International Journal of Scientific Research and Management (IJSRM)
||Volume||14||Issue||07||Pages||206-216||2026||
Website: https://ijsrm.net ISSN (e): 2321-3418
DOI: 10.18535/ijsrm/v14i07.ps02

The Evolution of State Power: Strategic Potential in the Cybernetic Age

Wanderlino Moreno Junior[1]

Brazilian Army, Doctoral Student

Abstract: This study addresses the growing need to conceptualize and measure power relations in cyberspace, a domain that is increasingly central to contemporary international dynamics. Despite the proliferation of models aimed at assessing cyber power, a significant gap persists in the development of methodologies capable of capturing the long-term strategic potential of states in this environment. To fill this gap, the article proposes a new analytical framework for assessing Perceived Cyber Strategic Potential (PCSP), based on a multidimensional approach that integrates structural and functional components of cyberspace. The results demonstrate that the model constitutes a systematic and scalable tool for identifying patterns of cyber strategic positioning among states, contributing to long-term planning and high-level decision-making. By shifting the analytical focus from immediate cyber power to perceived strategic potential, the study contributes to the advancement of cyber geopolitics and offers a new perspective for understanding state behavior in the Information Age.

Keywords: Cyberspace, Potential, Power, Geopolitics, Mathematical Model.

Introduction

Cyberspace has become one of the main strategic domains of contemporary international relations. The growing dependence on digital infrastructures, global communication systems, artificial intelligence, cloud computing, and emerging technologies has transformed the cyber environment into a space of economic, technological, military, and political competition among states.

In this context, the assessment of national cyber capabilities has become an object of growing interest in both academia and government sectors. Several models have been developed to measure the cyber power of states, highlighting approaches based on offensive capabilities, cyber defense mechanisms, institutional maturity, and control of digital infrastructures.

However, most existing models focus on measuring currently available capabilities, offering limited ability to anticipate the future evolution of states' strategic positioning in cyberspace. This limitation is particularly relevant in an environment characterized by rapid technological transformation and the growing interdependence between economic, energy, industrial, social, and geopolitical factors.

Authors such as Joseph Nye, Richard Clarke, Robert Knake, and the researchers of the National Cyber Power Index recognize that cyber power does not result exclusively from technical capabilities, but also from structural factors capable of sustaining long-term technological development. However, a methodological gap remains related to the construction of instruments aimed at assessing the future strategic potential of States in the cyber environment.

Starting from this problem, this article proposes the Perceived Cyber Strategic Potential (PCSP), a multidimensional analytical framework designed to assess the potential capacity of States to project power and influence in cyberspace over time. Unlike traditional cyber power indices, the PCSP seeks to integrate structural factors related to technological resources, energy, innovation, governance, digital infrastructure, military capacity, satellite development, and population insertion in the digital environment.

The main contribution of this study is the proposition of a methodology capable of supporting prospective analyses and decision-making processes at the political-strategic level. Furthermore, the model offers a quantitative framework that can be continuously updated and comparatively applied among States, contributing to the advancement of studies in cyber geopolitics and national strategic planning.

Based on the gap identified in the literature, this study was developed from the following research hypotheses:

H1: The cyber strategic potential of States is positively associated with their capacity for technological innovation.

H2: States that exhibit high levels of integration between energy resources, digital infrastructure, and technological capacity tend to achieve higher levels of cyber strategic potential.

H3: Multidimensional models based on structural factors produce more consistent assessments of cyber strategic potential than approaches based exclusively on current cyber capabilities.

The verification of these hypotheses underpins the construction of the Perceived Cyber Strategic Potential (PCSP), contributing to the expansion of prospective approaches applied to cyber geopolitics and national strategic planning.

In addition to its contribution to the study of cyber geopolitics, PCSP can be understood as a data-driven decision support framework for the strategic analysis of national innovation systems, digital infrastructures, and technological capabilities. From this perspective, the model approaches the areas of Information Systems and Analytical Intelligence by transforming large volumes of heterogeneous indicators into structured knowledge to support decision-making processes at the political-strategic level.

From an Information Systems perspective, PCSP can be understood as a decision support model based on the integration of data from multiple heterogeneous sources. By employing normalization techniques, multi-criteria analysis, and statistical clustering, the framework transforms large volumes of dispersed information into structured knowledge, contributing to analytical intelligence processes, strategic monitoring, and the formulation of evidence-based public policies.

The article is structured in four parts. Initially, the theoretical foundation related to cyber power and the conditioning factors of cyberspace is presented. Next, the methodology used in the construction of PCSP is described. Subsequently, the results obtained and the strategic groupings identified are discussed. Finally, the conclusions, limitations, and future research perspectives are presented.

1. Theoretical Framework

The assessment of cyber power has been the subject of increasing academic interest, especially about competition between great powers. Existing models, such as composite cyber indices and capability-based frameworks, generally focus on three aspects: offensive capability, defensive resilience, and dependence on digital infrastructure.

Despite their contributions, there are three main limitations to these models:

a. Presentism: emphasis on present capabilities to the detriment of a promising future;

b. Reductionism: excessive focus on technical aspects; and

c. Insufficient integration: limited inclusion of socioeconomic and geopolitical factors.

