ASSESSMENTS ON NATIONAL CYBER CAPABILITY

A BRAZILIAN PERSPECTIVE IN A COMPARISON WITH SPAIN

Marcelo Garcia, Fabio Mendonça, Robson de Oliveira Albuquerque
Professional Post-Graduation Program in Electrical Engineering - PPEE - Electrical Engineering Department
Faculty of Technology, University of Brasília (UnB), Brasília, Brazil, Zip Code 70910-900
marcelo.garcia.inbox@gmail.com, fabio.mendonca@redes.unb.br, robson@redes.unb.br

Abstract — **This work proposes a comparison of Brazilian and Spanish cyber capabilities according to organisational and technical assessment criteria. Results show that some of the Spanish strategies could inspire development of Brazilian cyber capability, with benefits for both countries, who share common geopolitical goals such as the stability of Latin America and the suppression of transnational organized crime in Iberoamerica.**

Keywords - cyber; intelligence; security; strategy.

I. INTRODUCTION

In the context of iberoamerican countries, Spain and Portugal have already established more mature cyber capabilities when compared to Latin American nations [1].

Nevertheless, they as well would benefit from a timelier development of cyber capabilities in Latin America, since these countries are already their natural partners in the fight against the transnational organized crime responsible for much of the illegal trafficking of drugs and people in place between the two continents [2].

Comparing national cyber capabilities can illustrate what other countries are doing and whether the directions taken sound right or not. Besides, it exposes patterns that indicate common success factors and lessons from other countries, that policymakers can consider when designing or evaluating their own cyber strategies.

Comparisons must, though, keep a sense of proportion in order to be useful. The United States, for instance, has cyber demands, capacity and resources so disproportionally larger than those of Brazil, not to mention geopolitical goals, that it renders any comparison between the two impractical to the Brazilian policy maker and may sound irrelevant to any other.

With such mindset, this paper proposes a set of assessment criteria focused on the development of effective national cyber capabilities. Brazil and Spain were selected as the initial countries to start this assessment because Brazil is the authors' country; and Spain is perceived as a country that achieved excellent results in cyber with modest means. They are also the biggest economies on either iberoamerican side of the Atlantic. Other countries such as Portugal, Colombia, Mexico, Chile and Argentina are in the roadmap to be included in further studies.

The results shows that the two countries – Brazil and Spain – have significantly different cyber strategies and, considering the reviewed work and the comparison criteria used, this study assesses that Spain has a quite superior national cyber capability than Brazil.

However, the order of magnitude of the resources employed to implement Spain's cyber strategies looks well within reach of Brazilian possibilities, deeming it a feasible and rational model for Brazil to consider.

Since Brazil and Spain share common strategic goals, such as fighting transnational organized crime in South America and stimulating a healthy and secure digital commerce environment in the region, it is expected that the results presented in this paper will inspire Brazilian and other Latin-American policymakers in accelerating their cyber capacity development.

II. RELATED WORK AND BACKGROUND

This section is divided in related work – where relevant research work within cyber strategies is considered, and the background – where conceptual assumptions are considered.

A. Related work

Many organizations have created assessments in the last decade in order to analyse and compare national cyber capabilities. The European Union Agency for Cybersecurity (ENISA) has one of the most comprehensive in terms of criteria evaluated [3]. Others are the International Telecommunications Union (ITU) [1] and the Potomac Institute [4], aiming at a global scale; the Swiss Federal Institute of Technology (ETH) [5] on European countries plus Israel; Belfer Center [6] on 30 top countries with perceived cyber capability; the Organization of American States (OAS) [7] for Americas; the International Institute for Strategic Studies (IISS) [8] on geopolitical allies and adversaries in the US-China conflict; and so on.

These assessments also differ in the criteria evaluated, with most institutions developing its own set of criteria, except for OAS, who employed the Oxford Global Security Capacity Centre's Cybersecurity Capacity Maturity Model (CMM) [9].

Oxford's CMM, however, bears a caveat, when it places specialist cyber intelligence advice too late in the cybersecurity chain [10]. As we will establish in the *Background* section, it is not possible to design reasonable cybersecurity without cyber intelligence informing it first.

