).

The policy of individual indictments of Chinese operatives allegedly responsible for cyber-attacks, although highly unlikely to result in successful prosecutions, signal U.S. priorities and exert public shaming on China (FARRELL; GLASER, 2017, p. 14).

Signalling, for cyber DbP, as for any other domain, is essential and must be effective, reducing the risks of misunderstanding or misinterpretation, which could result in an increased risk of escalation and conflict. “It can be done overtly, covertly, or through diplomatic, economic, or military channels” (IASIELLO, 2014, p. 57–58).

National strategies, position papers, doctrines and rules of engagement, as said, increase credibility. They also can serve as “declaratory policies”, since they declare intentions that are perceived by possible opponents. As such, they have to be verifiable, meaning that behaviour and capabilities need to be consistent with declarations. They must, as well, be robust under change, meaning that they must resist for some time without requiring amendments (LUKASIK, 2010, p. 111).

Beyond declaratory policy, the United States will also use strategic communications as a deterrence tool. In some cases, the Administration may highlight investigations, criminal charges, successful prosecutions, or other law enforcement activities that enhance the U.S. deterrence posture. (U.S. WHITE HOUSE, 2015, p. 15)

Furthermore, “early warning systems” that can detect and “ascertain adversarial intentions, [...] might be necessary to display capabilities as a means of signalling resolve to potential and actual enemies” (STEVENS, 2012, p. 150).

#### 5.4.2.4 Compellence, Inducements and Persuasion

One of the failures of the debate on ‘deterrence’ so far is a misunderstanding of the real context of cyber-coercion. In most of the cases that nations confront today “the more pressing issue is not *deterring* an actor from choosing to conduct hostile intrusions in cyberspace but *compelling* them to stop conducting intrusions that already have been highly successful” (HARE, 2012, p. 126, emphasis added).

In July 2011, the Joint Chiefs of Staff General James Cartwright “expressed the hope that the Department of Defense would within a decade change from being ‘90% focused on defense to 90% focused on deterrence’”(STEVENS, 2012, p. 154). There is no doubt that the U.S. posture will remain an aggressive one. Remembering that Schelling observed that defence has become a euphemism to war, the interpretation of the following text is quite illustrative.

To preserve as well as further national/homeland security, it is therefore important to think through, develop, and sustain over time in a quickly evolving (technological and security/defense) ecosystem the requisite U.S. capabilities and capacities to support the country, credibly and effectively, in standing ready and being able to **dissuade, deter, and compel its adversaries**. (CILLUFFO e colab., 2012, p. 6, emphasis added)

In 2012, Presidential Policy Directive 20 (PPD-20) instructed “the military to draw up a list of overseas targets ‘of national importance’ where it would be easier or more effective for

the United States to attack with a cyber weapon than a conventional one” (HARRIS, 2014b, p. 54; U.S. WHITE HOUSE, 2012). “On the spectrum of cyber hostilities, the United States sits at the aggressive end” (HARRIS, 2014b, p. xxi).

More recently, the North-American policies of ‘Defending Forward’ and ‘Persistent Engagement’ showed their crescent disposition to offensively interfere whenever they consider they face a threat (SMEETS, 2020). In a similar vein, although a bit more restrained, the British developed their Active Cyber Defence concept (STEVENS e colab., 2019).

Inducements are often present in the development of norms. Strong states usually offer preferential trade arrangements or weapons deals, to incentivise weaker states to support creation and compliance with norms. Alternatively “old-fashioned coercion – economic sanctions and, at the extreme, military actions or credible threats thereof – can also be deployed to promote the norms of the strong” (FINNEMORE; HOLLIS, 2016, p. 449).

Persuasion is also usual in the negotiation of international norms. It can be understood as “causing someone to do or believe something by asking, arguing, or giving reasons”, being a “cognitive process of information exchange and argumentation that changes minds, opinions, and attitudes about causality and effect in the absence of coercion” (FINNEMORE; HOLLIS, 2016, p. 450).

Second, when confronted with a compellence situation in cyberspace, the greatest policy challenge is to identify the appropriate costs or pain to be inflicted on the attacker to make them change their behaviour in the desired manner (e. g., to get them off the critical networks). If the policy is restricted to taking retaliatory actions in cyberspace, then the victim’s options may be limited (HARE, 2012, p. 132).

The anonymity provided by cyberspace enables a flexible coercion strategy, allowing the compeller to communicate and apply the compellent measure reservedly, while letting the victim quietly plan its response with no influence of others (HARE, 2012, p. 138).

#### 5.4.2.5 Capabilities

Defence capabilities of middle powers should be dimensioned considering threats and opportunities posed by more powerful countries and involve their present intent and means, as well as their most likely future intent and capabilities (AUSTIN, 2016a, p. 5).

It is important to consider

“the highly dynamic character of the policy field represented by cyber-enabled war as countries accumulate capability, as technological options expand, and as key governments of interest continue to move decisively toward information dominance as an over-arching military strategy. (AUSTIN, 2016a, p. 15)

Capabilities must be credible and demonstrable for an adversary to be deterred by “detect and preempt” (GRIMAILA e colab., 2010, p. 24). The difficulty in demonstrating cyber capabilities (discussed in the section pertaining signalling) might cause cyber retaliation threats to be less credible than those of kinetic retaliation, because a state will have greater difficulty demonstrating its cyberattack capabilities (FARRELL; GLASER, 2017, p. 9).

The immaterial nature of cyber capabilities (software) “makes transparency of actual capabilities difficult, if not impossible” (LIFF, 2012, p. 412). Besides, “it is difficult to conceive of potentially nation-harming cyber demonstrations that are safe” (LUKASIK, 2010, p. 108).

Cyber-capabilities must be adequate and specific for the type of deterrence intended. Offensive software capabilities can serve to DbP; if used in pre-emptive attacks, which are considered a defensive move, what is not a pacified subject in International Law, they serve for DbD. Defensive software weapons apply exclusively to DbD.

#### 5.4.2.6 Will

Public declarations from the U.S., as well as the Stuxnet and Snowden cases, show that the North-Americans have the will to use their capabilities. Defend Forward and Persistent Engagement policies confirm it. Similarly, the British NCSS and the Active Cyber Defence policy confirm the U.K. will in using theirs. France public declarations regarding interference when there are identified cyber-threats to France signal the same posture.

Attributions made by the USA, the UK, France, Germany, Norway, Switzerland and Estonia, to cite a few, indicate that China, Russia, Iran, North Korea, and Canada used their capabilities. Thus, they show ‘will’ too. And some capabilities.

However, not a single significant public attribution has been made to Brazil, Germany, Japan, Mexico or India. Except if someone intends to consider that North Korea is more cyber-capable than those countries, the difference remains on will. Or, more precisely, the lack of it!

Besides, the USA, the U.K. and France have stated their right to respond not necessarily “in-kind” if a cyber-attack would cause significant effects on their countries. Thus, they have indicated that they can use kinetic attacks, even nuclear, to respond to a cyber-attack. Albeit, attacks continue to be reported. The reason might be simple. “The U.S. conventional and nuclear deterrents may be relatively ineffective against a ‘cyber-armed’ adversary if the adversary believes that the U.S. will not react to a cyberattack with a cross-domain response” (LIFF, 2012, p. 420).

#### 5.4.2.7 Credibility

Capability supports credibility. Both must be calibrated to cope with political objectives. Investments and efforts must reflect the desired offence/defence ratio, and permanent

recalibration must be carefully considered and adjusted as necessary (CILLUFFO e colab., 2012, p. 17).

Dissuasion requires convincing potential foes that the costs of hostile action exceed perceived benefits. Thus, developing and signalling defence capability and will reinforces credibility (CILLUFFO e colab., 2012, p. 17).

In DbP, threats must be dimensioned according to the size of the objective. An excessively large threat is often not credible, and smaller ones can provide a more dissuasive effect (FARRELL; GLASER, 2017, p. 9). In the case of the U.S., there is no lack of credibility on their capabilities and in their will (FARRELL; GLASER, 2017, p. 9, 10). Moreover, since their posture and culture are aggressive ones, focused on DbP, their threats should cause an effect. One possible reason why it is not might be the limited effect expected in cyberattacks.

A retaliatory attack might also have not been perceived, or have failed, or incorrectly attributed (LIBICKI, 2009, p. 72). It might also have been considered an operational error, or even deliberately ignored.

Good defences increase credibility. They reduce the likelihood of an attack to succeed, thus reducing the number of potential challengers, while also facilitating attribution (LIBICKI, 2009, p. 73–74).

The absence or the quality of rules of engagement and doctrines can also affect credibility (STEVENS, 2012, p. 152). In the lack of previous examples of behaviour, subsidiary elements as national strategies, white and green papers, position papers, doctrines and rules of engagement can subsidise the creation of a perception of maturity and capability, increasing credibility.

Robust public-private partnerships (PPP) also increase credibility, since they can “promote cybersecurity best practices; assist in building public confidence in cybersecurity measures; and lend credibility to national efforts to increase network resiliency” (U.S. WHITE HOUSE, 2015, p. 6). And they also can stimulate national providers of products and services of cyber-security.

## **5.5 Types of Cyber Dissuasion**

### **5.5.1 Punishment**

Cyber-Dissuasion by Punishment (C-DbP) relies on the ability to project power on the opponent’s cyberspace. Tactical objectives of C-DbP, derived from the general concept of DbP, can be either “stopping a cyberattack while it’s happening, punishing the offenders after it happened, or punishing the offenders prior to them launching an initial attack” (IASIELLO,



2014, p. 66). The latter, again, if the country understands that pre-emptive attacks are legally, morally and “culturally” acceptable.

DbP relies on having “counter value hostages”, threatening targets valued, not necessarily military ones, but valued for their ability to support military functions or operations. “Valuable targets include a state’s people, possibly its leadership, its economy, and related, the infrastructure that supports the state’s people and its economy” (FARRELL; GLASER, 2017, p. 8).

An important question related to the response of cyberattacks refers to proportionality. A lawful response must cause effects similar to those of the aggressor’s attack. However, depending on the level of technical, social and economic development of a country, it offers different ‘surfaces of attack’ for cyberattacks. A “‘response in kind’ may have totally different implications for the United States and for the aggressor” (KISSINGER, 2014, p. 346–347).

Furthermore, considering retaliatory cyberattacks offers risks of escalation, since “the capacity to conduct an orchestrated attack with predictable and controllable results is thought to be more an option under development than a current capability” (ELLIOTT, 2011, p. 38).

By 1995 the only punitive response available for Russia against cyberattacks was nuclear response; This was based on the belief that “even when defenses are poor, a capacity for devastating retaliation can prevent attacks from being mounted in the first place” (ARQUILLA, 2011, p. 63). Similarly, in 2011, it was expected that a similar policy would “well emerge in future efforts to cool the ardor of cyberwar enthusiasts, as in the new U.S. policy of threatening to respond to cyberattacks with conventional military means” (ARQUILLA, 2011, p. 65).

[I]f the adversary’s cyberattack had destroyed part of the U.S. electric grid, oil refineries, and or pipelines, the USA could retaliate against these infrastructure targets in the attacker’s homeland. Alternatively, the USA could choose to threaten a type of damage that was quite different from that inflicted by the cyberattack. For example, except when facing a major power, the USA could threaten to invade the attacker’s country or impose a new regime, if the country launched an extremely destructive countervalue cyberattack against the USA. These costs would be very different from those imposed by the adversary’s cyberattack, but the costs do not have to be of similar types for an adversary to be deterred. In terms of the basic effects-based approach, the key consideration for the United States should not be whether to respond in kind – either in terms of means or targets – but rather which threatened response is likely to be most effective. (FARRELL; GLASER, 2017, p. 9)

Policies threatening non-in-kind response by the U.S. were indeed communicated, but they did not result in effective deterrence, at least considering the frequent announcements and attributions.

The difficulties in attributing cyberattacks and intrusions are often reported as a problem that undermines C-DbP: “how can we respond effectively if we do not know who did what?” (BUCHANAN; RID, 2014; FINNEMORE; HOLLIS, 2016, p. 458; GRIMAILA e colab., 2010, p. 25). However, as already noted, attribution has a strong political component.

Support of credibility and capabilities for C-DbP incur high costs, and these costs are recurrent due to the short lifecycle of cyber-weapons.

To date costs undertaken to signal credibility for deterrence by threats of punishment in cyberspace for the United States include the development of 133 cyber national mission teams, the provision of billions of dollars of investment to stand up United States Cyber Command and the creation branch level-cyber forces in the Army, Navy, Air Force and Marine Corps. The NSA and CIA have also continued the development of cyber capabilities. By all accounts each of these organisations is developing a variety of exploits, defined in J.P. 3–12 Cyberspace Operations Doctrine as cyber capabilities. However, unlike in the physical domains of land, sea, air and space, the lifespan of the capabilities developed are temporally constrained by both changes in technology through the evolution of software and hardware platforms, the maintenance of existing platforms and the frequency with which those platforms are connected or able to be accessed via the Internet. (BRANTLY, 2020, p. 212)

To be able to retaliate in kind, cyberattack tools depend on careful planning and preparation. They have to be previously implanted in the targeted networks, demanding the need for means to maintain, update, and trigger implants to carry out a comprehensive, effective attack. This can be tricky. The opponent may find these implants before the attack being carried, and neutralise them before use, in which case the dissuader would think its weapons are still operative and count on them and, when needed, the weapon would not be effective. Alternatively, the implant itself could be considered the prelude to attack, triggering a pre-emptive strike, not necessarily in kind (BUCHANAN, 2017, p. 6).

Punishment also requires a somewhat high level of attribution. Except when “a victim of an anonymous attack discloses the attacker’s code so that patches can render it worthless, this can be costly to the attacker, particularly if expensive zero-day exploits (previously unknown software flaws) are involved” (NYE, 2017, p. 55).

### 5.5.2 Denial

Cyber-Deterrence by Denial (C-DbD) relies on defensive capabilities for implementing area denial in their cyberspace for undesired activities. Albeit Snyder defined defence as deterrence plus resilience, contemporary literature considers resilience as part of deterrence by denial. Hence, C-DbP relies on cyber-defences (called cyber-protection in the Brazilian doctrine) and cyber-resilience capabilities (MALAGUTTI, Marcelo, 2016d, p. 42–44).

Defence (or protection) includes measures to neutralise opposing offensive and exploratory actions against the defender's systems. It is materialised by the establishment of overlapping layers that offer different types and levels of resistance to intrusions in the protected systems. The overlapping of these protective layers will increase the protective layers' effectiveness (AMIN NAVES; MALAGUTTI, [S.d.]).

Exemplifying, protective measures comprise mechanisms and practices usual in cyberspace best-practices: the use of robust methods of authentication (identification) and authorisation (restriction of privileges) of users, the segregation of networks, the use of black and white access lists, the use of intrusion prevention systems and anti-virus tools, the adoption of encryption in sensitive information, not only when in transit but also when stored statically, the use of firewalls, the use of virtual private networks (VPN), monitoring network traffic, looking for spurious network protocols and addresses or abnormal volumes of traffic, and regularly installing security updates (AMIN NAVES; MALAGUTTI, [S.d.]).

Also imperative is establishing a comprehensive, agile and effective system of centres for cyber incidents prevention and treatment (CSIRTs). Cooperation between these centres, nationally and internationally, often helps identify, contain, and neutralise cyber-offences. Additionally, it allows the collection of data that supports investigative actions, before they can be possibly compromised by resilience actions (AMIN NAVES; MALAGUTTI, [S.d.]).

Overall, C-DbD is an everyday activity in cyberspace, practised via relatively well-known cybersecurity tools and procedures (DENNING, 2015, p. 14).

The costly nature of good defences is usually the first and most significant cited challenge for C-DbD. For each class of action there is a different type of tool (HUTCHINS e colab., 2010). Analysing the spectrum of activities and tools required for implementing the aforementioned measures, it is easy to conclude that the costs of acquisition, installation, configuration, operation and support of all of the items, multiplied by the number of networks and users in modern societies, are high (MALAGUTTI, Marcelo, 2016d, p. 42–44).

The second historic challenge relates to the common perception that systems must be defended at their borders, their interfaces. This Maginot Line approach will fail, given that

firewalls and IDSs only detect what they already know, and would miss out on new threats (ARQUILLA, 2011, p. 61). Some intrusions will escape detection at the borders of systems, and defenders must be able to hunt intruders once they are within the perimeter (LYNN, 2010). This is why resilience must be considered as a fundamental element of C-DbD. Preparation “to operate under duress” sends a robust dissuasive signal to potential adversaries, indicating that the country intends to deny benefits derived from cyberattacks (BEEKER e colab., 2013, p. 35).

The National Security Agency has pioneered systems that, using warnings provided by U.S. intelligence capabilities, automatically deploy defenses to counter intrusions in real time. Part sensor, part sentry, part sharpshooter, these active defense systems represent a fundamental shift in the U.S. approach to network defense. They work by placing scanning technology at the interface of military networks and the open Internet to detect and stop malicious code before it passes into military networks. Active defenses now protect all defense and intelligence networks in the “. mil” domain. (LYNN, 2010, p. 103)

In-depth defence, however, is not an easy task. Over 600 assessments dismissed the old belief on the security of “air-gapped” systems (enclosed in isolated networks); “the average length of time for detection of a malware intrusion is four months and they are typically identified by a third party”; threats evolve faster measures and countermeasures, and “far faster” than policies; and demand for trained cyber defenders with control systems knowledge vastly exceeds supply (AUSTIN, 2016a, p. 19–20).

The third often cited challenge of C-DbD is that it must include the private sector. The economic expression of national power is directly connected to the military one. Industrial espionage and isolated acts of sabotage put aside, historically, there have been only two ways to target a country’s economy and civil infrastructure militarily. Indirectly, through blockades, or directly, through bombing. Defender’s superior military power would avoid both cases. In modern times, however, cyberweapons have changed this paradigm. Software Power made it possible to avoid confrontation with superior military forces by using cyber sabotage (sometimes called cybotage) in power projection against the private sector, which in modern societies encompasses much of the civil infrastructure (MALAGUTTI, Marcelo, 2016d, p. 42–44).

Hence, national cyber defences require government commitment not only to protect their own networks but also to cooperate with private infrastructure owners (or concessionaires) (IASIELLO, 2015). Such cooperation would be costly and certainly outside the scope of regular business activity for companies (ELLIOTT, 2011). Consequently, it demands new mechanisms for public-private partnerships.

Against state-sponsored cyber-attacks, private companies' defenders must presume their networks will be invaded. "If experienced and well-funded foreign intelligence agencies are interested in hacking a business, it is a good bet that at least some of the time they will succeed (BUCHANAN, 2018). How they will prepare to live with this reality will make the difference.

Besides, private cybersecurity companies and other software companies can become government partners in creating defence mechanisms, as is already the case in the USA. Microsoft and other computer technology companies develop sophisticated strategies to detect malicious code (such as Juniper Networks' backdoor) and prevent its deployment in their global supply chains (LYNN, 2010). Nevertheless, the investigations of a recent cyberattack against FireEye, a renowned cybersecurity firm, revealed a breach in SolarWind software supply chain allowing hackers to access the US Treasury Department and the US Department of Commerce's National Telecommunications and Information Administration (NTIA), as well as many private companies as Microsoft itself (CIMPANU, 2020).

Moreover, private companies can help in many types of cyber-dissuasion: "the attribution efforts of private security companies in regard to punishment, the actions of multinational companies in entanglement, or the entrepreneurial actions of international and transnational organisations in norm creation and enforcement" are good examples (NYE, 2017, p. 68).

Overall, the goal of C-DbD is not to keep attackers out of the defender's cyberspace, but to "raise the bar" of costs to make it next harder for them to gain the assets they pursue (CARR, 2015). "Regardless of the coercive measure taken, stronger defenses and increased resilience of the critical infrastructure must be a part of any strategy to increase the costs of conducting hostile actions in cyberspace" (HARE, 2012, p. 135).

"While there will always be sophisticated actors able to thwart the most robust cyber security defenses, the success of hostile activity against networks are the result of poor cyber security practices" (IASIELLO, 2014, p. 54).

Hence, denial offers the best means of dissuasion, whether in cyberspace or not, in those situations where it can be applied and is cost-effective (DENNING, 2015, p. 15).

C-DbD is difficult, albeit possible; and it is a primary response to cyberattacks (ELLIOTT, 2011, p. 38). And although costly, it is much less expensive than the costs of doing nothing, as recent figures on damages caused by cyberattack show.

Kopp (2010, p. 29–30) listed ways of deterrence existing in biology. Analogies with them can provide interesting C-DbD mechanisms. The first example is what he called

Degradation (also Denial of Information). It relates to “concealment and camouflage, or stealth”, basically intended to hiding the signal amidst enough noise, so that the attacker cannot be sure of what means what. In cyber, a parallel could be a “flood of information” with hundreds of files (or virtual servers) with similar names and content, making it challenging to identify the true one. The second example Kopp named Corruption (or Deception or Mimicry), meaning “the insertion of intentionally misleading information, making the receiver not able to “distinguish the deceptive signal from the real signal”. The use of “honeypots”<sup>6</sup> in cyberspace correspond to this technique. The third was named Subversion, which would be equivalent to weaponising a file so that, when the attacker accesses it, the embedded malware triggers a self-destructive process in the opponent’s system.

Costs of failures to maintain cyber hygiene are often higher to a country than the costs to private individuals and firms (NYE, 2017, p. 57). Furthermore, whilst a problem for C-DbP, attribution difficulties favours C-DbD (STEVENS, 2012, p. 150).

It has been said that C-DbD, although imperfect, might be better than no dissuasion at all, and “for this reason alone, perhaps, [...] has tended to become a default option, both in its pre-event (defence) and post-event (resilience, consequence management, ‘risk absorption’) forms (STEVENS, 2012, p. 153). Indeed, it might be the better option, but not for this reason alone, as will be shown ahead.

### 5.5.3 Futility

Cyber Deterrence by Futility (C-DbF) would consist in attempting to convince a nation that there is no point in investing in cyber-capabilities because it would never be possible to achieve a competitive advantage against the means of superpowers. The problem with this concept is that it considers almost exclusively an offensive perspective, focusing on searching for “a competitive advantage”.

Nation-states must consider Vegetius’ always valid formulation: *Si vis pacem para bellum*<sup>7</sup> (if you want peace, prepare for war) (VEGETIUS, 1767, book III, Prologus). No country can decide not to invest in defensive capabilities because it considers that it will never have decisive offensive conditions.

Defensive capabilities matter. In Schelling’s words:

---

<sup>6</sup> Honeypots are systems deliberately built, generally with known vulnerabilities open, to become attractive to opponents, and provide deceptive information (counter-intelligence) while allowing to trace and identify the attacker (KASPERSKY LABS., [S.d.]).

<sup>7</sup> The actual phrase reads “*qui desiderat pacem, praeparet bellum*”. However, it has become well-known by the variant used above.

Forcibly a country can repel and expel, penetrate and occupy, seize, exterminate, disarm and disable, confine, deny access, and directly frustrate intrusion or attack. It can, that is, if it has enough strength. “Enough” depends on how much an opponent has. (SCHELLING, 2008, p. 1)

Besides, when there is already a conflict, even inferior capabilities can create some distress in more powerful countries, as Iranian and North Korean cyber-capabilities used against the U.S. have shown so far. Another factor that plays against C-DbF is the relatively low cost of offensive cyber capabilities compared to other military capabilities.

Operational cyberwar has the potential to contribute to warfare— how much is unknown and, to a large extent, unknowable. Because a devastating cyberattack may facilitate or amplify physical operations and because an operational cyberwar capability is relatively inexpensive, it is worth developing. That noted, success at cyberwar is not only a matter of technique but also requires understanding the adversary’s networks in the technical sense and, even more, in the operational sense (how potential adversaries use information to wage war). [p. xx] (LIBICKI, 2009, p. xx)

However, all considered, the asymmetry of cyber capabilities can indeed exert some dissuasive effect, mainly by “filtering” the number of potential adventurers, but not against declared opponents.

#### 5.5.4 Norms

Cyber-Dissuasion by Norms (C-DbN) is the variant of DbN for cyberspace. It is the first lineage of dissuasion born after the rebirth of deterrence and dissuasion as an area of study due to cyber threats’ growth. Until 2017, norms had long been considered a supporting element of dissuasion strategies. However, the approach had often been that of the “threat of retaliation” for non-compliance with established norms (FREEDMAN, 2004, p. 65–74).

Stevens (2012, p. 155), in *Deterrence and Norms in Cyberspace*, observed that both Lewis (2010) and Nye (2010) had considered that norms could reinforce deterrence of cyber-offences, whilst none of the authors had “explicitly categorise [d] norms as a form of deterrence”. Stevens also observed that the U.S. International Strategy for Cyberspace, of 2011, explicitly indicated “the emergence of national cyber strategy in which cyber deterrence may be pursued not only through national security capabilities, but through diplomatic, information, economic and political means also” (STEVENS, 2012, p. 159).

In 2015, again focused on cyber-dissuasion, Davis claimed that “other forms of influence, including laws and social and international norms, also have considerable potential for reducing some kinds of cyberattacks. Attitudes and norms arguably have more potential

than laws per se, but they can be mutually reinforcing” (DAVIS, 2015, p. 20). Then, in 2017, Nye finally named “Deterrence by Norms” the normative attempts of regulating cyber-behaviour (NYE, 2017).

The popular understanding of norms is generally related to the existence of a formal agreement or law. However, as explained in Chapter 3, norms can be “institutionalised”, formal or informal, as internal law, cultural, moral or religious traditions, rites, taboos and even myths, and affect behaviour.

Norms are often considered as related to the Constructivist Theory of International Relations (I.R.) (FREEDMAN, 2004, p. 69–70). Moreover, the constructivist approach is arguably “predominant in the literature common to cyber and I.R.”; and “the constructivist view tends to focus on how cyberspace assists in the expansion of defining and transforming ideals, which contributes to changes in the social status quo” (MEDEIROS; GOLDONI, 2020, p. 46).

However, usual takes on norms development consider the Realist view, centred in power. Treaties require the express consent of States. Gary Corn, a former USCyberCom legal adviser, notes that the basic principle of any negotiation is that “no one negotiates against himself” (DASKAL e colab., 2019). Insofar having capabilities that are strategically or operationally useful, some States have no incentive to limit the option of using them (MAČÁK, 2016, p. 133). These same countries, however, are also vulnerable to hostile operations by other states with similar or even lower capabilities. Therefore, different bodies in the same country see national interests from different perspectives and may differ in how that country should characterise a particular practice (SCHMITT; VIHUL, 2014, p. 20). Despite, while the rationale points to a net advantage of the pros facing the cons, the case in favour of the maintenance of strategic advantage prevails. Libicki states that “the broader rule applies: norms established in state-to-state negotiations require proponents to give up something as well as receive if such norms are to persist” and that “as a rule, countries agree to asymmetric deals only under coercion. In the Obama era, the threat was sanctions” (LIBICKI, 2019, p. 3). However,

Coercive powers—bribes and threats—raise important questions not only about norm processes but about the nature of normativity itself. Does something “count” as a norm if the desired behavior is coerced (or bribed) rather than being sincerely believed or accepted? Is a norm really a norm if we do not like its contents? (FINNEMORE; HOLLIS, 2016, p. 450)

Nye indicates two different characteristics of norms. One concerns the obvious opportunity for retaliation, as it can be denoted from the claim that “some degree of attribution is necessary for norms to work” (NYE, 2017, p. 60). The other he expresses in terms related to



the idea of culture and values, although still with a realist approach: “an *incipient aggressor* may be inhibited by his own conscience, or, more likely, by the prospect of losing moral standing, and hence political standing, with uncommitted countries” (NYE, 2017, p. 52, emphasis added). However, it does not seem plausible to consider that only “incipient aggressors” would be inhibited by conscience or moral and political stances. General Michael Hayden, former commander of the USCyberCom and director of the NSA, stated that:

NSA AND GCHQ senior leadership meet annually, alternating which side of the Atlantic would host. [...]

Besides, GCHQ was having its own issues with Britain’s growing “Europeanness”. The overlay of the European Convention on Human Rights onto British law, policy, and practice was a broad issue for the government. For GCHQ, it meant additional administrative burdens and procedures to be able to demonstrate compliance.

[...], on balance, we Americans spent a fair amount of time explaining ourselves. Such as explaining our views on the use of force in international relations. Differences were more stark with many Continental Europeans, of course, but we were representing a government and (I think) a people with, let’s say, a more robust view of the utility of force than even our British cousins. (HAYDEN, 2016, p. 36–37)

As exposed, the American government view on the use of force is different than that of the British and other European U.S. allies (and possibly that of the American people too). And this does not mean that all of the latter are incipient aggressors.

Discussing the ethics of offensive cyber operations in a book dedicated to *Projecting the U.K.’s values abroad*, Devanny states that what he calls cyber-skirmishing (operations aimed at pre-empting an attack, prevent a ransomware campaign, or punish a hostile state actor) and cyber operations during armed conflict, supporting integrated operations) are “most compelling”. However, operations aimed at “deterrent signalling of capabilities to undermine critical infrastructure, are ethically and legally more complex, to say nothing about their strategic efficacy” (DEVANNY, 2020, p. 56).

It is essential to notice that the legality of pre-emptive attacks, assumed by Devanny, is not consensual in the international arena. Influential Brazilian internationalists, for instance, do not accept its legality. While the principle of self-defence has a legal provision of customary nature, there is no legal support for preventive actions (PEREIRA, 2010, p. 30–1). The Bush Doctrine, published a year after the 9/11 terrorist attacks, reiterated that the USA has long insisted on the possibility of pre-emptive attacks, and went further advocating for the legitimacy of preventive strikes (BUSH, 2002, p. 15). A pre-emptive attack is carried out when an attack is imminent; a preventive attack is carried out to prevent the enemy from being able to attack

in the non-imminent future. Notwithstanding such a differentiation, both are carried out before an enemy attack occurs, and thus cannot be considered self-defence in line with the legally accepted framework (PEREIRA, 2010, p. 33).

As the hypothesis of this research states, the above examples show that cultural, moral, ethical and other institutionalised values (and taboos, possibly) permeate the discussion on the use of offensive cyber capabilities.

Despite, most of the writings on C-DbN presuppose negotiations within international fora and the existence of legal instruments (international treaties, agreements or law). These instruments are frequently referred to in the NCSSs studied in Chapter 6. Not surprisingly, much more frequent among non-aggressive nations than among the aggressive ones.

Much effort has been put on international fora in the discussion of norms for regulating cyber operations. In November 2019, the U.N. Assembly approved two separate proposals to debate the regulation of cyberspace activities: one from the USA, creating one more Group of Government Experts (GGE); and another from Russia, creating an Open-Ended Working Group (OEWG) (ACHTEN, 2019; COLATIN, 2018; GRIGSBY, 2018).

GGEs are common in the U.N. routine, constituted *ad hoc* when any subject deserves U.N. attention, with experts from 15 to 25 countries, but they are rarely successful (ACHTEN, 2019; NYE, 2018). GGEs related to cyber regulation are nothing new. Those of 2004-5 and 2009-10 did not obtain significant results. However, the 2012-13 one had considerable success. For the first time, 15 countries, including Russia, China, USA, India, the United Kingdom, France and Germany, came to the understanding that the *jus ad bellum* (the U.N. Charter) would apply to cyberspace, although there was no agreement on *jus in bello* (International Humanitarian Law). The 2014-15 GGE developed new rules to guide the activity of States in cyberspace in times of peace but did not achieve the same success of its predecessor, as intended by the USA (FIDLER, 2018; GRIGSBY, 2017, p. 112).

Differently, OEWGs are forums open to all nations. The USA opposed this one arguing that the existence of two separate discussion groups would divide efforts and that Russia's intention was, in a broader forum, to delay the discussion (ACHTEN, 2019; COLATIN, 2018; GRIGSBY, 2018). However, already in 1998, Russia was the first nation to propose an international U.N. treaty to ban electronic and informational weapons (including for propaganda purposes), which could be used to "adversely affect the security of states", with a resolution passed by the Assembly General (GRIGSBY, 2017, p. 110; NYE, 2018). In 2011, Russia, China, Tajikistan and Uzbekistan proposed the U.N. should regulate "the dissemination

of information incompatible with the domestic policy and the social and economic stability of countries, as well as their cultural and social environment” (STEVENS, 2012, p. 162).

In any analysis, however, the approval of these two groups by the General Assembly shows that international concern with the issue is general and that both sides’ arguments are being heard. This concern is also evident in other initiatives.

A key issue in the debate is the applicability of the current *jus ad bellum* and *jus in bello* to cyber activities. On the one hand, it is argued that, in the absence of specific rules, states should work by analogy, either by equating cyberattacks to traditional armed attacks and treating them under the laws of war or by equating them to criminal activities and dealing with them in the manner of internal criminal laws (SKLEROV, 2010). The USA and its allies, particularly in NATO, favour this argument, even though some fundamental principles remain unresolved, such as what would be a cyberattack or characterise the use of force in cyberspace. On the other hand, Russia, China and Brazil, among others, express considerable reluctance to agree with non-specific rules’ applicability, considering the need for specific agreements as an imperative (GILES; MONAGHAN, 2014; SCHMITT; VIHUL, 2014).

It was in the context of the applicability of the current rule that, under the auspices of NATO, an international group of academics produced the *Tallinn Manual on the International Law Applicable to Cyber Warfare* (SCHMITT, 2013). The work was later expanded with the ‘Tallinn 2.0’ Project, published four years later, full of examples that illustrate an interpretation of the application of current rules to cyber operations (SCHMITT, 2017). The Chinese often argued the initiative is a clear example of an attempt to legalise military use of cyberspace by western powers (HENRIKSEN, 2019, p. 4; HUANG; MAČÁK, 2017, p. 299).

Although doctrine is a secondary source of international law, it constitutes a “highly persuasive” element in interpreting the provision of treaties and the identification of international custom. A doctrine common to several states can evolve into a “general legal principle recognised by civilised nations” (*jus cogens*), and later develop into a custom (ICJ, [S.d.], Article 38). Therefore, in the absence of conventions or customs related to cyber-conflicts, academic works such as the Tallinn Manual can be a relevant tool for identifying and formatting legal norms for cyberspace (SCHMITT; VIHUL, 2014, p. 3–4). And this may be contrary to the interests of those who oppose the primacy of the USA.