Simultaneously, other branches of geopolitical theory--especially those based on classical authors--also emphasize the relevance of structural factors such as resources, population, and strategic alliances. However, these frameworks have not been fully adapted to the cyber context.

This work develops a unified analytical model that integrates concepts from geopolitics, innovation studies, and cyber strategy, drawing on these traditions.

1.1State Of The ArtOnCyber Power

The growing strategic relevance of cyberspace has driven the development of different models aimed at measuring the cyber capabilities of states. In the last two decades, governments, research centers, and international organizations have sought mechanisms capable of assessing the relative position of countries in an environment characterized by high technological dependence, rapid digital transformation, and increasing geopolitical competition.

Among the most relevant initiatives is the National Cyber Power Index (NCPI), developed by the Belfer Center at Harvard Kennedy School, which assesses the ability of states to achieve national objectives using cyber instruments. The model considers multiple dimensions related to offensive, defensive, and influence capabilities, representing one of the most comprehensive methodologies currently available.

Another widely used reference is the Global Cybersecurity Index (GCI), developed by the International Telecommunication Union (ITU), which focuses on assessing the maturity of national cybersecurity ecosystems. The index analyzes legal, organizational, technical, capacity-building, and international cooperation aspects.

In the strategic field, Clarke and Knake proposed a methodology based on three central pillars: offensive capability, defensive capability, and cyber dependency. In parallel, authors such as Joseph Nye introduced the concept of Cyber Power, arguing that the ability to influence behaviors through informational and technological resources has become a fundamental component of contemporary national power.

Despite the observed advances, the literature still presents important limitations. The first refers to the predominance of approaches focused on measuring the current capabilities of States, to the detriment of prospective assessments. The second is related to the predominance of strictly technological indicators, often dissociated from structural factors such as energy, strategic resources, governance, and international insertion. Finally, there is reduced integration between studies of cyber power and classical approaches to geopolitics.

Given these limitations, this work proposes the Perceived Cyber Strategic Potential (PCSP), an analytical framework designed to assess not only existing capabilities, but primarily the structural factors capable of sustaining the strategic positioning of States in cyberspace over time.

1.2Factors Conditioning Cyberspace

Returning to the direction outlined for the development of the content of this article, a model aimed at quantifying state relations in Cyberspace, whether immediate or prospective, should consider the state's capacity to control and/or develop the following factors:

a. Technological inputs: the basic elements for the existence of interactions that justify the current importance of cyberspace are those linked to enabling communications and processes carried out on the Internet.

b. Energy sources: digital technologies form a global system integrated by terminals that are connected to each other through network infrastructures (terrestrial and submarine cables, mobile network antennas, fiber optics, etc.) that allow the exchange of information stored and processed in the Data Centers that represent the heart of this system.

c. Innovation: thinking about cyberspace inevitably means imagining disruptive technologies capable of optimizing the flow of information. In most forward-looking books, the future is characterized using technological means to optimize human relations, enhance data storage and processing capacity, and produce automation.

d. The promotion of public-private relations: the public-private relationship can be analyzed in three major trends:

1) those focused on Cybersecurity: most critical infrastructures within Cyberspace are controlled by the private sector. This relationship is based on defining the boundary between responsibility for providing Security and Defense in this environment.

2) those directed towards research and development: the promotion of dual research is a strong link between the public and private sectors, usually enabled by the triple helix.

3) regulatory mechanisms: the development of rules and laws that regulate the public-private relationship is essential for directing the efforts that flow between the integral parts of Cyberspace.

e. The development of emerging disruptive technologies: the ability to monitor or generate these technologies is a key factor in the power game unfolding in cyberspace.

In this context, the following are identified as drivers of this scenario: autonomous vehicles, 3D printers, advanced robotics, new materials, the Internet of Things (IoT), Artificial Intelligence (AI), Quantum Computing (QC), Big Data, Synthetic Biology, etc.

f. The establishment of strategic partnerships: in cyberspace marked by volatility, ambiguity, and uncertainty, the construction of strategic partnerships increases the capacity for action of States and the promotion of freedom of action.

g. Satellite development: this capacity is a reality for few nations globally. This situation generates a concentration of power, insofar as communications satellites focused on the Internet allow for increased global coverage, greater data transmission capacity at higher speeds, simplicity, and high availability.

h. Control of structural convergence points: the physical infrastructure of cyberspace converges at points called nodes or hot points.

These points are strategic in the power game in Cyberspace because they concentrate a high number of infrastructures necessary for the flow of information, representing vulnerability in the distribution architecture of data that navigate the cyber ecosystem.

The entry and exit points of submarine cables are considered hot points due to the volume of data that navigates these structures interconnecting the entire planet; and

The degree of insertion of the population in Cyberspace: Cyberspace is a creation of Man, having a layer constituted by users or individuals and their identifications in the virtual layer.

In the context of studies focused on models directed to cyberspace, a significant volume of methodologies has been developed that quantify and classify actors, particularly state actors, regarding their degree of Cyber Power. Examples of methodologies focused on the topic include the one developed by the Belfer Center, which formulates a ranking of Cyber Power.

1.3Strategic Attributes

Based on this reality, the aim was to aggregate knowledge focused on a long-term vision, through a line of thinking that promoted the calculation of the Perceived Cybernetic Strategic Potential (PCSP), based on the conditioning factors of cyberspace that were addressed earlier in this article.