The Belfer assessment suggests more realpolitik objectives than those of CMM. It chose a very appealing visualization, quite like the Gartner's "magic quadrant" [11]. However, to assess the criteria, the Belfer study uses 27 indicators, some of which appear to be intended proxies, rather than directly related

Brazilian Intelligence Agency sponsored this research.

2022 17th Iberian Conference on Information Systems and Technologies (CISTI)
22 – 25 June 2022, Madrid, Spain
ISBN: 978-989-33-3436-2

to cyber capability (for example, "mobile speed", "global soft power" and generic "patent applications").

Moreover, the reduction from 27 indicators to 7 objectives, with multiple indicators corresponding to multiple objectives is bound to propagate eventual errors in the weight balance among the criteria. This might only be visible when comparing known realities pairwise. Brazil, for example, figures in the Belfer study as more cyber capable than Italy. Well, we know for a fact that quite the opposite is true.

Curiously, Brazil also comes ahead of Italy in ITU's ranking. It must be noted, though, that ITU assesses governmental commitments rather than capabilities ([5], p. 130). Indeed, there was an acute improvement in perception on Brazilian commitment to the cyber agenda, with ITU placing it third in the Americas, after US and Canada; and 18th in the world, having jumped from the 70th place in previous editions.

Overall, the variety and complexity of cyber assessment models can be intimidating to policymakers, especially from countries that are still in the formative stage of their national cyber capacity, like Brazil itself. For these countries, we deem it more sensible and effective to adapt logical proven paths followed by countries that had success, than to aim at a final evolved top-down structure detached from organic and incremental field experience.

B. Background

"Cyber" abridges a field of knowledge and practice that, from historical and empirical evidence, is formed by 3 disciplines: cyber operations, cyber security and cyber intelligence, as Fig. 1 shows.

Cyber operations appeared first, as a means to collect needed, but otherwise denied, information residing in adversarial computational or network resources or even disrupt them for strategic purposes. Cyber security followed thereupon as the discipline to protect one's own computational and network resources from adversarial cyber operations.

Finally, cyber intelligence compiles relevant knowledge on both, so that its sponsor can continuously improve its operations and security and better determine its adversarial cyber capacity.

From this perspective, it was only logical that the first cyber intelligence groups inside the national intelligence apparatus continuously and progressively informed all other government sections about the matter and eventually helped them form their own cyber teams, either by training, lending or transferring personnel.

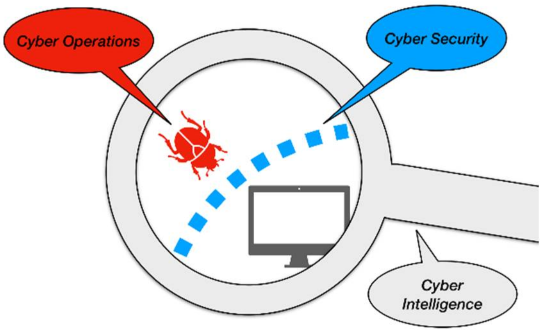


Figure 1. The three core disciplines of cyber.

As the IISS concluded, "*at the heart of any nation's cyber capability, both defensive and offensive, is the ability to* ***identify and understand threats and opportunities in cyberspace***" and "*a* ***core cyber-intelligence capability is the primary foundation of cyber power***" ([8] pp. 3 and 171).

III. Methodology

This section presents the core assumptions considered to evaluate cyber capability, in a perspective meaningful to orient countries at the formative stage of that capability, commencing by addressing their advancements in the key basic cyber disciplines –***intelligence***, ***operations*** and ***security***.

However, technical bodies, especially in government, do not form and act out of self-determination. They must be organized, have legal authority delegated to them, tasked with clearly defined missions and rationally provisioned with resources to fulfil those missions. Therefore, this methodology suggests key ***institutional governance*** criteria needed for appropriate development of the technical ones.

It was also noticed, empirically and in accordance with all assessments, that a synergic relation with the private sector has been a key success factor in the countries' evolution of their cyber capability. Therefore, we also convened criteria for this ***synergy with society*** that will allow solid advancements on a country's cyber capabilities.

We have therefore identified five disciplines – two of them organizational in nature and three technical – and assembled a set of criteria to represent the essential conditions for their adequate development. The criteria will be presented in the next section, as well in the final assessment Fig. 2.