Since 2010, the USA has been relatively successful in getting some of the top cyber powers to agree to an increasingly prescriptive set of rules on what they could and could not apply in cyberspace. However, the process failed in obtaining explicit consent to the applicability of laws of war to cyber-conflicts. Among others, Russia, China and Cuba have

refused to do so, ruled by the suspicion that this would constitute a ‘green light’ for hostile actions in cyberspace (GRIGSBY, 2017, p. 109).

Not only traditional USA opposers disagree in some aspects of the applicability of existing international laws, however. Even NATO members work to shape the formation of customary law, expressing their particular (and frequently conflicting) views in fundamental aspects (DEPARTMENT OF FOREIGN AFFAIRS AND TRADE, 2017; IRANIAN ARMED FORCES CYBERSPACE CENTER, 2020; MINISTÈRE DES ARMÉES, 2019; MINISTRY OF FOREIGN AFFAIRS OF THE KINGDOM OF THE NETHERLANDS, 2019; NEW ZEALAND, 2020; UK MINISTRY OF DEFENCE, 2016).

In the end, “norms [and institutions] can impose costs on an attacker even if the attack is not denied by defense and there is no retaliation” (NYE, 2017, p. 60).

### **5.5.5 Entanglement**

DbE is another concept that arose from the renewed interest in dissuasion research come from cyber threats. Cyber DbE (C-DbE) is the cyber version of it. Its central idea is that a cyberattack could backfire, imposing severe costs to the aggressor itself due to its interdependences with the victim (NYE, 2016).

Because China benefits from U.S. and European markets it is dissuaded from harming them with cyber-attacks that degrade/deny, destroy or disrupt or in any way damage their existing benefits both in the short and the long-term (BRANTLY, 2020, p. 226).

The concept somewhat benefits from the fear of the “unpredictable and uncontrollable propagation” of malware (MALAGUTTI, Marcelo, 2016c, p. 280–281). Stuxnet, although targeting Iranian centrifuges, infected installation in more than 150 countries, and later was used to create two other malware: Duqu and Flame (ARQUILLA, 2011; STERLING, 2015). A more contemporary example is NotPetya. Publicly attributed to Russia by all of the nations that integrate the Five Eyes “intelligence club” (USA, UK, Canada, Australia and New Zealand), this malware intended to attack Ukraine. However, it infected and crippled computers worldwide, causing losses of more than USD 300 million to logistics giant FedEx and more than USD 350 million to Maersk, the largest shipping company in the world, to cite a few. The global estimated losses rise up to USD 10 billion. It also stroked the Russian state oil company Rosneft, back in “mother Russia” (GREENBERG, 2018).

### 5.5.6 Individualisation

Cyber-Dissuasion by Individualisation (C-DbI) is the third new type of dissuasion born under the debate of cyber-dissuasion. The concept developed from an initiative of President Obama Administration in 2015.

Law enforcement can also be an effective deterrent to cyber threats both through denial (e.g., taking down a criminal botnet that could be used in an attack) or cost imposition (e.g., arresting the perpetrators of cyberattacks). Although investigation and prosecution are challenging in the cyber context, the United States Government uses this tool effectively to disrupt and degrade adversary cyber capabilities. (U.S. WHITE HOUSE, 2015, p. 11)

Ciaran Martin, former chief of the British National Cyber Security Centre (NCSC), a branch of GCHQ, observed that instead of the traditional approach of prosecuting internal criminals, however, the U.S. government adopted a different approach.

The Obama Administration ingenious innovation of issuing criminal indictments against hostile state actors did more to deter hostile state activity than any retaliatory cyberattack: not just by embarrassing the states they accused, but by removing, for life, the prospect of traveling to the West for any of those indicted. (MARTIN, 2020, p. 10)

C-DbI “focuses on what individual hackers or attackers are most likely to value, and bases deterrence on that individual cost-benefit analysis” (BRAW; BROWN, 2020, p. 51). Since individuals value things differently than States, this shall exert a more significant impact on the first than in the latter (BRAW; BROWN, 2020, p. 52). If a hacker, or his family, has “ambitions to travel or study abroad, or to hold international financial assets, the possibility of forfeiting such opportunities as a result of an employment choice may give them pause” (BRAW; BROWN, 2020, p. 52).

Indictments of this type were issued in 2018, when “the U.S. Department of Justice (DoJ) charged North Korean national Park Jin Hyok with conspiring to conduct cyberattacks and intrusions, accusing him of involvement in the Sony incident”, when the “the U.S. Department of the Treasury imposed sanctions on him and against the regime-linked Chosun Expo Joint Venture, where he worked” (BRAW; BROWN, 2020, p. 53).

In the same 2018, 12 members of the GRU, the Russian Military Intelligence Agency have been indicted for allegedly having been involved in the interference with the U.S. presidential elections of 2016 (THE GRAND JURY FOR THE DISTRICT OF COLUMBIA, 2018).

In 2019, however, CrowdStrike, a cybersecurity firm, indicated in its Annual Threat Analysis:

In many respects, 2018 appeared to be a markedly different year than the one before. Absent some of the high-profile events observed in 2017, such as WannaCry and NotPetya, headlines in 2018 were defined instead by a series of U.S. Department of Justice (DoJ) indictments against individuals linked to named, state-sponsored adversaries. Possibly affected by these public disclosures, ongoing tool development activity and changes in tactics, techniques and procedures (TTPs) seem to indicate 2018 was a transition year for many adversaries. *One thing was clear: Law enforcement efforts have not yet halted or deterred nation-state sponsored activities.* (CROWDSTRIKE, 2019, p. 6, emphasis added)

In October 2020, the U.S. Department of Justice indicted six Russian citizens, members of the GRU, Russian military intelligence, for their responsibility in several cyberattacks, including: that of the 2017 French presidential elections; the 2018 Winter Olympics; that of Pennsylvania (USA) healthcare companies and facilities in 2018; those of the Ukrainian power grid, in 2015 and 2016; and NotPetya, 2017 (SCHMIDT; PERLROTH, 2020).

An essential aspect of this individualised approach “is signalling the likelihood of specific consequences to individual hackers”, “publicising the range of possible consequences in advance, and taking the response well beyond notifications, beyond even naming and shaming, to naming, shaming and blaming” (BRAW; BROWN, 2020, p. 54).

C-DbI also presents less potential for “explosive consequences in the case of error”, since it “allows states to avoid the sticky attribution problem that sponsoring states have used to their advantage for the past two decades” (BRAW; BROWN, 2020, p. 54).

## 5.6 A Comparison Among the Different Types of Dissuasion

Snyder (1959, p. 3–7) proposed a comparison between the two types of ‘deterrence’ then defined: “by Punishment” and “by Denial”. His model considered four parameters and their relative weight, classified in three grades (Low, Constant or High) for each deterrence type, viewed from the attacker’s perspective. The result can be found in Table 6.

Table 6 – Comparison Between Punishment and Denial

Parameter	Punishment	Denial
The credibility of the threat	Generally low	High
Costs resulting from the response	High	Relatively low
Valuation of the prize	Constant	Constant
Probability of success of the attack	High	Low

Source: Compiled by the author based on (SNYDER, 1959, p. 3)

Snyder’s objectives seemed intended to be more enlightening than methodologically rigorous. Despite, his attempt suggests a template for comparing the six types of the broader ‘Dissuasion Theory’.

Table 7 presents a comparison, considering the findings of this research related to the conceptual elements described in this Chapter, from the dissuader’s perspective.

Table 7 – Comparison Among the Six Types of Cyber Dissuasion

Element	C-DbP	C-DbD	C-DbF	C-DbN	C-DbE	C-DbI
Sovereignty	Low	High		High		
Weapons	Offensive	Defensive		Forensic		Forensic
Attribution	High			Medium		High
Asymmetry	High	Medium				Medium
Culture	Aggressive	Non-Aggressive				
Coercion	Positive/Negative	Negative	Negative	Negative	Negative	Negative
Resilience	Low	High				
Signalling	High	Low				High
Persuasion	High	Low				
Dissuasion	Low	High	Low	Medium	High	High
Capabilities	High	High	High	Low	Low	High
Will	High	Medium	Low	Low	Low	Medium
Credibility	High	Medium	Medium	Low	Low	Medium

Source: Compiled by the author

As the convention used in this work states, empty cells mean “Not-Applicable” or “Irrelevant”. Concerning “Sovereignty”, “high” and “low” indicate the possible impact resulting on claims of violation of sovereignty by the dissuaded. The line named “Weapons” presents the class of tools necessary to implement that type of dissuasion (Offensive, Defensive or Forensic). Regarding “Asymmetry”, values indicate the trend of the dissuaded effort in challenging the dissuader. In other words, it is expected that the dissuader gets more challenged by smaller forces when implementing C-DbP (as in the example of Iran and North Korea challenging the U.S.). On all other elements, values are self-explanatory.

## 5.7 Cyber-Dissuasion in the Brazilian Doctrine

The lack of an adequate corpus on dissuasion and deterrence in Brazil shows a particularly relevant limited view in what regards cyber defence and cybersecurity. Let us recall the definition of dissuasion present in the Brazilian National Strategy of Defence:

DISSUASION - Strategic attitude that, through means of any nature, including the military, aims to advise or divert opponents, real or potential, from possible or presumed **warlike purposes**. Same as DETERRENCE. (BRASIL-MD, 2020b, p. 75, emphasis added)

Several nations devise cyber defence and cybersecurity strategies seeking to deter actions of non-military purposes, such as commercial, industrial and political espionage, terrorism, threats to interrupt the operation of critical or strategic infrastructures, and other forms of state cyber-defence. However, by the definition adopted, Brazil would be signalling not to act dissuasively in these situations, given that “not warlike”.

In the same vein, we have the determination concerning “strategic projects”, “inducers of the transformation process” of the Brazilian Army, whose continuity is necessary to reach the “desired degree of deterrence”, among which the Cyber Defence System, which they act by increasing mobility, the activity of monitoring and controlling borders and the ability to act in the denial of unwanted access to areas or strategic systems of interest to National Defence” (BRASIL-MD, 2020b, p. 54, free translation). Notably, the Brazilian defence strategy is based on the denial approach (including cyber defence).

## 5.8 Conclusion

Cyber-dissuasion is still a nascent field of research (and practice). However, empirical evidence shows that the traditional deterrence option for (threat of) punishment (C-DbP) has not generated the effects expected from the Cold War history lessons. The option for C-DbD, despite the difficulties, particularly those related to the cost of development and deployment and management of adequate defences, still seems to be the best option, particularly when the dissuader does not have an institutional framework that supports offensive actions. C-DbF does not seem to be promising, except when the asymmetry is so significant that it will de-characterize the competition. C-DbN tends to consolidate itself only in the long-run.

Nonetheless, it is a promising option, although the difficulties observed in the negotiations of the GGEs and the OEWG indicate a still quite tortuous path. C-DbE remains a theoretical field of research. The NotPetya case, which backfired in Russia, may have served as a lesson, although it is not yet possible to assure that. Finally, C-DbI has its effectiveness questioned because indicted people from nations such as Russia, North Korea and China have



relatively low prospects of actually suffering the sanctions stipulated by foreign courts. However, as the mechanism is established, and reaches the companies and organizations for which individuals work, the soft power shaking in their respective countries may cause some relevant reflection.

The most important finding, however, is that these types of cyber-dissuasion are not mutually exclusive. They can (and must) be exercised in conjunction, considering means, objectives, and culture of the dissuader.



## 6 COMPARED ANALYSIS OF CYBERSECURITY STRATEGIES

In this chapter, the most recent strategies of twelve countries are analysed, using a quantitative content analysis based on the frequency of occurrence of terms categorised in nine categories and 62 thematic subcategories to infer the main concerns reflected in these documents. The study indicates that the documents considered, although relatively homogeneous concerning the selected categories of analysis, are significantly different when the subcategories are considered, showing very different emphases with regard to the various topics covered. These differences can be considered in elaborating updates of the documents themselves or developing the first versions by “new entrants”. The data obtained here can also provide insights to scholars interested in the subject.

### 6.1 Introduction

The growing importance of cyberspace in modern societies, coupled with the accelerated growth of the underlying threats, has made it common practice for several countries to publish National Cybersecurity Strategies (NCSSs) periodically. In the context of comparative policies, an understanding of these public policies' commonalities and idiosyncrasies becomes relevant to identify the priorities and deficiencies perceived by different nations and world trends.

One of the principles adopted in this comparative analysis is that “the public and routine presentation of defence policies and strategies is one of the cornerstones of governance and serves diplomacy to preserve, protect and support international peace and security” (PROENÇA JR.; LESSA, 2018).

It is also considered that such documents have the primary objective of establishing the nation's vision of future regarding perceived threats and guiding and directing society in elaborating public policies and the planning and execution of its preparations for the mitigation of these threats. In this line, the Brazilian e-Ciber establishes that “[the] Strategy constitutes a clear orientation from the federal government to the Brazilian society on the actions it intends, in national and international terms, in the area of cybersecurity”.

In this chapter 12 NCSSs are analysed to identify if empirical data reveals significant distinct pattern among Aggressive and Non-Aggressive nations regarding their priorities and emphasis regarding cybersecurity and cyber defence.

### 6.2 Methodology

The methodology adopted was Quantitative Content Analysis, going through the phases and steps below, as defined by Bardin (2016).

## 6.2.1 The Pre-Analysis Phase

### 6.2.1.1 Documents Preparation

Documents to integrate the corpus were selected based on four motives. The first group, composed by the USA, the UK, China, France and Germany, constitutes a set of nations often praised by their cyber-capabilities, sometimes even called cyber-superpowers. By this criterion, the NCSSs of Russia, Israel, Iran and North Korea should also integrate the corpus. However, there is no public availability of these strategies, making it impossible to analyse.

The second group, integrated by the Netherlands, Australia, and Estonia, constitutes a group of nations that have actively engaged in the debate of international norms for regulating nations' cyber-behaviour.

A third group is that of the G-20 non-aggressive nations: Brazil, Germany, Japan and Mexico. Brazil, in particular, has a somehow strange behaviour regarding cyberspace. Brazil is one of the ten richest countries; it is often appointed as one of the three largest victims of cyber-crime in the world; it has been targeted by the NSA, and engaged in the U.N. against abuses in cyberspace; and it has a remarkable dependency on cyberspace, with the most automatised electoral process in the world, an entirely on-line revenue taxation, and one fully on-line financial system, only behind the U.S. in number of on-line transactions. Despite, only in December 2019 Brazil has started its accession to the Budapest Convention on Cybercrime and only in February 2020 it published its first NCSS. Thus, it is interesting to compare its strategy with those of its peers.

Italy constitutes the fourth set, chosen for being a member of G-7 and due to its political-cultural-economic similarities with Brazil.

The comparison is based on the documents themselves. To make it feasible, English language versions of the documents were used. In the cases of the USA, the United Kingdom, Italy, Estonia, the Netherlands, and Australia, documents issued by their governments in English were used. Regarding China, the analysis was based on a version of the document previously translated into English by a North-American website specialized in Chinese legal documents. Regarding the strategies of Germany, France and Brazil, a translation to English was provided by this author. In this way, it became possible to use a unified “dictionary” of terms to be processed.

The search for the most recent national strategies in the 16 mentioned countries resulted in what is shown in Table 8. The ICC column indicates the Internet Country Code for each country, associated with their Internet domains.

Table 8 – Corpus Candidate Documents

Country	ICC	Year	Language	Used	Observations
Australia	AU	2020	English	Yes	
Brazil	BR	2020	Portuguese	Yes	Since published only in Portuguese, it was necessary to translate it into English to make the comparison feasible.
China	CH	2016	Mandarin	Yes	Since published only in Mandarin, a version translated into English by a USA website specialized in Chinese legislation was used.
Estonia	EE	2019	English	Yes	–
France	FR	2018	French	Yes	Since published in French only, it was necessary to translate it into English to make the comparison feasible.
Germany	DE	2016	German	Yes	Since published in German only, it was necessary to translate it into English to make the comparison feasible.
Italy	IT	2017	English	Yes	–
Iran	IR	–	–	No	Iran has not published a national cyber defence and cybersecurity strategy.
Israel	IL	2017	English	No	Only a summary of the strategy was published, not the full document, which prevented its analysis.
Japan	JP	2018	English	Yes	
Mexico	MX	2017	English	Yes	
Netherlands	NL	2018	English	Yes	
North Korea	KP	–	–	No	North Korea has not published a national cyber defence and cybersecurity strategy.

Country	ICC	Year	Language	Used	Observations
Russia	RU	–	–	No	The Russian Federation has not published a specific document for cyberspace, including it in the context of the National Defence Strategy. This prevents a comparison based on a particular theme.
United Kingdom	UK	2016	English	Yes	–
USA	US	2018	English	Yes	–

Source: Compiled by the author

Henceforth, to facilitate the reading and standardize this work, to refer to the respective strategies, each country's ICC will be used followed by the last two digits of the year of publication of the document. Thus, AU-20 is the Australian strategy of 2020, while DE-16 is that of Germany in 2016, and so on.

The following documents compose the analysed *corpus*:

- From Australia: Australia's National Cyber Security Strategy, 2020 (AUSTRALIA, 2020).
- From Brazil: Estratégia Nacional de Segurança Cibernética (e-Ciber), 2020 (BRASIL-GSI, 2020);
- From China: National Cyberspace Security Strategy, 2016 (CHINA, 2016);
- From Estonia: Cybersecurity Strategy, 2019 (ESTONIA, 2019);
- From France: Revue Stratégique de Cyberdéfense, 2018 (FRANCE, 2018);
- From Germany: Cyber-Sicherheitsstrategie für Deutschland, 2016 (GERMANY, 2016);
- From Italy: Cybersecurity Action Plan, 2017 (ITALY, 2017);
- From Japan: Cybersecurity Strategy (Provisional Translation), 2018 (JAPAN, 2018);
- From Mexico: National Cybersecurity Strategy, 2017 (MEXICO, 2017);
- From the Netherlands: National Cyber Security Agenda, 2018 (NETHERLANDS, 2018)
- From the UK: National Cybersecurity Strategy, 2016 (UNITED KINGDOM, 2016);
- From the U.S.: National Cyber Strategy, 2018 (UNITED STATES, 2018b);

Documents were evaluated following the criteria proposed by Bardin (2016). As for exclusivity, once a paper has been chosen to be part of the research corpus, it cannot be left out of the analysis. As for representativeness, the sample was selected based on the criteria explained above, being rigorous and representative of the intended universe. As for homogeneity, the documents used are all of the same nature, and do not have any singularity outside the selection criteria mentioned. As for pertinence, they are all official documents from their respective countries (or reliable translations), to correspond to the analysis' objective.

#### 6.2.1.2 Filtering to Get the 'Strict' Text

To provide more objectivity to the analysis, the texts of the corpus were previously edited, excluding pre-textual elements (cover, cover pages, prefaces, abstracts, executive summaries, presentations, indexes and lists of images, tables or symbols) and post-textual elements (bibliographic references, glossaries, appendices and back cover), as well as pages used as a publishing or editing resource (blank pages and pages containing only illustrations without relevant textual content). This smaller version of the documents was called "strict text".

#### 6.2.1.3 Indexes Selection and "Floating Reading"<sup>8</sup>

A procedure of "floating reading" of the documents allowed identifying the first indexes, understood here as references to words and terms with specific semantics, candidate for use in coding, from the texts themselves. This process was repeated a few dozen times with the US-18 document, one of the smallest and most objective, and with the UK-16 one, as it is one of the most extensive and broadest in the diversity of content.

Initially, the Atlas TI 8.4.18.0 software tool was used<sup>9</sup>. Such a tool revealed quite interesting for those who intend to work with qualitative content analysis, have already identified a fixed (non-mutable) set of indexes, and have a small collection of documents, that can be coded manually. However, if the indexes are still evolving and the analyst works with many documents, it proved very difficult to change them in the already coded documents, since the entire process has to be done manually. Besides, the quantitative analysis of that tool proved to be limited, since working only with 'words' as a semantic unit of counting. To better understand the difficulty posed, the term "cyber" was the most

---

<sup>8</sup> Establishing a first contact with the documents to be analyzed for knowledge of the text, capturing perceptions, characteristics, orientations and terminology.

<sup>9</sup> <https://atlasti.com/>

frequent in the two initial documents. Albeit, cyber is commonly used in the English language as an adjective, which only makes sense when connected to the noun to which it refers: “cyber deterrence”, “cyber security”, and so forth. Despite, a first quantitative analysis of the two first documents was carried out in full with Atlas, providing relevant subsidies for the comparative analysis, but highlighting the limitations of the process so far.

To eliminate such limitations, it was considered necessary to develop a specific application capable of comprehensively analysing the corpus. This was the project option adopted, and the program developed by this author will be described later.

#### 6.2.1.4 Coding the Material

The process of coding and index selection developed iteratively and incrementally, literally in hundreds of executions. Whenever a new document was added to the analysis, new indexes were identified, and the process was refined for the next execution.

#### 6.2.1.5 Text adjustments

Although trying to be as little “invasive” as possible in the original text, a few operations were necessary on texts exported from strict PDFs:

- Reconnecting words with syllable separation: the breaking of words affects the proper counting of terms that will not be reunified.
- Reconnecting phrases in page breaks: the formatting of documents usually includes page headers and footers, which can separate expressions of interest from coding, making them unidentifiable by the search engine;
- Elimination of editing characters: some documents use highlighting features that prevent the correct identification of the term, for example, the use of blanks between letters (P I L L A R I);
- Verification of possible deletions of characters: in particular, due to editing, for example in a situation where the first character of a paragraph uses a typology of a different font from that of the rest of the paragraph, or because of the internal representation of the PDF format that can cause occasional errors in the export of the text (as in some cases when the syllable ‘fi’, when exported, results in an invalid character, making the word unrecognizable).

#### 6.2.1.6 Selection of Registration Units

Registration Units are the elements whose meaning corresponds to a unit that can be counted, or quantified, in a frequency count, and can be of quite different nature and



sizes. As explained earlier, words did not provide adequate registration units. In addition to the issue of adjectives and associated nouns discussed above, one of the difficulties recurrently cited in articles that aim at comparative analyses of documents related to cybernetics refers to the absence of terminological uniformity in the area (LUIIJF e colab., 2013; SHAFQAT; MASOOD, 2016). Not even in English. Therefore, references to “cyberspace”, “cyber-space” or “cyber space” can be found in the corpus. All the different spellings have the same meaning and deal with the same ‘theme’ or topic. Albeit, if the unit of record is the word, they will be counted as distinct elements.

Therefore, it revealed necessary to work with the notion of theme, characteristic of content analysis. “In fact, the theme is the unit of meaning [not form] that naturally breaks free from a text analysed according to certain criteria related to the theory that serves as a guide to reading” (BARDIN, 2016, p. 135).

Themes are often classifiable into four groups. First, ‘objects’ or ‘referents’, around which the discourse is organized; in this research, cyberspace, data, computer networks, information systems, software and hardware, and other information technology assets. Second, ‘characters’: perpetrators, their victims and stakeholders are examples of identified characters. Third, ‘events’: events, such as cases of famous cyber-attacks, or classes of events, such as cyberterrorism, hacktivism, cybercrime, and so on. Fourth, ‘documents’: strategies, laws and policies are good examples of this group (BARDIN, 2016, p. 136–7).

#### 6.2.1.7 The enumeration: choice of counting rules

The enumeration element adopted was the relative frequency, or frequency count, corresponding to the postulate that the importance of a recording unit increases with a higher frequency of appearance.

Furthermore, “terms” were treated by ‘regular expressions’, (from now on abbreviated as ‘regex’, in the singular, or ‘regexes’, in the plural) for the identification of themes, being replaced by the corresponding “categorisation triple” (Category, Subcategory, Group) for their frequency counting. However, Groups were disregarded in this report, which only accounted for Categories and Subcategories.

#### 6.2.1.8 Classification and aggregation: choice of categories

Based on the indexes identified in the “floating reading”, a set of nine Categories of themes was elaborated, with 62 Subcategories. Categories and Subcategories are presented in Table 9.

Table 9 – Categories and Subcategories of NCSS Elements

Category	Subcategory
Assets	Communications
	Cyberspace
	Hardware
	SocialMedia
	Software
	SupplyChain
Institutional	IntFora
	IntLaw
	Partners
	LawEnforce
	Policy
National	Country
	Nation
Objectives	Assessment
	Capabilities
	Education
	Innovation
	Intelligence
	Interests
	Market
	Values
Offences	Cases
	Crime
	Disinformation
	Hactivism
	IndEspionage
	PolEspionage
	Terrorism
	Threats
Perpetrators	Attackers
	Criminals
	Hackers
	Hactivists
	Insider
	Kiddies
	Militia
	NonState
	OrgCrime
	Proxies
	States
Terrorists	
Resources	Actions

Category	Subcategory
	Budget
	Funding
	Personnel
Security	ActivePosture
	Defence
	Dissuasion
	Industry
	PassivePosture
	Personal
	Resilience
	Security
	Strategy
Stakeholders	Academia
	General
	Government
	Infrastructure
	Media
	NGO
	Person
	Private

Source: Compiled by the author

As said, the process has been iterative and incremental, with the submission of the regexes created in an iteration to a text, verification of the results, identification of new expressions that would correct the deviations identified, adjustments of the “dictionary” of regexes and terms, and sometimes of the table of categories and subcategories to a new envisioned reality. The latter situation was more common when a new corpus document was included in the analysis, as a different way of referring to a particular topic was identified. A good example refers to the category of Perpetrators. Initially, it was supposed to be possible to identify each type of actor individually. However, there was a relatively high frequency of occurrences of the term “non-state actors” in some documents, and it was not plausible not to compute them. Thus, a subcategory was created to accommodate this set of terms.

Bardin (2016, p. 150–1) explained that a group of categories and subcategories must have the following five qualities. First, ‘mutual exclusion’, whereby each element cannot exist in more than one division; in other words, categories must be construed in such a way that an element cannot be classified into two or more categories. Second, homogeneity: in the same categorical set there can be only one record, with one dimension of analysis. Third, ‘relevance’, for which a category is considered relevant when it is suitable for the chosen analysis material. Fourth, ‘objectivity and fidelity’, whereby different parts of the

same material, to which the same categories apply, must be coded in the same way, even when subjected to various analyses, a principle that the use of software helps to ensure. Finally, ‘productivity’: a set of categories is productive if it provides new inferences or hypotheses and accurate data. All of these principles were observed in the established categorical grid.

### 6.2.2 The Analysis Phase

As referred, the Atlas TI software proved inadequate to the ends of this research. The project decision was to develop an application that could be flexible, adaptable, and fast. I have programmed the application in Java language, using only free or open-source libraries.

Input documents are entered in the form of a text file (.TXT) extracted from the respective published PDF files. For extracting the texts, the Apache PDFBox library, version 2.17 was used<sup>10</sup>. The regexes to be applied are read from an Excel spreadsheet, and another Excel spreadsheet, containing the resulting counts, is generated as an output from the program. The reading and writing of Excel spreadsheets use the Apache POI version 4.1.0 free software library, from Apache Foundation<sup>11</sup>. Regex processing uses the Java Development Kit’s native library for processing regular expressions<sup>12</sup>.

To avoid possible double counting of any term, the regexes of each term are processed following the order of the line number of the rules sheet, having the input text being replaced by its corresponding coding. Thus, when the next regex is processed, the words counted with the previously identified terms will no longer exist in the text, avoiding double counting.

The rules spreadsheet can contain multiple distinct tabs, housing four different types of regexes sets. The ‘Cleaning’ type has regexes for cleaning the text, for example, removing special tab characters and replacing them with blanks, pulling strings of numbers, repetition of hyphens, dashes, blank characters and the like.

‘Stopwords’ constitute the second type. Stopwords<sup>13</sup> are lists of words without thematic significance, which are neglected in different kinds of processing. For example,

---

<sup>10</sup> <https://pdfbox.apache.org/>

<sup>11</sup> <https://poi.apache.org/apidocs/dev/org/apache/poi/xssf/usermodel/XSSFWorkbook.html>

<sup>12</sup> <https://docs.oracle.com/javase/7/docs/api/java/util/regex/package-summary.html>

<sup>13</sup> The Brazilian Institute of Information in Science and Technology (IBICT / MCTIC) defines stop words as “words that do not need to be indexed, as they have little meaning, such as prepositions, articles, conjunctions and others” ([http://wiki.ibict.br/index.php/Stop\\_words\\_e\\_sinonimos](http://wiki.ibict.br/index.php/Stop_words_e_sinonimos)).

by Internet search engines, like Google or Bing. This is the case with articles, prepositions, conjunctions, several pronouns and adverbs and some other words.

The ‘Preparation’ type contains rules for converting terms that can be confusing in an interpretation. Exemplifying, the term “US\$” could be considered as the word US, since the character “\$” is not part of a valid word for regex processing, and US is itself a word in English; indeed, a StopWord. Thus, there would be a processing error if the terms were not adequately prepared. For this purpose, “US\$” is replaced by “USD”, a term used internationally to represent the United States Dollar. Similarly, "R\$" is replaced by "BRL" (the international representation for Brazilian Real), "£" is replaced by "GBP", "¥" by JPY and "€" by EUR, and “\$” by AUD in the Australian document.

Conversely, IT (in capital letters) is the acronym for Information Technology. Still, if considered without capitalisation, as is usually the case, it would correspond to the personal pronoun of the third person of the singular in English, ‘it’, also a StopWord, and would therefore be erroneously disregarded. Therefore, to avoid the loss of relevant content on the topic, “IT” is replaced by “Information Technology” not to be treated as a StopWord and to remain in the text until some regex gives it the appropriate treatment. In fact, this is the only set of rules whose processing is "case sensitive", differentiating between upper and lower case. In all other sets of rules there is no such differentiation. Regexes from the “Preparation” group are always processed ahead of the others.

The fourth type is that of ‘coding’ itself. Two sets of these rules were applied to each national strategy. Firstly, those rules for terms that are specific to a country or document. For example, they reflect the country’s name, the name given to the document, or even the names of other Countries considered allies, enemies, or even cited as references of emblematic cases. For example, US-18 nominally cites "China" as an opponent. Conversely, in CH-16, the term “China” refers to the name of the Country itself. Therefore, the regex for this term must be treated in each strategy’s specific tab, associating the term to a different index. The second set of coding rules encompasses the ‘generic’ vocabulary and contains general application terms. Regexes of this set have undergone dozens of successive refinements. One reason lies in the terminological difference between the countries. For example, what the USA calls “Cyber Strategy”, the British call “Cyber Security Strategy” and the French “Digital Strategy”. Therefore, the regex dealing with these terms considers mandatory one of the words “Digital” or “Cyber”, optionally followed by the word "Security", obligatorily followed by the word "Strategy". The regular

expression for treating all these cases equally is not very complex but needs to provide for all of these possibilities.

Table 10 presents the number of regexes implemented per type in the last processing of the corpus and generation of the dataset used in this research.

Table 10 – Regexes per Type

Group	Qty
Cleaning	12
Preparation	25
StopWords	171
Coding	1581
<i>Total</i>	<i>1789</i>

Source: Compiled by the author

Initially, only three types of rules were used, given that the need for the “Preparation” tab had not yet been realized. It should be noted that the commercial tool AtlasTI works with a single set of rules, which, as demonstrated, limits its application.

The process was refined in more than two hundred iterations, with approximately a quarter of them only for US-18 and UK-16, when the construction of the dictionary and the categorical grid began. At each iteration, the frequency of terms resulting from the process was analyzed, identifying those that should have been counted as part of some specific term, and adjusting the regexes, categories and subcategories, as appropriate. The satisfaction criterion for identifying the iterations' closure was that all semantically significant terms with a relative frequency greater than 0.25% should be treated.

The source and executable codes of the program, as well as the documents, the input and output data generated were made publicly available in a GitHub repository (<https://github.com/InstitutoVegetius/Compared-NCSSs>).

### 6.3 Validation of Gathered Data

In this section, data obtained are verified, with regard to their consistency among themselves, among the various documents, and concerning the content of the documents that originated them, against the observations arising from the reading of the texts.

#### 6.3.1 On the Number of Terms

The first element to be observed concerns the number of terms resulting from the transformations (substitutions of terms and expressions by the corresponding categorisation triples. For example, a text that originally has the expression “National Cyber Security Strategy” repeated 20 times, after the application of the corresponding regex, will have 20

occurrences of the triple (Institutionalisation, Policy, NCSS), counting only 20 terms, not the 80 (20 occurrences x 4 words) of the original text.

Table 11 indicates the number of terms resulting from each of the documents after the respective transformations.

Table 11 – Terms per Document

Category	Terms
AU-20	7.650
BR-20	9.677
CH-16	2.512
DE-16	5.276
EE-19	10.493
FR-18	28.506
IT-17	2.050
JP-18	10.442
MX-17	3.295
NL-18	5.274
UK-16	10.644
US-18	4.348
<i>Total</i>	100.167
<i>Avg</i>	8.347

Source: Compiled by the author

The colour convention adopted considers each line's average, applying a threshold (tolerance margin) of 15% upwards or downwards. In blue are those above the superior limit. In red those below the inferior one. In green are those within this threshold. We opted for this notation, which is more intuitive than the one usually used in statistics, based on variance and standard deviation. In this way, blue or red elements indicate the outliers ("points outside the curve"). The "Total" entry displays the total number of considered terms, after the texts were cleaned and the stopwords discarded, while the "Avg" line indicates the average number of terms among the documents.

Table 11 shows that the number of terms present in the documents is quite varied, with FR-18 presenting roughly 14 times the number of terms used in IT-17. Would this difference be indicative of a problem that would negatively affect the analysis? The answer is found ahead.

### 6.3.2 On Categories

Table 12 shows the distribution of terms found for each of the nine categories, and the total of terms not categorised (the 'Uncategorised' line entry).

The line "Uncategorised" shows that, despite the total number of terms (or document size), the percentage of terms categorised by the adopted dictionary is very homogeneous, with

only IT-17 outside the selected tolerance range, indicating the best-categorised document. Furthermore, despite the quite different size of the documents, the percentage of terms not categorised is adequate in all of them. This information corroborates the adequacy of the criteria for selecting terms for categorisation.