The studies developed to establish the Perceived Cybernetic Strategic Potential (PCSP) model required the multidisciplinary integration of knowledge to foster a global perspective on the proposed theme. Thus, it drew from various disciplines such as Political Science, History, Sociology, Anthropology, Geography, etc.

In this context, bibliographic research allowed for the evaluation and exploration of existing content focused on the integral aspects of power and strategic potential, to contribute to a better understanding of the object of study.

The model employs the following attributes, which were extracted from the conditioning factors of Cyberspace and reinforce the thesis that cyberspace is integrated by a relevant portion of elements existing in its physical layer, namely: Technological Inputs (TI); Energy Sources (ES); Innovation (I); Public-Private Partnerships (PPP); Emerging Disruptive Technologies (EDT); Strategic Partnerships (SP); Structural Convergence Points (SCP); Satellite Capacity (SC); Population Insertion Degree (PID); and Military Capacity (MC).

Thus, the main attributes that integrate the composition of power present in the theories developed by renowned scholars were analyzed. The result of this action was added to the perception defended in relation to the conditioning factors of Cyberspace, promoting the construction of a weighted equation.

In the development of the PCSP, each attribute was broken down into dimensions that were integrated by indicators which, when processed, quantified the strategic cyber potential of the States.

The methodology was based on the understanding that quantifying the conditioning factors of Cyberspace allows for a long-term strategic vision, producing useful knowledge aimed at assisting the high-level decision-making process in the context of existing state relations in Cyberspace.

It should be noted that the conditioning factors were called attributes, which were broken down into specific dimensions, and these were refined into strategic indicators.

The Technological Input attribute was constructed based on two dimensions:

a. Strategic Mineral Reserves (SMR), which refer to mineral deposits considered vital for the security and economic development of a country; and

b. Exploration Capacity (EC), built upon exploration technology, technical expertise, regulation and licensing, access to markets, and logistical infrastructure. Energy Sources were analyzed in four dimensions, namely:

1) The Degree of Energy Consumption (DEC), referring to the total amount of energy used within state borders during a given period. This consumption encompasses various activities, such as industrial production, transportation, residences, and services;

2) The Degree of Renewable Energy Use (DRE), which is crucial for diversifying the energy matrix, reducing dependence on fossil fuels and environmental impacts;

3) The Degree of External Dependence (DED), influenced by the availability of local energy resources and adopted energy policies; and

4) The Degree of Maturity of Climate-related Policies (DMCP), reflecting the level of development, implementation, and effectiveness of strategies to address climate change;

Innovation was integrated by two dimensions. The first [dimension] focuses on continuous investments in research and development that drive cyber technologies, and the second relates to the pool of technology and cybersecurity specialists, including researchers, software engineers, cybersecurity analysts, and other qualified professionals, resulting from educational programs and training available to develop cyber skills in the population. Thus, innovation was decomposed into the dimensions of Innovation Capacity (IC) and Human Resource Qualification Capacity (HRQC);

The Public-Private Relationship was quantified in two dimensions: the Degree of Political Stability (DPS), directed at analyzing the existence of solid institutions, robust democratic systems, and respect for human rights, and the Degree of Governance (GG), referring to the effectiveness and quality of the institutions that govern the country, measured based on criteria such as transparency, accountability, citizen participation, political stability, and control of corruption;

Emerging Disruptive Technologies were explored in a single dimension focused on Research and Development Capacity (RDC), involving Investing in talent, infrastructure, and strategic partnerships to remain at the forefront of technological progress;

Strategic Partnerships are being developed through the dimension constituted by Global Competitiveness Capacity (GCC), measuring the potential for state insertion in the International Community to enable the development of competitiveness;

The Structural Convergence Point was decomposed into three dimensions, namely:

Technological Infrastructure Capacity (TIC), materialized by the infrastructures available to enable digital activities and connected consumers;

Information Flow Control Capacity (IFCC), understood as the effective use of tools, policies, and technologies to manage the movement of information; and

The Degree of Internal Integration (DII), directed at the extent to which different technological components and systems can work in a coordinated and efficient manner.

Satellite Capacity, directed at the dimension focused on Satellite Development, Launch, and Control Capacity (SLCC);

The Degree of Population Insertion in Cyberspace was analyzed in two dimensions, the first referring to the National Population Size (NPS) and the second focused on the Degree of Population Insertion (DPI) in said space; and

Military Capacity analyzed by the Degree of Military Capacity (DMC) directed at evaluating the country's military capacity, considering its technological infrastructure, security policies, investments in research and development, specialist training, and its capacity to respond to cyber threats.

The results of the attributes were formulated by the weighted average of the strategic indicators that make up the dimensions, being normalized and inserted into a model based on a mathematical equation aimed at estimating the potential of the established attributes.

The data produced were inserted into a clustering algorithm, to group the States into similar sets, defining patterns that will serve to assist in the various decision-making processes.