For the criteria assessment scale, we will employ a mix of the 5-level scales found in the CMM and ENISA models, plus a preceding "Absent" level that we found necessary to distinguish from the "Initial" level in those models, resulting in the scale shown in Table I.

TABLE I. TABLE OF ASSESSMENT LEVELS

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

IV. Results and Discussion

Considering the framework and the assessment levels previously defined, we provide a summarized comparison of Brazil and Spain cyber capabilities, discussing the results for each criteria assessed, for both countries, per set of criteria.

A. Institutional Governance

Institutional governance is the basis for effective and coordinated agency, especially in complex matters with multiple parties, which is the case of cyber.

1) Clearly defined institutional leadership over cyber intelligence.

Expediting the flow of information regarding cyber issues in government will accelerate the development of national capacity. This will happen sooner where there is institutional access to cyber intelligence specialists.

Brazil: Brazilian Intelligence Agency (ABIN) and its Center of Research and Development for the Security of Communications (CEPESC), Brazil's main cryptographic unit, hold increasing de facto responsibility over national cyber intelligence. However, this mission has not yet been embraced with energy in a systematic approach, being therefore still in a FORMATIVE stage.

Spain: In Spain, the institution that had the core expertise and disseminated it to others was Spain's signals intelligence branch (CCN) under Spain's intelligence agency (CNI). CNI-CCN has managed to project great influence, for its cyber intelligence systems are present in most areas of government and even in the private sector [12], yielding it a DYNAMIC grade in this assessment.

2) Established military Cyber Command and Doctrine

Brazil: Armed Forces Cyber Command (ComDCiber) was established in 2014 under the Ministry of Defence, incorporating the joint forces Centre for Cyber Defence previously created in 2012. Cyber Defence Military doctrine [13] has been established also in 2014 in very clear and objective language, including precise definitions of roles and responsibilities and rules of engagement. This status yields a STRATEGIC grade for this assessment criterion.

Spain's Joint Cyberspace Command (MCCE - Mando Conjunto de Ciberespacio) was created in 2013, originally under the name Mando Conjunto de Ciberdefensa - MCCD [14]. Its doctrine appears to be still under development [15] and suggests it will be largely informed by NATO's [16]. The doctrine gaps signal this item is in an ESTABLISHED capacity rather than STRATEGIC.

3) Legal mandate for Cybersecurity

Since cyberspace pervades now practically all aspects of society, its security also becomes of universal interest. To organize efforts in such a wide scope, it is important to have them coordinated under a legal mandate negotiated with society's interested parties [17].

Brazil: in Brazil, responsibility over cyber security is dispersed among many actors with insufficient statutory power. The Institutional Security Cabinet (GSI) harbours a Department of Information Security with normative mandate over government institutions but no instruments to enforce or audit them, much less over private sector entities. It also runs a cyber incident response center for government institutions which is severely constrained in manpower. ABIN, Federal and State Police forces and ComDCiber also share the task of protecting Brazilian cyberspace under different aspects and conditions, but with no inter-agency coordination yet established. This scenario places Brazil in an INITIAL stage in this item, with basic discussion and consensus among stakeholders still to be reached.

Spain: Cybersecurity responsibility in Spain is legally mandated and shared among three main entities: the Centro Criptologico Nacional (CCN) for government and public enterprises; the Joint Cyber Command for the defence forces; and the Instituto Nacional de Ciberseguridad (INCIBE) for the private sector, citizenry and all remaining entities [18]. Spain gets a DYNAMIC level in this item, because it has demonstrably adapted and evolved its legal cybersecurity mandate over the years.

4) Well-defined roles and responsibilities for all government institutions with cyber mandates

Well-defined and inter-coordinated roles and responsibilities are important for effective and efficient government action.

Brazil' cyber military doctrine is well defined, but public security and state intelligence still lack defining their rules of engagement and cooperation in more concrete terms. Such condition means Brazil is still in a FORMATIVE stage here.

Spain's National Cybersecurity Council - Consejo Nacional de Ciberseguridad [19] - is the forum where roles and responsibilities regarding cyber are discussed and decided. It was created by and responds to the National Security Council, assembling at least once every two months.