In the case of percentages related to a limited universe, which must add up to 100%, the columns reflect a “zero-sum game”; for one value to increase, another (or others) has to decrease in the same proportion. Furthermore, it is natural that in the column where there is an outlier in blue, there must be at least one in red (or vice versa), which we at this moment call Behaviour-A. It is noted that, technically, the use of tolerance margins can mask this effect, with many categories varying in the same direction, but within the threshold, and a single one, or possibly even none, going in the opposite direction, which we call B-behaviour. Behaviour-A was observed in most of the documents, while Behaviour-B was observed in US-18 and BR-20, in opposite directions.

### **6.3.3 On Subcategories**

Table 13 represents the distribution of terms found for each of the 62 subcategories, plus the Uncategorised line. The blank cells indicate that the corresponding subcategory was not found in the related document (0% frequency).

Once again, each column, individually, totals 100%, indicating that no term has been disregarded, and the “zero-sum game” by which the growth of one item implies the decrease of another is still valid.



Table 12 – Frequency per Category

Category	Avg	AU-20	BR-20	CH-16	DE-16	EE-19	FR-18	IT-17	JP-18	MX-17	NL-18	UK-16	US-18
Assets	4,90%	3,37%	4,53%	8,24%	4,19%	3,71%	3,91%	3,51%	6,02%	6,80%	5,48%	3,95%	5,15%
Institutional	3,81%	2,13%	3,44%	3,94%	5,38%	3,74%	3,59%	6,34%	3,00%	5,16%	2,58%	2,68%	3,77%
National	3,29%	3,80%	2,93%	2,87%	3,41%	4,16%	2,07%	2,78%	2,07%	3,76%	3,34%	2,78%	5,54%
Objectives	6,38%	5,74%	6,00%	6,57%	6,69%	5,37%	4,94%	11,37%	6,02%	4,31%	5,76%	6,67%	7,18%
Offences	4,11%	4,69%	3,92%	3,30%	3,68%	2,81%	4,45%	4,88%	3,33%	4,07%	3,91%	5,60%	4,69%
Perpetrators	0,66%	1,07%	0,35%	0,24%	0,44%	0,10%	0,88%	0,24%	0,35%	0,55%	0,74%	1,50%	1,47%
Resources	5,45%	6,72%	5,30%	5,25%	4,98%	5,09%	3,12%	6,39%	5,32%	4,49%	3,94%	6,45%	8,28%
Security	6,44%	6,78%	6,07%	5,81%	7,28%	7,01%	5,54%	9,41%	5,03%	5,31%	6,20%	6,74%	6,09%
Stakeholders	5,42%	7,62%	4,76%	2,59%	5,52%	4,53%	3,87%	6,34%	5,84%	5,52%	6,12%	6,49%	5,84%
Uncategorised	59,53%	58,07%	62,70%	61,19%	58,43%	63,48%	67,65%	48,73%	63,01%	60,03%	61,93%	57,14%	51,98%
<i>Total</i>	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%

Source: Compiled by the author

Table 13 – Frequency per Subcategory

Category	Subcategory	Avg	AU-20	BR-20	CH-16	DE-16	EE-19	FR-18	IT-17	JP-17	MX-17	NL-18	UK-16	US-18
Assets	Communications	0,33%	0,16%	0,53%	0,44%	0,25%	0,24%	0,19%	0,39%	0,42%	0,61%	0,11%	0,18%	0,48%
Assets	Cyberspace	1,91%	1,08%	1,32%	3,78%	1,93%	1,47%	1,20%	1,12%	1,99%	3,34%	2,14%	1,37%	2,21%
Assets	Hardware	0,88%	0,98%	1,00%	1,35%	0,63%	0,50%	0,71%	0,73%	1,10%	0,70%	1,31%	0,96%	0,60%
Assets	SocialMedia	0,03%	0,01%	0,04%				0,07%		0,03%			0,01%	
Assets	Software	1,68%	1,03%	1,58%	2,63%	1,38%	1,51%	1,73%	1,12%	2,25%	2,15%	1,92%	1,40%	1,45%
Assets	SupplyChain	0,13%	0,10%	0,05%	0,04%			0,02%	0,15%	0,23%			0,03%	0,41%
Institutional	IntFora	0,67%	0,04%	0,58%	0,52%	0,47%	0,97%	0,67%	1,66%	0,30%	1,70%	0,34%	0,32%	0,46%
Institutional	IntLaw	0,71%	0,43%	0,63%	1,75%	0,82%	0,56%	0,68%	1,27%	0,43%	0,67%	0,57%	0,23%	0,48%
Institutional	Partners	0,80%	0,39%	0,51%	0,72%	1,31%	1,16%	1,06%	0,78%	0,63%	0,39%	0,70%	0,61%	1,33%
Institutional	LawEnforce	0,37%	0,46%	0,17%	0,16%	0,57%	0,15%	0,28%	0,59%	0,29%	0,52%	0,25%	0,51%	0,51%
Institutional	Policy	1,26%	0,81%	1,56%	0,80%	2,22%	0,89%	0,89%	2,05%	1,35%	1,88%	0,72%	1,01%	0,99%
National	Country	1,37%	1,28%	0,90%	0,80%	1,02%	1,81%	0,56%	0,10%	0,74%	1,46%	1,86%	1,94%	4,00%
National	Nation	1,92%	2,52%	2,04%	2,07%	2,39%	2,35%	1,50%	2,68%	1,33%	2,31%	1,48%	0,84%	1,54%
Objectives	Assessment	1,61%	0,68%	1,86%	1,39%	2,20%	0,91%	1,34%	4,34%	1,42%	1,09%	1,61%	1,54%	0,99%
Objectives	Capabilities	1,26%	1,70%	0,51%	0,76%	1,36%	1,12%	1,00%	2,44%	1,20%	0,58%	1,16%	1,89%	1,45%
Objectives	Education	0,96%	0,88%	1,48%	0,40%	0,99%	1,14%	0,62%	1,56%	0,98%	0,85%	0,89%	0,76%	0,97%
Objectives	Innovation	0,83%	0,43%	1,05%	0,60%	0,66%	0,84%	0,42%	1,76%	1,09%	0,52%	0,72%	0,83%	1,01%
Objectives	Intelligence	0,28%	0,26%	0,26%	0,12%	0,25%	0,11%	0,52%	0,88%	0,13%	0,12%	0,08%	0,27%	0,37%
Objectives	Interests	0,49%	0,38%	0,13%	2,43%	0,63%	0,17%	0,26%	0,15%	0,08%	0,24%	0,40%	0,53%	0,51%
Objectives	Market	0,74%	1,35%	0,58%	0,56%	0,49%	0,97%	0,71%	0,24%	0,98%	0,55%	0,64%	0,74%	1,06%
Objectives	Values	0,23%	0,07%	0,13%	0,32%	0,11%	0,10%	0,07%		0,15%	0,36%	0,27%	0,11%	0,83%
Offences	Cases	0,08%	0,03%				0,03%	0,25%		0,02%		0,04%	0,13%	0,05%
Offences	Crime	0,33%	0,58%	0,29%	0,44%	0,13%	0,22%	0,31%	0,10%	0,22%	0,24%	0,63%	0,51%	0,28%
Offences	Disinformation	0,10%	0,01%	0,01%	0,24%	0,06%		0,15%						0,11%
Offences	Hactivism	0,02%	0,01%	0,01%				0,01%					0,03%	
Offences	IndEspionage	0,07%	0,03%	0,04%	0,24%	0,02%	0,03%	0,04%		0,05%	0,03%		0,05%	0,21%

Category	Subcategory	Avg	AU-20	BR-20	CH-16	DE-16	EE-19	FR-18	IT-17	JP-17	MX-17	NL-18	UK-16	US-18
Offences	PolEspionage	0,15%	0,07%	0,07%	0,20%	0,23%		0,14%	0,29%		0,03%	0,15%	0,14%	0,14%
Offences	Terrorism	0,11%		0,01%	0,60%			0,02%		0,03%	0,03%		0,09%	0,02%
Offences	Threats	3,43%	3,97%	3,48%	1,59%	3,24%	2,54%	3,53%	4,49%	3,02%	3,73%	3,09%	4,65%	3,89%
Perpetrators	Attackers	0,30%	0,37%	0,22%		0,28%	0,03%	0,61%	0,24%	0,27%	0,24%	0,34%	0,39%	0,32%
Perpetrators	Criminals	0,22%	0,51%	0,03%	0,08%	0,06%	0,06%	0,14%		0,01%	0,30%	0,38%	0,45%	0,37%
Perpetrators	Hackers	0,03%		0,05%	0,04%			0,02%					0,02%	
Perpetrators	Hacktivists	0,02%		0,01%									0,04%	
Perpetrators	Insider	0,04%	0,01%										0,07%	
Perpetrators	Kiddies	0,02%						0,00%					0,03%	
Perpetrators	Militia													
Perpetrators	NonState	0,04%		0,02%		0,04%		0,04%						0,07%
Perpetrators	OrgCrime	0,03%		0,02%	0,04%		0,01%	0,01%					0,06%	0,05%
Perpetrators	Proxies	0,02%												0,02%
Perpetrators	States	0,13%	0,14%		0,04%		0,01%	0,02%		0,05%		0,02%	0,23%	0,53%
Perpetrators	Terrorists	0,08%	0,04%		0,04%	0,06%		0,03%		0,03%			0,23%	0,11%
Resources	Actions	4,30%	5,12%	3,99%	4,82%	3,71%	3,56%	2,30%	5,12%	4,46%	3,46%	3,20%	4,99%	6,88%
Resources	Budget	0,05%		0,03%			0,01%	0,03%	0,20%	0,03%			0,01%	
Resources	Funding	0,35%	0,69%	0,51%	0,20%	0,17%	0,30%	0,17%	0,54%	0,25%	0,12%	0,38%	0,47%	0,46%
Resources	Personnel	0,76%	0,90%	0,78%	0,24%	1,10%	1,22%	0,61%	0,54%	0,57%	0,91%	0,36%	0,99%	0,94%
Security	ActivePosture	0,09%	0,08%	0,03%		0,02%	0,01%	0,20%	0,05%	0,07%	0,03%	0,11%	0,30%	0,09%
Security	Defence	1,00%	0,73%	0,45%	1,27%	1,25%	1,00%	1,39%	2,00%	0,73%	0,30%	0,51%	1,48%	0,94%
Security	Dissuasion	0,15%	0,16%		0,08%	0,02%	0,04%	0,08%	0,05%	0,12%		0,06%	0,40%	0,48%
Security	Industry	0,44%	0,50%	0,27%	0,32%	0,45%	0,63%	0,74%	0,39%	0,21%	0,18%	0,61%	0,59%	0,39%
Security	PassivePosture	0,03%	0,03%			0,02%		0,06%		0,03%			0,02%	0,02%
Security	Personal	0,02%												0,02%
Security	Resilience	0,46%	0,27%	0,73%	0,08%	0,47%	0,26%	0,13%	1,85%	0,20%	0,33%	0,51%	0,32%	0,34%
Security	Security	3,59%	3,74%	3,94%	3,66%	4,40%	3,86%	2,50%	4,05%	3,26%	3,40%	4,23%	2,71%	3,29%
Security	Strategy	0,73%	1,28%	0,64%	0,40%	0,64%	1,22%	0,45%	1,02%	0,41%	1,06%	0,17%	0,92%	0,51%

Category	Subcategory	Avg	AU-20	BR-20	CH-16	DE-16	EE-19	FR-18	IT-17	JP-17	MX-17	NL-18	UK-16	US-18
Stakeholders	Academia	0,22%	0,20%	0,27%		0,11%	0,31%	0,04%	0,24%	0,32%	0,46%	0,09%	0,26%	0,09%
Stakeholders	General	0,51%	0,18%	0,30%		0,09%	0,29%	0,37%	1,46%	0,81%	0,79%	0,66%	0,39%	0,28%
Stakeholders	Government	2,08%	3,02%	1,62%	0,52%	3,26%	1,87%	1,39%	1,76%	2,42%	1,70%	1,59%	2,69%	3,17%
Stakeholders	Infrastructure	0,75%	1,31%	0,61%	0,76%	0,32%	0,44%	0,57%	1,76%	0,51%	0,67%	0,40%	0,50%	1,15%
Stakeholders	Media	0,01%					0,01%	0,00%		0,01%			0,01%	
Stakeholders	NGO	0,02%		0,01%			0,03%			0,01%				
Stakeholders	Person	0,52%	0,26%	0,43%	0,64%	0,45%	0,51%	0,36%	0,15%	0,22%	0,97%	1,54%	0,57%	0,14%
Stakeholders	Private	1,39%	2,65%	1,52%	0,68%	1,27%	1,07%	1,13%	0,98%	1,54%	0,94%	1,84%	2,07%	1,01%
Uncategorised	Uncategorised	59,53%	58,07%	62,70%	61,19%	58,43%	63,48%	67,65%	48,73%	63,01%	60,03%	61,93%	57,14%	51,98%
	<i>Total</i>		100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%

Source: Compiled by the author

#### 6.4 Computing the Degree of Relative Thematic Incidence (DRTI)

The raw data, in the form presented so far, is hampered by two factors. First, due to the percentages referring to the total number of terms of each document, impacted by different amounts (albeit close) of terms not categorised in the defined rules. In the same way that StopWords were disregarded in the counting, as they are not relevant, non-categorised terms are also irrelevant. In other words, what is relevant is knowing the percentage of participation of each category or subcategory exclusively concerning the total of categorised terms.

The second complicating factor refers to the practical difficulty of dealing with fragmented percentage values, with two decimal digits. However, it is possible (and desirable) to relativize these values in the form of a “degree of relative thematic intensity”, from now on named DRTI. To do so, divide each relative amount by the lowest value of the corresponding line, and proceed with a simple rounding. Exemplifying, if 0.15% is the lowest value in a given row, and 0.41% is another value in the same row, dividing 0.41% by 0.15% results 2.733, which is rounded up to 3. For the lowest value, dividing 0.15% by the same 0.15% results 1. This means that the incidence of that theme in a document was three times higher than in the other.

The application of this algorithm converts the fractional values into natural numbers, facilitating their interpretation. However, this technique eliminates the columns' vertical consistency: the sum of the relative values is no longer necessarily the same across all columns. This is why the name of the DRTI transformation includes the T (thematic); to indicate that it considers the theme, the table line, and not the column. Once this side effect is understood, the benefits outweigh the negative impacts.

##### 6.4.1 Categories (adjusted by DRTI)

Table 14 represents the DRTI adjusted distribution of terms concerning Categories.

Table 14 – Frequency per Category (adjusted DRTI)

Category	Avg	AU-20	BR-20	CH-16	DE-16	EE-19	FR-18	IT-17	JP-18	MX-17	NL-18	UK-16	US-18
Assets	2	1	2	3	1	1	2	1	2	2	2	1	2
Institutional	2	1	2	2	3	2	2	2	2	3	1	1	2
National	2	2	1	1	2	2	1	1	1	2	2	1	2
Objectives	1	1	1	2	1	1	1	2	2	1	1	1	1
Offences	1	1	1	1	1	1	2	1	1	1	1	2	1
Perpetrators	6	9	3	2	4	1	9	2	3	5	7	12	11
Resources	1	2	1	1	1	1	1	1	1	1	1	2	2
Security	1	1	1	1	1	2	1	1	1	1	1	1	1
Stakeholders	2	3	2	1	2	2	2	2	2	2	2	2	2

Source: Compiled by the author

Regarding the category Perpetrators, while UK-16 (12), US-18 (11), FR-18 (9) and AU-20 (9) are emphatic on this topic, EE-19 (1) shows minimal concern, with CH-16 (2) and IT-17 (2) also presenting low intensity of the theme in comparative terms.

While the horizontal analysis allows evaluating the presence of the themes among the different strategies, the columns' study allows assessing which are the most relevant themes, proportionally, for each Country, in relation to its peers. This presents an interesting perspective, different from that of the columns' analysis on the original table. As an example, taking the UK-16 column in the original table (Table 12), one can see that the UK devoted 1,50% of its attention to Perpetrators and 5,55% to Resources. Conversely, taking the UK-16 column in the DRTI table (Table 14), it can be seen that the United Kingdom, in relation to its peers, devoted a grade 12 attention to Perpetrators and just 2 to Resources. Hence, significantly inverting the original perception. Except for this category, the documents are relatively homogeneous with respect to the categories, revealing no other relevant preferences in general.

#### **6.4.2 Subcategories (adjusted by DRTI)**

If the analysis within the Categories shows little divergence in comparing the incidence of themes, the study of the Subcategories, presented in Table 15, shows how different the documents are from each other, concerning the distribution adjusted by the Degree of Relative Thematic Incidence (DRTI).

Table 15 – Frequency per Subcategory (adjusted DRTI)

#	Category	Subcategory	Avg	AU-20	BR-20	CH-16	DE-16	EE-19	FR-18	IT-17	JP-18	MX-17	NL-18	UK-16	US-18
1	Assets	Communications	3	1	5	4	2	2	2	3	4	5	1	1	3
2	Assets	Cyberspace	2	1	2	4	2	2	2	1	2	4	3	1	2
3	Assets	Hardware	2	2	2	3	1	1	2	1	2	1	3	2	1
4	Assets	SocialMedia	2	1	5	-	-	-	10	-	4	-	-	1	-
5	Assets	Software	2	1	2	3	2	2	2	1	3	2	2	1	1
6	Assets	SupplyChain	4	5	3	2	-	-	1	5	11	-	-	1	16
7	Institutional	IntFora	18	1	17	14	12	28	22	35	9	45	10	8	10
8	Institutional	IntLaw	3	2	3	9	4	3	4	5	2	3	3	1	2
9	Institutional	Partners	2	1	1	2	3	3	4	2	2	1	2	2	3
10	Institutional	LawEnforce	2	3	1	1	3	1	2	3	2	3	2	3	3
11	Institutional	Policy	2	1	2	1	3	1	1	2	2	2	1	1	1
12	National	Country	18	16	13	11	13	26	9	1	10	19	26	24	44
13	National	Nation	3	3	3	3	3	3	2	3	2	3	2	1	2
14	Objectives	Assessment	2	1	3	2	3	2	3	5	2	2	3	2	1
15	Objectives	Capabilities	2	3	1	1	2	2	2	4	2	1	2	3	2
16	Objectives	Education	2	2	4	1	2	3	2	3	3	2	2	2	2
17	Objectives	Innovation	2	1	3	1	2	2	1	3	3	1	2	2	2
18	Objectives	Intelligence	4	3	3	2	3	2	8	9	2	2	1	3	4
19	Objectives	Interests	6	4	2	30	7	2	4	1	1	3	5	6	5
20	Objectives	Market	4	7	3	3	2	6	5	1	6	3	4	4	5
21	Objectives	Values	3	1	2	5	2	2	1	-	3	6	4	2	11
22	Offences	Cases	2	1	-	-	-	2	15	-	1	-	2	6	2
23	Offences	Crime	4	7	4	6	2	3	5	1	3	3	9	6	3
24	Offences	Disinformation	5	1	1	22	5	-	17	-	-	-	-	-	9
25	Offences	Hacktivism	-	1	1	-	-	-	1	-	-	-	-	2	-
26	Offences	IndEspionage	3	1	2	13	1	2	2	-	3	2	-	2	9

#	Category	Subcategory	Avg	AU-20	BR-20	CH-16	DE-16	EE-19	FR-18	IT-17	JP-18	MX-17	NL-18	UK-16	US-18
27	Offences	PolEspionage	4	2	3	7	7	-	6	8	-	1	5	4	4
28	Offences	Terrorism	6	-	1	56	-	-	2	-	3	3	-	8	2
29	Offences	Threats	2	2	2	1	2	2	3	2	2	2	2	3	2
30	Perpetrators	Attackers	9	11	7	-	9	1	24	6	9	8	11	11	9
31	Perpetrators	Criminals	19	47	3	8	5	6	16	-	1	29	38	41	30
32	Perpetrators	Hackers	1	-	3	2	-	-	1	-	-	-	-	1	-
33	Perpetrators	Hacktivists	-	-	1	-	-	-	-	-	-	-	-	3	-
34	Perpetrators	Insider	1	1	-	-	-	-	-	-	-	-	-	5	-
35	Perpetrators	Kiddies	1	-	-	-	-	-	1	-	-	-	-	6	-
36	Perpetrators	Militia	-	-	-	-	-	-	-	-	-	-	-	-	-
37	Perpetrators	NonState	1	-	1	-	2	-	2	-	-	-	-	-	3
38	Perpetrators	OrgCrime	2	-	2	4	-	1	2	-	-	-	-	5	4
39	Perpetrators	Proxies	-	-	-	-	-	-	-	-	-	-	-	-	1
40	Perpetrators	States	8	13	-	4	-	1	3	-	5	-	2	21	42
41	Perpetrators	Terrorists	1	1	-	1	2	-	1	-	1	-	-	7	3
42	Resources	Actions	2	2	2	2	1	1	1	1	2	1	1	2	2
43	Resources	Budget	3	-	4	-	-	1	4	17	4	-	-	1	-
44	Resources	Funding	3	5	4	2	1	3	2	3	2	1	3	4	3
45	Resources	Personnel	3	3	3	1	4	5	3	2	3	4	2	4	3
46	Security	ActivePosture	8	7	3	-	2	1	23	4	7	3	11	27	7
47	Security	Defence	3	2	2	4	4	4	6	5	3	1	2	5	3
48	Security	Dissuasion	6	8	-	4	1	2	5	2	7	-	3	21	22
49	Security	Industry	3	3	2	2	2	4	5	2	1	1	3	3	2
50	Security	PassivePosture	1	1	-	-	1	-	4	-	2	-	-	1	1
51	Security	Personal	-	-	-	-	-	-	-	-	-	-	-	-	1
52	Security	Resilience	5	3	10	1	6	3	2	18	3	4	7	4	4
53	Security	Security	1	1	2	1	2	2	1	1	1	1	2	1	1
54	Security	Strategy	4	7	4	2	3	7	3	4	2	6	1	5	2



#	Category	Subcategory	Avg	AU-20	BR-20	CH-16	DE-16	EE-19	FR-18	IT-17	JP-18	MX-17	NL-18	UK-16	US-18
55	Stakeholders	Academia	5	4	7	-	3	8	1	4	8	11	2	6	2
56	Stakeholders	General	5	2	4	-	1	3	5	13	10	9	8	4	3
57	Stakeholders	Government	4	5	3	1	6	4	3	3	5	3	3	5	5
58	Stakeholders	Infrastructure	2	4	2	3	1	2	2	4	2	2	1	1	3
59	Stakeholders	Media	1	-	-	-	-	2	1	-	2	-	-	2	-
60	Stakeholders	NGO	-	-	1	-	-	3	-	-	1	-	-	-	-
61	Stakeholders	Person	5	2	4	6	4	5	4	1	2	9	14	5	1
62	Stakeholders	Private	2	4	2	1	2	2	2	1	2	1	3	3	1

Source: Compiled by the author

## 6.5 Analysis of the Outliers by Subcategories

The observation of Table 15 indicates many outliers, analysed in this section. Subcategories are distinguished by their name followed by the corresponding line number, found in the “#” column. DRTI values are once more presented between parenthesis.

In the category Assets, subcategory Cyberspace (#2), CH-16 (4) and MX-17 (4) present more than twice the average (2), while AU-20 (1), IT-17 (1) and UK-16 (1) form the base reference. Regarding the subcategory SocialMedia (#4), FR-18 (10) reflects twice the concern of BR-20 (5), with AU-20 and UK-16 (1) being the base reference. No other document deals with this topic, although many deal with disinformation, generally disseminated through Social Networks. SupplyChain (#6) is a relevant concern expressed by the USA (16), followed by JP-18 (11), far from AU-20 (5) and Italy (5). The theme is absent from DE-16, EE-19, MX-17 and NL-18.

In the category Institutionalisation, International Fora (#7) presents significant differences. The leading group comprehends MX-18 (45), IT-17 (35) and EE-19 (28), while AU-20 (1) forms the base. International Law (#8), also presents significant outliers, with CH-16 (9) presenting the highest emphasis, followed by IT-17 (5), while UK-16 (1) shows the lowest concern.

In the category National, subcategory Country (#12), US-18 (44) stands out in relation to the second, EE-19 (26) and NL-18 (26), with IT-17 (1) showing the lowest incidence of references to the country in the document. The American emphasis is consistent with the America First policy of the government that issued the document.

For the category Objectives we have Intelligence Capabilities (#18) being highlighted by Italy (9), France (8) and the USA (4). Interestingly, Australia, Brazil, Germany and the UK, countries with very different cyber intelligence capabilities, denote the same emphasis (3). Also noteworthy is the case of National Interests (#19), with the reiteration of the theme by China (30) five times higher than the average (6), while Brazil (2), Estonia (2), Italy (1) and Japan (1) showing little concern. As for Values (#21), it is observed that US-18 (11) presents an incidence roughly two times higher than that of MX-17 (6) and CH-16 (5) and four times higher than the average (3).

Regarding the category Offences, Cases (#22), FR-18 (15) is more than twice as incisive than UK-16 (6), while BR-20, CH-16, DE-16, IT-17 and MX-17 do not cite cases of cyberattacks or malware with international repercussions. Concerning Disinformation (#24), China (22) and France (17) devote much more relative space than the USA (9) or Germany (5).

Estonia, Italy, Japan, Mexico, the Netherlands and the United Kingdom do not address the issue. On Industrial Espionage (#26), CH-17 (13) devotes much greater attention to the topic than the runner-up, US-18 (9), even though the most common accusations of this type of practice are made by the USA precisely against China. Political Espionage (#27) is a significant concern in IT-17 (8), CH-16 (7) and DE-16 (7). BR-20 (3) and MX-17 (1) show a relatively low concern with the subject, although having been target by political espionage by the NSA, as revealed in the Snowden Case (GREENWALD, 2014). Terrorism (#29), including radicalism, subversion, betrayal, and other terms used, is a frantic concern of the Chinese (56), cited seven times more intensely than by the British (8), which are also far from the JP-18 (3) and MX-17 (3). Australia, Germany, Estonia, Italy and the Netherlands do not cite this type of offence.

The category Perpetrators is the most dispersed among its subcategories. The generic subcategory Attackers (#30) is repeatedly cited by France (24), almost three times more than the average (9). Criminals (#31) are intensely cited by AU-20 (47), UK16 (41), NL-18 (38) and MX-17 (29). The lowest values are present in IT-17 (0), JP-18 (1) and BR-20 (3), although Brazil is, according to its strategy, plagued by cybercrime. Hacktivists (#33), are a concern only for the British (3) and Brazilians (1), being ignored by the others. Insiders (#34), are cited only by the UK (5) and Australia (1). For their part, Script Kiddies (#35), are mentioned only by the British (6) and the French (1), while Proxies (#39), only by the USA (1). The subcategory States (#40), draws attention due to the high index of the USA (42), with the UK (21) in second, Japan (5) in third and China (4) in fourth. Brazil, Germany and Mexico did not express concern about this issue, even though, again, they were victims of political espionage by the U.S. National Security Agency (NSA) in 2013 and protested at the U.N., having passed a General Assembly resolution on the matter (GREENWALD, 2014). Finally, Terrorists (#41), are a relevant concern for the United Kingdom (7) followed by USA (3), but not mentioned by Brazil, Estonia, Italy, Mexico and the Netherlands.

The category Resources shows that Budget (#43) is a significant concern for Italy (17), approximately six times higher than the average (3). The sub-category Funding for RD&I (#44), however, is more relevant for Australia (5), Brazil (4) and the United Kingdom (4).

In the category Security, the Active Posture (#46) subcategory stands out, where United Kingdom (27) is the most incisive, which is consistent with the premise of its Active Cyber Defence (STEVENS e colab., 2019). France (23) comes close and expresses its interest in becoming a cyber-superpower. The Netherlands (11) comes in third in the category, followed by Australia (7) and the USA (7). The U.S. position is not consistent with its Defend Forward and Persistent Engagement strategies (SMEETS, 2020). The Defence subcategory (#47), is

relatively homogeneous, being more emphasized by France (6) and having an average of three points, with the base being provided Mexico (1). Another subcategory with wide variations is Dissuasion (#48), where U.S. (22) and UK (21) are very distant from the next, Australia (8), Japan (7), France (5) and China (4). The only country that not addresses it is Brazil. Still in this category, Resilience (#52), shows Italy (18) and Brazil (10) lead, with China (1) being the basis of comparison.

In the Stakeholders category, there are very different emphases. Academia (#55) stands out for Mexico (11), Estonia (8) and Japan (8), Brazil (7) and United Kingdom (6). Another subcategory that calls attention is Person (#61), with NL-18 (14), MX-17 (9) and CH-16 (6) leading, whereas IT-17 (1) and US-18 (1) form the base of comparison.

## 6.6 Analysis by Country

The analysis of columns, as said, provides a perception of the most rated subcategories for each country relatively to its peers. The highest values (up to five) for some of the countries are here highlighted, in the notation “Category-Subcategory (#X, Y)”, where X is the line number and Y its value:

- Australia (AU-20): Perpetrators-Criminals (#31, 47), Nation-Country (#12, 16), Perpetrators-States (#40, 13), Perpetrators-Attackers (#30, 11) and Security-Dissuasion (#48, 8).
- Brazil (BR-20): Institutional-IntFora (#7, 17), National-Country (#12, 13), Security-Resilience (#52, 10), Perpetrators-Attackers (#30, 7) and Stakeholders-Academia (#55, 7).
- China (CH-17): Offences-Terrorism (#28, 56), Objectives-Interests (#19, 30), Offences-Disinformation (#24, 22), Institutional-IntFora (#7, 14) and Offences-IndEspionage (#26, 13).
- Germany (DE-16): National-Country (#12, 13), Institutional-IntFora (#7, 12), Perpetrators-Attackers (#30, 9), Objectives-Interests (#19, 7) and Offences-PolEspionage (#27, 7).
- France (FR-18): Perpetrators-Attackers (#30, 24), Security-ActivePosture (#46, 23), Institutional-IntFora (#7, 22), Offences-Disinformation (#24, 17) and Perpetrators-Criminals (#31, 16).
- Japan (JP-18): Assets-SupplyChain (#6, 11), National-Country (#12, 10), Stakeholders-General (#56, 10), Institutional-IntFora (#7, 9) and Perpetrators-Attackers (#30, 9).

- United Kingdom: Perpetrators-Criminals (#31, 41), Security-ActivePosture (#46, 27), National-Country (#12, 24), Perpetrator-States (#40, 21) and Security-Dissuasion (#48, 21).
- USA (US-18): National-Country (#12, 44), Perpetrator-States (#40, 42), Perpetrators-Criminals (#31, 30), Security-Dissuasion (#48, 22) and Assets-SupplyChain (#6, 16).

Tabulating the five top-rated (hereinafter “Top-5”) subcategories for all countries, and ordering the result in decrescent order by the sum (“Total”) of each subcategory, the product is that of Table 16.

Table 16 – Top-5 Subcategories per Country

Rank	#	Category	Subcategory	AU-20	BR-20	CH-16	DE-16	EE-19	FR-18	IT-17	JP-18	MX-17	NL-18	UK-16	US-18	Total
1	31	Perpetrators	Criminals	47				6	16			29	38	41	30	207
2	12	National	Country	16	13		13	26			10	19	26	24	44	191
3	7	Institutional	IntFora		17	14	12	28	22	35	9	45				182
4	40	Perpetrators	States	13										21	42	76
5	30	Perpetrators	Attackers	11	7		9		24		9		11			71
6	46	Security	ActivePosture						23				11	27		61
7	28	Offences	Terrorism			56										56
8	48	Security	Dissuasion	8										21	22	51
9	24	Offences	Disinformation			22			17							39
10	19	Objectives	Interests			30	7									37
11	56	Stakeholders	General							13	10	9				32
12	52	Security	Resilience		10					18						28
13	6	Assets	SupplyChain								11				16	27
14	55	Stakeholders	Academia		7			8				11				26
15	61	Stakeholders	Person									9	14			23
16	43	Resources	Budget							17						17
17	26	Offences	IndEspionage			13										13
18	18	Objectives	Intelligence							9						9
19	27	Offences	PolEspionage				7									7
20	54	Security	Strategy					7								7

Source: Compiled by the author

Table 16 provides some insights. A first observation that can be drawn is that out of the 62 subcategories considered, only 20 are present among the Top-5 for the 12 countries assessed, resulting in 60 possibilities (5 subcategories x 12 countries). A second observation concerns the dispersion of the “Total” concern for each subcategory.

Considering the distinction of Aggressive and Non-Aggressive regarding G-20 countries, as specified in Section 3.4, Table 16 can be subdivided into two parts. Table 17 presents the Top-5 subcategories for the “Aggressive” nations.

Table 17 – Top 5 Subcategories per “Aggressive” Nation

Rank	#	Category	Subcategory	AU-20	CH-16	FR-18	IT-17	NL-18	UK-16	US-18	Total
1	31	Perpetrators	Criminals	47		16		38	41	30	172
2	12	National	Country	16				26	24	44	110
3	40	Perpetrators	States	13					21	42	76
4	7	Institutional	IntFora		14	22	35				71
5	46	Security	ActivePosture			23		11	27		61
6	28	Offences	Terrorism		56						56
7	48	Security	Dissuasion	8					21	22	51
8	30	Perpetrators	Attackers	11		24		11			46
9	24	Offences	Disinformation		22	17					39
10	19	Objectives	Interests		30						30
11	52	Security	Resilience				18				18
12	43	Resources	Budget				17				17
13	6	Assets	SupplyChain							16	16
14	61	Stakeholders	Person					14			14
15	26	Offences	IndEspionage		13						13
16	56	Stakeholders	General				13				13
17	18	Objectives	Intelligence				9				9

Source: Compiled by the author

It can be observed that the universe of subcategories was reduced from 20 to 17. International Fora lost one position relatively to Table 16, while ActivePosture gained one, and Attackers lost two positions.

However, differences become more evident when considered the “Non-Aggressive” nations strategies, as seen in Table 18. The first difference stands for the number of subcategories present, reduced to 11, against 17 on the previous group. This event could be partially explained by the smaller number of countries (seven aggressive and four non-aggressive).

If quantitatively there is not much difference, qualitatively differences are significant. International Fora ranks as first. PolEspionage, absent for the Aggressive, enters in the scope of Non-Aggressive. Conversely, ActivePosture is missing for the Non-Aggressive, as well as Dissuasion. On the latter, it shall be noticed that Dissuasion, on the analysed documents, stands for the classic concept of Deterrence; thus an “offensive” posture.