1.4Theoretical Justification ofTheAttributes

The selection of attributes that comprise the Perceived Cyber Strategic Potential (PCSP) was based on the convergence between the classic literature on national power, geopolitics, and contemporary studies on cyber power. The attributes Technological Inputs, Energy Sources, and Innovation reflect the structural capacity of States to sustain continuous processes of technological development. The attributes Public-Private Relations and Strategic Partnerships represent institutional mechanisms capable of accelerating the diffusion of innovation and expanding the international insertion of countries.

In turn, the attributes Emerging Disruptive Technologies, Structural Convergence Points, and Satellite Capacity reflect elements directly associated with the functioning of the physical infrastructure of cyberspace. Finally, the Degree of Population Insertion and Military Capacity represent factors related to the scale of use of the digital environment and the state's capacity for protection and power projection.

The integration of these attributes allows us to represent the multidimensional nature of contemporary cyber development, overcoming approaches restricted to observable technical capabilities in the present.

2. Methodology

The construction of the Perceived Cyber Strategic Potential (PCSP) was carried out through a multi-criteria quantitative approach based on the integration of structural indicators related to the development of cyberspace.

2.1Data Sources

The construction of the PCSP required the integration of data from multiple international sources recognized by the scientific community and widely used in comparative studies on technological development, governance, defense, and innovation.

The empirical basis was structured from information provided by the World Bank, International Telecommunication Union (ITU), World Intellectual Property Organization (WIPO), International Energy Agency (IEA), Stockholm International Peace Research Institute (SIPRI), World Governance Indicators (WGI), Global Innovation Index (GII), National Cyber Power Index (NCPI), United Nations Development Programme (UNDP), and United States Geological Survey (USGS).

The data were collected from open databases referring to the most recent period available, seeking to ensure international comparability between the States analyzed. Indicators widely used in the specialized literature and that presented consistent global coverage were prioritized.

The selection of indicators observed three fundamental criteria: strategic relevance for the development of cyberspace; availability of comparable data at the international level; and the ability to represent structural attributes associated with the strategic potential of States.

The use of consolidated international sources contributed to reducing methodological biases and increasing the robustness of the model, allowing its replication and periodic updating by other researchers interested in the subject.

2.1.1Indicator Selection Criteria

The construction of the Perceived Cyber Strategic Potential (PCSP) required the selection of indicators capable of representing, in an objective and comparable way, the structural factors that condition the development of state capabilities in the cyber environment. Considering the multidimensional nature of the model, the choice of indicators was guided by the need to integrate technological, energy, economic, institutional, military, and social variables into a coherent analytical framework.

The selection process was developed in three complementary stages. In the first stage, a literature review was conducted on the specialized literature in geopolitics, national power, technological innovation, cybersecurity, and strategic development, allowing the identification of the factors most frequently associated with the formation of state power in the Information Age. This stage enabled the definition of the ten structuring attributes of the model: Technological Inputs (TI), Energy Sources (ES), Innovation (I), Public-Private Partnerships (PPP), Emerging Disruptive Technologies (EDT), Strategic Partnerships (SP), Structural Convergence Points (SCP), Satellite Capacity (SC), Degree of Population Insertion (DPI), and Military Capacity (MC).

In the second stage, each attribute was decomposed into specific analytical dimensions, designed to represent different aspects of the conditioning factors of cyberspace. The dimensions were structured in a way that preserves the conceptual coherence between the theoretical elements identified in the literature and the empirical data available for measurement. Finally, in the third stage, quantitative indicators obtained from international databases recognized by the scientific community were selected. The choice observed three fundamental criteria: strategic relevance for the development of national cyber potential; availability of comparable data on an international scale; and methodological reliability of the institutions responsible for collecting and disseminating the information.

Seeking to ensure the analytical robustness of the model, indicators widely used in international studies on innovation, governance, technological development, digital infrastructure, energy, and defense were prioritized. This strategy allowed for the reduction of biases arising from the use of isolated sources and broadened the possibility of replicating the research by other researchers.

Table 1 presents the consolidated structure of the attributes, dimensions, strategic indicators, and respective data sources used in the construction of the PCSP. The adoption of this methodological architecture allowed for the transformation of heterogeneous variables into a comparable and integrated base, enabling the estimation of the strategic cyber potential of States through standardized quantitative procedures.

Therefore, the selected indicators should not be understood as isolated measures of national performance, but as interdependent components of a complex system aimed at evaluating the structural conditions that underpin the projection of power in cyberspace over future horizons long term.

Table 1 Structure of the P CSP Indicators

Attribute	Dimension	Indicator	Source
IT	RME	Strategic Mineral Reserves	USGS
IT	CE	Critical Mineral Production	World Bank
FE	GCE	Per Capita Energy Consumption	IEA
FE	GEER	Renewable Energy Share	IEA
FE	GDE	External Energy Dependence	IEA
I	CI	Expenditure (% PIB)	UNESCO/ World Bank
I	CQRH	per million inhabitants	UNESCO
RPP	GEP	Political Stability	WGI
RPP	GG	Government Governance	WGI
TDE	CPD	Investment in Emerging Technologies	GII
PE	CCG	Government Governance	WEF
PCE	CIT	Digital Infrastructure	ITU
PCE	CCFI	Information Flow Capacity	ITU
PCE	GII	Internal Digital Integration	World Bank
CS	CDLCS	Space and Satellite Capacity	UNOOSA
GIP	TPN	Total Population	World Bank
GIP	GIP	Internet Users (%)	ITU
CM	GCM	Aggregate Military Capacity	SIPRI

2.2Model Structure

The model was composed of ten strategic attributes: Technological Inputs (TI), Energy Sources (ES), Innovation (I), Public-Private Partnerships (PPP), Emerging Disruptive Technologies (EDT), Strategic Partnerships (SP), Structural Convergence Points (SCP), Satellite Capacity (SC), Degree of Population Insertion (DPI), and Military Capacity (MC).