The Council is presided by the Director of CNI - Spain's intelligence agency - and counts with representatives from several Ministries. Its goal is to promote coordination, cooperation and collaboration among all public entities with cyber competencies; it is also responsible for issuing and updating the Cybersecurity Strategy, as well as overseeing its implementation. The demonstrated evolution of the Spanish institutional arrangements regarding cyber (e.g., INCIBE's creation), yields this item a DYNAMIC assessment.

B. Cyber Intelligence Capabilities

Cyber Intelligence capabilities reflects the core competences necessary to produce intelligence on cyberspace.

1) Autochthonous cryptography and cryptanalysis

Cryptography is omnipresent in securing data and authenticating its access. From accessing a web page to opening a nuclear plant floodgate, almost any human-computer transaction involves cryptography, and it must not be taken for granted that policymakers know this. Additionally, to operate cyber intelligence on the strategic level, there is no "trusting" crypto implementations other than the ones you know and continually tests.

Brazil, in this aspect, once had a strategic stance, but as technological means progressed and national capacity stagnated, it got back to ESTABLISHED capability.

Spain has kept its STRATEGIC stance on this matter, given its ability of evaluating and certifying a broad range of commercial communications and cryptographic solutions, plus guides for safe use of said solutions in government [20].

2) *Large scale collection capacity*

To build situational awareness on national cyberspace and produce intelligence on the major risks and threats therein, one needs to be able to access, collect, and aggregate large volumes of data from smartly deployed sensors in that national cyberspace.

Brazil has no capacity established yet (thus ABSENT) for large-scale collection, according to the authors' knowledge.

Spain clearly has it, as demonstrated by CNI/CCN's sensor systems in full production in around 200 institutions in 2018 [21]. This places this criterion at a STRATEGIC level since it attends the country's planned demand.

3) *International cooperation*

Brazil is open to cooperation, albeit with limited capacity, conditioning this aspect to an ESTABLISHED level. Requests of information from intelligence bodies are processed by ABIN. Letters rogatory from foreign courts regarding judicialized cases are processed by the Ministry of Justice and Public Security. Both institutions are agnostic in relation to which country seeks cooperation, as long as feasible within rule-of-law.

Spain apparently cooperates much with Portugal and other European countries. It also collaborates with iberoamerican countries with its extensive training programmes [22], placing it in a STRATEGIC level in this criterion.

4) *Analytical and attributional capability*

One of the missions of cyber intelligence is to investigate authorship of adversarial cyber operations. This involves both deep forensic analysis of traces left by attackers, as well as correlation of observed tactics, techniques and procedures, against available threat intelligence [23] obtained from large scale collection and international cooperation.

Brazil has effective capacity on forensic analysis to analyse malware on some but not all technologies. For threat intelligence, it is still largely dependent on outsourced solutions and international cooperation. The overall status here is FORMATIVE.

Spain has an ESTABLISHED capacity for attribution analysis [24]. It is not clear how much of this capacity is dependent of international cooperation and we could not ascertain whether the current capacity has yet to grow or already attends Spain's strategic demand.

C. *Cyber Operations Capabilities*

We graded cyber operations in three very distinctive tiers: at the entry-level, short missions - mostly single-targeted and short in duration, to answer very specific demands. At the intermediate level, systematic operations, which span over time in the pursuit of a broader and longer-term objective - assuming, thus, permanency and operational management capacity. Finally, at the advanced level, complex operations involve multilayered penetrations, flexible and secure vulnerability management and stealth exfiltration of large volumes of data sifting.

1) *Short missions*

Brazil has the capacity ESTABLISHED in several institutions, including at state levels. Lack of better coordination among them impedes optimised overall efficiency and timeliness in results.

Spain has had this capacity long enough so that it is credible that is probably DYNAMIC.

2) *Systematic operations*

Brazil: technical ability is present in multiple Brazilian institutions, although we believe none of them have yet implemented it as an established capacity, leaving the item with a FORMATIVE assessment level.

Spain: mirroring from its consolidated experience in large scale cyber intelligence, we infer Spain holds a STRATEGIC grade in systematic operations. The "dynamic" grade in this item would mean that the country could adapt its strategic operations even in face of new technologies.