Table 18 – Top 5 Subcategories per “Non-Aggressive” Nation

Rank	#	Category	Subcategory	BR-20	DE-16	JP-18	MX-17	Total
1	7	Institutional	IntFora	17	12	9	45	83
2	12	National	Country	13	13	10	19	55
3	31	Perpetrators	Criminals				29	29
4	30	Perpetrators	Attackers	7	9	9		25
5	56	Stakeholders	General			10	9	19
6	55	Stakeholders	Academia	7			11	18
7	6	Assets	SupplyChain			11		11
8	52	Security	Resilience	10				10
9	61	Stakeholders	Person				9	9
10	19	Objectives	Interests		7			7
11	27	Offences	PolEspionage		7			7

Source: Compiled by the author

## 6.7 Conclusion

The quantitative content analysis of the strategies reveals intriguing and thought-provoking aspects. Although in all the strategies analysed here, the entire set of identified analysis categories is somewhat homogeneous, the subcategories' developments provide insights regarding the priorities, in the cyber domain, of the states that formulated them. The frequency of citation of terms denotes quite different intensities for the concerns expressed by these Countries in their cybersecurity and cyber defence strategies, and the determination of their formulators concerning their feasibility.

From the insights provided by the quantitative data, it is possible to deepen qualitative research on particular topics of specific interest, including by grouping the desired subcategories. For example, Dissuasion relates to subcategories as Dissuasion, Defence, Resilience and Active Posture. Therefore, a researcher interested in this topic can use data pertaining to these subcategories, gathered in this work, to support this subject's research.





## 7 WHEN TWO BECOME NONE

It was only in February 2020 that Brazil published its first national strategy of cybersecurity (e-Ciber). It was the penultimate among the 15 largest economies. Besides being late, e-Ciber brought a peculiarity: it is the only strategy that only deals with cybersecurity, explicitly excluding cyber defence. Applying qualitative content analysis on e-Ciber and the cyber-strategies of some of these countries, this chapter presents the Brazilian document's peculiarities. It is shown that these particularities have deep roots in the way the Brazilian society perceives national security and defence issues, reflecting on the political and strategic choices made by decision-makers, with impacts on national capacities in the medium and long terms. The analysis also shows that, despite addressing several important issues and pointing out objectives and possible lines of action, e-Ciber is not very deterministic in allocating resources and responsibilities for the execution of these actions. This indicates that the country, although having the fifth largest territory, the sixth population, the ninth economy, and the tenth most powerful military force in the world, shall remain for some time with neither cyber defence nor cybersecurity capabilities compatible with that of its peers.

### 7.1 Introduction

In 2010, Brazil seemed to be in pace on cybersecurity with many of its peers. After the publication of *Cyberwar* (CLARKE; KNAKE, 2010) and in the wake of the initial Stuxnet revelations, the Army created the core of its Cyber Defence Centre, while the Institutional Security Office of the Presidency of the Republic (GSI) published the Green Book of Cybersecurity (MANDARINO; CANONGIA, 2010).

It was in that same year the United States created USCyberCom, the country's military cyber defence command, operating in conjunction with the National Security Agency (NSA), that country's Signal Intelligence Agency (SIGINT).

However, it was only ten years later that Brazil published its first national strategy for cyber, named e-Ciber. It was the penultimate country to do so among the 15 largest economies: United States, China, Japan, Germany, India, United Kingdom, France, Italy, Brazil, Canada, Russia, South Korea, Spain, Australia and Mexico (IMF, 2019).

Cybersecurity has developed from a niche technical subject to a long-term security policy issue over the past ten years. One of the reasons for this is the steep increase in strategically motivated cyber incidents led by state actors, which is a reflection of current geopolitical tensions. (SWI, 2020)

Brazilians often use the word *jabuticaba* (or *jaboticaba*), name of a fruit only found there, to indicate something unique to the country. E-Ciber brought a huge *jabuticaba* in its

scope: it explicitly excluded cyber defence, allegedly focusing on cybersecurity. It is not the only idiosyncrasy present in Brazilian cyber-related measures, as it will be shown. Many of them relate to national culture.

This chapter engages with the origins and impacts of the ‘Brazilian-way’ on security and defence issues, particularly on cyber. It explores historical, doctrinal and legal national evolution to bring light to some of the choices made, apparently bizarre, at first sight, to those not familiar with the Brazilian-style. Findings show that not even a recent topic like that of cyber can escape society’s culture and tradition. Comparisons take into account the documents and data quantitatively analysed in Chapter 6.

## **7.2 On Security and Defence**

### **7.2.1 The Classic Distinction and the Securitization Merge**

Traditionally, States provided two different ways of protecting their citizens and interests. Protection against external threats constituted defence, a duty of the Armed Forces, while protection against internal threats constituted security, attributed to polices. Recently, however, it is increasingly difficult to distinguish between defence and security. The process of ‘securitization’ made issues traditionally unrelated to Defence and Security begin to receive special attention from nation-states, with an expanded politicisation of specific topics and the allocation of extraordinary resources and means for their mitigation, in the name of ‘national security’ (BUZAN e colab., 1998).

Most of the arrangements made by middle powers are subordinated to international themes securitised by those at the centre of the system (BUZAN; WÆVER, 2009). The Crusades and the Global War on Terror would constitute examples of Macrossecuritization, a large-scale securitisation process in the international system, promoted by central actors of the system and involving other regional actors (BUZAN; HANSEN, 2009).

### **7.2.2 The Fusion of National Security and Defence in the Cold War**

In line with Macrossecuritization, securitisation arrangements during the Cold War are framed by the confrontation between East and West, primarily a clash between capitalism, defended by the West (USA, Western Europe and Japan), and that communism, supported by the East (USSR and the People’s Republic of China) (BUZAN; WÆVER, 2009).

In this process, great powers intensified their interference in internal affairs of smaller powers. The USSR exposed its interest in bringing ‘the revolution’ to all corners of the globe, in the beginning openly (Komintern and Kominform initiatives), and later more discreetly, but permanently.

The capitalist West (majorly the USA), by its side, felt having the right to intervene directly wherever the communist threat was present. Henry Kissinger, National Security Advisor to President Nixon, referring the election of Salvador Allende in Chile in 1971, clearly materialised this premise: “The issues are much too important for the Chilean voters to be left to decide for themselves ... I don’t see why we need to stand by and watch a country go communist due to the irresponsibility of its people” (FAGEN, 1975; LEWYS, 1975).

External interference led several nations to consider the fight against communism a matter of ‘national security’. Often engaging their armed forces. In Brazil, Argentina, Chile, Paraguay and Uruguay, to name a few, elected governments were deposed and replaced by military regimes. Their armed forces were widely used to contain the communist threat, pursuing, arresting, torturing and even executing ‘subversive elements’, terrorists or guerrillas. This would have profound repercussions on these countries' culture, so that still today there is a great difficulty in equipping their Armed Forces with the means necessary for defence due to the lack of a clear perception of who would be the enemy to be fought (SAINT-PIERRE, 2011). This situation persists in recent years since most of the political elites in these countries have been affected by the repression at that time to a greater or lesser extent or proximity.

### **7.2.3 The Institutionalization of Defence and Security in Brazil**

Coincidence or not, Brazilian military doctrine, expressed by the Brazilian War College (ESG), does not define security and defence in terms of external or internal threats. ESG, a think tank of the Ministry of Defence, created in 1950, was very influential during the military regime. Three of the five military Presidents passed through it. ESG’s doctrine establishes that security “is the necessary and indispensable guarantee of a society and each of its members, against *threats of any kind*” (BRASIL-MD, 2014, p. 76, emphasis added). It also states that “Security is a sensation, whereas Defence is action” (BRASIL-MD, 2014, p. 77).

Significantly, it establishes that insecurity can “assume very subtle forms, such as those arising from the undue intrusion of external cultures that attack the national cultural identity” (BRASIL-MD, 2014, p. 76, free translation). “Defence” is the mitigation of these threats, that can come from social, political or cultural factors, internal and external. Emblematically, it states that “National Defence is the set of attitudes, measures and actions of the State [...] against *predominantly external, potential or manifest threats*” (BRASIL-MD, 2014, p. 82, free translation, emphasis added).

The doctrinal merge of security and defence is even more explicit:

In view of the source of the threats, National Security must be analysed in two areas:  
External and Internal.

When coming from threats of any origin, form or nature, located in the environment of international relations, National Security will be sought through External Defence actions. In the face of threats that may manifest or produce effects within the country, this is Internal Defence. (BRASIL-MD, 2014, p. 82, free translation)

Therefore, within National Security, there can be External Defence and Internal Defence. Thus, doctrinally, Brazil does not differentiate defence and security in the context of external or internal threats.

In its Article 144, the Brazilian Constitution stipulates that public security is exercised by federal and state police forces. However, Article 142 states that the Armed Forces “are destined to defend the Homeland, guarantee constitutional powers and, by an initiative of any of these powers, guarantee law and order” (BRASIL-CN, 1988, free translation). Thus, armed forces can be employed for guaranteeing law and order by an initiative of any constitutional power.

#### **7.2.4 Post-Cold War Securitisation**

Since the end of the Cold War, Europe and South America are, respectively, the two most peaceful areas on the planet, without the occurrence of major interstate conflicts (FRANCHI e colab., 2017; HERZ, 2010). In the European Union, the (at least momentary) absence of a perceived external enemy, and the logic of securitisation, were arguments for justifying the use of Armed Forces and national intelligence agencies, along with public security forces, for controlling activities such as terrorism, transnational crimes, or even human migrations: two become one (BIGO, 2000).

A similar process occurred in Brazil. Since 2010 (Complexo do Alemão), Brazilian armed forces have been ostensibly and increasingly engaged in public security, culminating with the Federal Intervention in the State of Rio de Janeiro in 2018. The prestige of the Armed Forces and the population’s sense of insecurity, resulting from the failure of other internal security mechanisms, as well as the need to present responses of public appeal in the short term, also weighed in, leading government officials to the temptation of using the military regularly in public security actions (SAINT-PIERRE, 2011).

For years, military reluctance against engaging in public security focused on their lack of legal support in case of prosecution: if a military, involved in street combat, would injure or kill civilian citizens, criminals or not, he would face common justice. A law<sup>14</sup> passed in October 2017 determined these cases will be carried under military justice (AQUINO; 2017). Proposed

---

<sup>14</sup> Law 13,491/2017.

to Congress in early 2016, it intended legal support for the military involved in the security of the Rio Olympics of July. Still, it was only approved more than a year after the games' closure, exemplifying the Congress's lack of attention to military issues, even when involving the security of international events.

Brazilian armed forces themselves apparently seek to justify investments by participating in security actions, as seen on two of the Army's strategic programs. The Brazilian Army Project Management Office (EPEX) describes the Integrated Borders Monitoring System (SISFRON) main guideline as "the integrated action of public security bodies, the Armed Forces and the Federal Revenue Service, in addition to other federal, state and municipal [security] agencies" (EPEX, [S.d.]). In the same vein, on the Cyber Defence program, it states:

The program will also contribute to the increase of the national capacity of **fighting cybercrime**, linked to transnational threats, by integrating the actions of the MD, the Armed Forces and the government agencies involved in these activities. (EPEX, [S.d.], free translation, emphasis added)

Amidst this conceptual misty between security and defence, Brazil today lives a paradoxical scenario. As a military regime's legacy, it has the most potent armed forces in South America (GLOBALFIREPOWER.COM, 2020). However, due to the absence of a substantial and perceivable external threat, Brazilian society does not clearly understand the need for investments on armed forces, making them gradually become obsolete and under-equipped.

Additionally, there is a historical distrust regarding military interventions in the political environment, particularly, the military regime, with many of those then considered 'subversive elements' nowadays in prominent political or media positions. This makes the negotiation for budgets and legal issues very difficult. Symptomatic, perhaps even emblematic, is the attempt to 'escape' of the terminology of that period. While previously there would be a National Defence Strategy, where national was the defence, nowadays there is the National Strategy of Defence, where 'national' is the 'strategy'. Even in the case of the National Policy of Defence which, according to the legislation, should be named National Defence Policy, but adopts an 'artistic name' less associated with that of the past (BRASIL-CN, 1999; BRASIL-MD, 2016).

In this context, the so-called 'defence documents' – National Policy of Defence (PND), National Strategy of Defence (END) and White Paper on National Defence (LBDN) – are legally required to be submitted to Congress every four years (BRASIL-CN, 1999). The Ministry of Defence presented them in 2008-2009, 2012 and 2016. The 2012 version was never discussed by the Congress, while the 2016 one only passed on December 2018 (BRASIL-SENADO NOTÍCIAS, 2018).

Not even the projects of the strategic sectors determined since 2008 by END for each branch progress adequately. For the Air Force, the Brazilian space program faces successive delays and cuts. The Alcântara Launch Base has not launched a rocket since the accident with the Satellite Launch Vehicle (VLS) VLS-3 in 2003 (D'ALAMA, 2013). The forecast launching of VLS-4 in 2017 did not materialise. In 2017, it was predicted that instead of a VLS, a Microsatellite Launch Vehicle (VLM), smaller and cheaper, would be launched in 2019 (MALTCHIIK, 2017). This launch did not occur.

For the Navy, the Nuclear Submarine Program (PROSUB) advances slowly. Still, for this purpose, the Navy sacrifices the maintenance of its surface fleet. With more than 9,000 kilometres of coast, Brazil has only eight frigates, all of them more than 30 years old, and many moored due to the lack of replacement parts. Besides, their lifespan is limited to the middle of the decade, and they shall be replaced by corvettes, smaller, cheaper, and with less firepower (NAVAL, 2017).

For the Army, the cyber program is still in its infancy. The Cyber Defence Command (ComDCiber), created in 2015, counts roughly 200 military personnel. France, for example, having an economy of similar size, a smaller contingent in its Armed Forces, and a population less than a third of the Brazilian, has more than 6,000 military personnel on cyber defence (MALAGUTTI, Marcelo, 2017a). Brazilian National School of Cyber Defence (ENaDCiber), planned to start operating in 2017, only began in 2019 (BRASIL-MD, 2019; OKAMURA, 2017).

### **7.3 On Strategy and Strategic Communication**

Strategy, in the Brazilian doctrine, is “[the] art of preparing and applying power to achieve and preserve goals, overcoming obstacles of all kinds” (BRASIL-MD, 2014, p. 56). Therefore, a national strategy must specify the intended objectives, perceived obstacles, and actions to prepare and apply available means for achieving and preserving the objectives, overcoming all kinds of obstacles. In other words, they must establish the nation’s future vision regarding objectives and perceived threats, and drive the society in the elaboration of public policies and the pursuit of its objectives and the mitigation of these threats.

Besides, National Strategies, by definition, must be strategic communication pieces. As such, they must be based on the principles governing this type of communication. The seminal definition of strategic communication is “using communication with a purpose” for an organisation to fulfil its objectives (HALLAHAN e colab., 2007, p. 3). Critics

observed that it is not enough to define strategic communication as communication with a purpose, because “whether to inform or amuse, request or command, implore or proselytise, frighten or calm down, all communication is imbued with some essential intention” (BETZ; PHILLIPS, 2017, p. 46).

The words *strategic* and *communication* are particularly significant: communication activities must be strategic, not “random communications” (HALLAHAN e colab., 2007, p. 4). Strategic is something “substantial or significant for an organisation’s or other entity’s development, growth, identity, or survival” (ZERFASS e colab., 2018, p. 493).

In the political context, strategic communication is practised by public officials, politicians, and interest groups to build consensus on the exercise of power and for the allocation of resources in society. At the international level, this includes communication in support of official diplomacy and military stabilisation (HALLAHAN e colab., 2007, p. 6). The practitioners of strategic communication are agents used to establish corporate ideologies, in a process of influence usually associated with the creation of meaning in the exercise of power (HALLAHAN e colab., 2007, p. 15).

Strategic actions have no immediate consequences; therefore, they cannot be quickly corrected or reversed; when they are mistaken, it is usually too late to choose another path (ZERFASS e colab., 2018, p. 493).

Besides, “the public, regular presentation of defence policies and strategies is one of the cornerstones of democratic governance and serves diplomacy to preserve, protect, and support international peace and security” (PROENÇA JR.; LESSA, 2018).

Consequently, a National Strategy must attend to the principles of: (1) communicating what is essential for influencing and achieving the intended purposes; (2) maintaining terminological cohesion for creating meaning; (3) considering that the proposed actions are long-term and that their correction or adequacy in case of error will be a time-consuming and challenging process; (4) indicating the intended objectives and the actions and resources to be allocated to achieve the established goals.

It will be shown that e-Ciber failed in all of the four premises. As observed by Patricia Peck, e-Ciber ‘falls short’:

In comparison with the strategies developed by other places, such as Chile, the United States or the European Union (Directive No. 2016/1148), Brazil is still far behind in terms of writing, organisation, and mainly of orientation and execution of essential points, such as how the financial resources will be gathered to implement the fundamental dimensions to be worked on. (apud HAIKAL, 2020)

#### 7.4 Impacts in Brazilian Cyber Defence and Cybersecurity

USA, China, France, the United Kingdom and Germany are commonly cited as cyber-superpowers. For its cyber defence, Germany opted for a new branch of its armed forces. China for a strategic command. The USA, the United Kingdom and France<sup>15</sup> created joint commands bringing together personnel from their various military services, subordinate to the Joint Chiefs of Staff or similar. Conceptually, a joint command is subordinated to the Head of Government, the Ministry of Defence, or at least the Joint Chiefs of Staff, rotating commanders among the branches, and ensuring greater cohesion of defence efforts. In all of these countries, the command of military cyber defence is exercised by a 4-stars general. Moreover, they all integrate their cyber forces with their Signal Intelligence agencies (SIGINT) (MALAGUTTI, Marcelo, 2017a).

Brazil, differently, opted for a 'joint command' under a single service branch, the Army. Besides, within the Army, ComDCiber is under the Directorate of Science and Technology (DCT), a research and development department, and not one of the Army's operational commands (BRASIL-MD, 2020a). Finally, ComDCiber is a 3-stars command. Possibly due to its relatively minuscule staff compared to those of the countries mentioned (which, due to limitations of scope and space of this Chapter, cannot be discussed here).

Despite these (severe) limitations, critics argued that the focus of resource allocation in Brazil should be on cybersecurity, and not on cyber defence, since the country suffers the second largest number of cybercrimes in the world (DINIZ e colab., 2014; MUGGAH; THOMPSON, 2016). Notwithstanding the already mentioned fact that the Brazilian Army itself indicates that ComDCiber will help in fighting cybercrime and that the Command's history of success commonly refers to the "protection of major events" (CAIAFA, 2018). Possibly, this misperception of a concentration in cyber defence comes from the national capillarity, size and organization of the Army in comparison with other institutions. The staff of ComDCiber, although relatively small in international comparison, is larger than that of other Brazilian government institutions, and when working in interagency operations the military are usually preponderant in number and structure.

Once more, the increased visibility of security aspects induces reasoning of greater urgency than defence issues. Although the three most mediatic episodes involving cyberspace relate to state-sponsored cyber-offences: WikiLeaks, Stuxnet and Snowden. WikiLeaks showed thousands of USA diplomatic messages regarding many countries, including Brazil. Stuxnet,

---

<sup>15</sup> In April 2018, France announced its intention of creating a 'fourth force'.



although infecting Brazilian installations, did not cause damage (but many concerns!), since targeting specifically Natanz (MALAGUTTI, Marcelo, 2016c). In the Snowden case, USA espionage involving the Brazilian President and its largest company, Petrobras, became evident (GREENWALD, 2014).

In the wake of the Snowden case, in 2013, a Parliamentary Commission of Inquiry (CPI) investigated foreign electronic espionage in Brazil. It unfolded another nefarious consequence of the historical mistrust of the political class in the military. The use of the National Information Service (SNI), including the interception of telephone communications, by the security apparatus during the military regime, put intelligence activity under suspicion. Legislation after the military government has significantly restricted these capabilities. SNI itself was extinguished in 1990, and only in 1999 the Brazilian Intelligence Agency (ABIN) was created, with no SIGINT capabilities. The CPI report, in 2014, suggested the creation of such an agency, which has not yet been done (BRASIL-CN, 2014).

Similarly, the Brazilian cyber legal framework has been rapidly evolving regarding the protection of individual guarantees and the classification of crimes carried out with cyber means. Examples are the *Carolina Dieckmann Law* (2012), *Marco Civil da Internet* (2014) and LGPD (2018), the Brazilian version of the European GDPR (EUROPEAN UNION, [S.d.]). No legislation, however, grants the State cyber intelligence capabilities.

Another usual criticism is the lack of participation of the ‘organised civil society’, academia and the private sector in the formulation of cyber-related policies (BEER, 2015; DINIZ e colab., 2014).

## **7.5 A ‘Brazilian-Way’ Cyber Strategy**

In October 2019, GSI released a public consultation on the preliminary text of the future Brazilian e-Ciber, consolidated and published in February 2020. As expected, it reflects much of the Brazilian culture, social memory, tradition, historical institutionalism and ‘face’, as shown ahead.

### **7.5.1 On Scope**

E-Ciber differed from other strategies in its scope. Despite Brazilian doctrine merging security and defence issues, every nation combining security and defence in its cyber strategy, and indeed Brazilian ComDCiber reinforcing cybersecurity, e-Ciber explicitly excludes cyber defence, that shall be in a separate future document under the responsibility of the Ministry of Defence. The justification, rhetorical, argued that the National Information Security Policy

(PNSI) states that the National Strategy of Information Security (ENSI) “will be divided into the following modules, *among others*”:

I - cybersecurity;

II - cyber defence;

III - critical infrastructures’ security;

IV - sensitive information security; and

V - protection against data leakage. (BRASIL-GSI, 2018, Article 6, free translation, emphasis added)

The separation based on this, though, generates a paradox regarding critical infrastructures (CIs). In fact, “security of critical infrastructures”, as stipulated in item III, is more comprehensive than “cybersecurity” of CIs, “sensitive information security” of CIs, and also “protection against data leakage” of CIs. Thus, there should not be any reference to the cybersecurity of CIs in e-Ciber, since it should be in the CIs module.

If, oppositely, one understands that cybersecurity is an item that encompasses cybersecurity of CIs, it can be deduced that the same principle applies to the cyber defence of CIs, to sensitive information security of CIs and the protection against data leakage of CIs. Each should be included in its corresponding module. In such a case, there would be very little left, under information security, for a module related to the protection of CIs.

Both alternatives sound logically absurd. Therefore, it appears that the legislator (GSI itself), understood that the National Strategy for Information Security should be one strategy comprehending at least those five modules, but not separately. Yet, this seems to be their new interpretation.

Nonetheless, e-Ciber complies with the Brazilian doctrinal tradition of mixing up security and defence and the technical difficulty of separating these topics in the cyber realm. Concerning the first, it states it intends to reduce the vulnerability of “government organisations” (only) “against any type of cyber threat” and attacks “carried out by countries, groups or individuals”. Thus, ‘external and internal defence’. On the latter, e-Ciber cites Cyber Guardian, an interagency exercise promoted by the military with the participation of GSI and representatives of CIs and other agencies, for exercising the decision-making process, responsibilities, and communication flow in face of different kinds and levels of cyber threats, thus reinforcing the need of joint security and defence efforts in what regards the cyber realm.

Everything indicates that the real motivation for this sui-generis separation is not, then, a legal imposition. One hypothesis is that the cyber defence module was not yet ready and could not be integrated into the document. Another possibility is that of the greater importance attributed to security, in opposition to defence. It would be justified by: (1) the public perception of the need for cybersecurity, due to the large volume of cybercrime and its repercussion in the media; (2) public criticism to Brazilian investments in cyber defence, although already small; (3) the absence of clear visibility (and the desire for NOT naming any “external enemies” for cyber defence; (4) the lack of culture on the importance of SIGINT and the fear of its use against civil rights. Indeed, e-Ciber states, in section 1.1, that cybersecurity is considered the “most critical and present area [of ENSI] to be addressed”. In any case, it signalled internationally that cyber defence remains secondary to Brazil.

Although allegedly focused in cybersecurity, thus on fighting cybercrime, and clearly stating that the country intends to sign bilateral and multilateral agreements on the matter, the largest international treaty on cybercrime, the Budapest Convention, is not cited once in it. Even though Brazil officially announced, two months before the publication of e-Ciber, its intention on joining that convention (BRASIL-MRE; BRASIL-MJSP, 2019).

### **7.5.2 On Objectivity, Verbal Moods and Language**

As seen, in strategic communication, every topic must be relevant to the entity’s mission. Information must be restricted to the minimum necessary and sufficient. This argument for simplicity is consistent with the logical principle known as Occam’s Razor, whereby if in everything else the various explanations of a phenomenon are identical, the simplest is the best. Moreover, the adage “writing is the art of cutting words” should always be kept in mind (NOGUEIRA, 2010). Despite, e-Ciber’s text lacks simplicity and denotes the concern of not being incisive or deterministic in its propositions, making the text too copious, extensive and repetitive.

The cyber strategies of the USA, the United Kingdom, Germany, China and Italy are incisive and affirmative. They primarily use verb tenses of the indicative mood, particularly with frequent use of the future tense. E-Ciber, for its part, makes extensive use of verb tenses in the subjunctive mood.

This option impacts the strategy’s credibility. Verbal forms in the indicative mood refer to facts credible or considered as such: I sing, I sang, I will sing; the subjunctive mood refers to uncertain events: maybe I sing, if I sing (BECHARA, 2009, p. 264). The subjunctive mood, then, expresses unfinished, liable to be carried out, uncertain, fanciful or imaginative actions,

usually denoting condition, hypothesis, desire, request or doubt. The subjunctive mood is associated with the use of ‘if’, ‘when’ and ‘that’ associated with verbs (BECHARA, 2009, p. 302–3; 306–7).

One example of uncertainty and lack of objectivity is:

It is noteworthy that the country intends to seek bilateral cooperation agreements on cybersecurity with the largest possible number of countries, as a demonstration of our intention to establish, in this field, relations **that shall be** appropriate, fruitful, constructive and transparent. (BRASIL-GSI, 2020, free translation, reference added)

The expression “that shall be” reflects a future intention. If deleted would not alter the meaning of the text in any way. Besides, the set of words “intends [...] demonstration [...] intent” shows an ideal perceived as distant. The text maintains its cohesion and informational content if replaced by

Brazil will establish, with the largest possible number of countries, appropriate, fruitful, constructive and transparent bilateral cooperation agreements on cybersecurity.

But why would a country intend to establish an agreement that is not appropriate, fruitful, constructive or transparent? Hence, the text could reflect the objectivity required in strategic communications and found in the other cyber strategies analysed:

Brazil will establish bilateral cooperation agreements on cybersecurity with the largest possible number of countries.

Even in e-Ciber proposed “Strategic Actions” this non-deterministic nature is present. Action 2.3.1 states “Among the actions **that can be adopted** in this regard [...]” (emphasis added). Action 2.3.6 establishes that “can be taken actions as”, while 2.3.7 cites “actions to be considered”. Similar situations there are in actions 2.3.8, 2.3.9 and 2.3.10.

Finally, reinforcing its non-deterministic nature, (very Brazilian, indeed) there are at least two dozen recommendations (not determinations), mostly written literally in the form “E-Ciber recommends [...]”.

### 7.5.3 On Document Structure

No other cyber strategy has an introductory section proportionally as long as the Brazilian one. Only the French presents a contextualisation as extensive as that of Brazil. No other has a section with bibliographic references.

E-Ciber structure differs even from those of the National Policy of Defence and the National Strategy of Defence (END) (BRASIL-MD, 2016). This raises some questions. Why

is e-Ciber structurally different from END? Will other ENSI modules follow this pattern? Or will ENSI be a set of modules of different structures?

E-Ciber also presents an unjustified concern in describing its elaboration methodology, making it more an academic document or a technical study than a strategic communication piece. No other cyber strategy describes the methodology used in its development. E-Ciber concern seems related to criticisms on the lack of previous public debate (DINIZ e colab., 2014).

One other aspect refers to the extensive references to legal provisions and past actions. In the other strategies, references to specific legal instruments are rarely found. Only the French does them, but only a few and using footnotes. For its part, e-Ciber is prolific in 'in-text' citations to laws, decrees and even normative instructions (and more surprisingly, their addenda). This indicates a constant concern in showing compliance with the legal framework, disregarding the premise that a national strategy approved by a Head of State and Government is expected to conform with the legal framework, being unnecessary to mention each norm systematically. E-Ciber concern seems a previous defence against accusations, typical during the military regime, of State agents breaking the law.

Moreover, as a strategic document e-Ciber should point to and indicate future trends and actions. As it states, it "constitutes a clear guidance from the federal government to Brazilian society on the actions it intends". Therefore, it should focus on the future, not in the past. However, in several points, it describes past actions, some almost two decades old, denoting a concern in explaining or justifying the options made or decisions taken then, or even some institutions' existence. The other strategies only refer to the past when citing emblematic cyberattacks, as examples of threats. E-Ciber does not mention any famous cyber incident.

#### **7.5.4 On References**

When official documents cite companies or individuals, they offer a form of 'endorsement' that gives international importance and relevance to those named. This endorsement has commercial value. When the British cite Cisco and Symantec, it states the UK's Government confidence in them, enabling both to develop marketing campaigns exploiting such credibility. It also makes room for questioning why it used data from Symantec and not from any other renowned competitor. The USA, which houses many IT giants, does not mention a single company, research or researcher in its strategy. Neither does Germany, China or Italy. E-Ciber cites many companies and persons.

Many citations relate to data with no strategic relevance. Information science consolidated the concept of knowledge hierarchy, or DIKW chain (an acronym for data, information, knowledge, wisdom). Conceptually, raw data carries no information, information in itself does not carry knowledge, and so forth. A photo, without any context, says little or almost nothing to a random person. It is merely raw data. However, if the person analysing the picture has some context, such as the date it was taken, the location or name of the person photographed, that photo becomes information. A popular metaphor associates data to ‘know-nothing’, information to ‘know-what’, knowledge to ‘know-how’ and wisdom to ‘know-why’ (ZELENY, 1987).

Shortly after, ‘understanding’ was added to the chain, making it DIKUW, and a new metaphor created. Data are just absolute symbols; information is the data processed, answering questions such as ‘who’, ‘what’, ‘when’ and ‘where’; knowledge is the application of data and information to answer ‘how’ questions; understanding is the appreciation of ‘why’; and wisdom is the gauged understanding (ACKOFF, 1989).

Hence, decontextualised data is not useful for decision-making. Nonetheless, e-Ciber brings dozens of decontextualised or statistically irrelevant data. As the case of a poll conducted with 200 large and medium Brazilian companies. Is this a relevant number? Of those, 34% (68 companies) faced some sort of cyber incident. Of them, 29% (thus 20) had an operational impact. Is this much? Also, among those 68, 4% (therefore 2.7) had a reputational impact with customers. What are the international figures? Is it a solid foundation for strategic decision-making? One more example regards the use of digital certificates, where the text states that from issued certificates “only 8.4%” are for citizens personal use, while 45.9% were for corporations, silencing about the remaining 45.7%. Are these numbers relevant for making or communicating strategy?

Besides, there is an unnecessary detailed, copious, lengthy list of Brazilian CSIRTs and another one of exemplificative international fora these CSIRTs could participate in for improving their networking.

## 7.6 Conclusion

The development of security and defence capabilities in any society depends on the cultural factors that determine its strategic posture: its perceptions, traditions, reputation (face) and institutions. Furthermore, the Brazilian cyber strategy reflects much of the ‘Brazilian-Way’: avoiding incisiveness, confrontation, or even resource or responsibility allocation. Also, as institutionalised in the last 40 years, a resistance to any hint of state empowerment.

Besides being quite late, e-Ciber ‘falls short’ failing in all four pillars that construe a good national defence and security strategy. First, it does not communicate what is essential for the exercise of influence and the achievement of the intended purposes. Indeed, it is ‘shy’ in its intentions, with too many ‘would’ and a few ‘will’. Second, it does not maintain linguistical cohesion for creating meaning and unity. Third, it does not consider that the proposed actions are long-term and that their correction or adequacy in case of error will be a time-consuming and challenging process. Fourth, although it does indicate intended objectives, it does not specify responsibilities and resources for the intended actions to achieve their goals. E-Ciber seems, in fact, a letter of (good) intentions, not a national strategy. It fosters neither security nor defence. The *jabuticaba* of splitting cybersecurity and cyber defence strategies risks resulting in two becoming none: neither security nor defence.

It has some merit, however. Mainly that of being implemented in a collaborative and participatory way, from the diagnosis phase to the prescription of actions, and open to public consultation. This consultation allowed the correction of many points, with the final result being much better than the original one.

In a very Brazilian-Way, still, it shall be said that although strategic errors are difficult (and take longer) to correct, time fixes everything. Thus, in the long run, the final result can be significant, even satisfactory, since at least e-Ciber points, even if vaguely, in some direction.





## 8 BRASILIAN CYBER CAPABILITIES

This chapter analyses the need of upgrading Brazilian Cyber Defence Command (ComDCiber) to meet the needs of the country, considering aspects such as the placement of the body within the organizational structure of Brazilian Ministry of Defence, its mission and structure, as well as factors related to the sizing, acquisition and retention of personnel, either military and civilian.

### 8.1 Introduction

Between the creation of the Army's Cyber Defence Centre (CDCiber) in 2010 and the launch of e-Ciber in 2020, Brazil's "peers" moved faster, allocating significant resources to their cyber defence structures.

In 2014, four years after the creation of USCyberCom, the USA announced its intention to, by 2018, create a Cyber Mission Force (CMF), to be constituted by 133 Cyber Mission Teams (CMTs), distributed among the different singular forces of the country and constituted by a total of 6,200 professionals, operationally prepared to perform offensive and defensive military cyber operations (U.S. ARMYCYBER, 2020). In August 2017, USCyberCom received Full Combatant Command status. Thus, it became independent from USStratCom (U.S. Strategic Command), therefore better able to manage its budget (MARKS, 2017).