The indicators were subjected to the Min-Max standardization process:

$X'=(X-X_{min})/(X_{max}-X_{min})$

allowing comparability between variables originally expressed on different scales.

The determination of weights was carried out through a combination of the Analytic Hierarchy Process (AHP) and Principal Component Analysis (PCA). The AHP allowed the incorporation of expert judgments about the relative relevance of the attributes, while the PCA made it possible to identify the statistical contribution of each variable to the total variance observed.

The PCSP index was calculated using the following expression:

$PCSP_i = \Sigma\ (w_k \times A_{ik})$

where $PCSP_i$ represents the perceived cyber strategic potential of country i; A_{ik} represents the normalized value of attribute k for country i; and w_k represents the weight assigned to the corresponding attribute.

After calculating the index, cluster analysis was applied using the K-Means algorithm. The optimal number of clusters was defined using the Elbow Method and validated by the Silhouette Score.

The resulting clusters allowed the identification of similar strategic positioning patterns among the analyzed states, providing an analytical basis for the development of public policies and national strategies related to the cyber environment.

2.3DeterminationOfAttribute Weights

The assignment of weights to the attributes of the Perceived Cyber Strategic Potential (PCSP) was carried out through a combination of qualitative and quantitative techniques, seeking to reduce subjective biases and increase the statistical robustness of the model.

Initially, the Analytic Hierarchy Process (AHP), developed by Saaty, was used to establish the relative importance of strategic attributes. The method allowed for pairwise comparison of attributes, considering their relevance to the formation of national cyber strategic potential.

To assess the consistency of the judgments, the Consistency Ratio (CR) was calculated, according to the methodology proposed by Saaty. The result obtained was CR = 0.08, a value lower than the limit of 0.10 recommended by the literature, indicating adequate coherence between the judgments used in the paired comparison matrix.

The application of the AHP was conducted based on specialized literature in geopolitics, national power, technological innovation, and cybersecurity. The comparative judgments were organized into decision matrices and subjected to the calculation of the Consistency Ratio (CR), ensuring coherence between the evaluations performed.

Additionally, Principal Component Analysis (PCA) was applied to identify the statistical contribution of each variable to the total variability of the dataset. The use of PCA allowed us to verify the explanatory power of the attributes and reduce possible redundancies between correlated indicators.

The application of Principal Component Analysis resulted in the retention of four components with eigenvalues greater than 1, responsible for explaining approximately 82.4% of the accumulated variance of the dataset. This result demonstrates the high explanatory power of the multidimensional structure adopted by the model.

The combination of AHP and PCA provided a balance between the strategic perception derived from specialized knowledge and the statistical validation of the attributes employed. In this way, the final weights used in the calculation of the PCSP simultaneously reflect theoretical criteria and empirical evidence.

With the aim of ensuring the methodological consistency of the weight assignment, the judgments used in constructing the paired comparison matrix of the Analytic Hierarchy Process (AHP) were subjected to verification of the Consistency Ratio (CR), according to the criteria proposed by Saaty. The results indicated acceptable levels of consistency, allowing the use of the weights obtained in the composition of the model.

Complementarily, a Principal Component Analysis (PCA) was performed to verify the explanatory capacity of the selected attributes and identify possible statistical redundancies. The retained components showed a high capacity to represent the variability observed in the data, reinforcing the adequacy of the multidimensional structure adopted by the PCSP.

The convergence between the results produced by the AHP and the PCA contributed to increasing the analytical robustness of the model, reducing potential distortions arising from exclusively subjective or exclusively statistical evaluations.

Table 2 Strategic Weights of the PCSP Attributes

Attribute	Abbreviation	Weight
Technological Inputs	TI	0,15
Energy Sources	ES	0,10
Innovation	I	0,18
Public-Private Partnerships	PPP	0,08
Emerging Disruptive Technologies	EDT	0,12
Strategic Partnerships	SP	0,07
Structural Convergence Points	SCP	0,10
Satellite Capacity	SC	0,08
Degree of Population Integration	DPI	0,05
Military Capacity	MC	0,07

Σ Weight= 1,00

Table 3 Variance

Component	Variance Explained (%)
PC1	35,2
PC2	21,7
PC3	14,3
PC4	11,2
Total	82,4

The weights presented in Table 2 were initially obtained through the application of the Analytic Hierarchy Process (AHP). The paired comparison matrix showed a Consistency Ratio (CR) of less than 0.10, indicating acceptable consistency of the judgments made.

Complementarily, Principal Component Analysis (PCA) was applied to verify the explanatory power of the attributes. The retained components explained more than 80% of the total variance observed, corroborating the adequacy of the adopted dimensional structure.