3) *Complex operations*

Brazil does not have the experience nor capacity for performing complex cyber operations yet, in the way described in this assessment — therefore, ABSENT.

Spain likely has an ESTABLISHED capacity for complex operations, but we do not have enough information to ascertain whether this capacity attends Spain's strategic demands.

D. *Cyber Security Capabilities*

Computers are inherently fallible: Turing's mathematical proof yields that nothing will stop a digital computer from eventually returning unexpected results in face of unexpected inputs [25]. Hackers use this mathematical idiosyncrasy of computers to exploit and clandestinely crash or control them.

On top of that, technologically competitive countries have little incentive to fix vulnerabilities before making good use of them: as Geer puts it [26], the 80 billion dollars of capital invested in the promising cyber security sector have not made its way to profit yet, suggesting investors might have realised this is an artificially capped market, insofar as a portion of known vulnerabilities will never be fixed, being rather covertly kept in reserve for national security purposes.

This exerts yet greater a stress on civil cybersecurity, mobilising governments to coordinate a basic level of incident response and critical infrastructure protection for society.

1) *Cyber Security strategy*

Brazil's cyber security strategy was recently defined [27] at an INITIAL level, but without enough concrete instruments for effective implementation nor compliance assurance. As some put it, the document is "exceptionally vague" [28], and the lack of government leadership in this area is possibly one of the reasons cybercrime thrives in Brazil [29].

Spain's cyber security strategy was first issued in 2013 and is already in its second edition [30], much evolved from the first one, demonstrating Spain managed to plan, execute, evaluate and adapt its strategy, completing a full policy implementation cycle, securing it a DYNAMIC quality.

2) *Incident response capability*

Brazil: traditional multi-stakeholder and governmental incident Response Centres (CERT.br and CTIR.gov, respectively), do extensive work in keeping public record of incidents and disseminating information thereabout. They do not have, though, provisioned capacity (nor mandate, for that matter) to send teams during security incident crises. For this kind of support, ABIN is summoned ad-hoc upon prioritised incidents, yielding this item a FORMATIVE assessment.

ISBN: 978-989-33-3436-2

Spain’s cyber incident capacity looks mature and informative, drawing from long-term experience of its CCN-CERT (Computer Emergency Response Team). Recently, INCIBE joined the scene for the government to better cope with demand from the private sector. For the combined deep expertise from CCN and volume-capacity aggregated by INCIBE, Spain achieves a DYNAMIC status for this item.

3) *Critical infrastructure protection capability*

Brazil’s ComDCiber has successfully initiated dialogue and joint cyber drills (2018) with critical infrastructure sectors, especially energy and financial services, yielding this item a FORMATIVE assessment.

Spain has since 2007 a dedicated center for the protection of critical infrastructure, the Centro Nacional para la Protección de Infraestructuras y Ciberseguridad (CNPIC). The Center is supported by INCIBE for incident response, but we could not find enough material to ascertain whether the protection capability is beyond the FORMATIVE stage.

E. Synergy with society

1) *Partnership with Academia and Research Centres*

Brazil: few initiatives exist, mostly in a localised and sporadic fashion. ABIN sponsors a Programme at UnB, under which this research was conducted; GSI and Defence sponsor scholarship grants, but their impermanent nature mean an INITIAL level for this item.

Spain’s National Network of Excellence in Cybersecurity Research (RENIC) was created in 2016 to support and coordinate research in the field of cybersecurity involving INCIBE and the top academic institutions in the country in a STRATEGIC initiative [31].

2) *Partnership with high-tech entrepreneurship and Venture Capital*

Brazil: Ministry of Science, Technology and Innovation has signaled intent of dedicating resources to technology start-ups [32], but effective efforts directed at making cyber entrepreneurship more viable in the country are still INITIAL.

Spain: one of INCIBE's core missions is to promote innovation in cybersecurity through investments in start-ups; its project looks solid and avails the market with more than 100 million euros per year across different phases of the start-up businesses, with the programmes *#INCIBEinspira*, *Ciberempreende* and *Cybersecurity Ventures*. If the STRATEGIC programmes yield their fruits, Spain is likely to secure a place in the map of global cybersecurity innovation.