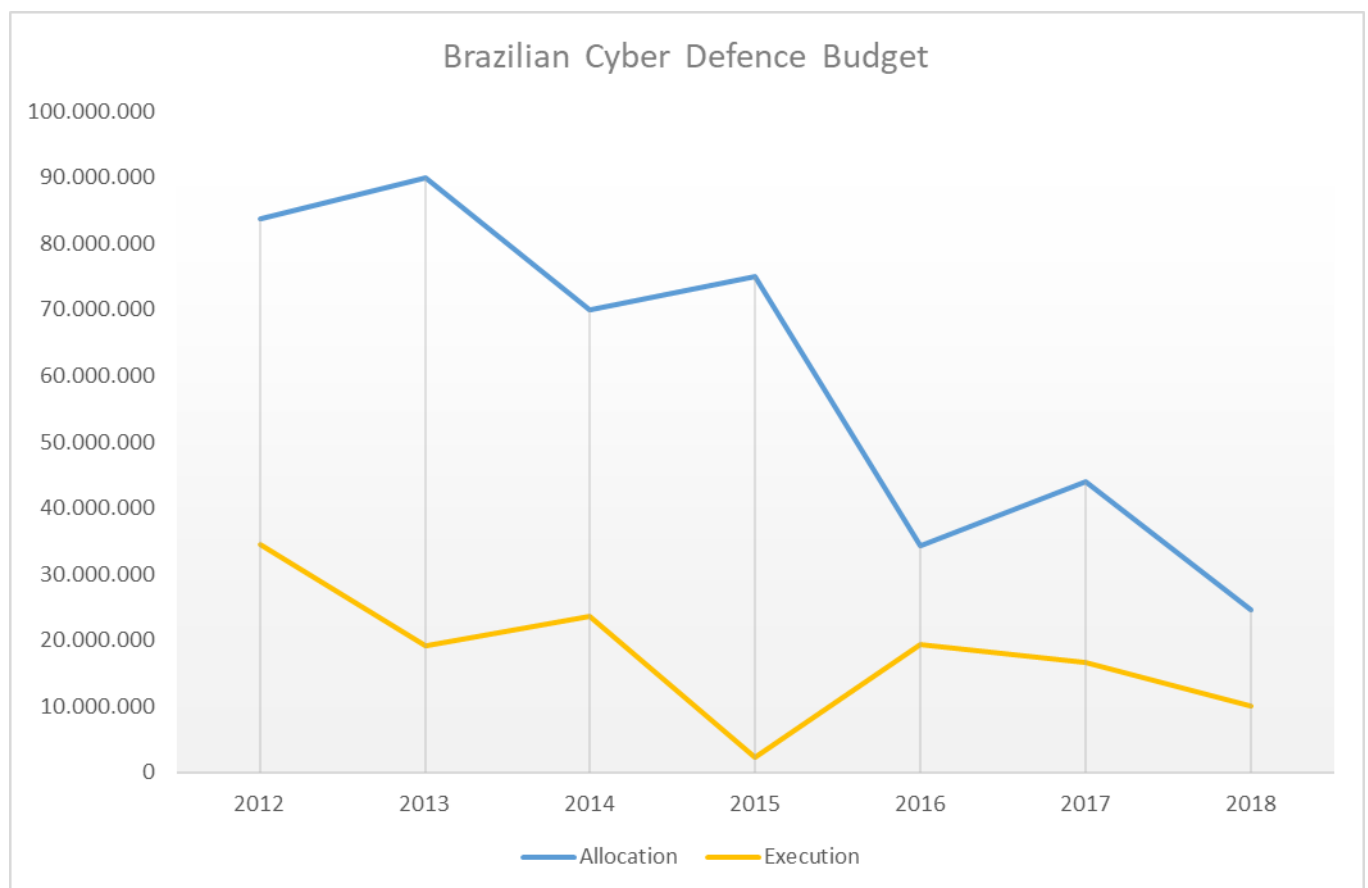
The United Kingdom, in turn, in 2015 announced the recreation of the 77th Battalion, with 1,500 members, to fight information warfare, focusing on social networks (PAGANINI, 2015). In 2016, at the launch of its Cyber Security Strategy 2016-2021, it announced investments of 1.9 billion sterling pounds (GBP), equivalent to Brazilian Reals (BRL) 13.5 billion, in the UK's cybersecurity over the next ten years (UNITED KINGDOM, 2016). The value corresponds to an average of BRL 1.35 billion annually. In 2017, the National Cyber Force was announced, with an eminently offensive character, linked to the Ministry of Defence and the GCHQ (UK SIGINT agency), with an initial staff of 500 professionals from the Armed Forces, GCHQ and third parties, which shall be expanded to more than 2,000 professionals in three years, at the cost of GBP 250 million (BRL 1.78 billion) (HAYNES, 2018; SABBAGH, 2020).

Australia, in August 2020, published a new version of its Cyber Security Strategy (AUSTRALIA, 2020). The document foresees Australian government investments of 1.67 billion Australian dollars (AUD), or BRL 6.5 billion, over ten years (AUSTRALIA, 2020, p. 4). It also emphasizes that its precursor, the 2016 cyber-strategy, promoted an investment of AUD 230 million (circa BRL 900 million) in its four years of effectiveness (AUSTRALIA,

2020, p. 8). Furthermore, the Australian government's average investment was BRL 225 million per year between 2016-2020 and shall raise to BRL 650 million between 2020-2024. The investment would be justified based on estimates that cyber incidents can cause losses of up to AUD 29 billion, or 1.9% of the country's GDP, annually (AUSTRALIA, 2020, p. 10).

Brazilian e-Ciber makes no mention to investment amounts. A report by the Federal Senate pointed out that the Brazilian cyber defence budget in 2020 was only BRL 22 million (or USD 4.16 million), of which only BRL 6.1 million have been allocated to ComDCiber (AMIN, 2019, p. 56). Moreover, as shown in Figure 4, the cyber defence budget has been decreasing over the years, in the opposite direction to what is observed in other countries.

Figure 4 – Evolution of Brazilian Cyber Defence Budget



Source: Compiled by the author with data from Amin (2019, p. 55)

The Senate report also points out that losses resulting from cyber incidents in Brazilian companies in 2018 would have been USD 20 billion (AMIN, 2019, p. 25). This is equivalent to AUD 28 billion, an amount similar to that of Australian losses. However, in comparative terms, the Brazilian cybersecurity budget corresponds to only 3% of the Australian one, even though the Australian GDP corresponds to about 70% of the Brazilian. Moreover, the report

indicates that the budget should be BRL 60 million by 2020 (or USD 11.5 million), and BRL 120 million (USD 22.7 million) per year for the next three years (AMIN, 2019, p. 56).

## 8.2 Compared Analysis of Cyber Defence Structures

Table 19 shows public data on cyber defence structures in various countries, considering intelligence agencies and signals counterintelligence, cybersecurity (civilian) and cyber defence (military) and the year of publication of its first cyber strategies.

Table 19 – Organisations of Cyber Defence and Security.

Country	Intel.	Counter Intel.	Security	Defence	Attack	1 <sup>st</sup> NCS S	Staff Size
USA	NSA CIA NGA	FBI	DHS NIST	NSA	USCyberCom	2003	7,000 (NSA) 6,200 (USCyberCom)
China	3rd Dep (EM-EPL)	3rd Dep (EM-EPL)	3rd Dep (EM-EPL)	4th Dep (EM-EPL)	4th Dep (EM-EPL)	2003	“hundreds or thousands” (Unit 61398)
France	DGSE	DGSI	ANSSI	CALID	ComCyber	2008	3,500 (CyberCom) 600 (ANSSI)
UK	GCHQ (NCSC)	GCHQ (NCSC)	GCHQ (NCSC)	GCHQ (NCSC)	GCHQ & MoD	2009	1,900+ (NCSC) 2,000 (NCF)
Germany	BND BSI KSA	BfV	BSI	CIR	CIR	2011	13,600 (CIR)
Brazil	N/A	N/A	GSI/DSIC	ComDCiber	ComDCiber	2020	180~

Source: Compiled by the author with data from (BARLOUET, 2016; BRANGETTO, 2015; BRASIL-CN, 2014, p. 137; HAYDEN, 2016, p. 127–152; OSBORNE, 2015; OSULA, 2015; PERNIK e colab., 2016; RAUD, 2016; SCHULTE, 2017; STOKES, 2015)

Of the countries listed above, Germany and China opted for the creation of independent forces, while the USA, France<sup>16</sup> and the United Kingdom act with commands that bring together personnel from different individual forces under a unified command, subordinated to the Joint Chiefs of Staff or a national strategic command, while also maintaining teams dedicated to the

<sup>16</sup> In April 2018, France announced that it intends to follow Germany in creating a dedicated “fourth force”.

defence of the specific networks of each singular armed force. Such actions aim to ensure greater cohesion of cyber defence efforts. Except for Brazil, all nations integrate their cyber defence forces with their signal intelligence agencies (SIGINT), and in all of them the command of military cyber defence is exercised by a 4-stars General, the highest military post in conditions of peace.

### 8.3 The Peculiar Organization of Brazilian Cyber Defence

Among the countries analysed, Brazil opted for a unique organization. The current structure of Brazilian cyber defence is composed of the Cyber Defence Command (ComDCiber), a “joint command” subordinated to the Army Command (Brazilian Army). Although political arguments can be used to try to justify this option, it constitutes another *jabuticaba*. Furthermore, unlike the cases of the nuclear program, which is an exclusive strategic responsibility of the Brazilian Navy, and the space program, an exclusive strategic commitment of the Air Force, cyber defence, although assigned to the Army, constitutes a joint command of the three singular branches of the armed forces. Conceptually, a joint command would be expected to be linked to the Joint Chiefs of Staff of the Armed Forces (EMCFA) or the Ministry of Defence (MD), as is the case of the other countries analysed, and not to a single force.

In addition to the unusual situation mentioned above, Brazil presents another idiosyncratic feature. Within the Army structure, ComDCiber is under the Department of Science and Technology (DCT), an organ eminently linked to technological research and development (BRASIL-MD, 2020a). Subordinate to ComDCiber is CDCiber, which is its operational branch, both defensive and offensive. Therefore, it is an operational command linked to a science and technology body, which constitutes another unusual situation (BRASIL-MD, 2020a).

ComDCiber, alongside CDCiber, has a Joint Chiefs of Staff (EMC) and a Department of Management and Education (DGE). ComDCiber is commanded by a 3-stars General, while CDCiber, EMC and DGE commanders are 2-stars Generals. As the Army has the formal responsibility for cyber defence, both ComDCiber and CDCiber commanders come exclusively from Army ranks. Therefore, the “joint” characteristic restricts the Navy and the Air Force’s participation in commanding EMC and DGE (BRASIL-MD, 2020a).

There are some problems with this Brazilian conception. The relatively low hierarchy of ComDCiber poses difficulties regarding the coordination of actions, even within the Brazilian Ministry of Defence (MoD). An example of this can be found in the National Defence

Strategy of 2016, which, while reaffirming that cyber defence is a strategic sector under the responsibility of the Army (BRASIL, 2016, p. 31) states what follows:

Considering that **the Air Force** is configured as a **highly technological organization**, it is essential the protection capacities of the **Command and Control Systems and Strategic Structures of the Country, especially those that involve cyberspace**. It must therefore maintain the level of security and defence of its computer systems to a high degree. (BRASIL-MD, 2016, p. 30, emphasis added)

Despite several criticisms on the excerpt, including from myself, the new version of END, sent in July 2020 for Congress deliberation, kept exactly that same text (BRASIL-MD, 2020b, p. 55).

Second, being hierarchically in a relatively low position within the Army's organization chart, its fight for resources becomes quite unbalanced. Only after the defence budget has been divided among the MoD and the singular forces will ComDCiber have its budget determined, competing with the various priority projects within the Army. Besides, although it is a *de facto* operational command, as it is under the Army's R&D structure, Brazilian culture makes it overlooked in the dispute for resources with the *de jure* operational areas. An example of this is found in the Senate Report on Cyber Defence Policy, which poses:

We presented an amendment suggestion to the Committee on Foreign Relations and National Defence - CRE, in the amount of R\$ 60 million for Cyber Defence, however the Commission approved, **by choice of the Force** [the Brazilian Army], the Program related to the Army Aviation, as a priority. (AMIN, 2019, p. 56, emphasis).

In other words, the Brazilian Army has passed over what the END establishes as its strategic sector to allocate resources to Army's Aviation, which would aim to ensure the supply of the Border Platoons, under the argument that the Air Force does not prioritize this activity (DEFESANET, 2020a). Was this an actual national defence priority, it would be wiser for the MoD to reallocate Air Force priorities than institute a fixed-wing Aviation within the Army. The decree authorizing the Army Aviation recreation was published on June 2, 2020, but under strong opposition from the Air Force it was revoked on June 8 (DEFESANET, 2020b). Therefore, cyber defence, a strategic sector determined by the National Strategy of Defence, lost resources to an Army internal project that did not materialize.

Difficulties can also be perceived in the personnel administrative context of the Army itself. As in any army, there are many specialised branches: Infantry, Cavalry, Artillery, Engineering, Communications, Logistics and Materiel, to name just the most relevant ones. In the Brazilian Army, cyber historically was an 'intrinsic' attribution of the Communications branch, so that officers from other branches have operational difficulties in making a career at

ComDCiber. It happens that the branches' career plans require that their officers go through certain positions along their professional trajectory. Hence, for an infantry officer to advance in his career, he must necessarily work in infantry units and functions for long periods, even if he has excelled, at a certain point in his career, with cyber operations and would like to continue in this path. Thus, human resources that would be significant assets for cyber defence, whose skills are unlikely to be easily replaced in such a small structure, are relocated to other areas for bureaucratic requirements.

Another difficulty with this historical link with the Communications branch relates to the aforementioned distribution of the scarce financial resources within the Army. Until 2018 (10 years after the first END designated cyber defence as a strategic national defence sector) all ComDCiber commanders had been Communications' Generals. In this entire period, there was not a single 4-stars from this branch. Thus, there has never been a representative of it in the Army's High Command. Such a situation might hopefully be mitigated soon, since in 2018, for the first time, an Artillery 3-stars General assumed the command of ComDCiber.

Furthermore, among all the nations analysed, only Brazil does not have a Signals Intelligence (SIGINT) agency, even though it was recommended by the Senate Investigative Committee on Electronic Espionage instituted in the wake of the Snowden Case in 2013 (BRASIL, 2013). Consequently, Brazilian national cyber capabilities are even more limited when compared with others, increasing the relative importance of ComDCiber and demanding greater agility and speed in its operationalization and effectiveness.

## **8.4 The Need for Increasing the Staff of ComDCiber**

### **8.4.1 On the Size of an Adequate Staff**

According to the limited public data available, ComDCiber's workforce accounts for approximately 180 people (OKAMURA, 2017). Consequently, a staff smaller than that of a traditional Company, with the operational responsibility of a Brigade, commanded by a Division General. This number is unsuitable for a nation with the economic, demographic, geopolitical, and even military characteristics of Brazil.

It is possible to draw comparisons, considering the data from Table 19 and the Global Fire Power website (GLOBALFIREPOWER.COM, 2020).

#### **8.4.1.1 GDP Purchase Parity Power**

Comparisons based on GDP provide insights considering some proportionality regarding the dimensions of the interests to be defended. Table 20 presents a sample of the countries whose NCSSs are studied in this work, ordered according to their GDP adjusted by

Purchasing Power Parity (PPP). The PPP does not consider the absolute value of the GDP in USD, but its relative value considering local costs.

Table 20 – Population, Military Personnel and GDP (PPP)

Country	Population	Active Military Personnel	%Actv	GDP (billion USD)	Def. (billion USD)	%Def
China	1,384,688,986	2,183,000	0.16%	24,810	237	0.96%
USA	329,256,465	1,400,000	0.43%	19,850	750	3.78%
Germany	80,457,737	182,650	0.23%	4,300	50	1.16%
Russia	142,122,776	1,013,628	0.71%	4,025	48	1.19%
Brazil	208,846,892	334,500	0.16%	3,300	28	0.84%
United Kingdom	65,105,246	192,660	0.30%	2,974	55	1.85%
France	67,364,357	268,000	0.40%	2,904	42	1.43%
Italy	62,242,674	175,000	0.28%	2,344	28	1.19%

Source: Compiled by the author with data from Global Firepower Index (GLOBALFIREPOWER.COM, 2020)

As noted, China has a GDP (PPP) of 24.81 trillion dollars, the United States one of 19.85 trillion dollars, Brazil of 3.30 trillion, and so on. Brazil's GDP-PPP is 11% higher than that of the United Kingdom and 13% higher than that of France. Therefore, it is presumed that Brazil has to defend economic interests of the same order of magnitude as those of these countries. This establishes a first parameter for comparing the need for strength.

#### 8.4.1.2 Proportionality of Cyber Staff as Total Staff

Table 21 presents data on the military personnel of some of the countries, complemented with public data on the respective cyber defence personnel. It should be noted that the CyberCom column reports only the military personnel of each country. Therefore, the more than 7,000 US NSA employees are not considered, as it is a signals intelligence agency, not a military command. In the British case, Battalion 77 was not considered, as it was dedicated to informational warfare, a different theme not treated in this research.

Among the countries listed in Table 21, the USA is the country with the largest active military force, with Brazil in second, and so on. When considering personnel engaged in cyber defence in relation to the total number of active military personnel (column “%Cyber”), however, Brazil appears as an absolute outlier.

Table 21 – Compared Cyber Defence and Defence Staff

Country	Active	CyberCom	%Cyber	%Avg	%UK	%FR	%US
USA	1,400,000	6,200	0.44%	14,943	14,533	18,284	6,200
Brazil	334,500	180	0.05%	3,570	3,472	4,368	1,481
France	268,000	3,500	1.31%	2,861	2,782	3,500	1,187
United Kingdom	192,660	2,000	1.04%	2,056	2,000	2,516	853
Germany	182,650	13,500	7.39%	1,950	1,896	2,385	809
	2,377,810	25,380	1.07%				

Source: Compiled by the author

In comparative terms, Germany has a unique cyber force, with 7.39% of the total active personnel. France accounts for 1.31%, and the United Kingdom 1.04%, while the USA has 0.44% and Brazil only 0.05%. The overall average is 1.07%. If the average percentage is considered to be an adequate parameter, the national staff of each country should be that in the “%Avg” column. If the British rate is to be considered, numbers would be those of the “%UK” column, for adopting the French rate numbers are those of the “%FR” column and for the USA one those of the “%US” column. Based on these rates, respectively, the size of the Brazilian cyber defence staff should be 3,570, 3,472, 4,368 or 1,481 professionals, according to the adopted index, to maintain a certain proportionality with these countries.

Nevertheless, as already mentioned, Brazilian economic interests are comparable to those of the French and British (in fact, more than 10% higher). Therefore, the adequate staff size, including military, civilian and outsourced personnel, should be 3,472, by the British index, or 4,368 by the French one, considering the balance of cyber forces as a proportion of other domain forces. Although the numbers may seem somewhat high, the largest corresponds roughly to the number of a traditional Brigade.

#### 8.4.2 How Big Should ComDCiber Be, and How to Get There?

As seen in the previous section, the staff of the Brazilian ComDCiber is relatively small, considering usual parameters of relative comparison. The justification for maintaining this state of affairs is often based on the lack of material and human resources due to budget restrictions, and on the argument that Constitutional Amendment 95 (EC95) froze national government spending until 2037. It so happens that the countries mentioned in the comparison also face budget cuts in their defence spending. The aforementioned U.S. Cyber Mission Force units, announced in 2014, were completed in May 2018, four months ahead of schedule. Albeit, between 2014 and 2018 the DoD budget was reduced by about 8.5%, while the USCyberCom



budget was increased by 8%. Therefore, a relative growth of more than 18% in times of general reduction, demonstrating that the USA works with a different prioritization for cyber defence. Similarly, data from the United Kingdom and Australia show similar prioritization.

From the theory of strategy, it is known that ends must be prioritised in the absence of means. PND and END stipulate the intended priority areas of each force. The Brazilian Navy signals it is prioritizing the nuclear-powered submarine programme (PROSUB) even sacrificing its surface fleet's maintenance. But the space domain makes little progress with the Air Force, as does cyber in the Army.

Considering the previous conclusion that Brazilian interests have the same order of magnitude than those of the United Kingdom and France, and following the logic of relative proportionality between military and cyber personnel, ComDCiber's personnel should be at least 3,500 professionals. However, growth of this magnitude takes time. An ambitious but feasible possibility would be a growth in eight years, or four phases of two years (average time for changing the commander of a Brazilian military unit). A total of 3,500 professionals would be reached according to the scale of Table 22, with the increases planned in the "1<sup>st</sup> Semester" and "2<sup>nd</sup> Semester" columns.

Table 22 – Proposal of Evolution of ComDCiber Staff

Year	Initial Staff	1 <sup>st</sup> Semester	2 <sup>nd</sup> Semester	Final Staff	Growth
2021	150	30	45	225	50%
2022	225	60	90	375	67%
2023	375	120	140	635	69%
2024	635	175	200	1,010	59%
2025	1,010	225	250	1,485	47%
2026	1,485	275	300	2,060	39%
2027	2,060	325	350	2,735	33%
2028	2,735	375	390	3,500	28%

Source: Compiled by the author

This staggering growth foresees the recruitment, selection, absorption, training and operationalization of personnel in all different sectors of ComDCiber. It predicts that as the structure grows, it will be all the more capable of absorbing larger contingents in absolute terms, but smaller in relative terms. But it also considers the need for more accelerated growth in the initial phases to reduce the gap that exists today.

### 8.4.3 The Need for Civilian Staff

It is common ground that cyber defence should involve military personnel and civilians, particularly (but not solely) due to the impossibility of finding enough people with the necessary qualifications exclusively within military ranks. On this subject, the main discussion in the USA, United Kingdom, France and Germany is how to capture and retain civilian personnel and use them in military operations. Some understand that, in the nation's service, and outside a traditional combat zone, there is little difference between being in uniform or not. For these, it is enough to hire civilians directly in the armed forces, even by contracting outsourced companies, to have the necessary personnel, formalising in their contracts the requirements of secrecy, hierarchy and discipline (BRACKNELL, 2018; PAUL e colab., 2014, p. 26–7; SCHNEIDER, 2018). Those with a more conservative view understand that the uniform and the military ethos must also be demanded from the “cyber-warriors”. For many of these, civilian trained professionals could be admitted, but only as temporary officers or in non-combatant careers (ARMSTRONG, 2018). A relevant issue is the existence of cyber-career development prospects. This has already been done by the U.S. Army and the U.S. Marines, who have created specific careers, ensuring professional progression, although we are aware that they might not be long-term careers (POMERLEAU, 2018).

#### 8.4.3.1 On the Commissioning of Civilians

In the U.S. Army CyberCom website there is an online application for personnel trained in programming, systems analysis or hacking (U.S. ARMY CYBER, [S.d.]). Another webpage offers the possibility of applying for the commissioning as army officers (U.S. ARMY CYBER, [S.d.]). Once accepted (after a “social investigation” process and proof of technical competence), the selected undergo a short (6 weeks) military instruction and become officers of the U.S. Army CyberCom. Similarly, the USAF maintains a page for recruiting Cyberspace Operations Officers (U.S. AIR FORCE, [S.d.]) and the U.S. Navy one for recruiting Cyber Warfare Engineers (U.S. NAVY, [S.d.]).

Although this is not the ideal form of recruiting civilians, it is easily adaptable to the Brazilian case, where there is also a provision for regular entry of officers into technical careers in the Armed Forces. The remuneration of the military officers in 2020 corresponds to that indicated in Table 23. It is observed that the salary constitutes the basic remuneration, being increased by bonuses, of which the most relevant are the Availability Additional (*Adicional de Disponibilidade*), “due to permanent availability and exclusive dedication” and the Qualification Additional (*Adicional de Habilitação*), “due to courses taken successfully” during their careers (BRASIL-CN, 2019). The Availability Additional is also indicated in Table 23.

Table 23 – Brazilian Military Officers Wages

Rank	Wage (BRL)	Availability Additional
Colonel	11,451.00	32%
Lieutenant Colonel	11,250.00	26%
Major	11,088.00	20%
Captain	9,135.00	12%
First-Lieutenant	8,245.00	6%
Second-Lieutenant	7,490.00	5%

Source: Compiled by the author based on Law 13,954/2019 (BRASIL-CN, 2019)

Table 24 shows the percentage of Qualification Additional according to the courses taken, with the annual additions provided for by law.

Table 24 – Qualification Additional

Qualification/Courses	From 01/07/20	From 01/07/21	From 01/07/22	From 01/07/23
Doctorate/High Studies - Category I	42%	54%	66%	73%
Doctorate/High Studies - Category II	37%	49%	61%	68%
Masters/Command and General Staff	27%	34%	41%	45%
Specialization	19%	22%	25%	27%
Graduation	12%	12%	12%	12%

Source: Compiled by the author based on Law 13,954/2019 (BRASIL-CN, 2019)

Hence, a systems analyst with a degree in computer science and a master's degree, starting a career as a Second-Lieutenant in 2021, would perceive a salary of BRL 7,490.00, plus an Availability Additional of BRL 374.50 (5%) and a Qualification Additional in the amount of BRL 2,022.30 (27%), totalling a gross wage of BRL 9,886.80. Entry into the same rank in subsequent years would correspond to an even greater amount, given the Qualification Additional scheduled increase for the coming years.

Compared to the Brazilian market conditions, this remuneration is very attractive for IT professionals. The average market wage for the category is much lower, as can be seen in Table 25.

Considering the Army as a large company, it is straightforward that there would be no difficulty in hiring professionals up to the level of Senior Analyst (8 years of experience) comparable to a Captain, whose gross remuneration would be BRL 12,697.45. Considering the

other benefits provided by the military career (food, transportation, health insurance, and possibly housing), the attractiveness is very high.

Table 25 – Average Monthly Wage of Systems Analysts in Brazil

Company Size	Experience Level				
	Trainee	Junior	Full	Senior	Master
Experience (years)	<3	3-4	5-6	7-8	>8
Small	R\$ 2,492.81	R\$ 3,116.01	R\$ 3,895.01	R\$ 4,868.76	R\$ 6,085.95
Medium	R\$ 3,240.65	R\$ 4,050.81	R\$ 5,063.51	R\$ 6,329.39	R\$ 7,911.74
Large	R\$ 4,212.84	R\$ 5,266.05	R\$ 6,582.56	R\$ 8,228.20	R\$ 10,285.25

Source: Compiled by the author with data from TrabalhaBrasil.org (2020)

Besides, the Army is entitled to “call and incorporate Brazilians with recognized technical-professional competence or with a notorious scientific culture in the active service of the Army, on a voluntary and temporary basis” (BRASIL-PR, 2018, free translation). Under these conditions, the attractiveness is even higher. Commissioned as a Major, a graduate in Computer Science, with a Doctorate, for example, would receive a salary of BRL 11,088.00, plus an Additional Availability of BRL 2,217.60 (20%) and a Qualification Additional of BRL 4,656.96 (42%), totalling a gross remuneration of BRL 17,962.56. A value 75% higher than the average of Master systems analysts (over eight years of experience) in large companies in the Brazilian market.

Moreover, the impossibility of extending the army staff imposed by EC95 does not constitute a *de facto* restriction. A rearrangement of priorities would allow the relocation of Temporary Technical Officers (OTT) or Complementary Staff Officers (QCO) from the three singular forces to ComDCiber. OTTs could be deployed quickly, and even the limitation of eight years of exercise allows for a reasonably long life-cycle in defence. At the end of their service, they could strengthen the ranks of cyber defence and cybersecurity in the private market or the civilian public sector, continuing to contribute to national cyber defence.

#### 8.4.3.2 Civilian Positions

Commissioning civilians is a kind of “quick conversion” of civilians into military. But it will not interest to a particular group of professionals, who would prefer to serve cyber defence while remaining civilians, escaping from the peculiarities of military life, such as marches, formations, physical fitness tests, wearing uniforms, and so forth. In addition to expanding the spectrum of available professionals, hiring civilians would allow for greater continuity and retention of knowledge associated with the function, given that the military, due to their career requirements, is frequently moved to carry out courses and command

assignments. Civilians, exempt from these obligations, could ensure the stability and continuity of processes.

Nevertheless, there is a need for a career path that allows civilians to ascend decision making and strategic positions in the cyber defence structure. In technical terms, this is not a problem. Still, in practical ones, this coexistence of military and civilians in equivalent functions will require a normative (and mainly cultural) adaptation in the Armed Forces. The possible creation of the ‘state career’ of Defence Specialist that now appears in the proposed 2020 END can help to fill this gap (BRASIL-MD, 2020b, p. 43). This civilian-military integration in cyber defence has already started in other countries, and ComDCiber may benefit from the experiences of “friendly nations” in this process.

#### 8.4.3.3 Creating a Military Cyber Career

In the medium term, it is necessary to create a cyber force, with specific rules and a new culture. Meanwhile, in the short term, there is an urgent need to develop cyber careers that allow the military from different branches of the various forces to rise professionally, averting them to be removed to serve in specific positions and functions as a requirement of their original branches. Once entering this “career” (or cadre) a military would only temporarily withdraw for technical, staff, politics and strategy courses, as was done by the U.S. Army, Navy, Marine Corps and Air Force.

### **8.5 Where to Locate ComDCiber in the Context of the Ministry of Defence?**

There is also the need to consider the placement of ComDCiber within the structure of the MoD. Two alternatives are more appropriate than the current subordination to the Army DCT.

#### 8.5.1.1 Alternative 1 – Under the Joint Staff (EMCFA)

The most consistent proposal, considering the experiences of the countries of the military “Arc of Knowledge”, would be the allocation of ComDCiber under the Joint Chiefs of Staff (EMCFA), in the MoD. This option would raise the status of cyber defence, given that it would no longer be linked to a single force, even if the command would still permanently be given to the Army. This, in theory, would make it easier to obtain resources, including the relocation of OTT and QCO positions from the singular forces, as well as reducing two “levels” (among forces and Army branches) in the dispute for resources. In practical terms, it should not pose a problem to the Army. As it would ‘lose’ the equivalent budgetary allocation, it would also ‘lose’ the corresponding expenditure, without losing prestige, as it would remain in charge as established by the END.

Nevertheless, this option shall face difficulties of political nature, given the incipient joint action of the MoD in its 20 years of existence. Albeit, sooner or later, this joint action has to become effective. The sooner, the better. Furthermore, the growing importance of cybernetics in the international military context can even leverage the development of this capacity for joint action.

#### 8.5.1.2 Alternative 2 - Adoption of the Model of the Command of Special Operations (COPEsp)

In the impossibility of having a structure directly linked to EMCFA, an alternative within the Army itself would be endowing ComDCiber with a condition similar to that of COPEsp. In fact, the nature of cyber operations is, to some extent, “similar” to that of special operations (PAUL e colab., 2014). They are essentially two operational commands. Both involve the development of specific doctrines and techniques, distinct and complementary to those of the rest of the Army, so that they may have similar “administrative treatment”.

Although the solution adopted for COPEsp may look like another *jabuticaba*, at least there would be two commands that would make use of the same exception, and not two different exceptions, one for each command.

### **8.6 The OAS and Oxford Report on Brazilian Cyber Capabilities**

On August 2020, the Organization of American States, the Brazilian Government and the University of Oxford published the Cybersecurity Capabilities Review of Brazil (OXFORD GCSCC, 2020).

Capability Maturity Models are relatively common in the cyber field. The most famous of these is the CMM/CMMI, developed by the renowned Software Engineering Institute of Carnegie-Melon University, which assesses the maturity of software development of institutions (SEI/CMU) (CMMI INSTITUTE, [S.d.]). Brazil adopted its own methodology, called MPS-BR (Improvement of Brazilian Software Processes), created in 2003 by the Association for the Promotion of Excellence of Brazilian Software (Softex), more adequate to the national reality, particularly concerning the costs of international certifications (SOFTEX, [S.d.]). These models generally consider that when a single key process area (KPA) required for a level is missed, that level is not reached entirely, with the final classification being that which all KPAs have been certified. Hence, if any of the requirements (KPAs) of level 4 is not met, the report indicates it as a level 3 organisation.

A careful reading of the Review shows, despite the language carefully used by the authors of it, that Brazil is in a very primary stage in its cyber capabilities.

The Oxford model accounts for 5 “stages” of capacity (Start-up, Formative, Established, Strategic, Dynamic). The “Start-up” stage, however, has the following description:

at this stage either *no cybersecurity maturity exists, or it is very embryonic in nature*. There might be initial discussions about cybersecurity capacity building, but no concrete actions have been taken. There is an absence of observable evidence of cybersecurity capacity at this stage. (OXFORD GCSCC, 2020, p. 29, emphasis added)

Consequently, the stages that indeed show some capacity are the following four. To simplify the analysis, here, each stage will be considered as corresponding to a number, with “Formative” equivalent to 1, “Established” to 2, “Strategic” to 3 and “Dynamic” to 4, the highest possible “score”.

There are five dimensions in the model, comprising a total of 24 areas, as shown in Table 26.

Table 26 – Dimensions & KPAs of the Oxford GCSCC Maturity Model

Dimension	Area	Description
Cybersecurity Strategy and Policy	D1.1	National Cybersecurity Strategy
	D1.2	Incident Response
	D1.3	Critical Infrastructure (CI) Protection
	D1.4	Crisis Management
	D1.5	Cyber Defence
	D1.6	Communications Redundancy
Cybersecurity Culture And Society	D2.1	Cybersecurity Mind-set
	D2.2	Trust and Confidence on the Internet
	D2.3	User Understanding of Personal Information Protection Online
	D2.4	Reporting Mechanisms
	D2.5	Media and Social Media
Cybersecurity Education, Training, and Skills	D3.1	Awareness Raising
	D3.2	Framework for Education
	D3.3	Framework for Professional Training
Legal and Regulatory Frameworks	D4.1	Legal Frameworks
	D4.2	Criminal Justice System
	D4.3	Formal and Informal Cooperation Frameworks to Combat Cybercrime
Standards, Organizations, and Technologies	D5.1	Adherence to Standards
	D5.2	Internet Infrastructure Resilience
	D5.3	Software Quality
	D5.4	Technical Security Controls
	D5.5	Cryptographic Controls
	D5.6	Cybersecurity Marketplace
	D5.7	Responsible Disclosure

Source: Compiled by the author with data from Cybersecurity Capabilities Review of Brazil (2020)

In the Brazilian Review, unlike the traditional models, there are intermediate stages. For example, in area D1.1, where Brazil was classified as “Formative-Established”, and not as “Formative”, as it would be in the usual models. It should be noted that the assessment carried out in 2015, with the same methodology, on the United Kingdom’s cyber capabilities, does not contain these intermediate levels. However, the corresponding report graph indicated intermediate levels in that case, too (OXFORD GCSCC, 2016). It is, therefore, an “adjustment” made to the model after the assessment conducted in the United Kingdom.