The definition of the optimal number of clusters was carried out using the Elbow Method, which indicated six clusters as the most appropriate solution. Complementarily, the Silhouette Score was calculated, whose average value was 0.61, indicating adequate separation and cohesion between the identified groups.

3. Results

3.1AnalysisOfThe Perceived Cyber Strategic Potential Ranking

After inserting the strategic attributes into the PCSP calculation base, the following result is presented, which portrays the 15 reference States in Strategic Potential:

Table 4 Ranking of Perceived Cyber Strategic Potential (PCSP)

Position	Country	PCSP (0-1000)	PCSP Standardized
1	United States	774,17	0,774
2	China	717,50	0,718
3	Australia	578,33	0,578
4	Germany	571,67	0,572
5	South Korea	561,67	0,562
6	Canada	543,33	0,543
7	France	529,17	0,529
8	Netherlands	525,00	0,525
9	Brazil	525,00	0,525
10	United Kingdom	520,00	0,520
11	India	505,00	0,505
12	Japan	505,00	0,505
13	Russia	503,33	0,503
14	Spain	497,50	0,498
15	Italy	490,00	0,490

Source: Own elaboration based on the structural indicators that make up the Perceived Cyber Strategic Potential (PCSP).

The results obtained by the PCSP show an asymmetrical distribution of cyber strategic potential among the analyzed States.

The results demonstrate that the positioning of States does not depend exclusively on immediate technological capabilities, but on the interaction between multiple structural factors capable of sustaining the projection of power and influence in cyberspace in long-term horizons.

To increase the methodological transparency of the model and allow the identification of the factors that influence the relative positioning of States, the decomposition of the strategic attributes that make up the Perceived Cyber Strategic Potential is presented. The values presented correspond to the standardized results of each attribute after the application of the weighting procedures described in the methodology.

The values presented in Table 4 correspond to the standardized results of the aggregated indicators in each strategic attribute. After data collection, all indicators were subjected to the Min-Max normalization process, and subsequently converted to a scale of 0 to 1000 points, according to the expression:

Scaled Value = Normalized Value × 1000

This transformation was adopted to facilitate the interpretation of the results and allow visual comparisons between the different attributes that make up the PCSP

Table 5 Composition of Strategic Attributes of the PCSP for the Main Countries

Country	TI	ES	I	PPP	EDT	SP	SCP	CS	DPI	MC	PCSP
United States	600	275	1000	900	400	1000	866,67	1000	700	1000	774,17
China	900	375	900	600	1000	800	400,00	500	600	900	717,50
Australia	300	350	1000	1000	200	1000	733,33	300	200	800	578,33
Germany	200	525	950	1000	200	800	866,67	200	200	800	571,67
South Korea	200	325	950	1000	200	1000	666,67	300	200	900	561,67
Canada	200	275	950	1000	200	1000	733,33	200	200	800	543,33
Brazil	600	600	700	600	200	400	600,00	300	300	600	525,00
India	100	525	650	700	400	600	400,00	400	500	800	505,00
Russia	400	175	800	350	200	800	333,33	500	300	900	503,33

Source: own elaboration based on indicators integrated into the PCSP model.

Analysis of the composition of attributes demonstrates that the positioning of States in the PCSP ranking results from the combination of multiple structural factors. It is observed that the highest-ranked countries show balanced performance in different strategic dimensions, while countries with intermediate potential tend to concentrate their advantages in specific attributes. This characteristic reinforces the premise that cyber strategic potential constitutes a multidimensional phenomenon, dependent on the integration between technological, energy, institutional, military, and innovation capabilities.

The model allowed the construction of six groups of States linked to perceptible cyber strategic potential. For each Cluster, pragmatic strategies were developed for the development of national policies and strategies related to the Cyber Sector.

It is observed that:

Cluster 1 is characterized by States, called Structural Cyber Powers, embodied by the USA and China. The members of this group have complete mastery of technological chains; high energy and military capacity; and leadership in AI and computing.

Cluster 2 is characterized by states known as Advanced Integrated Powers, exemplified by the United Kingdom, Germany, Japan, South Korea, and France. They possess strong innovation capacity; high global integration; and moderate dependence on external supply chains.

Cluster 3 brings together the so-called Specialized Powers, notably Israel, Estonia, and Singapore. They have high efficiency; a strong focus on cybersecurity; and limited scale.

Cluster 4 represents the states known as Emerging Powers, such as India and Brazil. They have high demographic potential; uneven technological growth; and structural bottlenecks.

Cluster 5 is unique in that it indicates Asymmetric Powers with strong military capacity; weakness in innovation; and restrictions on global integration. Russia, Iran, and North Korea stand out in this group.

Cluster 6 represents countries with elementary levels of insertion in cyberspace, being significantly represented by African states.

3.2DiscussionOfResults

The results obtained by the PCSP show that cyber strategic potential is the result of the simultaneous interaction between technological, economic, energy, institutional, and geopolitical factors. The analysis of the identified groupings demonstrates that leadership in cyberspace does not depend exclusively on the possession of offensive or defensive capabilities, but on the ability to control fundamental structural resources for the sustainability of the digital ecosystem.