3) *Access to local Cybersecurity workforce*

Brazil: the heavily automated financial services sector maintains a sizeable ESTABLISHED local cyber security labour market. However, technical talent often expatriates due to better salaries and/or life standards abroad [33].

Spain: the country had historically suffered from the same "brain drain" malaise as Brazil [34] but plans to turn the tables with a STRATEGIC all-out effort from the now called Ministry of Economic Affairs and Digital Transformation, where INCIBE was placed.

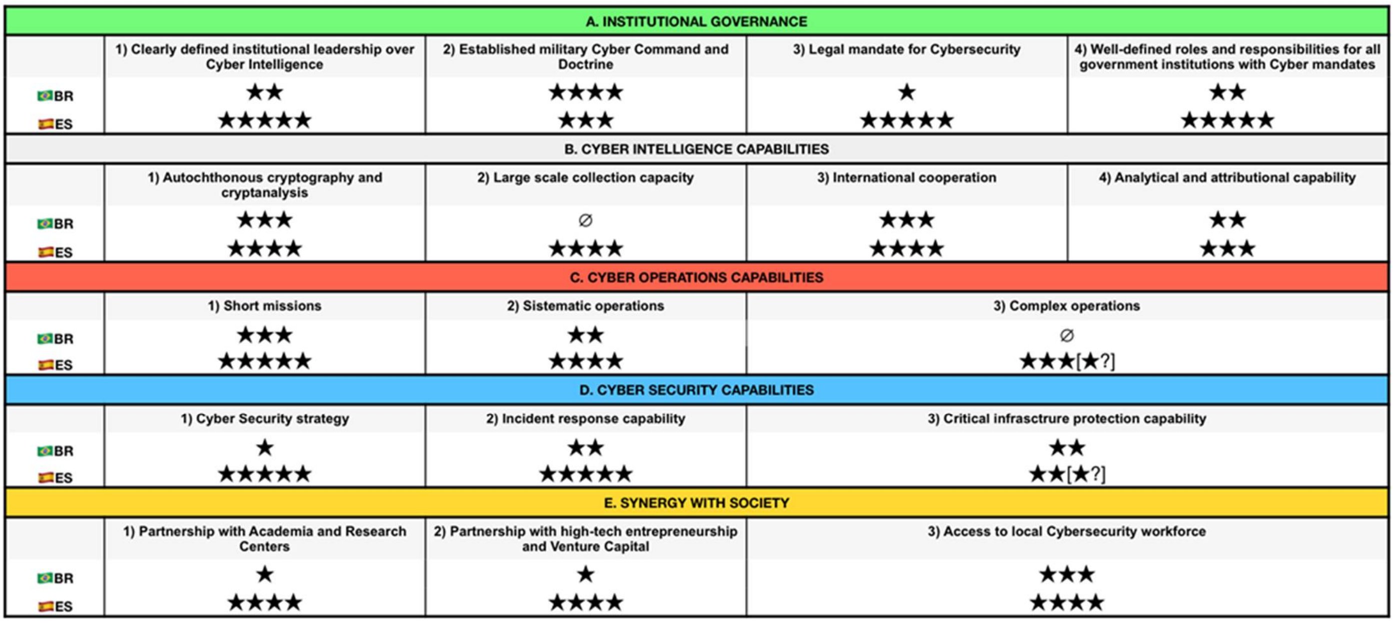
Synthesis of the Results

The overall result is shown in Fig. 2, where it is arranged in an approximate order of institutional evolution and complexity of implementation, from left to right and top to bottom.

Colours were used with mnemonic purpose: green alluding to the organic growth unlocked by institutional governance; white, red and blue to the usual colour code in cyber exercise drills for, respectively, monitor, offensive and defensive teams; and golden for the synergy with society that opens the gateway to advanced cyber capacity.

V. Conclusions

Overall results show superior cyber capability in Spain, likely due to earlier, steadier and more coordinated efforts from governmental structures.