Comparing Brazil with the United Kingdom is justifiable, as demonstrated in Section 8.4, since defending interests of a similar magnitude. The assessment of Brazilian capabilities in the OAS report indicates that considering the “hybrid” or “intermediate” stages, Brazil presents the situation shown in Table 27.

Table 27 – Areas per Stage in Brazilian Capacities

Stage	Qty	%
Formative	10	42%
Formative-Established	7	29%
Established	6	25%
Established-Strategic	1	4%
Strategic	0	0%
Strategic-Dynamic	0	0%
Dynamic	0	0%

Source: Compiled by the author with data from Cybersecurity Capabilities Review of Brazil (2020)

If considered with the same rigour used in the assessment of UK capacities in 2015, however, the Brazilian and British scenario would be as shown in Table 28.

Table 28 – Areas per Stage in Brazilian and British Capacities (no Hybrid Stage)

Stage	Qty	BR	UK
Formative	17	71%	14%
Established	7	29%	62%
Strategic	0	0%	14%
Dynamic	0	0%	10%

Source: Compiled by the author with data from Cybersecurity Capabilities Review of Brazil (2020) and Cyber Capabilities Review of the UK (OXFORD GCSCC, 2016)

A better comparison is possible by using the numerical values assigned as corresponding to the identified stages, and considering that the hybrid stages would correspond to an increase of 0.5 (“virtue is in the middle”, as stated in a popular Brazilian dictum). Using this process, Brazilian capacities would be “scored” as presented in Table 29.



Table 29 – Score of Each Area of the Brazilian Capacities

Area	Description	Stage	Points
D1.1	National Cybersecurity Strategy	Formative-Established	1.5
D1.2	Incident Response	Established-Strategic	2.5
D1.3	Critical Infrastructure (CI) Protection	Established	2.0
D1.4	Crisis Management	Established	2.0
D1.5	Cyber Defence	Formative-Established	1.5
D1.6	Communications Redundancy	Formative	1.0
D2.1	Cybersecurity Mind-set	Formative	1.0
D2.2	Trust and Confidence on the Internet	Formative-Established	1.5
D2.3	User Understanding of Personal Information Protection Online	Formative	1.0
D2.4	Reporting Mechanisms	Formative	1.0
D2.5	Media and Social Media	Formative	1.0
D3.1	Awareness Raising	Formative-Established	1.5
D3.2	Framework for Education	Formative	1.0
D3.3	Framework for Professional Training	Formative	1.0
D4.1	Legal Frameworks	Established	2.0
D4.2	Criminal Justice System	Formative	1.0
D4.3	Formal and Informal Cooperation Frameworks to Combat Cybercrime	Formative	1.0
D5.1	Adherence to Standards	Formative-Established	1.5
D5.2	Internet Infrastructure Resilience	Established	2.0
D5.3	Software Quality	Formative	1.0
D5.4	Technical Security Controls	Established	2.0
D5.5	Cryptographic Controls	Established	2.0
D5.6	Cybersecurity Marketplace	Formative-Established	1.5
D5.7	Responsible Disclosure	Formative-Established	1.5

Source: Compiled by the author with data from Cybersecurity Capabilities Review of Brazil (2020)

This results in an average of 1.5 points, or the equivalent of the “Formative-Established” hybrid stage or, in the case of the original rigour, the “Formative” stage. Furthermore, without the “hybrid” stages, in the strictness of the original methodology, the Brazilian average would correspond to 1.3.

The United Kingdom, in turn, in 2015, would be “scored” as presented in Table 30

Table 30 – Points of Each Area of the UK Capacities

Area	Description	Stage	Points
D1.1	National Cybersecurity Strategy	Strategic	3.0
D1.2	Incident Response	Established	2.0
D1.3	Critical Infrastructure (CI) Protection	Established	2.0
D1.4	Crisis Management	Established	2.0
D1.5	Cyber Defence	Established	2.0
D1.6	Communications Redundancy	Established	2.0

Area	Description	Stage	Points
D2.1	Cybersecurity Mind-set	Formative	1.0
D2.2	Trust and Confidence on the Internet	Established	2.0
D2.3	User Understanding of Personal Information Protection Online	Formative	1.0
D2.4	Reporting Mechanisms	Established	2.0
D2.5	Media and Social Media	N/A	N/A
D3.1	Awareness Raising	Established	2.0
D3.2	Framework for Education	Established	2.0
D3.3	Framework for Professional Training	Established	2.0
D4.1	Legal Frameworks	Dynamic	4.0
D4.2	Criminal Justice System	Strategic	3.0
D4.3	Formal and Informal Cooperation Frameworks to Combat Cybercrime	Formative	1.0
D5.1	Adherence to Standards	Established	2.0
D5.2	Internet Infrastructure Resilience	Established	2.0
D5.3	Software Quality	Established	2.0
D5.4	Technical Security Controls	Dynamic	4.0
D5.5	Cryptographic Controls	Strategic	3.0
D5.6	Cybersecurity Marketplace	N/A	N/A
D5.7	Responsible Disclosure	N/A	N/A

Note: N/A indicates that the area was not evaluated in that version of the methodology, or that it was part of another area.

Source: Compiled by the author with data from Cybersecurity Capabilities Review of the United Kingdom (OXFORD GCSCC, 2016)

The British “score”, then, corresponded to an average of 2.2 (even without the “increase” provided by the hybrid stages).

In other words, five years ago, the UK had much better cyber capabilities than Brazil has today. And, in these five years, they have invested an average of BRL 1.35 billion annually, while the Brazilian average at the time was mere BRL 15 million. A nominal rate of 90:1, but if considered that the Brazilian GDP-PPP is 11% higher than the British, the actual rate can be rounded to 100:1.

On the part of the United Kingdom, it can be assumed that the significant investments made by that country in recent years, in the opposite direction to what occurs in Brazil, have further accentuated the technological gap that separates it from Brazil. And as is well known, one does not put an alarm in his car to prevent it from being stolen; if the thief wants to take it, he will; there is a dissuasive effect on the alarm, but it is to make the thief, motivated by ‘the law of least effort’, look for a similar easier to steal car.

## 8.7 On the Good News

There is some good news, too. Brazilian law requires the Supreme Commander’s authorisation for the deployment of military capabilities on behalf of the State. This is often

authorized by a Presidential decree within a limited period. Specific joint commands, however, can have a “permanent” authorization to engage. This is the case of the Brazilian Air Defence Command (COMAE). In November 2020, an ordinance of the MoD paved the way for ComDCiber also to become “permanently activated”. The MoD now must submit a request to Presidential consideration, possibly resulting in the necessary decree.

Moreover, in recent conversations with the ComDCiber commander, Gen. Div. Guido Amin Naves, he indicated that the joint part of the command’s budget shall be increased by a factor of ten for 2021, raising the total budget from circa BRL 21 million to roughly BRL 74 million, according to the budgetary proposal now in discussion in the Government and the Congress.

These two changes constitute very significant steps in the right direction for the evolution of Brazilian cyber defence. However, comparatively, they are still quite timid ones.

## **8.8 Conclusion**

Cyberspace, unequivocally, constitutes as a new space for interstate coercion and statecraft. Even countries with a non-aggressive culture and tradition, which favour the peaceful settlement of disputes, and who are willing to give up the competitive advantages potentially offered by the offensive potential of cyberspace, cannot feed the expectation that their peers will do the same.

State action in cyberspace is real, happens daily, involves significant economic, strategic and geopolitical interests, is global, ignores the traditional battlefield and is growing. Many nations already operate day by day, while expanding their knowledge, arsenals and legal support.

Brazil needs to be adequately prepared as soon as possible, and the findings of the research carried out show that Brazil’s progress in this area is too slow when compared to that of nations with similar economic and geopolitical interests, and even those of “smaller powers” such as Australia, Israel, Iran and North Korea.

The conclusions and propositions in this Chapter point to a coherent path, based on solid data and concepts, collected in broad research on different countries' practices, to provide a scientific approach on a topic as controversial as contemporary.



## 9 THE STRATEGIC OPPORTUNITY POSED BY SOFTWARE POWER

This chapter analyses the opportunities that a coordinated strategy of Cyber-Dissuasion by Denial present to non-aggressive countries such as Brazil. Analysing economic data related to the global I.T. market, it shows that such a strategy can offer a good return on investment and boost national economy.

### 9.1 Introduction – “It’s the Economy, Stupid!”<sup>17</sup>

The economy is the basis of a state’s welfare, and the most frequent reason for the pursuit of power (and often its primary source, as well). And, tightly connected to all other expressions of national power. It is also an essential element of Dissuasion Theory. However, the concepts of cost and value could, and often do, relate to moral, ethical or cultural aspects, it is more likely to be expressed in economic terms. Moreover, the case for Punishment against Denial is, usually, based on the cost of Denial being much higher.

But what about the economic return of cyber dissuasion? As a science, economy shows that there are two fundamental ways of improving economic results: cutting costs and increasing income.

#### 9.1.1 Cutting Costs

Strong defences will limit direct losses from stolen intellectual property. The U.S. Government often complains about the theft of intellectual property from American companies by foreign countries. In 2018 that government even issued an official public document entitled Foreign Economic Espionage in Cyberspace, where it stated:

Foreign economic and industrial espionage against the United States continues to represent a significant threat to America’s prosperity, security, and competitive advantage. Cyberspace remains a preferred operational domain for a wide range of industrial espionage threat actors, from adversarial nation-states, to commercial enterprises operating under state influence, to sponsored activities conducted by proxy hacker groups. (UNITED STATES, 2018a, p. 4)

Although naming China, Russia and Iran as particularly aggressive actors interested in economic cyberespionage, the report also points out that other actors incur in this practice.

Countries with closer ties to the United States have conducted cyber espionage and other forms of intelligence collection to obtain U.S. technology, intellectual property, trade secrets, and proprietary information. U.S. allies or partners often take advantage

---

<sup>17</sup> Mantra coined by strategist James Carville for President Clinton's campaign in 1992, that focus in the economy as the most important political element.

of the access they enjoy to collect sensitive military and civilian technologies and to acquire know-how in priority sectors. (UNITED STATES, 2018a, p. 5)

There is no reason to suppose that this is a problem exclusively for the U.S., and not for smaller countries. The commercial value of the ‘ultra-deepwater oil exploration’ technologies developed by Brazilian oil company Petrobras is tremendous. As also that of technologies developed by Brazilian aircraft maker Embraer.

Good cyber defences will also limit losses by being outflanked in international negotiations as that of the Fifth Summit of The Americas, or that of the billionaire acquisition of the Brazilian SIVAM (Amazonia’s radar surveillance) where the French company Thomson-CSF has been deceived by the American Raytheon, with the support of NSA signals espionage (CAMPBELL, 1999, p. 18; GREENWALD, 2014, p. 139).

Good defences can reduce the economic damage caused by state-sponsored malware like WannaCry and NotPetya, which caused significant economic impact worldwide. Although dissuasion, in this research, is focused on state-sponsored cyber-offences, raising the bar of defences also might reduce the impact of cybercrime. Thus, it has to be accounted for in any costs and gains rationale.

In 2015, the CEO of the British insurance group Lloyds estimated losses caused by cyber offences to private companies worldwide somewhere between 400 and 500 billion dollars a year (GANDEL, 2015). CSIS, a U.S. think tank, estimates that while cybercrime accounted for 0.62% of global GDP in 2014, in 2016, it grew to 0.8%, reaching the figure of USD 600 billion (LEWIS, 2018, p. 6). In 2017, Brazil was considered the second largest victim of cybercrime, with losses of USD 22.5 billion (BRASIL-GSI, 2019).

### **9.1.2 Increasing Revenue**

The global market for Software and Services has continuously increased in the last decades. As a product of the “post-industrial era”, dependent on ingenuity more than on complex industrial capabilities or complex engineering skills, it offers the possibility to skip steps for economic growth.

For better understanding this alternative, it is necessary to comprehend the relevance of this market, in socio-economic terms. This is the subject of the next sections.

## **9.2 The Global Software Market**

This section presents and compares data relative to the American and European software and services markets, as well as the Brazilian one. Data gathered shows that this industry is relevant in terms of employment and revenue generation.

### 9.2.1 The U.S.

Table 31 presents data regarding the importance of the software industry in the U.S. economy in 2014, 2016 and 2018, allowing the analysis of its growth and relative importance. The software industry's direct gross product increased by 77.8% between 2014 and 2018, whilst the number of direct jobs increased by 24% and wages grew by 4.8%. Besides, while in 2014 there were 3.92 total jobs for each direct job, this number rose to 4.64 in 2018.

Moreover, the participation of the sector in Research and Development (R&D) grew 59% in the period, more than twice the national R&D growth rate (28.5%). Furthermore, the average I.T. salary maintains a somehow regular ratio of 2.2:1 compared with the average wage in the U.S.

Table 31 – U.S. Software Market Evolution between 2014 and 2018

Item	2014	2016	Diff. 16/14	2018	Diff. 18/14
Direct GDP (USD billion)	475.3	564.4	18.7%	845.0	77.8%
Total GDP (USD billion)	1,070.0	1,140.0	6.5%	1,600.0	49.5%
Direct Jobs (millions)	2.5	2.9	16.0%	3.1	24.0%
Total Jobs (millions)	9.8	10.5	7.1%	14.4	46.9%
Salaries I.T. (USD p.a.)	108,760	104,360	-4.0%	114,000	4.8%
Salaries Average (USD p.a.)	48,320	49,630	2.7%	51,960	7.5%
R&D (USD billions)	52.0	63.1	21.3%	82.7	59.0%
R&D Rate (%)	17.2	19.6	14.0%	22.1	28.5%

Source: Compiled by the author with data from BSA Foundation (2016b, 2017, 2019).

### 9.2.2 Europe

Table 32 presents data relative to the European software market between 2014 and 2016, allowing a direct comparison with the U.S. market in the same period.

While the U.S. direct GDP of the sector grew 18.7% at that time, the E.U. market grew 22.1%. The U.S. growth of participation in total GDP was 6.5%, and the European was 9.9%. In 2016, the European total/direct jobs ratio was 3.53, very similar to the 3.62 from the U.S.

Two major differences between the European and the U.S. software sectors can be observed. First, on the I.T./global salary ratio: only 1.34:1 in Europe, against 2.25:1 in the U.S. in 2014 (available data indicated a non-confirmed similar rate in 2016). This difference is probably related to the history of welfare policies in Europe since WWII, which have reduced social inequalities in Europe, not observable in the U.S. Second, in the participation (rate) of the sector in R&D. The U.S. software sector rate was 17.2%, against 7.3% in Europe in 2014.

Table 32 – E.U. Software Market Evolution between 2014 and 2016

Item	2014	2016	Diff. 16/14
Direct GDP (EUR billion)	249.0	304.0	22.1%
Total GDP (EUR billion)	910.0	1,000.0	9.9%
Direct Jobs (million)	3.1	3.6	16.1%
Total Jobs (million)	11.6	12.7	9.5%
Salaries I.T. (EUR p.a.)	45,333	45,307	-0.1%
Salaries Average (EUR p.a.)	33,790	N/A	N/A
R&D (EUR billion)	12.7	N/A	N/A
R&D Rate (%)	7.3	N/A	N/A

Source: Compiled by the author with data from the BSA Foundation (2016a, 2018).

### 9.2.3 Brazil

Business Software Alliance (BSA) has not produced reports of the Brazilian market similar to those of U.S. and European ones so far. However, Brazilian Software Companies Association (ABES) produces annual reports that allow some insights.

Figure 5 shows the distribution of the World I.T. market regarding Software, Services and Hardware markets. It is divided into three groups: Global Average, Developed Markets, and Emerging Markets.

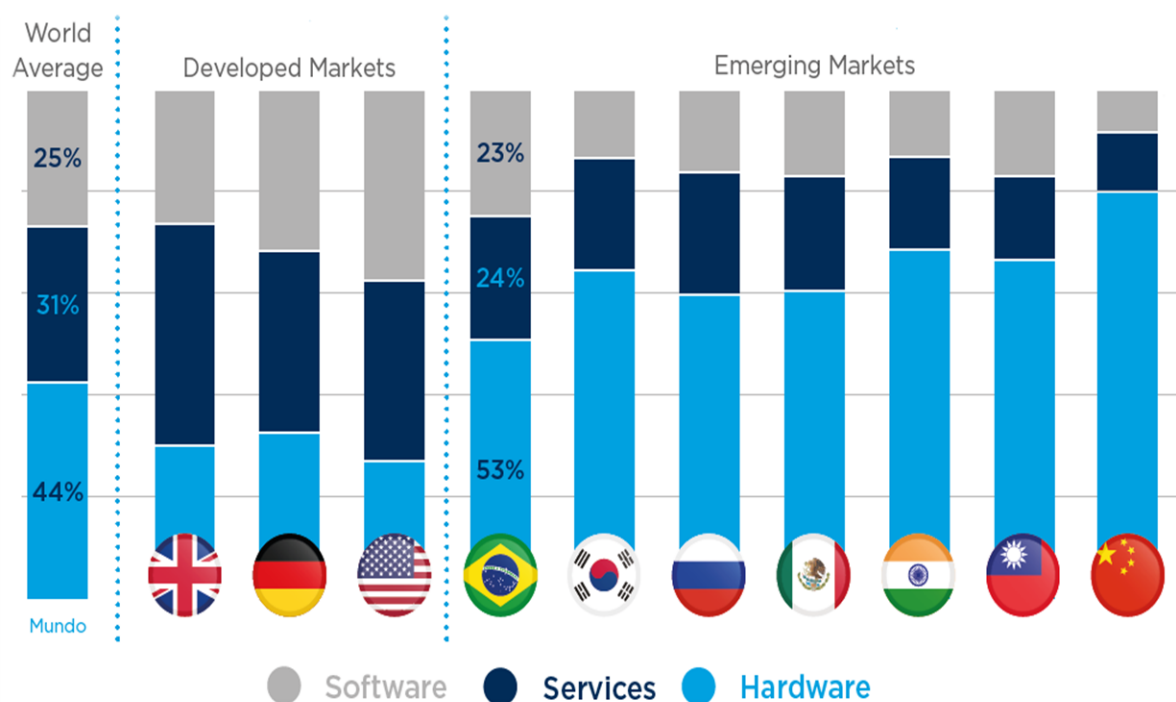
Concerning the Developed Markets area, it can be observed that Germany has similar distributions among the three sectors in its market, with roughly a third for each one. The U.S. market is slightly more concentrated in Software than in Hardware. The U.K. market is more concentrated in Services than in Software and Hardware. In any case, Hardware, as a product of the “industrial era”, responds for less than Software or Services, products of the “post-industrial era”.

Conversely, in the Emerging Markets area, Hardware accounts for more than Software and Services together in all cases. The situation is consistent with the fact that China, Taiwan, South Korea and India (as well as Singapore and Malaysia) concentrate the bulk of electronic components factories in the world. The famous “Designed by Apple in California - Assembled in China” phrase, present in iPhones and iPads, synthesises the idea. Mexico, by its way, concentrates a large number of *maquiladoras*, companies that import components with tax-free deductions, assemble them and export the finished product to the U.S. and Canada. It resulted from the *North American Free Trade Agreement* (NAFTA), from 1994, and its substitute, the *United States–Mexico–Canada Agreement* (USMCA), signed in 2018 and approved by the U.S. Congress in 2020.



The only country in the sample that gets close to the World Average, going in the direction of the Developed Markets, is Brazil, denoting an I.T. market that is becoming mature, although still slightly more concentrated in Hardware than in Software and Services.

Figure 5 – World IT Market Distribution



Source: ABES (2020, p. 6).

Table 33 presents the evolution of the Brazilian software and services market between 2015 and 2019. It is observable that until 2018 it had not yet recovered from the Brazilian crisis of 2015 (which ultimately resulted in the impeachment of President Dilma Roussef), and then in 2019 it felt again.

Table 33 – Brazilian Software Market Evolution between 2015 and 2019

Area	Item	2015 (USD mil.)	2016 (USD mil.)	2017 (USD mil.)	2018 (USD mil.)	2019 (USD mil.)
Software	Domestic Development	2.736	1.947	1.961	2.256	1.995
	Foreign Development	9.601	6.528	6.220	8.223	8.061
	Export Market	245	177	174	200	213
Services	Domestic Development	12.799	9.167	9.360	10.985	9.411
	Taylor Made Software	1.404	989	996	1.198	1.003
	Foreign Development	97	70	69	79	68
	Export Market	680	499	495	566	608
<b>Total</b>		<b>27.562</b>	<b>19.377</b>	<b>19.275</b>	<b>23.507</b>	<b>21.359</b>

Source: Compiled by the author with data from ABES (2016, 2017, 2018, 2019, 2020).

ABES (2020, p. 10) shows that only 19.4% of the Brazilian software market was filled with domestic Software, while 78.5% came from abroad. Moreover, in 2019, there were 21,020 software related companies in operation: 26.3% in software development; 32% in services; and 41.7% in distribution and commercialisation. Besides, Small and Medium Enterprises (SME) constitute 95.3% of them.

Finance (26.4%) and Telecom (23.2%) constitute roughly half of the local market, followed by Industry (20%), Commerce (10.8%) and Government (6.3%) as the primary consumers of Software.

Table 34 presents the leading players in the global market of Software and services in 2018. It can be observed that Brazil stands behind Australia in the worldwide ranking, even though the Brazilian economy is circa 30% larger than Australian. Besides, the U.K. and France have much larger markets than Brazil, although with similar-sized economies. Hence, there is room for growth of Brazilian software industry.

Table 34 – Global Market of Software and Services in 2018

Country	Rank	Software & Services 2018 (USD billions)	Global Share 2018
USA	1	563	46.1%
Japan	2	79	6.5%
United Kingdom	3	75	6.2%
Germany	4	65	5.4%
France	5	47	3.9%
China	6	41	3.4%
Canada	7	31	2.5%
Australia	8	24	2.0%
Brazil	9	23	1.9%
Netherlands	10	21	1.7%
Italy	11	20	1.6%
Spain	12	17	1.4%
India	13	16	1.3%
Switzerland	14	16	1.2%
Sweden	15	13	1.1%
South Korea	16	12	1.0%
Denmark	17	9	0.7%
Others	---	148	12.1%
Total	---	1,220	100.0%

Source: Compiled by the author with data from ABES (2019, p. 8).

The Brazilian situation gets even worse in 2019, as shown in Table 35. Symbols on the right of each column indicate the relative status in comparison with 2018. Brazil went down two positions globally and now stands behind the Netherlands and Italy as well.

Table 35 – Global Market of Software and Services in 2019

Country	Rank		Software & Services 2019 (USD Billions)		Global Share 2019	
USA	1	●	615.4	▲	46.2%	▲
Japan	2	●	83.1	▲	6.2%	▼
United Kingdom	3	●	81.9	▲	6.2%	▼
Germany	4	●	72.9	▲	5.5%	▲
France	5	●	52.8	▲	4.0%	▲
China	6	●	49.1	▲	3.7%	▲
Canada	7	●	32.8	▲	2.5%	▼
Australia	8	●	26.0	▲	2.0%	▼
Netherlands	9	▲	23.1	▲	1.7%	▲
Italy	10	▲	22.1	▲	1.7%	▲
Brazil	11	▼	20.5	▼	1.5%	▼
Spain	12	●	18.6	▲	1.4%	▼
India	13	●	17.3	▲	1.3%	▼
Switzerland	14	●	17.1	▲	1.3%	▲
Sweden	15	●	14.1	▲	1.1%	▼
South Korea	16	●	13.0	▲	1.0%	▼
Denmark	17	●	10.3	▲	0.8%	▲
Others	---	●	160.9	▲	12.1%	▼
Total	---	●	1,331.0	▲	100.0%	●

Source: Compiled by the author with data from ABES (ABES, 2020, p. 8).

Besides, it was the only country to present a shrunken market in comparison, in a scenario of global growth. This is partially explained by the fact that the local software and services industry is concentrated in and highly dependent on the national market, with only 2.3% of its revenue coming from abroad. Hence, when the local economy does not perform well, there is no other market to support that industry. Moreover, Brazil also reduced its already small market share in 2019.

Japan, the UK, Canada, Australia, Spain, India, Sweden, and South Korea, while increasing their industries, also lost global market share compared to the previous year.

Conversely, the U.S., Germany, France, China, the Netherlands, Italy, Switzerland and Denmark increased their global share.

### 9.3 Cyber Security and Defence Market

In 2015 alone, the U.S. invested USD 75 billion in cybersecurity, and global expenditures are estimated to achieve USD 1 trillion between 2017 and 2021 (MORGAN, Steve, 2016). This trillionaire spending is an attempt to “stop bleeding” not only from crimes, but also from espionage and coercion, practised with the use of cyber means, and sponsored by individuals or states. A common thought is that nations like Brazil, with the shortages of developing or emerging countries, will not be able to invest enough to have the adequate and necessary protection capacity, and that they will be so for a long time to come, at the mercy of “cyber superpowers” like the USA, China, Russia, the United Kingdom or even France.

Brazilian Cybersecurity market, in 2018, was estimated in circa USD 2 billion (BRIGATTO, 2018). This figure is much smaller than the U.S. one; actually, it is disproportionately smaller, considering the relative economy sizes and losses carried by cybersecurity breaches. Hence, the Brazilian market is most likely quite underestimated so far, probably due to a lack of adequate situational awareness. This might have started to change with a recent wave of high-end cyberattacks, such as the one that crippled *Superior Tribunal de Justiça* (Superior Court of Justice), closing the court for more than a week (LIMA, 2020; PAGANINI, 2020). Indeed, an attack that offended Brazilian sovereignty, since affecting the possibility of exerting a well-recognised elementary “function of state”, and involved the Brazilian Cyber Command and the Federal Police in the investigations (LIMA, 2020).

Israel, Iran and North Korea, however, demonstrate that it is possible for nations in inferior stages of development to ‘cut short’ in this new domain of geopolitics, and thus, become relevant players in cyberspace. However, international embargoes on Iran and North Korea limit their reach in the global market. Israel, on its way, has concentrated huge investments carried to cybersecurity focused start-ups, having become the second destination of this type of investment in the world (SOLOMON, 2018). In 2015 alone, 300 active cybersecurity companies exported USD 3.5 billion in Software, 5% of the worldwide cyber market (AZULAI, 2016). But the Israeli market is limited by their proximity with the U.S., and their historical confrontation with countries having Muslim majority.

With an eye in this growing market, the U.K. government issued its 2018 Cyber Security Export Strategy. Possibly the most relevant aspect of it was the official recognition of cybersecurity as an increasing market that deserves official attention and diplomatic efforts.

The accelerated pace of digital change brings a great opportunity to promote the U.K.'s cyber security expertise to international markets. Robust export control regimes will ensure that human rights are a key part of the process. (UK DEPARTMENT FOR INTERNATIONAL TRADE, 2018, p. 5)

Albeit it appoints to restrictions on its actions to specific markets: “*In priority markets*, DIT [Department of international Trade] will act as a trusted advisor to support U.K. companies bidding for major opportunities, primarily selling to overseas governments and Critical National Infrastructure (CNI) providers” (UK DEPARTMENT FOR INTERNATIONAL TRADE, 2018, p. 6, emphasis added).

Having a consolidated software industry, Brazil could also explore the growing international cybersecurity and cyber defence market, having some strategic advantage regarding the British, the Americans and the Israeli.

#### **9.4 Strategic Opportunity**

The defence products market is very representative in the world's economy. Albeit, since the majority of military products can be used both for attack and defence, exporters of these products have to be selective with to whom selling them; otherwise, they may sell a product that is going to be used against them.

Cyber vulnerabilities have also been responsible for restrictions on acquisitions and on selling products. As early as 2001, American intelligence officials believed “that certain equipment and software imported from Russia, China, Israel, India and France” were infected with “devices” capable of “reading data and destroying systems”, although this suspicion was difficult to prove (ADAMS, 2001, p. 105). More recently, counterfeit Hardware was identified in systems acquired by DoD (LYNN, 2010, p. 101). A report by the U.S. House Permanent Intelligence Commission in 2012 restricted the purchase of equipment from Chinese companies Huawei and ZTE (BANACH, 2012).

In 2015, Israel hacked the Russians and identified U.S. sensitive information in Russian databases. When the Israelis tipped the Americans, the investigations culminated in the prohibition of acquisition of Software from Russian cybersecurity company Kaspersky (NAKASHIMA, 2017; WHITTAKER, 2017).

Not even equipment provided by companies from traditionally neutral countries can be considered unsuspected and unreachable by the tentacles of aggressive countries. Swiss company Crypto AG, manufacturer of cryptographers used in more than 120 countries, belonged, between 1970 and 2018, to a highly secretive partnership between the CIA and the German intelligence service BND, and that the equipment sold by the company was sabotaged

so that those agencies had access to the information encrypted by it (MILLER, 2020). Russians and Chinese, diffident on the neutrality of the company, never used their devices. Moreover, it is relevant to notice that the Germans left the partnership, afraid of the consequences of possible public revelations, in the 1990s, with the Americans remaining alone in the operation for circa two decades more.

Now, the U.S. Government accuses Huawei, the world leader in 5G telephony, of having obscure connections with Chinese intelligence. The U.S. argues that it prefers the use of equipment from Swedish Ericsson and Finnish Nokia, even if more expensive, and personalities of the U.S. government have even suggested the acquisition of shares for controlling these companies (KHARPAL, 2020).

The United States is also pressuring its allies to veto the use of Chinese 5G technology. In 2019 the UK government announced that it would use Huawei 5G technology, although limiting its use to non-sensitive areas. Under heavy pressure of the U.S. government, in May 2020h, the United Kingdom announced a complete ban on the company from 5G and 4G networks. The German Deutsche Telekom (32% state-owned), answered that excluding Huawei from their 5G networks would be ‘Armageddon’, and although not restricting its participation, recently announced that Ericsson was chosen as its 5G supplier (ALLEVEN, 2020; ERICSSON, 2020; PETZINGER, 2020). Under enormous pressure from the U.S. regarding the participation of Huawei in Brazilian networks, with the U.S. ambassador threatening “consequences”, the Brazilian military reportedly told their government that “the same eventual exposure that Brazil may suffer from Chinese technology with Huawei will also occur with any other company” (AMADO e colab., 2020, free translation; ROSA; ANTUNES, 2020). Indeed, a very pragmatic position, considering the Crypto AG, Cisco and Juniper cases.

As stated in Chapter 2, weapons generally can be used either defensively and offensively. But not cyber defences. Thus, defensive Software would not become a problem for exporters, unless they could possibly intend to attack their costumers someday. And this is not likely to be the case for historically non-aggressive countries. On the other hand, customers would avoid defensive products produced by countries considered aggressive (or by countries with close ties with them), since fearing they could leave room to allow intentional vulnerabilities in the future. Again, this seems not to be the case for non-aggressive nations.

Thus, the international market for these products becomes virtually unlimited for non-aggressive states. And they are more likely to benefit from the trust they have gained in the last decades. Or at least they can capitalise the mistrust accumulated by nations considered cyber-

aggressive as the U.S., China, Russia, or even Israel or the U.K. (and Five Eyes), due to their aggressive behaviour and proximity with the U.S.

## **9.5 Conclusion**

There is an excellent opportunity to be explored by non-aggressive states that could allow the development of technologies and services for cyber defences, which could more than justify state-oriented investments guided by good public policies. In the globalised economy of today, every nation shall have interests that conflict with at least one of the cited aggressive countries. And then there is the need of protecting them accordingly.

Public policies targeting to increase national cyber defences can increase the resilience and reduce losses, partially (if not entirely) compensating the costs of these defences. And if these policies are designed in a way that also foments a vibrant and capable software industry, can consolidate a market for cybersecurity software and services, that generate employment and revenue much superior to industrial or agricultural ones. With diplomatic support for exploring international commercial initiatives, new markets can be opened and explored by non-aggressive nations while they develop their defences.





## 10 CONCLUSION

This research aimed to identify whether Software Power can be an alternative for nations with institutional culture and tradition (or personality) of non-aggression to dissuade their peers from committing cyber-offences against them.

The answer is Software Power is the best (if not the only) alternative for non-aggressive countries for dissuading cyber-offences, as well as defending against them and preserving their interests.

To reach this conclusion, the research has come a long way. Chapter 1 described the research plan, presenting the work's context and motivation, the research and support questions, objectives and delimitation of the work, and its theoretical and methodological frameworks.

Chapter 2 explained the idea of Software Power, showing that it is indeed an important element of hard power for modern nations. It offered solid arguments to support the claim that software has far more appeal to developing nations than hardware, presenting an alternative for reaching relevant capabilities faster and cheaper.

Chapter 3 put forward the concept of 'Non-Aggressive nations', developing on the definition of aggression developed and approved by the U.N. It also dug deep on institutionalism, showing how 'culture', 'traditions' and 'norms' become solidified in societies, and even define their 'character', 'personality' or 'face', the way they are identified and seen by other nations.

Chapter 4 dissected 'Deterrence Theory' from its very beginning (perhaps too extensively). It showed that 'deterrence' falls short, and using its limited premises might incur in the invalidation of a useful broader concept that deserves to be better studied. Besides, it also showed that the first wave of cyber-dissuasion theory might soon become the fourth wave of dissuasion theory: where there were only two types of deterrence (Punishment and Denial), now there are four more of dissuasion (Futility, Norms, Entanglement and Individualisation). All of them nurtured in the last twenty years, since the beginning of studies regarding cyber-dissuasion.

Chapter 5 drew on the application of each of the six types of dissuasion to the cyber realm, showing arguments usually used in favour or against each one, and arguing that some are not yet feasible in the short or mid-terms.

Chapter 6 worked on a quantitative content analysis of a significant number of National Cyber Security Strategies, searching for their commonalities and idiosyncrasies, focusing on possible distinctions of emphasis among those emanated from non-aggressive and aggressive countries. It indeed identified significantly different approaches and priorities. The difficulty of

working with very different terminologies and diverse structures made it necessary to develop a specific approach and tool. Although not foreseen at the beginning, it allowed increasing the sample of documents studied to an unprecedented number of cyber-strategies analysed in a single comparison.