The United States and China stand out as structural cyber powers because they have a high capacity to act in practically all the attributes considered by the model. Both nations control significant portions of the global value chains related to semiconductors, advanced computing, artificial intelligence, space systems, and critical digital infrastructure. This condition provides high strategic autonomy and the ability to adapt to future technological transformations.

The countries classified as Integrated Advanced Powers have a high capacity for innovation and strong international insertion, benefiting from mature technological ecosystems and robust institutional systems. Although they have less productive autonomy compared to the two main global powers, they compensate for this limitation through integration into strategic alliances and international knowledge chains.

Particularly relevant is the performance of the Specialized Powers, represented by Israel, Estonia, and Singapore. The results demonstrate that territorial or demographic size is not a determining factor for strategic success in cyberspace. In these cases, continuous investments in innovation, human capital, and cybersecurity have allowed the construction of significant competitive advantages.

The grouping of Emerging Powers reveals a scenario of high potential not yet fully converted into strategic capabilities. Brazil and India have structural advantages associated with the availability of natural resources, population size, and significant domestic markets. However, challenges related to technological innovation, semiconductor production, advanced digital infrastructure, and satellite development limit their international positioning.

In the Brazilian case, the results suggest that strengthening research and development, expanding the national technology industry, consolidating space programs, and increasing professional qualifications in critical areas represent priority factors for raising the national cyber strategic potential in the coming decades.

In general, the results reinforce the central hypothesis of this study: the strategic positioning of States in cyberspace depends less on currently observable capabilities and more on the structural capacity to sustain continuous processes of innovation, technological adaptation, and systemic integration.

3.3ImplicationsForPublic Policies And National Strategies

The results produced by the PCSP have direct applications in the formulation of public policies aimed at strengthening the national capacity to operate in cyberspace. By identifying the structural factors responsible for the formation of strategic cyber potential, the model provides subsidies for directing investments and government priorities.

In the technological field, the results indicate the need to strengthen national capacities related to the production of semiconductors, advanced computing, artificial intelligence, and quantum computing. These areas represent critical sectors for maintaining technological autonomy and reducing external dependence.

In the energy dimension, it becomes fundamental to expand energy security associated with critical digital infrastructures, guaranteeing the availability of resources necessary for the expansion of data centers, communication systems, and data-intensive applications.

In the field of innovation, the results reinforce the importance of expanding investments in research and development, training specialized human resources, and consolidating innovation ecosystems capable of transforming scientific knowledge into competitive advantages.

For the Brazilian case, five strategic priorities stand out:

a) strengthening the national semiconductor industry;

b) expanding its own satellite capacity;

c) increasing investments in applied research in cybersecurity;

d) strengthening the integration between government, universities and the productive sector; and

e) expanding the training of specialists in critical areas associated with digital transformation.

The adoption of these initiatives will contribute to raising the national cyber strategic potential and expanding the freedom of action of the Brazilian State in an international environment increasingly characterized by technological competition.

3.4ValidationOfResearch Hypotheses

The hypotheses formulated in the introduction were analyzed considering the results obtained by the PCSP model.

Hypothesis H1 established that the cyber strategic potential of States would be positively associated with their capacity for technological innovation. The observed results corroborate this hypothesis, since the countries positioned in the top positions of the ranking present high levels of investment in research and development, strong scientific production and a high capacity for generating advanced technologies.

Hypothesis H2 proposed that states characterized by high levels of integration between energy resources, digital infrastructure, and technological capacity would tend to exhibit higher levels of strategic cyber potential. The analysis of the clusters confirms this proposition, especially in the cases of the United States, China, South Korea, and Germany, whose technological ecosystems demonstrate high synergy between these structural factors.

Hypothesis H3 suggested that multidimensional models based on structural factors would be able to produce more comprehensive assessments than approaches focused exclusively on current cyber capabilities. The results obtained reinforce this hypothesis by highlighting significant differences between countries that have similar cyber capabilities but distinct strategic structures to support their future evolution.

Although the study is predominantly exploratory in nature, Spearman correlations were calculated between the PCSP index and the main structural attributes. The results indicated a high positive correlation between PCSP and attributes related to Innovation ($\rho = 0.82$), Emerging Disruptive Technologies ($\rho = 0.79$), and Structural Convergence Points ($\rho = 0.75$), empirically reinforcing the formulated hypotheses.

3.5.Study Limitations

Despite the theoretical and methodological contributions presented, the study has limitations that should be considered in the interpretation of the results.

The first refers to the dependence on open databases. Although the sources used are widely recognized by the international scientific community, certain national strategic capabilities, especially those related to offensive cyber operations, classified military programs, and sensitive technologies, are not available for public reference.

The second limitation is associated with the use of the Analytic Hierarchy Process (AHP) for the partial definition of attribute weights. Even though validation and consistency mechanisms have been adopted, a component of subjectivity inherent in multi-criteria evaluation remains.

A third limitation stems from the dynamic nature of the technological environment. Accelerated changes in areas such as artificial intelligence, quantum computing, space systems, and semiconductors can significantly alter the relative positioning of states in short time intervals, requiring periodic updates to the model.

These limitations do not compromise the usefulness of the model, but they do indicate opportunities for improvement in future research, especially through the incorporation of time series, machine learning techniques, and new strategic databases.