A. INSTITUTIONAL GOVERNANCE

	1) Clearly defined institutional leadership over Cyber Intelligence	2) Established military Cyber Command and Doctrine	3) Legal mandate for Cybersecurity	4) Well-defined roles and responsibilities for all government institutions with Cyber mandates
BR	★★	★★★★	★	★★
ES	★★★★★	★★★	★★★★★	★★★★★

B. CYBER INTELLIGENCE CAPABILITIES

	1) Autochthonous cryptography and cryptanalysis	2) Large scale collection capacity	3) International cooperation	4) Analytical and attributional capability
BR	★★★	∅	★★★	★★
ES	★★★★	★★★★	★★★★	★★★

C. CYBER OPERATIONS CAPABILITIES

	1) Short missions	2) Sistematic operations	3) Complex operations
BR	★★★	★★	∅
ES	★★★★★	★★★★	★★★[★?]

D. CYBER SECURITY CAPABILITIES

	1) Cyber Security strategy	2) Incident response capability	3) Critical infrasctrure protection capability
BR	★	★★	★★
ES	★★★★★	★★★★★	★★[★?]

E. SYNERGY WITH SOCIETY

	1) Partnership with Academia and Research Centers	2) Partnership with high-tech entrepreneurship and Venture Capital	3) Access to local Cybersecurity workforce
BR	★	★	★★★
ES	★★★★	★★★★	★★★★

Figure 2. Comparison between Brazil and Spain’s cyber capabilities.

Three main aspects seem to have strongly favoured success in Spain's cyber policymaking: being well-informed by cyber intelligence from early stages; establishing a multi-institutional forum to deliberate on cybersecurity policy, roles and responsibilities; and resolutely promoting private sector capacity development through academia and entrepreneurship.

Future work will include other iberoamerican countries, eventually extend and detail the criteria used in the assessment and include a summarized quantitative index.

Acknowledgments

The authors thankfully acknowledge the support of Brazilian Intelligence Agency - ABIN grant 08/2019. R.d.O.A. gratefully acknowledges the Attorney General of the Union- AGU grant 697.935/2019; the Att. Gen. of the Office of National Treasury - PGFN grant 23106.148934/2019-67 and the support from EC Horizon 2020 HEROES project grant 101021801.

References

[1] D. Bogdan-Martin, “Global Cybersecurity Index 2020”, January 2021, International Telecommunication Union (ITU) Publications.

[2] Europol, November 2020, https://www.europol.europa.eu/media-press/newsroom/news/over-40-arrested-in-biggest-ever-crackdown-against-drug-ring-smuggling-cocaine-brazil-europe.

[3] ENISA, “National Capabilities Assessment Framework”, December 2020, https://www.enisa.europa.eu/publications/national-capabilities-assessment-framework

[4] M. Hathaway, C. Demchak, J. Kerben, J. McArdle, F. Spidalieri, “Cyber Readiness Index 2.0”, November 2015, Potomac Institute.

[5] M. Baezner, S. Cordey, “National Cybersecurity Strategies in Comparison – Challenges for Switzerland”, March 2019, Center for Security Studies (CSS), ETH Zürich.

[6] J. Voo, I. Hemani, S. Jones, W. DeSombre, D. Cassidy, A. Schwarzenbach, “National Cyber Power Index 2020”, Sep. 2020, Harvard, Belfer Center for Science and International Affairs

[7] OAS, “Cybersecurity risks, progress, and the way forward in Latin America and the Caribbean – 2020 Cibersecurity Report”, July 2020, OAS Cybersecurity Observatory, http://dx.doi.org/10.18235/0002513.

[8] IISS, “Cyber Capabilities and National Power: A Net Assessment”, 2021,https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power

[9] Global Cyber Security Capacity Centre, “Cybersecurity Capacity Maturity Model for Nations (CMM)”, March 2021, University of Oxford, https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

[10] Ibidem, D1.4, p. 17; and D4.3, p. 45.

[11] Gartner Group, ”Gartner Magic Quadrant - Positioning technology players within a specific market", https://www.gartner.com/en/research/methodologies/magic-quadrants-research

[12] CCN-CERT, "Contención frente a los ciberataques”, https://www.ccn-cert.cni.es/documentos-publicos/3480-Catalogo-Servicios-Empresas/file.html

[13] Brasil, "Doutrina Militar de Defesa Cibernética", 2014, Min. Def., Portaria No 3.010/MD, DOU n. 224 de 19 de novembro de 2014.