Chapter 7 promoted a ‘case study’ focused on the Brazilian cyber strategy, (e-Ciber) discussing how the institutionalised Brazilian culture is represented in it, making that strategy insufficient for the needs of an emerging power as representative as Brazil in the international arena.

Chapter 8 worked on the evaluation of Brazilian cyber capabilities to conclude that they are not compatible with the international economic relevance of the country, and need to be updated, something that might be difficult unless there is a significant change in the concepts that culminated in e-Ciber.

Lastly, Chapter 9 worked on the global importance of the software and services industry for generating jobs, revenue and income for nations with a capable software industry and adequate governmental support. Conclusions are in-line with the fact that practically all National Cyber Security Strategies consider the need for an endogenous I.T. sector and market.

In the end, the research could demonstrate that non-aggressive countries are not able to pose credible threats, and that dissuasion based on threats in cyberspace have not yet produced results, not even for aggressive countries with confirmed capabilities. Hence, Dissuasion by Punishment, the prevailing alternative in the mainstream of the literature, is not an option.

Furthermore, the research could demonstrate that Software Power, in the form of cyber dissuasion by denial, presents the best option for non-aggressive countries. It preserves values that are relevant for non-aggressive countries, institutionalised in their societies. It elevates the costs of attacks while effectively reducing the losses caused by cyberattacks. And it opens a strategic business alternative for non-aggressive nations.

The most relevant limitation of the research was the fact that, although conceptually working with the general concept of non-aggressive nations until Chapter 6, it focused in Brazil. This is explainable in many ways. The first and more obvious is the fact that it was mostly conducted in the Brazilian Army Command and General Staff College. The second is the moment that the country has lived in its cybersecurity and cyber defence reality in recent years.

Brazil cannot “keep calm”, and must “mind the gap”! From lemons, caipirinha!<sup>18</sup>

---

<sup>18</sup> Brazilian national drink, made with *cachaça* (typical Brazilian spirit distilled from sugar cane juice), ice, sugar and lemons.

## 11 REFERENCES

- ABES. *Mercado Brasileiro de Software*. . [S.l: s.n.], 2016.
- ABES. *Mercado Brasileiro de Software*. . [S.l: s.n.], 2017.
- ABES. *Mercado Brasileiro de Software*. . [S.l: s.n.], 2018.
- ABES. *Mercado Brasileiro de Software 2019*. . [S.l: s.n.], 2019.
- ABES. *Mercado Brasileiro de Software 2020*. . [S.l: s.n.], 2020.
- ACHTEN, Nele. New U.N. Debate on Cybersecurity in the Context of International Security. *Lawfare*, 30 Jul 2019.
- ACKOFF, Russell. From Data to Wisdom. *Journal of Applied Systems Analysis*, v. 16, n. 1, 1989.
- ADAMS, James. Virtual Defense. *Foreign Affairs*, v. 80, n. 3, p. 98, 2001.
- ADAMSKY, Dmitry (Dima). From Moscow with coercion: Russian deterrence theory and strategic culture. *Journal of Strategic Studies*, v. 41, n. 1–2, p. 33–60, 2018. Disponível em: <<https://doi.org/10.1080/01402390.2017.1347872>>.
- ALLEVEN, Monica. Deutsche Telekom selects Ericsson for 5G RAN in Germany. *FierceWireless*, 22 Jul 2020. Disponível em: <<https://www.fiercewireless.com/operators/deutsche-telekom-selects-ericsson-for-5g-ran-germany>>. Acesso em: 8 ago 2020.
- AMADO, Guilherme e BARRETO, Eduardo e MATSUI, Naomi. O recado das Forças Armadas ao Ministério da Defesa sobre o 5G - Época. *Época*, 7 Ago 2020. Disponível em: <<https://epoca.globo.com/guilherme-amado/o-recado-das-forcas-armadas-ao-ministerio-da-defesa-sobre-5g-24571588>>. Acesso em: 8 ago 2020.
- AMIN, Espiridião. *Relatório de Avaliação de Política Pública: A Política Nacional sobre Defesa Cibernética*. . Brasília: [s.n.], 2019.
- AMIN NAVES, Guido; MALAGUTTI, Marcelo. Defesa Cibernética (ou Ciberdefesa). In: SILVA, F. C. T. DA e colab. (Org.). *Dicionário de História, Historiadores e Conceitos Militares*. [S.l: s.n.], [S.d.] .

AMORIM, Celso. *A Política de Defesa de um País Pacífico. Aula Magna Cursos de Altos Estudos* 2012. Rio de Janeiro: ESG. Disponível em: <[https://www.defesa.gov.br/arquivos/2012/mes03/esg\\_marco\\_2012.pdf](https://www.defesa.gov.br/arquivos/2012/mes03/esg_marco_2012.pdf)>. , 2012

ANGELO, Cláudio. “Eixo do mal” científico: Ministério pede explicações à Dell sobre exigências a físicos. *Folha de São Paulo*, São Paulo, 14 Set 2007. Disponível em: <<http://www1.folha.uol.com.br/fsp/ciencia/fe1409200703.htm>>.

APACHE SOFTWARE FOUNDATION. *Apache Accumulo*. Disponível em: <<https://accumulo.apache.org/>>. Acesso em: 27 ago 2020a.

APACHE SOFTWARE FOUNDATION. *Apache Hadoop*. Disponível em: <<http://hadoop.apache.org/>>. Acesso em: 27 ago 2020b.

ARENG, Liina. *Lilliputian States in Digital Affairs and Cyber Security*. . [S.l: s.n.], 2014.

ARMSTRONG, James. *The US Military Can't Just “Hire” Cyber Expertise. Here's Why*. Disponível em: <<https://mwi.usma.edu/us-military-cant-just-hire-cyber-expertise-heres/>>. Acesso em: 15 ago 2020.

ARNOLD, Jack. *The Mouse that Roared*. . [S.l: s.n.]. Disponível em: <<https://www.imdb.com/title/tt0053084/>>. Acesso em: 11 nov 2020. , 17 Jul 1959

ARQUILLA, John. From Blitzkrieg to Bitskrieg: The Military Encounter with Computers. *Communications of the ACM*, v. 54, n. 10, p. 58, 2011.

ARQUILLA, John; RONFELDT, David. Cyberwar is coming! *Comparative Strategy*, v. 12, n. 2, p. 141–165, 1993.

AUCHARD, Eric e FINKLE, Jim. Ukraine utility cyber attack wider than reported. *Reuters*, 2016. Disponível em: <<http://www.reuters.com/article/us-ukraine-crisis-malware-idUSKBN0UI23S20160104>>.

AUSTIN, Greg. Middle Powers and Cyber-Enabled Warfare: The Imperative of Collective Security. 2016a, [S.l: s.n.], 2016.

AUSTIN, Greg. Sino-US tensions in Cyberspace: All China's fault? *The Diplomat*, 2 Set 2015. Disponível em: <<http://thediplomat.com/2015/09/sino-us-tensions-in-cyberspace-all-chinas->

fault/>.

AUSTIN, Greg. Strategic culture and Cyberspace: Cyber militias in peacetime? *The Diplomat*, 12 Fev 2016b. Disponível em: <<http://thediplomat.com/2016/02/strategic-culture-and-cyberspace-cyber-militias-in-peacetime/>>.

AUSTRALIA. *Australia's Cyber Security Strategy 2020*. . [S.l: s.n.], 2020.

AVANT, Deborah. Political Institutions and Military Effectiveness: Contemporary United States and United Kingdom. In: BROOKS, R.; STANLEY, E. (Org.). *Creating Military Power*. [S.l.]: Stanford University Press, 2007. p. 80–105.

AZULAI, Yuval. Israel seeks larger slice of security market. *Globes*, 16 Nov 2016. , p. 11–15.

BALDWIN, David. Inter-nation influence revisited. *Journal of Conflict Resolution*, v. 15, n. 4, p. 471–486, 1971.

BANACH, William. *Investigative report on the U.S. National security issues posed by Chinese telecommunications companies Huawei and ZTE*. . [S.l: s.n.], 2012. Disponível em: <[https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE Investigative Report \(FINAL\).pdf](https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf)>.

BARDIN, Laurence. *Análise de Conteúdo*. São Paulo: Edições 70, 2016.

BARLOUET, Alain. La France muscle sa cyberdéfense. *Le Figaro*, Paris, 13 Dez 2016.

BARLOW, John. *A Declaration of the Independence of Cyberspace*. Disponível em: <<https://www.eff.org/cyberspace-independence>>. Acesso em: 30 nov 2020.

BARNES, Julian. U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say. *The New York Times*, New York, NY, 28 Ago 2019. Disponível em: <<https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html>>.

BARONE, João. *1942: O Brasil e sua guerra quase desconhecida*. Rio de Janeiro: Nova Fronteira, 2013.

BECHARA, Evanildo. *Moderna Gramática Portuguesa*. 37. ed. Rio de Janeiro: Editora Nova Fronteira Participações S.A., 2009.

BEEKER, Kevin R e colab. Operationally Responsive Cyberspace: A Critical Piece in the Strategic Deterrence Equation. In: LOWTHER, A. (Org.). *Thinking about Deterrence: Enduring Questions in a Time of Rising Powers, Rogue Regimes, and Terrorism*. [S.l.]: Air University Press, 2013. .

BEER, William. Cyber security in Brazil: Can a grassroots campaign help protect a country. *Georgetown Journal of International Affairs*, v. 16, p. 178–185, 2015.

BELL, Daniel. *The coming of post-industrial society: A venture in social forecasting*. [S.l.]: Basic Books, 1976.

BERGER, Thomas. Norms, Identity, and National Security in Germany and Japan. In: KATZENSTEIN, P. (Org.). *The Culture of National Security: Norms and Identity in World Politics*. [S.l.]: Columbia University Press, 1996. .

BETZ, David; PHILLIPS, Vaughan. Putting the Strategy Back into Strategic Communications. *Defence Strategic Communications*, v. 3, 2017.

BETZ, David; STEVENS, Tim. *Cyberspace and the state: Towards a strategy for Cyberpower*. [S.l.]: Routledge for the International Institute for Strategic Studies (IISS), 2011.

BIDDLE, Tami. Coercion Theory: A Basic Introduction for Practitioners. *Texas National Security Review*, v. 3, n. 2, p. 1–30, 2020.

BIERCUK, Michael J.; FONTAINE, Richard. The Leap into Quantum Technology: A Primer for National Security Professionals. *War On The Rocks*, p. 1–13, 2017.

BIGO, Didier. When two become one: Internal and external securitisations in Europe. In: KELSTRUP, M.; WILLIAMS, M. (Org.). *International Relations Theory and the Politics of European Integration: Power, Security and Community*. [S.l.]: Routledge, 2000. p. 171–204.

BOINC. *BOINC*. Disponível em: <<https://boinc.berkeley.edu/>>. Acesso em: 17 abr 2019.

BOL. Itamaraty pede política global no combate a crimes cibernéticos. *BOL Notícias*, 9 Set 2011. Disponível em: <<https://noticias.bol.uol.com.br/internacional/2011/09/09/itamaraty-pede-politica-global-no-combate-a-crimes-ciberneticos.htm>>.

BRACKNELL, Butch. *Who Says Cyber Warriors Need to Wear a Uniform?* Disponível em:

<<https://mwi.usma.edu/says-cyber-warriors-need-wear-uniform/>>. Acesso em: 15 ago 2020.

BRANGETTO, Pascal. *National Cyber Security Organisation: France*. [S.l.: s.n.], 2015.

BRANTLY, Aaron. Entanglement in Cyberspace: Minding the Deterrence Gap. *Democracy and Security*, v. 16, n. 3, p. 210–233, 2020.

BRASIL-CN. **Constituição Federal de 1988**. , 1988.

BRASIL-CN. **Lei 13.954/2019**. , 16 Dez 2019. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2019/lei/L13954.htm](http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13954.htm)>. Acesso em: 15 ago 2020.

BRASIL-CN. **Lei Complementar 97**. , 1999.

BRASIL-CN. *Relatório da CPI da Espionagem Eletrônica do Senado Federal*. . Brasília, Brasil: [s.n.], 2014.

BRASIL-EB. *Manual de Campanha: ESTRATÉGIA C-124-I*. [S.l.]: Exército Brasileiro, 2001.

BRASIL-GSI. *Estratégia Nacional de Segurança Cibernética*. . Brasília: [s.n.], 2020.

BRASIL-GSI. *Estratégia Nacional de Segurança Cibernética (e-Ciber)*. *Participa.Br*. Brasília: [s.n.], 2019. Disponível em: <<http://www.participa.br/seguranca-cibernetica/estrategia-nacional-de-seguranca-cibernetica-e-ciber>>.

BRASIL-GSI. **Política Nacional de Segurança da Informação**. , 2018.

BRASIL-IBGE. *Estatística do Povoamento - Evolução da População Brasileira*. Disponível em: <<https://brasil500anos.ibge.gov.br/estatisticas-do-povoamento/evolucao-da-populacao-brasileira.html>>. Acesso em: 12 abr 2020.

BRASIL-MD. *Escola Nacional de Defesa Cibernética é inaugurada em Brasília*. Disponível em: <<https://www.defesa.gov.br/noticias/52690-escola-nacional-de-defesa-cibernetica-e-inaugurada-em-brasilia>>. Acesso em: 14 abr 2020.

BRASIL-MD. *Exército Brasileiro - Organograma*. Disponível em: <<http://www.eb.mil.br/organograma>>. Acesso em: 14 abr 2020a.

BRASIL-MD. *Manual Básico Vol. 1*. Rio de Janeiro: ESG, 2014.

BRASIL-MD. *Missões de Paz*. Disponível em: <<https://www.defesa.gov.br/relacoes-internacionais/missoes-de-paz>>. Acesso em: 15 abr 2018.

BRASIL-MD. *Política Nacional de Defesa e Estratégia Nacional de Defesa*. . Brasília: [s.n.], 2016.

BRASIL-MD. *Política Nacional de Defesa e Estratégia Nacional de Defesa*. . Brasília: [s.n.], 2020b.

BRASIL-MRE; BRASIL-MJSP. *Processo de adesão à Convenção de Budapeste - Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública*. Disponível em: <<http://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/21146-processo-de-adesao-a-convencao-de-budapeste-nota-conjunta-do-ministerio-das-relacoes-exteriores-e-do-ministerio-da-justica-e-seguranca-publica>>. Acesso em: 11 dez 2019.

BRASIL-PR. **Decreto 9.637/2018**. , 2018.

BRASIL-SENADO NOTÍCIAS. Aprovadas em Plenário novas Política e Estratégia Nacional de Defesa. *Senado Notícias*, Brasília, 13 Dez 2018.

BRAW, Elisabeth; BROWN, Gary. Personalised Deterrence of Cyber Aggression. *RUSI Journal*, v. 165, n. 2, p. 48–54, 2020.

BRIGATTO, Gustavo. Tempest, empresa de segurança digital, compra integradora EZ-Security. *Valor Econômico*, São Paulo, 18 Fev 2018.

BRODIE, Bernard. Strategy as a Science. *World Politics*, v. 1, n. 4, p. 467–488, 1949.

BRODIE, Bernard. *Strategy In The Missile Age*. [S.l.]: RAND Corporation, 1959a.

BRODIE, Bernard. The Anatomy of Deterrence. *World Politics*, v. 11, n. 02, p. 173–191, 1959b.

BROOKS, Risa. Introduction: The Impact of Culture, Society, Institutions, and International Forces on Military Effectiveness. In: BROOKS, R.; STANLEY, E. (Org.). *Creating Military Power*. [S.l.]: Stanford University Press, 2007. p. 1–26.

BSA FOUNDATION. *Software: A € 910 Billion Catalyst for the EU Economy*. . [S.l.: s.n.], 2016a.



- BSA FOUNDATION. *Software: Growing US Jobs and the GDP*. . [S.l: s.n.], 2019.
- BSA FOUNDATION. *The \$1 Trillion Economic Impact of Software*. . [S.l: s.n.], 2016b.
- BSA FOUNDATION. *The Growing \$1 Trillion Economic Impact of Software*. . [S.l: s.n.], 2017.
- BSA FOUNDATION. *The Growing €1 Trillion Economic Impact of Software*. . [S.l: s.n.], 2018.
- BUCHANAN, Ben. Corporate Cybersecurity Is Becoming Geopolitical. Are U.S. Tech Companies Ready? *Harvard Business Review*, Ago 2018.
- BUCHANAN, Ben. *The Cybersecurity dilemma: Hacking, trust and fear between nations*. [S.l.]: C Hurst & Co Publishers, 2017.
- BUCHANAN, Ben; RID, Thomas. Attributing Cyber attacks. *Journal of Strategic Studies*, v. 38, n. 1–2, p. 4–37, 2014.
- BUSH, George W. The National Security Strategy United States of America. n. September, p. 1–31, 2002. Disponível em: <<http://www.state.gov/documents/organization/63562.pdf>>.
- BUZAN, Barry; HANSEN, Lene. *The Evolution of International Security Studies*. [S.l.]: Cambridge University Press, 2009.
- BUZAN, Barry; WÆVER, Ole. Macrosecuritisation and security constellations: Reconsidering scale in securitisation theory. *Review of International Studies*, v. 35, n. 2, p. 253–276, 2009.
- BUZAN, Barry; WÆVER, Ole; WILDE, Jaap De. *Security: A New Framework for Analysis*. London: Lynne Rienner Publishers, 1998.
- BYMAN, Daniel; WAXMAN, Matthew. *The Dynamics of Coercion: American Foreign Policy and the Limits of Military Might*. [S.l.]: Cambridge University Press, 2002.
- CAIAFA, Roberto. 10 perguntas para o general Okamura, comandante da Defesa Cibernética do Exército Brasileiro. *Tecnologia e Defesa*, 26 Mar 2018. Disponível em: <<https://tecnodefesa.com.br/10-perguntas-para-o-general-okamura-comandante-da-defesa-cibernetica-do-exercito-brasileiro/>>.

CALLEJA, Alejandro; TAPIADOR, Juan; CABALLERO, Juan. A look into 30 years of malware development from a software metrics perspective. 2016, [S.l.]: Springer Verlag, 2016. p. 325–345.

CAMPBELL, Duncan. *Development of Surveillance Technology and Risk of Abuse of Economic Information Part 2/5*. [S.l.: s.n.], 1999. Disponível em: <[http://www.europarl.europa.eu/RegData/etudes/etudes/join/1999/168184/DG-4-JOIN\\_ET\(1999\)168184\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/etudes/join/1999/168184/DG-4-JOIN_ET(1999)168184_EN.pdf)>.

CARR, Jeffrey. Cyber attacks: Why retaliating against china is the wrong reaction. *The Diplomat*, 6 Ago 2015. Disponível em: <<http://thediplomat.com/2015/08/cyber-attacks-why-retaliating-against-china-is-the-wrong-reaction/>>.

CHINA. *China National Cyberspace Security Strategy (translation)*. . [S.l.: s.n.], 2016. Disponível em: <<https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/>>.

CHURCHILL, Winston. *The Second World War, Volume 1: The Gathering Storm*. [S.l.]: Mariner Books, 1986.

CILLUFFO, Frank; CARDASH, Sharon; SALMOIRAGHI, George. A Blueprint for Cyber Deterrence: Building Stability through Strength. *Military and Strategic Affairs*, v. 4, n. 3, p. 3–23, 2012.

CIMPANU, Catalin. Microsoft, FireEye confirm SolarWinds supply chain attack. *ZDNet*, 14 Dez 2020. Disponível em: <<https://www.zdnet.com/article/microsoft-fireeye-confirm-solarwinds-supply-chain-attack/>>. Acesso em: 1 jan 2021.

CLARK, Don. U.S. Agencies block technology exports for supercomputer in China. *The Wall Street Journal*, 9 Abr 2015.

CLARKE, Richard A; KNAKE, Robert K. *Cyber war: The next threat to national security and what to do about it*. New York: HarperCollins Publishers, 2010.

CLAUSEWITZ, Carl Von. *On War*. Princeton: Princeton University Press, 1976.

CLINE, Ray. *World power assessment: A calculus of strategic drift*. Boulder, CO.: Westview Press, 1977.

CMMI INSTITUTE. *CMMI Institute*. Disponível em: <<https://cmmiinstitute.com/>>. Acesso em: 27 ago 2020.

COLATIN, Samuele. *A surprising turn of events: UN creates two working groups on cyberspace*. Disponível em: <<https://ccdcoe.org/incyber-articles/a-surprising-turn-of-events-un-creates-two-working-groups-on-cyberspace/>>. Acesso em: 3 nov 2019.

COUNCIL OF EUROPE. *Chart of signatures and ratifications of Treaty 185 (Convention on Cyber Crime)*. Council of Europe. Council of Europe: [s.n.]. Disponível em: <<https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures>>. , 2019

CROWDSTRIKE. *2019 Global Threat Report: Adversary Tradecraft and the Importance of Speed*. *2019 Global Threat Report*. [S.l: s.n.], 2019. Disponível em: <[https://crowdstrike.lookbookhq.com/email-global-threat-report-2019/crowdstrike-2019-gtr?ctm\\_campaign=2019\\_Global\\_Threat\\_Report\\_EMEA\\_prospects&ctm\\_medium=Email&ctm\\_source=Marketo](https://crowdstrike.lookbookhq.com/email-global-threat-report-2019/crowdstrike-2019-gtr?ctm_campaign=2019_Global_Threat_Report_EMEA_prospects&ctm_medium=Email&ctm_source=Marketo)>.

D'ALAMA, Luna. Tragédia em Alcântara faz dez anos e Brasil ainda sonha em lançar foguete. *G1*, 22 Ago 2013. Disponível em: <<http://g1.globo.com/ciencia-e-saude/noticia/2013/08/tragedia-em-alcantara-faz-dez-anos-e-brasil-ainda-sonha-em-lancar-foguete.html>>.

DAMATTA, Roberto. *O que faz do brasil, Brasil?* Rio de Janeiro: [s.n.], 1984.

DASKAL, Jennifer e colab. *Data and Sovereignty*. *CyCon US*. Washington: Army Cyber Institute. , 2019

DAVIS, Paul. Deterrence, Influence, Cyber Attack and Cyberwar. *International Law and Politics*, v. 47, n. 327, p. 327–355, 2015.

DAVIS, Paul. *Toward theory for Dissuasion (or deterrence) by denial: Using simple cognitive models of the adversary to inform strategy*. . [S.l: s.n.], 2014.

DEAN, Jeffrey; GHEMAWAT, Sanjay. MapReduce: Simplified Data Processing on Large Clusters. 2004, San Francisco: [s.n.], 2004. p. 137–147.

DEFENSE LOGISTICS AGENCY. *Defense Logistics Agency Strategic Plan 2015-2022*. . [S.l: s.n.], 2015. Disponível em: <<http://www.strategicmaterials.dla.mil/Pages/default.aspx>>.

DEFESANET. Aviação do Exército - Exército recria aviação de asas fixas e FAB critica. *DefesaNet*, Brasília, 6 Jun 2020a. Disponível em: <<https://www.defesanet.com.br/avex/noticia/37078/Exercito-recria-aviacao-de-asas-fixas-e-FAB-critica/>>. Acesso em: 14 ago 2020.

DEFESANET. Aviação do Exército - Urgente - Revogado Decreto sobre a Aviação do Exército. *DefesaNet*, Brasília, 8 Jun 2020b. Disponível em: <<https://www.defesanet.com.br/avex/noticia/37089/Urgente---Revogado-Decreto-sobre-a-Aviacao-do-Exercito/>>. Acesso em: 14 ago 2020.

DENNING, Dorothy. Rethinking the Cyber Domain and Deterrence. *Joint Forces Quarterly*, v. 77, n. 2nd Quarter, p. 8–15, 2015.

DEPARTMENT OF FOREIGN AFFAIRS AND TRADE. *Australia's International Cyber Engagement Strategy*. Department of Foreign Affairs and Trade. [S.l: s.n.], 2017. Disponível em: <[https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/pdf/DFAT\\_AICES\\_AccPDF.pdf](https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/pdf/DFAT_AICES_AccPDF.pdf)>.

DEVANNY, Joe. *The ethics of offensive cyber operations*. . London: [s.n.], 2020.

DINIZ, Gustavo; MUGGAH, Robert; GLENNY, Misha. *Deconstructing cyber security in Brazil: Threats and Responses*. Strategic Paper. Rio de Janeiro: [s.n.], 2014. Disponível em: <<https://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf>>.

DORATIOTO, Francisco. *Maldita Guerra*. São Paulo: Companhia das Letras, 2002.

DRAGOS. *CRASHOVERRIDE: Analyzing the Threat to Electric Grid Operations*. . [S.l: s.n.], 2017. Disponível em: <<https://dragos.com/blog/crashoverride/CrashOverride-01.pdf>>.

DUNFORD, Joseph. *Special Areas of Emphasis for Joint Professional Military Education in Academic Years 2020 and 2021*. . [S.l: s.n.], 2019

ELLIOTT, David. Deterring Strategic Cyberattack. *IEEE Security & Privacy Magazine*, v. 9, n. 5, p. 36–40, 2011.

EPEX. *Integrando capacidades na vigilância e na atuação em nossas fronteiras*. Disponível em: <<http://www.epex.eb.mil.br/index.php/sisfron>>. Acesso em: 4 jan 2020a.

EPEX. *Programa da Defesa Cibernética na Defesa Nacional*. Disponível em: <<http://www.epex.eb.mil.br/index.php/defesa-cibernetica/defesa-cibernetica-na-defesa-nacional>>. Acesso em: 20 nov 2017b.

ERICSSON. *Deutsche Telekom and Ericsson strengthen partnership with 5G deal - Ericsson*. Disponível em: <<https://www.ericsson.com/en/press-releases/2020/7/deutsche-telekom-and-ericsson-strengthen-partnership-with-5g-deal>>. Acesso em: 8 ago 2020.

ESTONIA. *Cybersecurity Strategy Republic of Estonia*. . Tallinn: [s.n.], 2019. Disponível em: <[https://www.mkm.ee/sites/default/files/kyberturvalisuse\\_strateegia\\_2022\\_eng.pdf](https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf)>.

EUROPEAN COMMISSION. *High-Performance Computing*. . [S.l.]: European Comission, 2017a.

EUROPEAN COMMISSION. *High Performance Computing (HPC) Factsheet*. . [S.l.]: European Comission, 2017b.

EUROPEAN UNION. *What is the LGPD? Brazil's version of the GDPR*. Disponível em: <<https://gdpr.eu/gdpr-vs-lgpd/>>. Acesso em: 2 abr 2020.

EYRE, Dana; SUCHMAN, Mark. Status, Norms, and the Proliferation of Conventional Weapons: An Institutional Theory Approach. In: KATZENSTEIN, P. (Org.). *The Culture of National Security: Norms and Identity in World Politics*. [S.l.]: Columbia University Press, 1996. .

FAGEN, Richard. The United States and Chile: Roots and Branches. *Foreign Affairs*, v. 53, n. 2, p. 297–313, 1975.

FALCO, Marco. *Stuxnet Facts Report*. . Tallinn: [s.n.], 2012.

FALLIERE, Nicolas; MURCHU, Liam O; CHIEN, Eric. *W32.Stuxnet Dossier. Symantec-Security Response*. [S.l: s.n.], 2011.

FARRELL, Henry; GLASER, Charles L. The role of effects, saliencies and norms in US Cyberwar doctrine. *Journal of Cybersecurity*, v. 3, n. 1, p. 7–17, 2017.

FELL, Andy e BASS, Bevan. World ' s First 1,000-Processor Chip. *UC Davis News*, Davis, 17 Jun 2016.

FIDLER, David. The UN Secretary-General's Call for Regulating Cyberwar Raises More Questions Than Answers. *Council on Foreign Relations Blog*, 15 Mar 2018. , p. 2–5.

FIGUEIREDO, Nice. Legislação de Informática no Brasil. *Revista de Biblioteconomia de Brasília*, v. 34, n. 81, 1986.

FINANCIAL TIMES. Quantum computing rivals muster software power in new ‘ arms race ’. *Financial Times*, p. 8–11, Out 2017.

FINNEMORE, Martha; HOLLIS, Duncan B. Constructing Norms for Global Cybersecurity. *American Journal of International Law*, v. 110, n. 3, p. 425–479, 2016.

FOLDING@HOME. *Folding@home stats report*. Disponível em: <<https://stats.foldingathome.org/os>>. Acesso em: 29 ago 2020a.

FOLDING@HOME. *Front Page - Folding@home*. Disponível em: <<https://foldingathome.org/home/>>. Acesso em: 29 ago 2020b.

FRANCE. *Revue stratégique de cyberdéfense 12 février 2018*. . [S.l: s.n.], 2018.

FRANCHI, Tássio; MIGON, Eduardo Xavier Ferreira Glaser; VILLARREAL, Roberto Xavier Jiménez. Taxonomy of interstate conflicts: is South America a peaceful region? *Brazilian Political Science Review*, v. 11, n. 2, p. 1–23, 2017.

FREEDMAN, Lawrence. *Deterrence*. London: Polity Press, 2004.

FREEDMAN, Lawrence. *Strategic coercion: Concepts and cases*. Oxford: Oxford University Press, 1998.

FREEDMAN, Lawrence. *Strategy: A history*. Oxford: Oxford University Press, 2015.

FU, Haohuan e colab. The Sunway TaihuLight supercomputer: system and applications. *Science China Information Sciences*, v. 59, n. 7, p. 1–16, 2016.

GALLUP INTERNATIONAL. *Voice of the People 2015: What the World Thinks*. Zurich: Gallup International, 2015.

GAMA NETO, Ricardo. Guerra cibernética/Guerra eletrônica – conceitos, desafios e espaços de interação. *Revista Política Hoje*, v. 26, n. 1, p. 201–218, 2017.

GAMA NETO, Ricardo; LOPES, Gils. Armas Cibernéticas e Segurança Nacional. In: FILHO, O. M.; NETO, W. B. F. G.; MOURA, S. L. DE (Org.). *Segurança e Defesa Cibernética: da fronteira física aos muros virtuais*. [S.l.]: Editora UFPE, 2014. .

GANDEL, Stephen. Lloyd's CEO: Cyber attacks cost companies \$400 billion every year | Fortune. *Fortune*, 23 Jan 2015. Disponível em: <<https://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/>>. Acesso em: 11 dez 2020.

GCHQ. *GCHQ History*. . [S.l: s.n.]. Disponível em: <<http://www.gchq.gov.uk/history/Pages/index.aspx>>. , 2016

GCHQ. *HIMR Data Mining Research Problem Book*. [S.l.]: GCHQ, 2011.

GERMANY. *Cyber-Sicherheitsstrategie für Deutschland*. . [S.l: s.n.], 2016.

GERRING, John. Mere Description. *British Journal of Political Science*, v. 42, p. 721–746, 2012. Disponível em: <[www.gly.uga.edu/railsback/](http://www.gly.uga.edu/railsback/)>. Acesso em: 26 jun 2020.

GILES, Keir; MONAGHAN, Andrew. *Legality in Cyberspace: An Adversary View. The Letort Papers*. [S.l: s.n.], 2014. Disponível em: <<http://www.carlisle.army.mil/ssi>>.

GIRALDI, Renata. Patriota: por ser um país pacífico, Brasil tem reconhecimento no cenário internacional. *Agência brasil*, 5 Set 2012.

GLOBALFIREPOWER.COM. *2020 Military Strength Ranking*. Disponível em: <<https://www.globalfirepower.com/countries-listing.asp>>. Acesso em: 27 abr 2020.

GOMES, Laurentino. *1808*. São Paulo: Planeta, 2007.

GOMES, Laurentino. *1822*. Rio de Janeiro: Nova Fronteira, 2010.

GOMES, Laurentino. *1889*. Rio de Janeiro: Globo, 2013.

GOMPERT, David; BINNENDIJK, Hans. Time for Washington to amp up the power to coerce. *War On The Rocks*, 2016.

GREENBERG, Andy. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *Wired*, p. 1–14, Ago 2018. Disponível em: <<https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>>.

GREENWALD, Glenn. *No place to hide: Edward Snowden, the NSA and the surveillance state*. [S.l.]: Penguin Books, 2014.

GRIFFITHS, William. *The Great War*. [S.l.]: Square One Publishers, 1986. Disponível em: <[https://books.google.it/books?id=Fw7Owo0USCwC&printsec=frontcover&dq=the+great+war+william+griffiths+amazon&hl=pt-BR&sa=X&ved=2ahUKEwiRouDK-dnrAhXOo4sKHc6TCIEQ6AEwAHoECAUQA#v=onepage&q=the great war william griffiths amazon&f=false](https://books.google.it/books?id=Fw7Owo0USCwC&printsec=frontcover&dq=the+great+war+william+griffiths+amazon&hl=pt-BR&sa=X&ved=2ahUKEwiRouDK-dnrAhXOo4sKHc6TCIEQ6AEwAHoECAUQA#v=onepage&q=the%20great%20war%20william%20griffiths%20amazon&f=false)>. Acesso em: 8 set 2020.

GRIGSBY, Alex. The end of cyber norms. *Survival*, v. 59, n. 6, p. 109–122, 2017.

GRIGSBY, Alex. The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased. *Council on Foreign Relations*, p. 1–4, Nov 2018.

GRIMAILA, Michael; MILLS, Robert; BEEKER, Kevin. Applying Deterrence in Cyberspace. *IO Journal*, v. 1, n. 4, p. 21–27, 2010.

GUEDES DE OLIVEIRA, Marcos Aurelio; PORTELA, Lucas Soares. As camadas do espaço cibernético sob a perspectiva dos documentos de defesa do Brasil. *Revista Brasileira de Estudos de Defesa*, v. 4, n. 2, p. 77–99, 2017.

GUTERRES, António. *Secretary-General's address at the Opening Ceremony of the Munich Security Conference*. . Munique: United Nations. Disponível em: <<https://www.un.org/sg/en/content/sg/statement/2018-02-16/secretary-general's-address-opening-ceremony-munich-security>>. , 2018

HAIKAL, Priscilla. Estratégia Nacional de Segurança Cibernética é aprovada mas redação deixa a desejar. *SEGS*, 11 Jan 2020.

HALLAHAN, Kirk e colab. Defining Strategic Communication. *International Journal of Strategic Communication*, v. 1, n. 1, p. 3–35, 2007.