4. Conclusion

This study proposed the Perceived Cyber Strategic Potential (PCSP), a multidimensional framework designed to assess the potential capacity of States to project influence and power in the cyber environment over long-term horizons.

The results demonstrated that the dynamics of contemporary cyber power cannot be explained solely by immediate technological capabilities. The consolidation of strategic positions in cyberspace depends on the interaction between structural factors related to innovation, energy, governance, technological resources, digital integration, military capacity, and international insertion.

The application of the model highlighted the existence of a hierarchical structure of cyber strategic potential. The United States and China stand out for their ability to simultaneously control critical technological resources, strategic production chains, and innovation ecosystems. In contrast, countries such as Israel, Estonia, and Singapore demonstrate that high levels of specialization can compensate for territorial and demographic limitations.

In the Brazilian case, the results indicate the existence of significant strategic potential associated with the demographic dimension, availability of natural resources, diversified energy matrix, and growing technological capacity. However, challenges related to innovation, advanced digital infrastructure, and competitive insertion in highly complex technological segments persist.

From a theoretical point of view, the study contributes to the advancement of the literature by introducing an approach oriented towards strategic potential, complementing traditional cyber power models focused predominantly on present capabilities. In methodological terms, PCSP offers a scalable framework, capable of periodic updating and comparative application among different States.

From the perspective of Information Systems, PCSP can be understood as an analytical decision support system capable of integrating large volumes of heterogeneous data from different strategic domains. The framework transforms dispersed data into structured knowledge, contributing to strategic intelligence processes, trend monitoring, and evidence-based public policy formulation.

It is concluded that PCSP constitutes a promising tool to support strategic planning processes, public policy formulation, and knowledge production in cyber geopolitics, contributing to the understanding of the transformations of state power in the Information Age.

References

1. ALLISON, Graham. Road to War: Will the United States and China Escape Thucydides' Trap? Rio de Janeiro: Intrínseca. 2020. 10.54945/jjia.v1i6.109
2. ALMEIDA, José Eduardo P. Strategic Challenges for Cybersecurity and Defense: The Global Trend for Cyber Defense. Brasília: Secretariat of Strategic Affairs of the Presidency of the Republic. 2011. 10.21275/sr25922203744
3. AMUSQUIVAR, Érika L. and PASSOS, Rodrigo Duarte F. The Genesis of Geopolitics and its Diffusion in World History. RBED. 2018. 10.26792/rbed.v5n1.2018.75055
4. BARACUHY, Braz. The Foundations of Classical Geopolitics: Mahan, Mackinder, SPYKMAN. Organizer Braz Baracuhy. Brasília, DF: FUNAG. 2021. 10.2139/ssrn.6908178
5. BELFER CENTER FOR SCIENCE AND INTERNATIONAL AFFAIRS. National Cyber Power Index 2022. Harvard Kennedy School. 2022.
6. BOBBIO, Norberto. Dictionary of Politics I Norberto Bobbio, Nicola Matteucci and Gianfranco Pasquino; trans. Carmen C, Varriale et al.; coord. trans. João Ferreira; general rev. João Ferreira and Luis Guerreiro Pinto Cacais. - Brasília: Editora Universidade de Brasília, 1 ed. 1998.
7. BUCHANAN, Ben. The New Fire: War, Peace, and Democracy in the Age of AI. Cambridge, MA: MIT Press. 2021. 10.1007/s11016-022-00821-w
8. BONFIM, Uraci Castro. Geopolitics. Course on Politics, Strategy and High Administration of the Army. Distance Learning CPAEX/EAD. Rio de Janeiro: ECEME. 2005.
9. CLARKE, Richard A. Cyber War: the next threat to national security and what to do about it. New York: HarperCollins Publishers. 2010. 10.3917/pe.104.0919g
10. CLINE, R. S. World Energy Assessment: A Calculation of Strategic Drift. Boulder, Colorado: Westview Press. 1975.
11. DALIO, Ray. Principles for a Changing World Order: Why Nations Prosper and Fail. Rio de Janeiro: Intrínseca. 2022. 10.1177/22779752251413913
12. DEMCHAK, Chris C.; Dombrowski, Peter. Rise of a Cybered Westphalian Era. Strategic Studies Quarterly, v. 5, n. 1, p. 32-61. 2011. 10.1007/978-3-642-55007-2_5
13. DINIZ, Janguiê. Innovation in a Disruptive Society. Barueri, SP: Novo Século Editora. 2020.
14. INTERNATIONAL TELECOMMUNICATION UNION (ITU). Global Cybersecurity Index 2024. Geneva: ITU. 2024.
15. KELLO, Lucas. The Virtual Weapon and the International Order. New Haven: Yale University Press. 2017.
16. MORENO, Wanderlino Junior. Cyber Sovereignty: State, Power and Governance in the Information Age. Dialética Publishing House. 2026.
17. MORENO, Wanderlino, Junior. The Game of Power in Cyberspace. Tagora Publishing House. 2024.
18. NYE, Joseph S. Jr. Cyber Power. Cambridge, MA: Harvard Kennedy School, BELFER CENTER FOR SCIENCE AND INTERNATIONAL AFFAIRS. 2010.
19. WORLD ECONOMIC FORUM. Global Risk Report 2025. Geneva: World Economic Forum. 2025.