[14] España, "Real Decreto 521/2020", May 2020, Min. Def., BOE n. 143, https://www.boe.es/eli/es/rd/2020/05/19/521/con

[15] Centre for Advanced National Defence Studies, "Doctrine Development Campaign Plan 2020-2025", 2019, https://emad.defensa.gob.es/Galerias/CCDC/files/Doctrine_Development_Campaign_Plan_2020-2025__Engl-version_updt_JANUARY_22.pdf

[16] NATO, "Allied Joint Doctrine for Cyberspace Operations", Jan. 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf

[17] P. Nicholas, K. Ciglic, “Building an effective national security agency”, 2018, Microsoft Corporation, https://www.microsoft.com/en-us/cybersecurity/content-hub/cybersecurity-agency-whitepaper

[18] España, "Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información", Ministerio de la Presidencia.

[19] España, "Orden PRA/33/2018", 2018, Min. Presid. BOE n. 20, https://www.boe.es/boe/dias/2018/01/23/pdfs/BOE-A-2018-799.pdf

[20] España, Bol. Inform., Dec. 2021, CCN-PyTEC, https://www.ccn.cni.es/index.php/es/menu-pytec-es/boletines-informativos-pytec.

[21] Revista Española de Control Externo, "La ciberseguridad y su relevancia en el Sector Público", January 2020, Vol. XXII, p. 83.

[22] Centro Criptologico Nacional, "Oferta Formativa 2022", https://angeles.ccn-cert.cni.es/index.php/es/docman/documentos-publicos/38-plan-de-formacion-ccn/file

[23] A. de Melo e Silva, J.J. Costa Gondim, R. de Oliveira Albuquerque, L.J. García Villalba, 2020, "A Methodology to Evaluate Standards and Platforms within Cyber Threat Intelligence". Future Internet 12, no. 6: 108. https://doi.org/10.3390/fi12060108

[24] CCN, "Cyber threats and Trends 2019", https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4041-ccn-cert-ia-13-19-threats-and-trends-report-executive-summary/file.html

[25] A.M. Turing, "On Computable Numbers, with an Application to the Entscheidungsproblem", 1937, Proceedings of the London Mathematical Society, 2, vol. 42, no. 1, pp. 230–65, doi:10.1112/plms/s2-42.1.230

[26] D. Geer, P. Kuper, "When $80 billion is not enough", September 2011, IEEE Security and Privacy, Vol. 9, Issue 5, pp 86–87, https://doi.org/10.1109/MSP.2011.146

[27] Brasil, Estratégia Nacional de Segurança Cibernética, Decreto nº 10.222, Feb. 2020, http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm

[28] A. Stronnel, “Brazil’s cyber security strategy leaves much to be desired”, IISS, Sep. 2020, https://www.iiss.org/blogs/analysis/2020/09/csfc-brazils-cyber-security-strategy

[29] Ponemom Institute, "The cost of cybercrime", 2019, Accenture Security, https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf

[30] España, Dept. de Seguridad Nacional, "National Cyber Security Strategy", 2019. https://www.ccn-cert.cni.es/en/pdf/documentos-publicos/3812-national-cybersecurity-strategy-2019/file.html

[31] Incibe, "Key findings from the Catalog and knowledge map of R&D+i in cybersecurity", 2017, https://www.incibe.es/sites/default/files/paginas/red-excelencia/estudios-caracterizacion/catalog_infographic.jpg

[32] Brasil, “Estratégia Nacional de Ciência, Tecnologia e Inovação 2016|2022”, 2018, p. 105. MCTIC, http://www.finep.gov.br/images/a-finep/Politica/16_03_2018_Estrategia_Nacional_de_Ciencia_Tecnologia_e_Inovacao_2016_2022.pdf

[33] A.M. Carneiro, A.M.N. Gimenez, C.D. Granja; E. Balbachevsky; F. Consoni; V. F. Andretta, "Diáspora brasileira de ciência, tecnologia e inovação: panorama, iniciativas auto-organizadas e políticas de engajamento", 2020, Ideias, v. 11, p. e020010, DOI: 10.20396/ideias.v11i0.8658500

[34] O. Nelson, “The Social Effects of the Spanish Brain Drain”, 2015, Social Impact Research Experience (SIRE). 35, https://repository.upenn.edu/cgi/viewcontent.cgi?article=1041