HARE, Forrest. The significance of attribution to cyberspace coercion: A political perspective. 2012, Tallinn: CCDCOE, 2012. p. 1–15.

HARRIS, Shane. *@War: The rise of the Military-Internet complex*. Boston: Eamon Dolan/Houghton Mifflin Harcourt, 2014a.



HARRIS, Shane. *@War*. Boston: Houghton Mifflin, 2014b.

HAYDEN, Michael V. *Playing to the edge: American intelligence in the age of terror*. New York: The Penguin Press, 2016.

HAYNES, Deborah. Britain to create 2,000-strong cyber force to tackle Russia threat | UK News | Sky News. *SkyNews*, 21 Set 2018. Disponível em: <<https://news.sky.com/story/britain-to-create-2-000-strong-cyber-force-to-tackle-russia-threat-11503653>>. Acesso em: 13 ago 2020.

HENRIKSEN, Anders. The end of the road for the UN GGE process: The future regulation of cyberspace. *Journal of Cybersecurity*, v. 5, n. 1, p. 1–9, 2019.

HERZ, Monica. Concepts of security in South America. *International Peacekeeping*, v. 17, n. 5, p. 598–612, 2010.

HOBBSAWM, Eric. *Age of Extremes: The Short Twentieth Century, 1914-1991*. [S.l.]: Abacus, 1995.

HOWARD, Michael. *Clausewitz: A Very Short Introduction*. Oxford: Oxford University Press, 2002.

HUANG, Zhixiong; MAČÁK, Kubo. Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches. *Chinese Journal of International Law*, v. 16, n. 2, p. 271–310, 1 Jun 2017.

HUBER, Max. *Reports of International Arbitral Awards Island of Palmas case (Netherlands, USA)*. . The Hague: [s.n.], 1928.

HUTCHINS, Eric M; AMIN, Rohan M; CLOPPERT, Michael J. *Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains*. . [S.l.: s.n.], 2010.

IASIELLO, Emilio. Are Cyber Weapons Effective Military Tools? *Military and Strategic Affairs*, v. 7, n. 1, p. 23–40, 2015.

IASIELLO, Emilio. Is Cyber deterrence an illusory course of action? *Journal of Strategic Security*, v. 7, n. 1, p. 54–67, 2014.

ICJ. *Statute of the International Court of Justice*. Disponível em: <<https://www.icj-cij.org/en/statute>>. Acesso em: 1 jan 2021.

IMF. *World Economic Outlook Database*. Disponível em: <<https://www.imf.org/external/pubs/ft/weo/2019/02/weodata/weorept.aspx?pr.x=57&pr.y=17&sy=2019&ey=2019&scsm=1&ssd=1&sort=country&ds=.&br=1&c=512%2C668%2C914%2C672%2C612%2C946%2C614%2C137%2C311%2C546%2C213%2C674%2C911%2C676%2C314%2C548%2C193%2C556%2C122%2C6>>. Acesso em: 8 abr 2020.

IRANIAN ARMED FORCES CYBERSPACE CENTER. General Staff of Iranian Armed Forces Warns of Tough Reaction to Any Cyber Threat. *Nour News*, 18 Ago 2020.

ITALY. *The Italian Cybersecurity Action Plan*. . [S.l.: s.n.], 2017.

JAPAN. *Cybersecurity Strategy (Provisional Translation)*. . [S.l.: s.n.], 2018. Disponível em: <<http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf>>.

JEPPERSON, Ronald; WENDT, Alexander; KATZENSTEIN, Peter. Norms, Identity, and Culture in National Security. In: KATZENSTEIN, P. (Org.). *The Culture of National Security: Norms and Identity in World Politics*. [S.l.]: Columbia University Press, 1996. .

JERVIS, Robert. Deterrence and Perception. *International Security*, v. 7, n. 3, p. 3–30, 1982.

JERVIS, Robert. Deterrence Theory Revisited. *World Politics*, v. 31, n. 2, p. 289–324, 1979.

JOWETT, Benjamin. *Thucydides, Translated into English, to Which Is Prefixed an Essay on Inscriptions and a Note on the Geography of Thucydides (Vol. I)*. Oxford: Clarendon Press, 1900.

KAHN, Herman. *The Nature and Feasibility of War and Deterrence*. [S.l.: s.n.], 1960. Disponível em: <<http://www.rand.org/content/dam/rand/pubs/papers/2005/P1888.pdf>>.

KASPERSKY LABS. *O que é um honeypot? Como os honeypots ajudam a segurança*. Disponível em: <<https://www.kaspersky.com.br/resource-center/threats/what-is-a-honeypot>>. Acesso em: 2 dez 2020.

KATZENSTEIN, Peter. Preface. In: KATZENSTEIN, P. (Org.). *The Culture of National Security: Norms and Identity in World Politics*. [S.l.]: Columbia University Press, 1996. .

KAUFMANN, William. *The Requirements of Deterrence*. . [S.l: s.n.], 1954.

KHALIP, Andrei. U.N. chief urges global rules for cyber warfare. *Reuters*, 19 Fev 2018. , p. 1–6.

KHARPAL, Arjun. US should take stake in Nokia, Ericsson to counter Huawei in 5G: Barr. *CNBC*, 7 Fev 2020.

KIER, Elizabeth. Culture and French Military Doctrine Before World War II. In: KATZENSTEIN, P. (Org.). *The Culture of National Security: Norms and Identity in World Politics*. [S.l.]: Columbia University Press, 1996. .

KISSINGER, Henry. *Diplomacy*. New York: Simon & Schuster, 1994.

KISSINGER, Henry. *World order*. New York: Penguin Group (USA), 2014.

KLIMBURG, Alexander; HELI TIRMAA-KLAAR. *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Action Within the EU*. . Brussels: [s.n.], 2011.

KOPP, Carlo. The Four Strategies of Information Warfare and their Applications. *IO Journal*, v. 1, n. 4, p. 28–33, 2010.

KREVER, Mick e SMITH-SPARK, Laura. Lavrov denies Russian influence over US election. *CNN*, 12 Out 2016.

KUEHL, Daniel. From Cyberspace to Cyberpower: Defining the Problem. *Cyberpower and National Security*. [S.l.]: National Defense University Press, 2009. .

LEWIS, James. *Cross-Domain Deterrence and Credible Threats*. . [S.l: s.n.], 2010. Disponível em: <papers3://publication/uuid/1B60D167-29DA-49E5-825F-06A77C1B17E2>.

LEWIS, James. *Economic Impact of Cybercrime — No Slowing Down*. . [S.l: s.n.], 2018.

LEWYS, Anthony. The Kissinger Doctrine. *The New York Times*, 27 Fev 1975.

LIBICKI, Martin. Cyberdeterrence and Cyberwar. *High Frontier*, 2009.

LIBICKI, Martin. Norms and Normalization. 2019, Washington: Army Cyber Institute, 2019.

LIBICKI, Martin. Pulling Punches in Cyberspace. 2010, [S.l.]: National Academies Press,

2010. p. 123–147.

LIDDELL HART, Basil. *The Method of Defence - by Attack or Defence? The defence of Britain*. New York, NY: Random House, 1939. p. 100–125.

LIDDELL HART, Basil. The strategy of indirect approach. *International Affairs Review Supplement*, v. 19, n. 6/7, p. 394, 1941.

LIFF, Adam P. Cyberwar: A New “Absolute Weapon”? The Proliferation of Cyberwarfare Capabilities and Interstate War. *Journal of Strategic Studies*, v. 35, n. 3, p. 401–428, 2012.

LIMA, Wilson. Ataque hacker no STJ: o que se sabe sobre o maior ataque da história. *Gazeta do Povo*, Brasília, 5 Nov 2020. Disponível em: <<https://www.gazetadopovo.com.br/republica/hacker-stj-tribunal-ataque-pf-investiga/>>. Acesso em: 13 dez 2020.

LINDORFER, Martina e colab. Lines of malicious code: Insights into the malicious software industry. *ACM International Conference Proceeding Series*, p. 349–358, 2012.

LINDSAY, Jon; GARTZKE, Erik. Introduction: Cross-Domain Deterrence, from Practice to Theory. In: LINDSAY, J.; GARTZKE, E. (Org.). *Cross-Domain Deterrence: Strategy in an Era of Complexity*. [S.l.]: Oxford University Press, 2019. p. 1–24.

LUIJF, Eric e colab. *Ten National Cyber Security Strategies: a Comparison*. 2013, [S.l.]: Springer Verlag, 2013. Disponível em: <<http://link.springer.com/10.1007/978-3-642-41476-3>>.

LUKASIK, Stephen J. *A Framework for Thinking About Cyber Conflict and Cyber Deterrence with Possible Declaratory Policies for These Domains*. 2010, [S.l.]: National Academies Press, 2010. p. 99–121.

LYNN, William. Defending a New Domain: The Pentagon’s Cyberstrategy. *Foreign Affairs*, v. 89, n. 5, 2010.

MAČÁK, Kubo. *Is the international law of cyber security in crisis?* 2016, Tallinn: NATO/CCDCOE, 2016. p. 127–139.

MALAGUTTI, Larissa. *Famous Cyberattacks in Light of Countries Positions Regarding*

*Principles of International Law*. 2020. University of Reading, 2020.

MALAGUTTI, Marcelo. Como a Política e a Estratégia Nacionais de Defesa de 2016 Dialogam Entre Si? *Meridiano 47*, v. Forthcomin, 2021.

MALAGUTTI, Marcelo. Estruturas de Ciberdefesa em Diferentes Países. 2017a, Rio de Janeiro: ECEME, 2017.

MALAGUTTI, Marcelo. O Papel da Dissuasão no Tocante a Ofensas Cibernéticas. *Doutrina Militar Terrestre em Revista*, v. 9, p. 18–27, 2016a.

MALAGUTTI, Marcelo. *Software Power*. Disponível em: <<http://www.strifeblog.org/2016/11/02/cybersecurity-in-practice-part-i-software-power/>>.

MALAGUTTI, Marcelo. State-sponsored cyber-offences. *Revista da Escola de Guerra Naval*, v. 22, n. 2, p. 261–290, 2016c.

MALAGUTTI, Marcelo. Statecraft within Cyberspace. *Cyber World Magazine*, n. December, Dez 2017b.

MALAGUTTI, Marcelo. *Why Should Nations Pursue Their Software Power ?* 2016d. 1–60 f. King's College London, 2016.

MALTCHIK, Roberto. Brasil deve lançar foguete no espaço em 2019. *O Globo*, 25 Jun 2017.

MANDARINO, Raphael; CANONGIA, Claudia (Org.). *Livro Verde Segurança Cibernética no Brasil*. [S.l.: s.n.], 2010.

MARKS, Joseph. At 7 Years Old, CYBERCOM Becomes a Full Combatant Command - Defense One. *Defense One*, 17 Ago 2017.

MARTIN, Ciaran. *Cyber-weapons are called viruses for a reason : Statecraft and security in the digital age*. . [S.l.]: King's College London. , 2020

MAZARR, Michael. The world has passed the old grand strategies by. *War On The Rocks*, 2016.

MAZARR, Michael. *Understanding Deterrence. Perspectives*. [S.l.: s.n.], 2018.

MEDEIROS, Breno Pauli; GOLDONI, Luiz Rogério Franco. The Fundamental Conceptual

Trinity of Cyberspace. *Contexto Internacional*, v. 42, n. 1, p. 31–54, 2020.

MEIRA MATTOS, Carlos De. *A Geopolítica e as Projeções do Poder*. [S.l.]: Biblioteca do Exército Editora, 1977.

MENDES, Gilmar Ferreira; FORSTER JÚNIOR, Nestor José (Org.). *Manual de Redação da Presidência da República*. 3. ed. Brasília: Presidência da República, 2018.

METZ, Cade. NSA mimics Google, Pisses off senate. *Wired*, Jul 2012. Disponível em: <<http://www.wired.com/2012/07/nsa-accumulo-google-bigtable/>>.

MEXICO. *National Cybersecurity Strategy*. . [S.l: s.n.], 2017.

MILLER, Greg. How the CIA used Crypto AG encryption devices to spy on countries for decades - Washington Post. *The Washington Post*, 11 Fev 2020.

MINISTÈRE DES ARMÉES. *International Law Applied to Operations in Cyberspace*. . [S.l: s.n.], 9 Set 2019. Disponível em: <<https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf>>.

MINISTRY OF FOREIGN AFFAIRS OF THE KINGDOM OF THE NETHERLANDS. *Appendix: International law in cyberspace*. . [S.l: s.n.], 2019. Disponível em: <<https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace>>.

MOON, Angela. Exclusive: Google suspends some business with Huawei after Trump blacklist - source - Reuters. *Reuters*, 19 Mai 2019.

MOREIRA, José de Albuquerque. Informática: o mito Política Nacional de Informática. *Revista de Biblioteconomia de Brasília*, v. 19, n. 1, p. 23–50, 1995.

MORGAN, Patrick M. Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm. 2010, [S.l.]: National Academies Press, 2010. p. 55–76.

MORGAN, Steve. *Cyber Security Industry Outlook : 2017 to 2021*. CSO. [S.l: s.n.], 20 Out 2016.

MORGENTHAU, Hans. *Politics Among Nations: The Struggle for Power and Peace*. New

York: Alfred Knopf, 1948.

MUGGAH, Robert; THOMPSON, Nathan B. *Brazil must rebalance its approach to cybersecurity*. Disponível em: <<https://www.cfr.org/blog/brazil-must-rebalance-its-approach-cybersecurity>>. Acesso em: 9 set 2016.

NAKASHIMA, E. Israel hacked Kaspersky, then tipped the NSA that its tools had been breached. *The Washington Post*, 10 Out 2017.

NATO. *Resilience and Article 3*. Disponível em: <[https://www.nato.int/cps/en/natohq/topics\\_132722.htm](https://www.nato.int/cps/en/natohq/topics_132722.htm)>. Acesso em: 24 nov 2020.

NAVAL, Poder. Marinha vai substituir fragatas por corvetas, revela Alm. Ivan Taveira. *Poder Naval*, 27 Jan 2017.

NETHERLANDS, The. *National Cyber Security Agenda*. . [S.l: s.n.], 2018.

NEW ZEALAND. *The Application of International Law to State Activity in Cyberspace*. . [S.l: s.n.], 1 Dez 2020. Disponível em: <<https://www.mfat.govt.nz/en/media-and-resources/ministry-statements-and-speeches/cyber-il>>. Acesso em: 7 dez 2020.

NOGUEIRA, Armando. *Escrever é a Arte de Cortar Palavras: De Que Mestre Teria Partido Esta Preciosa Lição?* Disponível em: <[http://portalimprensa.com.br/noticias/ultimas\\_noticias/32240/imprensa+republica+artigo+de+armando+nogueira+sobre+o+desafio+da+educacao+de+texto](http://portalimprensa.com.br/noticias/ultimas_noticias/32240/imprensa+republica+artigo+de+armando+nogueira+sobre+o+desafio+da+educacao+de+texto)>. Acesso em: 1 nov 2014.

NORTH, Douglass. *Institutions, Institutional Change and Economic Performance*. Cambridge: Cambridge University Press, 1990.

NORTH, Douglass. Institutions. *The Journal of Economic Perspectives*, v. 5, n. 1, p. 97–112, 1991.

NUGENT, Walter T K. *Habits of Empire*. New York: Vintage Books, 2009.

NYE, Joseph. Can China Be Deterred in Cyber Space? *The Diplomat*, 3 Fev 2016.

NYE, Joseph. Can Cyber Warfare Be Deterred? *Project Syndicate*, 10 Dez 2015a.

NYE, Joseph. *Cyber Power*. . [S.l: s.n.], 2010. Disponível em:

<<http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf>>.

NYE, Joseph. Cyber War and Peace. *Project Syndicate*, Abr 2012a.

NYE, Joseph. Deterrence and Dissuasion in Cyberspace. *International Security*, v. 41, n. 3, p. 44–71, 2017.

NYE, Joseph. How Will New Cybersecurity Norms Develop? *Project Syndicate*, p. 3–5, Set 2018.

NYE, Joseph. International Norms in Cyberspace. *Project Syndicate*, 11 Mai 2015b.

NYE, Joseph. Rules of the Cyber Road for America and Russia. *Project Syndicate*, Mar 2019.

NYE, Joseph. *Soft Power: The Means To Success In World Politics*. New York, NY: Public Affairs, 2004.

NYE, Joseph. *The future of power*. New York: PublicAffairs, 2012b.

NYE, Joseph. The Mouse Click That Roared. *Project Syndicate*, Set 2013.

OKAMURA, Ângelo. *Abertura do V Seminário Internacional de Defesa Cibernética*. . Brasília: [s.n.]. Disponível em: <<https://cryptoid.com.br/eventos/v-seminario-internacional-de-defesa-cibernetica/>>. , 2017

OSBORNE, George. Chancellor’s speech to GCHQ on cyber security. *Gov.Uk*, p. 1–12, 2015. Disponível em: <<https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security>>.

OSULA, Anna-Maria. *National Cyber Security Organisation: United Kingdom*. [S.l: s.n.], 2015.

OWEN, Taylor; GORWA, Robert. Quantum Leap: China’s Satellite and the New Arms Race. *Foreign Affairs*, 2016.

OXFORD DICTIONARY. *Deter | Definition of Deter by Oxford Dictionary*. Disponível em: <<https://www.lexico.com/definition/deter>>. Acesso em: 10 set 2020.

OXFORD DICTIONARY. *Oxford Advanced Learner’s Dictionary*. Oxford: Oxford University Press, 1992.



OXFORD GCSCC. *Cybersecurity Capacity Review of Brazil*. . [S.l.: s.n.], 2020.

OXFORD GCSCC. *Cybersecurity Capacity Review of the United Kingdom*. . [S.l.: s.n.], 2016.  
Disponível em: <[https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersecurity Capacity Review of the United Kingdom.pdf](https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersecurity%20Capacity%20Review%20of%20the%20United%20Kingdom.pdf)>.

PAGANINI, Pierluigi. Brazil's court system shut down after a massive ransomware attack. *Security Affairs*, 6 Nov 2020.

PAGANINI, Pierluigi. The British army creates the 77th battalion. *Security Affairs*, 15 Feb 2015.

PALETTA, Damian. U.S. Blames Russia for recent hacks. *The Wall Street Journal*, 7 Out 2016.

PAUL, Christopher; PORCHE, Isaac; AXELBAND, Elliot. Cyber Forces and U.S. Cyber Command. *The Other Quiet Professionals*. [S.l.]: RAND Corporation, 2014. .

PEREIRA, Antônio Celso Alves. A legítima defesa no Direito Internacional contemporâneo. *Revista Interdisciplinar de Direito*, v. 7, n. 1, p. 21–36, 2010.

PERNIK, Piret; WOJTKOWIAK, Jesse; VERSCHOOR-KIRSS, Alexander. *National Cyber Security Organisation: UNITED STATES*. [S.l.: s.n.], 2016.

PETZINGER, Jill. Deutsche Telekom describes potential Huawei ban as “Armageddon” scenario. *MSN*, 17 Jun 2020. Disponível em: <<https://www.msn.com/en-gb/money/technology/deutsche-telekom-describes-potential-huawei-ban-as-armageddon-scenario/ar-BB15BxQM>>. Acesso em: 8 ago 2020.

POLLPETER, Kevin. Chinese Writings on Cyberwarfare and Coercion. In: LINDSAY, J.; CHEUNG, T. M.; REVERON, D. (Org.). *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. [S.l.]: Oxford Scholarship Online, 2015. .

POMERLEAU, Mark. Why a long military career in cyber feels like a rarity. *FifthDomain*, 18 Set 2018.

PRICE, Richard; TANNENWALD, Nina. Norms and Deterrence: The Nuclear and Chemical Weapons Taboos. In: KATZENSTEIN, P. (Org.). *The Culture of National Security: Norms and Identity in World Politics*. [S.l.]: Columbia University Press, 1996. .

PROENÇA JR., Domício; LESSA, Marcus Augustus. Brazilian national defence policy and strategy reviewed as a unity. *Revista Brasileira de Política Internacional*, v. 60, n. 2, 2018.

RAUD, Mikk. *China and Cyber: Attitudes, Strategies, Organisation*. [S.l.]: NATO CCDCOE, 2016.

REILLY, James. A norm-taker or a norm-maker? Chinese aid in Southeast Asia. *Journal of Contemporary China*, v. 21, n. 73, p. 71–91, 2012.

RID, Thomas. *Cyber war will not take place*. New York: Oxford University Press, USA, 2012. v. 35.

RID, Thomas. *Rise of the Machines*. London: Scribe Publications, 2016.

RISSE, Thomas. “Let’s argue!”: Communicative action in world politics. *International Organization*, v. 54, n. 1, p. 1–39, 2000.

ROSA, Bruno e ANTUNES, Cláudia. Embaixador dos EUA alerta que se Brasil permitir chinesa Huawei no 5G enfrentará “consequências” - Jornal O Globo. *O Globo*, 20 Jul 2020.

RUIZ, Jose. Brazil, U.S. Co-host South American Defense Conference. *SOUTHCOM Public Affairs*, Natal, 21 Ago 2019.

RUMSFELD, Donald H. Transforming the military. *Foreign Affairs*, v. 81, n. 3, p. 20, 2002.

RUSSELL, Alison. Strategic anti-access/area denial in cyberspace. 2015, Tallinn: [s.n.], 2015.

SABBAGH, Dan. UK to launch specialist cyber force able to target terror groups. *The Guardian*, 27 Fev 2020.

SAINT-PIERRE, Héctor Luis. “Defesa” ou “segurança”? reflexões em torno de conceitos e ideologias. *Contexto Internacional*, v. 33, n. 2, p. 407–433, 2011.

SCHELLING, Thomas. *Arms and influence: With a new preface and Afterword*. [S.l.]: Yale University Press, 2008.

SCHELLING, Thomas. The Role of Deterrence in Total Disarmament. *Foreign Affairs*, v. 40, n. 3, 1962.

SCHELLING, Thomas. *The Strategy of Conflict*. [S.l.]: Harvard University Press, 1980.

SCHMIDT, Michael e PERLROTH, Nicole. U.S. Charges Russian Intelligence Officers in Major Cyberattacks. *The New York Times*, 19 Out 2020.

SCHMITT, Michael. France's Major Statement on International Law and Cyber: An Assessment. *Just Security*, n. 2, p. 2–6, 2019.

SCHMITT, Michael. *Tallinn Manual 2.0 on the International Law Applicable To Cyber Operations*. Cambridge: Cambridge University Press, 2017.

SCHMITT, Michael. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. [S.l.]: Cambridge University Press, 2013.

SCHMITT, Michael; VIHUL, Liis. The Nature of International Law Cyber Norms. *CCDCOE Tallinn Papers*, n. 5, 2014.

SCHNEIDER, Jacquelyn. Blue Hair In The Gray Zone. *War On The Rocks*, Jan 2018.

SCHULTE, Sebastian. German Cyber Command becomes operational. *Jane's*, n. 06 abr., 2017.

SHAFQAT, Narmeen; MASOOD, Ashraf. Comparative Analysis of Various National Cyber Security Strategies. *International Journal of Computer Science and Information Security*, v. 14, n. 1, 2016.

SHIDONG, Zhang. China offers five-year tax breaks to chip makers, software developers to bolster industry as trade war stretches to tech | South China Morning Post. *South China Morning Post*, Shanghai, 22 Mai 2019.

SINGER, J David. Inter-Nation Influence: A Formal Model. *The American Political Science Review*, v. 57, n. 2, p. 420–430, 12 Set 1963.

SKLEROV, Matthew. Responding to international cyber attacks. In: CARR, J. (Org.). *Inside Cyber Warfare: Mapping the Cyber Underworld*. Sebastopol, CA: O'Reilly, 2010. p. 46–62.

SMEETS, Max. U.S. cyber strategy of persistent engagement & defend forward: implications for the alliance and intelligence collection. *Intelligence and National Security*, 2020.

SMEETS, Max; SOESANTO, Stefan. Cyber Deterrence Is Dead. Long Live Cyber Deterrence! *Council on Foreign Affairs*, p. 1–6, 2020.

SNYDER, Glenn. Deterrence: A Theoretical Introduction. In: GARNETT, J. (Org.). *Theories of Peace and Security: A Reader in Contemporary Strategic Thought*. [S.l.]: Palgrave Macmillan, 1970. .

SNYDER, Glenn. *Deterrence and Defence: Toward a Theory of National Security*. [S.l.]: Princeton University Press, 1961.

SNYDER, Glenn. Deterrence and Power. *The Journal of Conflict Resolution*, v. 4, n. 2, p. 163–178, 1960. Disponível em: <<https://www.jstor.org/stable/172650>>.

SNYDER, Glenn. *Deterrence by Denial and Punishment*. . [S.l.: s.n.], 1959.

SOFTEX. *MPS-BR*. Disponível em: <<https://softex.br/mpsbr/>>. Acesso em: 27 ago 2020.

SOLOMON, Shoshanna. Israel wins second-largest number of cybersecurity deals globally. *The Times of Israel*, 15 Abr 2018.

STERLING, Bruce. Flame/Stuxnet/Duqu are attacking Kaspersky. *Wired*, Jun 2015.

STEVENS, Tim. A Cyberwar of ideas? Deterrence and norms in Cyberspace. *Contemporary Security Policy*, v. 33, n. 1, p. 148–170, 2012.

STEVENS, Tim e colab. *UK Active Cyber Defence*. . London: [s.n.], 2019. Disponível em: <<https://www.kcl.ac.uk/policy-institute/assets/uk-active-cyber-defence.pdf>>.

STEVENS, Tim; BETZ, David. Analogical Reasoning and Cyber Security. *Security Dialogue*, v. 44, n. 2, p. 147–164, 2013.

STOKES, Mark. *The PLA General Staff Department Third Department Second Bureau*. . [S.l.: s.n.], 2015.

STONE, John. Cyber war will take place! *Journal of Strategic Studies*, v. 36, n. 1, p. 101–108, 2013.

STRUMPF, Dan. Huawei's 5G Dominance Threatened by U.S. Policy on Chips - WSJ. *The Wall Street Journal*, New York, 21 Jun 2020.

SWI. Switzerland's new cybersecurity centre is a step in the right direction. *SWI (swissinfo.ch)*, 7 Set 2020. Disponível em: <<https://www.swissinfo.ch/eng/switzerland-s-new-cybersecurity->

centre-is-a-step-in-the-right-direction/46016444>. Acesso em: 7 set 2020.

TABANSKY, Lior. Basic Concepts in Cyber Warfare. *Military and Strategic Affairs*, v. 3, n. 1, p. 75–92, 2011.

TED. *Ralph Langner: Cracking Stuxnet, a 21st-century cyber weapon*. [S.l.: s.n.], 2011.

THE ECONOMIST. After Moore's Law. p. 1–37, Mar 2016.

THE ECONOMIST. The world's most valuable resource is no longer oil , but data. *The Economist*, Mai 2017.

THE GRAND JURY FOR THE DISTRICT OF COLUMBIA. *Annex B App5 Indictment*. . Wash: [s.n.], 2018. Disponível em: <<https://www.justice.gov/file/1080281/download>>.

THE NEW YORK TIMES. We Return to Brazil Airbase Used in War. *The New York Times*, Rio de Janeiro, 6 Out 1946. Disponível em: <<https://timesmachine.nytimes.com/timesmachine/1946/10/06/306249852.html?pageNumber=33>>.

TOFFLER, Alvin. *Powershift: Knowledge, wealth, and violence at the edge of the 21st century*. [S.l.]: Bantam Books (Transworld Publishers a division of the Random House Group), 1991.

TOFFLER, Alvin. *The Third Wave*. [S.l.]: William Morrow & Company, 1980.

TOFFLER, Heidi; TOFFLER, Alvin. *Revolutionary wealth: [how it will be created and how it will change our lives]*. [S.l.]: Alfred A. Knopf, 2006.

TONOOKA, Eduardo. Política Nacional de Informática: Vinte Anos de Intervenção Governamental. *Estudos Econômicos*, v. 22, n. 2, p. 273–297, 1992.

TOP500.ORG. *Top500 June 2016*. Disponível em: <<https://www.top500.org/lists/2016/06/>>. Acesso em: 1 jun 2016.

TOP500.ORG. *Top500 November 2015*. Disponível em: <<https://www.top500.org/lists/2015/11/>>. Acesso em: 1 jun 2016.

TOP500.ORG. *TOP500 November 2020*. Disponível em: <<https://top500.org/top500/lists/2020/11/>>. Acesso em: 17 nov 2020.

TRABALHABRASIL. *Salario para Analista de Sistemas. Media salarial paga no Brasil / Trabalha Brasil*. Disponível em: <<https://www.trabalhabrasil.com.br/media-salarial-para-analista-de-sistemas>>. Acesso em: 15 ago 2020.

TUATHAIL, Gearóid Ó; AGNEW, John. Geopolitics and discourse. Practical geopolitical reasoning in American foreign policy. *Political Geography*, v. 11, n. 2, p. 190–204, 1992.

U.S. AIR FORCE. *U.S. Air Force - Career Detail - Cyberspace Operations Officer*. Disponível em: <<https://www.airforce.com/careers/detail/cyberspace-operations-officer>>. Acesso em: 16 ago 2020.

U.S. ARMY CYBER. *Careers in Army Cyber*. Disponível em: <<https://www.goarmy.com/army-cyber/careers-in-army-cyber.html>>. Acesso em: 16 ago 2020a.

U.S. ARMY CYBER. *Cyber Direct Commissioning Program*. Disponível em: <<https://www.goarmy.com/army-cyber/cyber-direct-commissioning-program.html>>. Acesso em: 16 ago 2020b.

U.S. ARMYCYBER. *DOD FACT SHEET: Cyber Mission Force > U.S. Army Cyber Command > Fact Sheets*. Disponível em: <<https://www.arcyber.army.mil/Info/Fact-Sheets/Fact-Sheet-View-Page/Article/2079594/dod-fact-sheet-cyber-mission-force/>>. Acesso em: 12 ago 2020.

U.S. DEPT. OF COMMERCE. *Department of Commerce Announces the Addition of Huawei Technologies Co. Ltd. to the Entity List | U.S. Department of Commerce*. Disponível em: <<https://www.commerce.gov/news/press-releases/2019/05/department-commerce-announces-addition-huawei-technologies-co-ltd>>. Acesso em: 22 jun 2020.

U.S. DOD. *Quadrennial Defense Review Report. Quadrennial Defense Review: Assessing U.S. Defense and Security*. [S.l: s.n.], 2001.

U.S. NAVY. *Navy Cyber Warfare Engineer Officer Program*. Disponível em: <<https://www.navycs.com/officer/cyberwarfareengineer.html>>. Acesso em: 16 ago 2020.

U.S. WHITE HOUSE. *Presidential Policy Directive/PPD-20*. . Washington: [s.n.], 2012.

U.S. WHITE HOUSE. *Report on Cyber Deterrence*. . [S.l: s.n.], 2015.

UK DEPARTMENT FOR INTERNATIONAL TRADE. *Cyber Security Export Strategy*. . [S.l: s.n.], 2018.

UK MINISTRY OF DEFENCE. *Cyber Primer*. *Cyber Primer*. [S.l: s.n.], 2016.

UN GENERAL ASSEMBLY. *A/RES/29/3314 - Definition of Aggression*. . United Nations: [s.n.], 1974

UNITED KINGDOM. *Cyber Security Strategy*. . [S.l: s.n.], 2016. Disponível em: <<http://www.gov.uk/government/publications/cyber-security-strategy>>.

UNITED NATIONS. *Vienna Convention on the Law of Treaties (1969)*. . [S.l: s.n.], 23 Mai 1969

UNITED STATES. *Foreign Economic Espionage in Cyberspace*. . [S.l: s.n.], 2018a.

UNITED STATES. *National Cyber Strategy*. . [S.l: s.n.], 2018b.

US-DHS. *Resilience / Homeland Security*. Disponível em: <<https://www.dhs.gov/topic/resilience>>. Acesso em: 24 nov 2020.

US CENSUS BUREAU. *The Fourth of July: 2016*. Disponível em: <<https://www.census.gov/newsroom/facts-for-features/2016/cb16-ff13.html>>. Acesso em: 20 abr 2020.

VEGETIUS, Publius Flavios. *De Re Militari*.

VEN BRUUSGAARD, Kristin. Russian strategic deterrence. *Survival*, v. 58, n. 4, p. 7–26, 2016.

VITAL, Antonio. Tratado sobre crimes digitais sob desconfiança. *Congresso em Foco*, 5 Jun 2008.

WAGSTYL, Stefan. Germany points finger at Kremlin for cyber attack on the Bundestag. *Financial Times*, Berlin, 13 Mai 2016.

WHITE HOUSE. *The Trump Administration Is Investing \$1 Billion in Research Institutes to Advance Industries of the Future | The White House*. Disponível em: <<https://www.whitehouse.gov/articles/trump-administration-investing-1-billion-research->

institutes-advance-industries-future/>. Acesso em: 29 ago 2020.

WHITTAKER, Zack. What is Kaspersky ' s role in NSA data theft ? Here are three likely outcomes A bombshell news report on Kaspersky ' s alleged involvement in the theft of. *ZDNet*, 9 Out 2017. , p. 1–7.

WRIGHT, Jeremy. *Cyber and International Law in the 21st Century*. Chatham House. London: Chatham House. , 23 Mai 2018

YANG, Yuan e LIU, Nian. Beijing orders state offices to replace foreign PCs and software | Financial Times. *Financial Times*, 8 Dez 2019.

YOST, David. *Debating Security Strategies*. . [S.l: s.n.]. Disponível em: <[http://www.nato.int/docu/review/2003/issue4/english/art4\\_pr.html](http://www.nato.int/docu/review/2003/issue4/english/art4_pr.html)>. , 2003

ZAGARE, Frank; KILGOUR, Marc. *Perfect Deterrence*. [S.l.]: Cambridge, 2004.

ZELENY, Milan. *Management support systems: Towards integrated knowledge management*. *Human Systems Management*. [S.l: s.n.]. , 1987

ZERFASS, Ansgar e colab. Strategic Communication: Defining the Field and its Contribution to Research and Practice. *International Journal of Strategic Communication*, v. 12, n. 4, p. 487–505, 2018.

ZETTER, Kim. *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon*. New York: Random House USA, 2014.

ZETTER, Kim. Everything We Know About Ukraine's Power Plant Hack. *Wired*, Jan 2016.